LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Scienze Politiche

Cattedra: Diritto di internet: social media e discriminazione

SICUREZZA NAZIONALE E TUTELA DELLA PRIVACY SULLA RETE: PROFILI DI COMPARAZIONE

RELATORE

Prof. Pietro Falletta

CANDIDATO

Giammarco Gallo

Matr. 072652

ANNO ACCADEMICO: 2015/2016

INDICE:

Introduzione

Il diritto alla privacy oggi ampiamente riconosciuto e tutelato in tutti gli ordinamenti democratici, si trova, specialmente dopo gli atti terroristici che dall'11 settembre fino ad oggi hanno minacciato la sicurezza internazionale, ad essere messo in discussione dall'esigenza di lotta al terrorismo. In questa trattazione ci si propone di verificare quanta libertà si è disposti a sacrificare per la sicurezza dal momento che il terrorismo sul web ha spinto i governi ad una sorveglianza sempre più penetrante della vita privata a scapito del diritto alla privacy di ogni cittadino. Infatti in presenza di rischi di tal genere, il controllo e la vigilanza sui dati personali rappresentano uno strumento essenziale di prevenzione e repressione, largamente utilizzato in tutti gli stati democratici. Tuttavia il problema che si pone è quello dei limiti e delle garanzie a cui tali strumenti di controllo sono o dovrebbero essere assoggettati. Cioè bisognerebbe adeguare e rendere proporzionale all'obbiettivo lo strumento adottato. Lo sviluppo delle comunicazioni telefoniche e online di milioni di cittadini si basa infatti sulla fiducia che questi ripongono su un adeguato e solido sistema di garanzie, riguardanti il rispetto della segretezza delle comunicazioni e la salvaguardia dell'integrità dei dati personali. La contraddizione tra privacy e esigenze di sicurezza nazionale è quindi venuta alla luce sempre di più. In questa trattazione si cerca di dimostrare, come la contraddizione tra le due esigenze sia solo apparente e che è necessario e possibile, invece, trovare un'equilibrio. Il dibattito intorno a questo tema è molto attuale ed è inevitabilmente fonte di contrapposizioni ai vari livelli. Ciò che da spunto a questa riflessione è la recente vicenda svoltasi tra Apple, una delle aziende più note e produttive al mondo nell'era digitale, e l'Fbi, ente investigativo di polizia federale degli Stati Uniti, che ha portato l'attenzione ancora una volta sul rapporto tra privacy e sicurezza nazionale. Alla luce di ciò, si procederà analizzando nel primo capitolo il concetto di privacy, dal suo nascere fino al suo riconoscimento ufficiale. Lo si è analizzerà cioè sia come diritto "ad essere lasciato solo", che come diritto di controllo sulla circolazione delle proprie informazioni personali, aspetto questo sempre più pregnante e legato al veloce progresso tecnologico. Si dimostrerà che per una tutela efficiente della privacy si dovrà garantire non solo il riconoscimento dell'esistenza di un vero e proprio

diritto alla privacy, che trova cioè le proprie radici nei trattati internazionali, ma anche intensificando gli interventi normativi in materia di tutela del trattamento dei dati personali. Si analizzerà il concetto di sicurezza nazionale, sempre più invocato a causa dei sempre più frequenti atti terroristici verificatisi. La sicurezza nazionale si riterrà una delle tante espressioni del diritto di libertà, quindi non prerogativa del potere costituito ma diritto del popolo e del cittadino. Individuati i due concetti si analizzeranno, nel secondo capitolo, le fonti normative internazionali ed europee con particolare riguardo al nuovo regolamento europeo che entrerà in vigore nei prossimi due anni e che ha abrogato la precedente disciplina, e ci si soffermerà sul quadro normativo in materia vigente in Italia. Si esporranno le fonti dell'ordinamento statunitense e il recentissimo accordo Europa - Stati Uniti noto come *privacy shield* a cui gli stati interessati si adegueranno dal 12 luglio 2016. Si confronteranno il modello americano e quello europeo in materia di privacy evidenziandone le differenze. Nel terzo capitolo si ripercorrerà, passo dopo passo, la vicenda tra Apple ed Fbi, analizzando le varie tesi in merito, e si rifletterà che questa vicenda non può essere considerata né una mera questione di marketing, né un mero confronto tra parti opposte, quanto piuttosto uno spunto per considerare che la sicurezza dei cittadini e delle infrastrutture nel *cyberspazio* richiede tanto la consapevolezza dei rischi da parte degli utenti, quanto la loro fiducia sia nei servizi di comunicazione offerti dagli operatori che si sono impegnati a rispettare la privacy, sia nelle istituzioni governative che sempre di più devono comprendere che il *cyberspazio* è una realtà virtuale parallela dove servono garanzie per i cittadini e strumenti efficaci per la sicurezza nazionale e per la giustizia. Si giungerà alla conclusione che è possibile un'equilibrio tra le due esigenze basandosi sul senso di responsabilità intrinseco in ogni diritto di libertà, equilibrio raggiungibile solo attraverso un concreto dibattito politico. Ci si augura infine che dal momento che sono globali tanto le comunicazioni quanto le minacce terroristiche, gli strumenti di contrasto verranno previsti a livello internazionale.

Alexander Solzhenitysn: << *La nostra libertà è costruita su quello che gli altri non sanno della nostra esistenza* >>.

Capitolo 1

Il rapporto tra privacy e sicurezza nazionale sulla rete

Par. 1: *Nascita e riconoscimento del diritto alla privacy*

Il diritto alla privacy, elaborato dalla dottrina statunitense alla fine dell'800[1], si è modellato nel tempo in relazione all'evoluzione dei costumi e al veloce progresso tecnologico.

Il cosiddetto *"right to be let alone"*, così definito dal giudice americano Cooley è diventato via via, *"one theme that pervades the entire constitutional structure"*, non solo negli USA ma in tutti i paesi democratici. L'Unione Europea è oggi la regione con il più alto livello di protezione dei dati personali al mondo, grazie alla corposa normativa comunitaria sulla privacy degli ultimi anni. Inizialmente, da quando negli anni sessanta, la letteratura giuridica ha cominciato a interessarsi del tema, il "diritto di essere lasciati soli" è stata interpretato come strumento di tutela di una duplice esigenza individuale: da un lato, la protezione della sfera privata dall'altrui curiosità[2] e dall'altrui interesse a conoscere[3]; dall'altro, il "controllo" del flusso delle informazioni in uscita dalla sfera privata verso l'esterno[4]. Tuttavia, il veloce progresso dei mezzi di comunicazione telematica e particolarmente della rete Internet mondiale, sta via via mettendo in crisi gli strumenti normativi posti a tutela del trattamento dei dati personali. Così inteso, il diritto alla riservatezza non ha sollevato particolari problemi di tutela perché, facendo riferimento ai diritti fondamentali della persona, rientra nel dettato degli articoli 13, 14, 15 e 21 della Costituzione, nell'ambito cioè del più ampio riconoscimento accordato ai diritti

---

[1] S. Warren, L. Brandies, *The right to privacy*, vol. IV no. 5, in Harvard law review, Dicembre 1980.

[2] P. Rescigno, *Manuale di diritto privato italiano*, Napoli, 1992.

[3] A. Cataudella, *Riservatezza (diritto alla*), I) Diritto civile, in Enciclopedia giuridica, Roma, 1991.

[4] Convegno internet e privacy, relazione introduttiva a cura di S.Rodotà, Maggio 1998.

inviolabili dell'uomo dall'articolo 2. Per cui, se la tutela della libertà personale sembrava idonea ad impedire ingerenze nella sfera fisica e psicologica individuale, la previsione della segretezza e dell'inviolabilità del domicilio e della corrispondenza cautelavano l'individuo da intromissioni nella sfera privata operate attraverso invasioni realizzate fisicamente, e la tutela della libertà di manifestazione del pensiero forniva fondamento giuridico alla pretesa di non rendere noto a terzi quanto intimamente connesso al proprio modo d'essere. Già a metà degli anni ottanta, la nozione di riservatezza non coincide più con i concetti di riserbo dell'intimità domestica, del decoro e della reputazione, ma riguarda tutte quelle situazioni e vicende legate alla vita privata - personale e familiare -, prive di rilevanza sociale. Tant'è vero che secondo l'accezione accolta dalla Corte di Cassazione nella sentenza n.2199 del 1975, il diritto alla riservatezza si identifica con l'interesse a sottrarre alla conoscenza altrui le vicende private, verificatesi dentro e fuori del domicilio domestico, che non abbiano per i terzi un interesse socialmente rilevante. Ed è proprio in tale significato che anche la Corte costituzionale, nella sentenza n.38 del 1973, annovera la fattispecie nell'ambito dei diritti inviolabili dell'uomo.

Con lo sviluppo delle nuove tecnologie e il ricorso, sempre più frequente, all'utilizzo di trattamenti, specie automatizzati, di dati di carattere personale, le esigenze connesse alla riservatezza mutano in maniera significativa. Il nuovo contesto è dato dall'inserimento dell'individuo nella società "globale", nella quale la stragrande maggioranza delle azioni compiute e delle scelte individuali lasciano una "traccia" che ne consente la mappatura e con essa la ricostruzione dell'identikit della persona. In tale situazione, la tutela del domicilio è totalmente inidonea a garantire la riservatezza individuale, dal momento che le informazioni "in uscita" non sono solamente quelle acquisite attraverso l'accesso al luogo in cui si manifesta più immediatamente la personalità, né diramate consapevolmente attraverso i mezzi di comunicazione del pensiero, bensì, fornite inconsapevolmente attraverso i dati personali lasciati nell'ambiente, i quali, acquisiti e catalogati, permettono di ricostruire con precisione la personalità del singolo, violandone la riservatezza. Si afferma, quindi, l'esigenza che la raccolta organizzata delle informazioni personali disseminate nell'ambiente non avvenga all'insaputa dell'interessato, e non si presti ad utilizzi lesivi dei diritti e della

dignità della persona. Nello stesso tempo, data l'impossibilità di limitare le informazioni in uscita, si percepisce come fondamentale il potere di selezione delle comunicazioni in entrata, cioè l'interesse a prestare attenzione solo a ciò che si ritiene importante (c.d. diritto individuale alla quiete). E' proprio alla luce di queste esigenze che si comincia a parlare di "privacy", alludendo con tale espressione ad una sorta di diritto comprensivo, oltre che dei tradizionali aspetti connessi alla "riservatezza", anche del "potere di controllo sulla circolazione delle proprie informazioni personali"[5], e del complementare "diritto di essere lasciati in pace, inteso come esigenza di protezione del singolo dai tentativi di contatto realizzati da terzi secondo particolari modalità - connesse all'uso delle nuove tecnologie - , e tendenzialmente per fini di carattere commerciale"[6]. In tale prospettiva, la privacy da strumento di isolamento dagli altri come diritto di essere lasciato solo, diventa strumento di comunicazione: << A me serve avere tutela dell'anonimato, a me serve la tutela della riservatezza, della privacy, non per isolarmi ma per partecipare. Solo se sono certo del mio anonimato, potrò partecipare senza timore di essere discriminato o stigmatizzato a gruppi di discussione in rete su temi politicamente sgraditi al potere dominante in un certo momento. Solo se avrò la certezza di non essere discriminato, potrò denunciare gli abusi, magari nel luogo dove io stesso lavoro>>[7]. Ecco allora che la riservatezza non è un problema di silenzio, ma un vero e proprio strumento di comunicazione: la privacy diventa il diritto di controllare l'uso che altri fanno delle informazioni che mi riguardano, potendo attuarsi con facilità l'utilizzazione illecita dei dati stessi, sia l'alterazione dell'identità del soggetto, sia la divulgazione incontrollata di notizie, che impediscano al soggetto stesso di essere autonomo nelle scelte.

Nel sistema di circolazione planetaria delle informazioni, la privacy costituisce il fulcro intorno al quale si impernia l'utilizzo corretto della rete ed il suo potenziale sviluppo. E' infatti necessario che l'utente possa usufruire di tutti i servizi che Internet mette a disposizione, in sicurezza, nella convinzione cioè che i dati

---

[5] S. Rodotà, discorso di presentazione della "Relazione per l'anno 2000'', Luglio 2001.

[6] E.Varani, *Diritto alla privacy e trattamento dati sensibili in ambito sanitario: dalla Carta dei diritti fondamentali dell'Unione Europea al D.lgs. 30 Giugno 2003 n.196 "Codice in materia di protezione dei dati personali",* in www.Giur.it, 2005, p.1770.

[7] S. Rodotà, *Op. cit.* p.1.

personali che egli immette nel sistema, non vengano raccolti e rielaborati per costituire un profilo personale, suscettibile in futuro di invasioni nella sfera privata. La tutela efficiente della privacy può essere garantita allora non solo riconoscendo l'esistenza di un vero e proprio diritto alla privacy, che affonda cioè le proprie radici nei trattati internazionali, ma anche intensificando gli interventi normativi in materia di tutela del trattamento dei dati personali, dal momento che i nuovi strumenti tecnologici sono in grado di creare sempre più penetranti intrusioni, senza che gli individui se ne rendano conto e senza che i singoli stati siano in grado di tenere il passo con tale veloce evoluzione.

Par. 2: *La privacy come trattamento dei dati per un duplice fine*

Occorre premettere che quando si parla di protezione dei dati personali sono da considerare due aspetti: da una parte, il trattamento dei dati dei consumatori, al fine di studiare il comportamento umano attraverso le loro abitudini per esigenze di marketing, dall'altra il trattamento e la conservazione dei dati per esigenze sia di prevenzione che di eventuale repressione di illeciti, sia per esigenze di sicurezza nazionale[8]. I nuovi strumenti tecnologici hanno definito un nuovo confine tra lo spazio pubblico e lo spazio privato, facendo diminuire ancora di più quell'area qualificabile come privacy. Strumenti e applicazioni hanno fatto si che la sorveglianza e l'ingresso nella sfera privata dei cittadini sia diventato più agevole. Basti pensare che l'analisi dei dati consente addirittura di predire il futuro di un individuo; infatti, in più della metà degli stati degli Stati Uniti, i " big data " vengono utilizzati per valutare le probabilità che la persona in questione possa commettere un reato nei dodici mesi successivi al rilascio. Anche in alcune società assicurative è stata rilevata la tendenza ad applicare premi maggiori a guidatori che avevano avuto voti bassi a scuola, sulla base della rilevazione che chi ha avuto voti bassi a scuola ha una maggiore tendenza a provocare incidenti. Di conseguenza gli stati hanno dovuto riadattare le infrastrutture per inserire le funzionalità di intercettazione e per consentire una sorveglianza maggiore. La

[8] S. Aterno, *La sicurezza come diritto di libertà e il ruolo della privacy nel prossimo futuro,* in Leggioggi, 16 febbraio 2016.

natura dinamica della tecnologia non ha solamente mutato il modo in cui la sorveglianza viene effettuata, ma anche "che cosa" può essere monitorato. Questa "tentazione" è apparsa irresistibile anche per gli Stati democratici. A tal proposito un intellettuale bielorusso, Evgenij Morozov, descrive i tempi attuali nei termini di un "apocalisse informativa" egli sostiene che << Il vecchio e radicato mito, secondo cui esiste uno spazio virtuale autonomo dove è possibile avere più privacy e indipendenza dalle istituzioni politiche è morto. [..] Cosa succederà quando tra cinque anni tutti gli oggetti e i dispositivi avranno sensori avanzati e poco costosi, e saranno collegati tra loro? tutti questi oggetti lasciano tracce di dati […] Sostanzialmente la possibilità di inserire un sensore e un collegamento Internet in qualunque cosa, consente di mercificare tutto e attribuire un prezzo alle informazioni che se ne ricavano. >>[9].

Di fatto, per quanto riguarda almeno il primo aspetto della privacy, si è "colpevoli" del massacro del diritto: rifiutando di leggere le condizioni di contratto o le informative su *app* o *software* che scarichiamo sui nostri cellulari o personal computer, sostanzialmente neghiamo a noi stessi l'esercizio del diritto alla privacy pur di avere in cambio i servizi che ci vengono offerti[10]. Per quanto riguarda poi il secondo aspetto, vale a dire il trattamento dei dati al fine di accertamento, prevenzione, repressione dei reati e per esigenze di sicurezza nazionale, negli ultimi quindici anni abbiamo assistito a continue oscillazioni tra periodi di grandi richiami alla "privacy nel mondo"[11], e periodi tipici di stati di emergenza, in cui il rischio di mettere in discussione le garanzie democratiche conquistate è stato molto alto. Si dovrebbe tentare invece di trovare un equilibrio tra l'esigenza della privacy e quella della sicurezza nazionale. Alcuni ritengono che le due esigenze - privacy e sicurezza - siano inconciliabili[12]. Altri, invece, arrivano a conciliarle sulla base della considerazione che la sicurezza nazionale non è che una delle tante espressioni del diritto di libertà e come tale consacrata esplicitamente ed implicitamente nella nostra Costituzione[13]. Una "sicurezza

---

[9] E.Morozov, *Perché Internet non salverà il mondo,* in Linkiesta, 20 Maggio 2014.

[10] S. Aterno, *Op. cit.* p.4

[11] Ibidem.

[12] L. Poldelmengo, *Nel posto sbagliato, 2014.*

[13] S.Aterno, op. cit.; A. Soro, discorso del Presidente, Roma, 28 Giugno 2016

democratica”[14] appunto, che contiene in se i valori e i limiti propri di ogni diritto di libertà. Si supera così il concetto di sicurezza nazionale come prerogativa del potere costituito e quello di libertà come diritto del popolo e del cittadino di sottrarsi ad esso[15]. La sicurezza nazionale e il diritto alla privacy possono trovare un equilibrio nel richiamo al senso di responsabilità, dal momento che il concetto di libertà è strettamente collegato alla responsabilità con cui tale libertà deve essere esercitata: ciascuno può essere ritenuto responsabile del suo operato se questo è avvenuto in base ad una libera scelta e non per condizionamenti. << L'uomo è condannato ad essere libero […] nessuna scusa, nessun rammarico: se la libertà è assoluta io scelgo il significato dato all'esistenza […] perché dal momento del mio sbocciare all'essere, io porto il peso del mondo tutto da solo, senza che niente e nessuno possa alleggerirlo >> [16].

Il Web risulta oggi il contesto più propizio per l'esercizio da parte delle autorità pubbliche di un monitoraggio generale che trova come giustificazione più plausibile quella della tutela della sicurezza nazionale. Per questo è essenziale, per evitare di trovarsi di fronte ad un utilizzo non regolato di informazioni personali, trovare il punto di equilibrio tra la tutela della sicurezza nazionale e la tutela della privacy individuale.

Par. 3: *Equilibrio possibile tra privacy e sicurezza nazionale*

La sicurezza nazionale e il diritto alla privacy, rispecchiano due fenomeni che hanno caratterizzato in maniera pregnante la storia mondiale nel periodo che va dall'11 settembre 2001 ad oggi: gli atti terroristici e il veloce progresso tecnologico. Da una parte, la tecnologia consente di archiviare facilmente e a basso costo tutte le informazioni che riguardano l'individuo e le sue relazioni; dall'altra, gli atti terroristici richiedono sempre più strumenti nuovi al fine di una loro prevenzione e lotta, e di fronte ai quali diviene prioritario garantire la sicurezza nazionale. Tutto questo si traduce necessariamente in un maggior

[14] Ibidem.

[15] Ibidem.

[16] J.P. Sartre, *L'essere e il nulla,* 1943, IV parte, cap. I

controllo volto ad ottenere informazioni per prevenire violenze e aggressioni alla nostra vita. Tale controllo è reso possibile dalle nuove tecnologie di sorveglianza quali lenti a visioni notturna, microfoni parabolici in grado di captare conversazioni a voce ad oltre un kilometro di distanza, reti di sorveglianza televisiva a circuito chiuso, computer mobili in grado di intercettare le conversazioni trasmesse da telefoni mobili in un certo settore. Tali tecnologie, nate originariamente per i settori della difesa e dell'intelligence, si sono rapidamente diffuse nei servizi riguardanti il mantenimento dell'ordine pubblico e anche nel settore privato. Nel tempo si sono inoltre messi in atto veri e propri sistemi mondiali di intercettazione: "*l'Echelon",* comprendente attività di strutture di intelligence USA, e di intelligence inglese, e quello chiamato *EU FBI,* comprendente varie agenzie di ordine pubblico quali FBI e polizie di stato dell'Unione Europea. I siti di questo sistema sono situati negli USA, in Nuova Zelanda, in Australia, ad Hong Kong.

Il rapporto tra privacy e sicurezza nazionale ha subito notevoli evoluzioni in particolare dall'11 settembre: prima degli attacchi terroristici il dibattito ruotava sopratutto intorno alla fragilità della privacy dovuta al cyberspazio e all'uso di tecnologie sempre più ampio. Il dopo 11 settembre, invece, è stato caratterizzato dal dover trovare una risposta adeguata alle minacce terroristiche senza però, per questo, venir meno ai principi dello stato democratico.

A poco più di un mese dall'attacco – il 26 ottobre del 2001 - il Congresso varò l'*Usa Patriot Act*, legge federale intesa a contrastare il terrorismo, attraverso il potenziamento degli strumenti investigativi e di controllo ed il rafforzamento delle misure di sicurezza. La legge, tuttavia, insiste sulla sfera della libertà personale e interferisce profondamente nella vita degli americani: l'accresciuta sorveglianza sulle comunicazioni telefoniche e telematiche, l'uso di tecnologie avanzate per l'identificazione e l'archiviazione di informazioni (dalle cartelle cliniche ai dati bancari), il prelevamento delle impronte digitali nelle biblioteche, fino alla possibilità di effettuare ripetute perquisizioni in casa in assenza di mandato, sono solo alcuni esempi della massiccia interferenza nella vita quotidiana di ogni individuo[17].

[17] Agenzia informazioni e sicurezza interna, *Stati Uniti D'America, Patrioct Act,* In Gnosis, Marzo 2006.

La conseguenza diretta del nuovo quadro normativo si riscontra osservando l'impatto che l'emergenza del terrorismo esercita sulla scala gerarchica delle priorità e dei valori condivisi in uno Stato di diritto: la pubblica sicurezza assurge a valore primario, diventa diritto fondamentale e prioritario e si pone come origine della tendenza a comprimere le garanzie dei diritti individuali. La legislazione anti-terrorismo non si affianca al sistema normativo ordinario, ponendosi come strumentale al superamento di uno stato di eccezione, ma si ripercuote sul diritto interno integrandosi nell'ordinamento in modo permanente e minando di fatto l'apparato di garanzie fondamentali che costituisce la base delle democrazie moderne e che perciò dovrebbe essere intangibile, indiscutibile e indiscusso.

Sia il Canada che gli Stati Uniti hanno perseguito questa strada, introducendo per mezzo di fonti ordinarie, strumenti repressivi di carattere permanente[18]. Il *Patriot Act* aveva previsto che alcuni strumenti straordinari a disposizione delle forze di polizia e dell'intelligence fossero utilizzabili solo fino al 31 dicembre 2005, dopodiché sarebbe intervenuta una revisione delle relative disposizioni di legge. Di recente si è pervenuti alla "normalizzazione dell'emergenza": il controverso provvedimento, firmato dal Presidente Bush il 9 marzo 2006[19], ha reso meno severe alcune restrizioni e reso stabili 14 delle 16 disposizioni in scadenza[20]. La sezione 215 del *Patriot Act*, scaduta nel giugno 2015, regolamentava la raccolta da parte di agenzie governative, dei cosiddetti "metadati", cioè dei numeri di telefoni di chiamante e ricevente, durata delle conversazioni e altre informazioni "grezze" delle comunicazioni[21]. I mandati per ogni investigazione eseguita sulla base della sezione 215, venivano rilasciati da una corte federale degli Stati Uniti istituita per supervisionare le richieste di mandati di sorveglianza contro spie straniere all'interno degli Stati Uniti da parte delle forze dell'ordine e agenzie di intelligence federali, la FISA(*Foreign Intelligence Agency)*, che operava all'oscuro delle parti in causa. Per altro era previsto un ordine bavaglio, che impediva a coloro che avessero in qualunque modo collaborato all'indagine di

---

[18] C. Bassu, *La legislazione antiterrorismo e la limitazione della libertà personale in Canada e negli Stati Uniti,* in *Associazione Italiana Costituzionalisti,* Napoli, 2006.

[19] *Patriot Improvement and Reauthorization Act* 2005 (Patriot Act II, P.L. 109 – 177, 9 marzo 2006).

[20] Agenzia informazioni e sicurezza interna, *Stati Uniti D'America, Patrioct Act,* in Gnosis, marzo 2006.

[21] *La NSA deve sospendere la raccolta di dati telefonici,* in www.Ilpost.it, giugno 2015.

rendere nota a terzi l'indagine stessa. Ciò permetteva alla NSA(*National Security Agency)* di svolgere una raccolta indiscriminata di informazioni nella completa segretezza e di fatto senza autorizzazione[22]. È proprio sulla base della sezione 215 del *Patriot Act* e 702 del *Foreign Intelligence Surveillance Act* (FISA)[23], che con il programma PRISM sono stati raccolti dati relativi a milioni di telefonate di utenti. Il PRISM è un programma di sorveglianza elettronica, *cyberwarfare* e *Signal Intelligence*, classificato come di massima segretezza, usato per la gestione di informazioni raccolte attraverso Internet e altri fornitori di servizi elettronici e telematici. Il *Patriot Act* è stato sostituito dal *Freedom Act.* La nuova legge mira a garantire più trasparenza e più equilibrio tra la protezione delle libertà civili dei cittadini statunitensi e la priorità della sicurezza nazionale, specialmente dopo lo scandalo del Datagate, nato in seguito alle rivelazioni di alcuni documenti segreti, da parte di Edward Snowden, ex collaboratore dell'NSA venuto in possesso degli stessi quando lavorava per la Booz Allen Hamilton, un'azienda che collabora con il dipartimento della difesa e i servizi d'intelligence degli Stati Uniti. Secondo questi documenti, la compagnia di telecomunicazioni Verizon consegnerebbe all'FBI dati in grado di mettere a rischio la privacy dei propri utenti. In realtà risulta che siano stati raccolti dalla NSA, per un periodo ben superiore a tre mesi, non soltanto i dati dei clienti di Verizon, ma quelli di tutti i principali operatori: Google, Facebook, Apple e che fra essi vi fossero anche quelli relativi alle comunicazioni di cittadini europei, comprese quelle riservate, di esponenti di spicco di governi amici. Peraltro lo scandalo Datagate non è il primo caso in cui si denuncia l'esistenza di una massiccia vigilanza dei servizi di sicurezza: già nel 2005 era stata denunciata dal New York Times una massiccia attività di intercettazione, autorizzata dal presidente americano da parte dell'agenzia per la sicurezza nazionale, che aveva ad oggetto telefonate ed email. I professionisti intercettati avevano proposto azioni legali nei confronti dell'agenzia e delle compagnie telefoniche. Il giudice diede parzialmente ragione ai ricorrenti stabilendo che erano state violate le libertà fondamentali garantite dal *Bill of Rights,* e il principio della separazione dei poteri, visto che il programma di

---

[22] A. Massone, *Gli Stati Uniti riformeranno il Patriot Act ma l'NSA continuerà a spiarci,* in www.vulcanostatale.it, giugno 2015.

[23] M. Mensi e P. Falletta, *Il diritto del web,* Padova, 2015, p. 316.

sorveglianza anti terrorismo era stato autorizzato dal presidente senza la preventiva autorizzazione dell'autorità giudiziaria[24]. Il *Freedom Act* limita la sorveglianza elettronica delle comunicazioni telefoniche dei cittadini americani dalla NSA, venuta alla luce nello scandalo Datagate. Prevede infatti che l'archiviazione dei tabulati telefonici venga raccolta sempre dalle aziende di telecomunicazioni ma queste anziché girare questi dati alle agenzie governative saranno tenute ad inoltrarle solo in seguito a una richiesta esplicita del governo approvata dal tribunale di sorveglianza dell' *Intelligence* straniera degli Usa. Secondo un rapporto congiunto di *Epic*[25] e *Privacy International*[26], leggi molto simili al *Patriot Act* sono state emanate in molte nazioni: Australia, Canada, Danimarca, Gran Bretagna, Germania, India e Svezia. La cultura del sospetto si è ampliata tanto da poter ledere, almeno potenzialmente, la reputazione di chiunque, intaccando libertà che abbiamo dato sempre per scontate, come quelle di espressione, opinione, movimento.

L'Italia, dopo l'11 Settembre, avendo attraversato l'esperienza del terrorismo durante gli anni '70, non ha di fatto inserito particolari modifiche agli strumenti già in essere né particolari restringimenti alle libertà personali[27].

D'altra parte se in alcune nazioni l'operatore pubblico, lo Stato, è percepito come chi si occupa degli interessi di tutti, in Italia, invece, vige una sfiducia nello Stato, percepito come altro rispetto a noi e questo rende difficile la realizzazione di politiche che richiedono una forte coesione sociale. Diventa quindi necessario stimolare e alimentare la fiducia nelle istituzioni, non rinunciando però ad una vigilanza costante affinché non vengano intaccati i principi democratici. D'altra parte non si può tralasciare il fatto che il terrorismo è un nemico tra i più infidi perché non è identificabile. Quindi bisogna essere consapevoli che l'esigenza di raggiungere un più altro livello di sicurezza si impone. Potrebbe essere necessaria allora, una collaborazione tra stato e cittadino che tenda a integrare le diversità tra le culture, tra noi e chi manifesta rispetto per il nostro modo di vivere, in modo da isolare gli estremismi. Bisognerebbe tenere presente inoltre, che il sistema

---

[24] M.Mensi e P. Falletta, *Op. cit.* p. 8.

[25] Eletronic Privacy Information Center.

[26] ONG Inglese, per vigilare eventuali violazioni della privacy ad opera del governo.

[27] J. Bentham, *Cyber sorveglianza e tutela della privacy dopo l'11 Settembre 2001,*in www.altrodiritto.it capitolo 3.

democratico nel quale viviamo non tollera l'assegnazione di un potere non controllato a sua volta con autorizzazioni preventive ed altro: questo garantisce dai possibili abusi. La sicurezza non può più essere concepita in contrapposizione con la privacy e con la libertà di ognuno di noi, quasi che la richiesta dell'una necessariamente comporti una conseguente diminuzione dell'altra. La tutela della privacy resta una conquista dello stato liberale e democratico, ma è una conquista che può essere soggetta a nuove interpretazioni congiunturali che, senza far diminuire le prerogative dell'individuo, consentano di difendere la comunità[28].

[28] Agenzia informazioni e sicurezza interna, *Privacy e sicurezza, l'equilibrio possibile,* in Gnosis, Gennaio 2004.

Capitolo 2

Le fonti del rapporto

Par. 1: *Fonti internazionali*

All'affermazione del diritto alla privacy quale diritto fondamentale, hanno contribuito in maniera essenziale le convenzioni internazionali in materia di diritti umani: la Dichiarazione universale dei diritti dell'uomo del 1948 che all' Art. 12 prevede << Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni>>.

La Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, in particolare il primo comma dell'art. 8 riconosce il << diritto al rispetto della vita privata, del domicilio e la corrispondenza >>, e il secondo comma, afferma che non può esservi "interferenza" legittima da parte della pubblica autorità nell'esercizio di tale diritto, eccetto che nei casi dove ciò sia previsto dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale; la Dichiarazione dei diritti dell'uomo in relazione ai mezzi di comunicazione di massa del 1970 che all'Art.1 afferma come "il diritto alla privacy consiste essenzialmente nel vivere la propria vita con il minimo di interferenza necessario"[29]. La Corte Europea ha avuto modo di dichiarare che " l'interferenza " messa in atto dal legislatore deve rispettare specifici parametri di legittimità giuridica, e deve avere l'obbiettivo di mantenere la sicurezza nazionale o di combattere il terrorismo. Sulla base di tale previsione la Corte Europea dei diritti dell'uomo ha determinato, e progressivamente ampliato, il significato da ascrivere ai concetti di vita privata e corrispondenza, gettando le basi per il riconoscimento di un diritto al controllo consapevole su ogni forma di circolazione delle proprie informazioni personali. La nozione viene

[29] P.Perri, *Protezione dei dati e nuove tecnologie; aspetti nazionali europei e statunitensi*, 2007, p.64.

esplicitamente elaborata, nell'ambito del Consiglio d'Europa, dalla Convenzione n.108 del 1981 (c.d. Convenzione di Strasburgo), che reca una serie di principi a cui dovrebbero (o almeno, avrebbero dovuto) conformarsi le varie legislazioni nazionali, in modo da assicurare il rispetto del diritto alla privacy degli individui nei confronti di ogni elaborazione automatizzata di dati concernenti soggetti identificati o identificabili. In questi documenti si riscontra la nozione di *"privacy intimacy"* (diritto di essere lasciato solo), alla quale si è poi affiancata quella di *"informational privacy"*, quale diritto del soggetto di limitare e controllare la raccolta, la registrazione e l'utilizzazione dei dati a carattere personale. Quest'ultima nozione si riscontra nella Convenzione del 1981 del Consiglio D'Europa e nella direttiva 95/46/CE dell'Unione Europea, nonché nelle normative dei singoli stati attuative degli obblighi transnazionali, fino ad arrivare al regolamento europeo del 14 aprile 2016, che abroga la direttiva 46 del 1995, e alla direttiva[30] che lo affianca.

Par 2: *Fonti dell'ordinamento europeo in materia di privacy*, r*egolamento europeo 14.04.2016 e direttive 2016/680 e 2016/681 del Parlamento europeo e del Consiglio.*

La Direttiva 95/46/Ce, definita anche "Direttiva madre", ha costituito fino ad oggi il testo di riferimento – a livello europeo – in materia di protezione dei dati personali. A tal fine, la direttiva fissa limiti precisi per la raccolta e l'utilizzazione dei dati personali e chiede a ciascuno Stato membro di istituire un organismo nazionale indipendente incaricato della protezione di tali dati, il che ha condotto poi alla nascita delle Autorità nazionali di protezione dati. L'obiettivo della Direttiva è infatti quello di creare una disciplina armonica di tutela dei dati personali per evitare la formazione di una eccessiva differenza nei livelli di tutela dei diritti e delle libertà fondamentali, che può ostacolare non solo la salvaguardia delle posizioni soggettive, ma anche l'esercizio di una serie di attività economiche

[30] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

su scala comunitaria. Tuttavia, le disposizioni normative contenute nella direttiva 95/46/CE sono tali da vincolare gli Stati membri a conformarsi ad esse, lasciando, comunque, ai legislatori nazionali significativi margini di interpretazione, specie per quanto riguarda la disciplina delle deroghe in specifici settori. Essa ha introdotto l'idea che un elevato livello di protezione delle persone nel trattamento dei dati personali che li riguardano è condizione essenziale per consentire la libera circolazione di tali dati all'interno dei Paesi dell'Unione, e ne ha disciplinato i vari aspetti: le condizioni di liceità del trattamento, il regime di alcune categorie di informazioni (come ad esempio i dati sensibili), le regole di sicurezza, le condizioni per la trasmissione di dati all'esterno dell'UE. Occorre, tuttavia, rilevare che la direttiva 95/46/Ce è nata in un contesto tecnologico, politico ed economico molto diverso da quello attuale[31]. Per questo motivo, essa è stata abrogata dal Regolamento Privacy 2016/679, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Occorre sottolineare come in Europa sia il diritto alla privacy sia il diritto alla protezione dei dati costituiscono diritti fondamentali[32]. Alla Direttiva madre sono seguiti ulteriori interventi normativi, quali le direttive 97/66/Ce[33], e 2002/58/Ce[34], che appunto sanciscono definitivamente l'esistenza di un "diritto alla protezione dei dati di carattere personale" distinto e autonomo dal "diritto alla riservatezza". Tale distinzione viene confermata, nella Carta dei diritti fondamentali dell'Unione Europea, che reca nel capo secondo, dedicato ai diritti di libertà, l'esplicito riconoscimento del diritto alla protezione dei dati di carattere personale (art.8, c.1), distinguendolo dal diritto di ogni individuo al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni (sancito all'art.7). La Carta, quale fonte primaria di protezione dei diritti fondamentali nell'UE, diviene parametro di legittimità degli atti dell'Unione. La

---

[31] F. Pizzetti, *Lezione del 6 ottobre 2010, il percorso della Comunità europea che porta al riconoscimento del diritto alla protezione dei dati personali.*

[32] Art. 8 Carta dei diritti fondamentali dell'Unione Europea.

[33] Direttiva 97/66/Ce, relativa al trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni.

[34] Direttiva 2002/58/Ce, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

Carta di Nizza stabilisce una serie di disposizioni generali o principi aventi natura e rilevanza costituzionale; la privacy viene cioè concepita come uno dei "diritti dell'uomo" fondamentali, tutelato in rapporto al trattamento dei dati personali, soprattutto alla luce delle nuove sfide poste dalla rivoluzione tecnologica. Nonostante ciò, il rinvio ai principi di cui l'art. 8 della Carta di Nizza, come fondamento costituzionale della privacy in Europa, ha dato vita per lungo tempo a un singolare paradosso, in quanto essendo state inserite le disposizioni della Carta all'interno della seconda parte del fallito Progetto di trattato costituzionale (2005), è sembrato necessario a molti attendere il risultato delle nuove trattative per il trattato di riforma dell'Unione, al fine di sciogliere le riserve sulla piena forza vincolante di tali disposizioni[35].

Il Trattato di Lisbona, entrato in vigore il 1 dicembre 2009, sebbene non abbia incorporato il testo della Carta dei diritti, la include sotto forma di allegato, conferendole così carattere giuridicamente vincolante all'interno dell'ordinamento dell'Unione, secondo quanto disposto dall'art.6 : "L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adottata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati". Il diritto alla protezione dei dati trova un riconoscimento specifico anche nei Trattati e rispettivamente all'art. 16 TFUE[36], e all'art. 39 TUE[37].

Ciò significa che l'Unione dispone ora di una base giuridica specifica per adottare norme legislative volte a proteggere questo diritto fondamentale[38]. Lo sviluppo delle tecnologie informatiche e dell'accesso ai dati, hanno imposto una modifica

---

[35] U. Pagallo, *La tutela della privacy negli Stati Uniti D'America e in Europa,* Varese, 2008.

[36] L'art. 16 così statuisce: 1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti."

[37] Art. 39 TUE: "Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti."

[38] Da: www.consilium.europa.eu, consultato luglio 2016.

dell'approccio in tema di privacy, con una normativa, che riconosce al titolare delle informazioni il diritto di limitarne la circolazione.

Il 14 Aprile 2016 il Parlamento Europeo ha approvato il regolamento sulla protezione dei dati che sostituisce, abrogando, la direttiva 95/46/CE. Gli stati avranno ventiquattro mesi di tempo per adeguarsi al nuovo quadro normativo. Il pacchetto di protezione dati oltre che del regolamento, che interesserà la maggior parte delle norme sul trattamento dati, consta di una direttiva: la 2016/680, relativa al trattamento dati con riferimento alla prevenzione, accertamento e persecuzione di reati penali, affronterà i problemi di circolazione dei dati, posti dall'emergenza terrorismo; Recentemente è stata emanata anche la Direttiva 2016/681, circa la banca dati del PNR (*Passenger Name Record)*[39]*,* cioè tutte le informazioni di chi vola da e per l'Europa (per esempio data di viaggio, itinerario, modalità di pagamento etc.). La direttiva 2016/680/CE che unifica le norme sulla cooperazione transfrontaliera delle forza di polizia e in materia di giustizia, in quanto tale dovrà essere recepita dai singoli stati; il regolamento, invece, è direttamente applicabile, senza bisogno di norme interne di recepimento, circostanza che dovrebbe garantire una maggiore armonizzazione della materia a livello dell'intera Unione Europea. L'iter di tale regolamento è stato molto travagliato e sono trascorsi ben quattro anni dalla prima proposta della Commissione Europea. La necessità di emanare un regolamento nasce dalla continua evoluzione degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente alla diffusione del progresso tecnologico. Per quanto la matrice fosse la stessa, ogni paese aveva declinato e applicato a modo proprio la Direttiva 95/46. Una frammentazione di norme che però non ha ostacolato il formarsi di una coscienza collettiva del valore delle nostre informazioni personali. Il nuovo Regolamento risponde a queste esigenze: disposizioni comuni per dare ai cittadini maggiori tutele e alle imprese più facilità nell'applicarle. Uno strumento più efficace per difendersi, per esempio, da chi ci chiede un consenso indifferenziato all'uso dei nostri dati come condizione per accedere ad un servizio, cosa questa, molto frequente online. La Direttiva 95/46/ CE, fu adottata nel 1995 con due obiettivi: salvaguardare il diritto fondamentale

[39] www.eur-lex.europa.eu, consultato luglio 2016.

alla protezione dei dati e garantire la libera circolazione dei dati personali tra gli stati membri, ma l'aumento vertiginoso della condivisione e della raccolta dati ha frammentato le modalità di applicazione della protezione dei dati personali nel territorio dell'Unione. Di conseguenza, pur rimanendo valido in termini di obbiettivi e principi, il quadro normativo non ha eliminato l'incertezza giuridica e la diffusa percezione da parte dei cittadini - utenti che le operazioni online siano rischiose. E' quindi diventato necessario creare un quadro giuridico più solido e coerente in materia di protezione dei dati nell'Unione che, affiancato da efficaci misure di attuazione, possa garantire lo sviluppo dell'economia digitale nel mercato interno, il controllo dei dati personali delle persone fisiche e rafforzare la certezza giuridica e operativa per i soggetti economici e le autorità pubbliche.

Il Regolamento europeo consta di novantanove articoli e tra le novità più importanti possiamo riportare: il diritto dell'interessato alla portabilità del dato[40] ed il diritto all'oblio[41], per cui ogni individuo potrà chiedere la cancellazione dei propri dati in possesso di terzi per motivi legittimi; il principio della *"accountability",* cioè l'onere da parte del responsabile del trattamento di dimostrare l'adozione di tutte le misure privacy prese nel rispetto del regolamento; il registro delle attività di trattamento[42]: che richiede di redigere e conservare un registro in cui riportare tutte le attività di trattamento dati svolte sotto la responsabilità del titolare al trattamento; la cooperazione con l'autorità di controllo, notificando qualsiasi violazione dei dati personali alla stessa e al diretto interessato[43]; il *privacy impact assessment:* per cui saranno necessarie valutazioni di impatto sulla protezione dati in caso di trattamenti rischiosi e verifiche preliminari, per diverse circostanze, da parte del garante. Si citano espressamente i parametri di gravità e probabilità dell'evento[44]; si prevede inoltre la figura del *data protection officer:* un responsabile della protezione dei dati, interno o esterno, con ampia conoscenza della normativa, in relazione solo con i vertici

[40] Art. 20, Regolamento Unione Europea 2016/679.

[41] Art.17, i*vi.*

[42] Art. 30, *ivi.*

[43] Artt. 32 e 34, *ivi.*

[44] Art. 35, *ivi.*

dell'azienda e dotato di autonomia e indipendenza[45]. Questi predisporrà un sistema di misure di sicurezza finalizzate alla privacy che assicurino il rispetto del regolamento europeo e la sicurezza; In merito all'informativa e al consenso, le informative dovranno essere più dettagliate ma soprattutto più efficaci delle precedenti, usando a tal fine anche moduli, schemi o disegni. Il testo del regolamento europeo, al di là delle novità specifiche già rilevate, introduce un nuovo concetto di privacy, quello di *"privacy by design",* cioè la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali dovrà essere integrata nell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla sua ultima distribuzione, all'utilizzo e all'eliminazione finale. Inoltre, si affianca a questo concetto, quello di *"privacy by default"* e cioè le impostazioni di tutela della vita privata relative a servizi e prodotti dovranno rispettare i principi generali della protezione dati, quali la minimizzazione dei dati e la limitazione delle finalità per le quali sono raccolti[46]. Il regolamento ribadisce alcuni concetti fondamentali che erano alla base della direttiva 95/46/CE. Parte, infatti, dalla premessa che la tutela delle persone fisiche con riguardo alla protezione dei dati personali è un diritto fondamentale. I principi e le norme a tutela delle persone fisiche in materia di privacy, devono rispettare i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza degli interessati. Altra premessa in comune con il quadro normativo precedente è che il trattamento dei dati personali deve essere al servizio dell'uomo. Il diritto alla protezione dei dati non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e, in ottemperanza al principio del pari grado, contemperato con gli altri diritti fondamentali. Tra gli obbiettivi fondamentali del regolamento vi sono quelli di garantire certezza del diritto e trasparenza degli operatori economici; offrire alle persone fisiche in tutti gli stati membri lo stesso livello di azionabilità dei diritti, definire responsabilità e obblighi sia dei titolari che dei responsabili del trattamento, assicurare un monitoraggio costante nel trattamento dei dati personali e, infine, prevedere sanzioni equivalenti in tutti gli stati membri e una cooperazione efficace tra le autorità di controllo dei diversi stati membri. Non

[45] Artt. 37 - 39, Regolamento Unione Europea 2016/679.

[46] M.Colombo, *Privacy By Design & By Default,* in www.pharmasoft-fea.com, consultato 20 luglio 2016.

mancano dubbi in merito al regolamento; tra i punti più critici sono stati evidenziati[47], si cita innanzitutto l'ambito di applicazione materiale e territoriale delle nuove norme che appare sfumato. Per esempio, si dice che il regolamento riguarda solo il trattamento dei dati personali interamente o parzialmente automatizzato ma, anche il trattamento non automatizzato se i dati personali sono contenuti in un archivio o sono destinati a figurarvi. Da una parte, sembra difficile inquadrare precisamente il concetto di "destinazione ad essere archiviati "; dall'altro, rende perplessi l'esclusione dalle tutele del regolamento, dei dati contenuti in fascicoli non strutturati, il che infatti potrebbe esporre ogni persona ad alti rischi di violazione per il solo fatto della non strutturazione dei supporti[48]. Sull'ambito territoriale il criterio è che si applicherà il regolamento UE ad ogni trattamento di dati di persone di qualsiasi nazionalità quindi a tutti gli operatori di siti o app che offrono beni e servizi nell'Unione Europea, oppure che offrono funzioni in grado di monitorare i comportamenti di navigazione/utilizzo di persone che si trovano nell'Unione Europea; e tutto questo a prescindere dall'uso di strumenti situati all'interno dell'Unione oppure dall'esistenza o meno di strumenti dell'Unione[49]. Questo implica che la normativa sarà applicata se l'operatore ha una stabile organizzazione nell'Unione Europea anche se i dati sono trattati al di fuori dell'Unione. Non è chiaro invece se si applicherà la normativa del regolamento nel caso in cui l'operatore è stabilmente organizzato all'interno dell'Unione Europea e tratta dati per conto di clienti/titolari fuori dall'Unione Europea.

Seconda questione riguarda la sorte della vecchia normativa privacy: non è dato sapere la valenza che avranno tutti i provvedimenti generali del garante italiano prodotti in questi decenni. Il nuovo regolamento esplicitamente ritiene valide e quindi in corso tutte le autorizzazioni del Garante. Di fatto però, non menziona tutti gli altri provvedimenti emessi da questa autorità che quindi dovrebbero

---

[47] L. Bolognini, *Regolamento UE privacy, le quattro incognite da sciogliere,* in www.agendadigitale.eu, 21 Aprile 2016.

[48] Ibidem.

[49] Regolamento 2016/679 del Parlamento Europeo e del Consiglio, 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), Capo I *Disposizioni generali, Art. 3 Ambito di applicazione territoriale.*

essere via via sottoposti ad analisi per accertarne la compatibilità con il Regolamento. Questo lavoro che sicuramente richiede tantissimo tempo dovrà farsi in due anni, La terza questione, riguarda il fatto che la Commissione dell'Unione Europea ha avviato i lavori per la revisione della Direttiva 2002/58/CE, direttiva e-privacy. Questa revisione è urgente perché la "*cookie law"* che è recepimento della direttiva e-privacy e della direttiva 2009/136 CE, fatte salve dal nuovo regolamento, deve essere allineata al regolamento stesso e non è chiaro in che modo ciò avverrà. Una quarta questione riguarda il DPO (Responsabile della Protezione Dati). Quest'ultimo è una persona esperta nella protezione dati con il compito di valutare e organizzare la gestione del trattamento dei dati personali, la loro protezione, all'interno di un'azienda pubblica o privata, di un ente o di un'associazione affinché i dati siano trattati nel rispetto delle normative privacy europee e nazionali[50]. L'articolo 39 del Regolamento europeo sulla protezione dei dati personali ne elenca i principali compiti: informare e fornire consulenza al titolare del trattamento, al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento; sorvegliare che il Regolamento e le altre disposizioni dell'Unione e degli stati membri relative alla protezione dei dati vengono rispettati; fornire pareri se richiesti in merito alla valutazione di impatto sulla protezione dati; essere punto di contatto per l'autorità di controllo. Tale figura avrà quindi numerose funzioni e responsabilità. Il dubbio che nasce è se una singola persona sarà in grado di gestire strutture grandi e complesse o perfino più enti insieme. Data la complessità delle funzioni assegnate al DPO è stata istituita un'associazione dei *data protection officer* - ASSO DPO - che sosterrà le aziende, i consulenti privacy e gli attuali titolari e responsabili del trattamento dati, nella formazione professionale dei DPO. Solo grazie ad un'interpretazione puntuale e dettagliata del regolamento, questi e altri dubbi potranno essere sciolti in modo che il regolamento possa garantire di fatto un'elevata e uniforme tutela dei dati e possa offrire un maggior controllo ai cittadini sull'utilizzo dei loro dati[51].

---

[50] Associazione Data Protection Officer, *Cosa farà il DPO?,* 31 Maggio 2016.

[51] L. Bolognini, Presidente Istituto Italiano per la privacy, *Le quattro incognite da sciogliere,* in Agenda, www.digitale.eu.

Par. 3: *Fonti dell'ordinamento italiano in materia di privacy*

In particolare in Italia, la prima elaborazione del diritto alla privacy in Italia si riscontra a livello giurisprudenziale, con la sentenza della Corte di Cassazione n. 4487 del 1956, a seguito del ricorso presentato dagli eredi del tenore Enrico Caruso. Nella sentenza il diritto alla privacy veniva identificato nella tutela di tutte quelle vicende personali e familiari anche se svoltesi fuori dal domicilio domestico che non si presentavano socialmente apprezzabili per i terzi. In essa si manifesta un atteggiamento rivolto alla decisa negazione del diritto alla riservatezza affermando che «nessuna disposizione di legge autorizza a ritenere che sia stato sancito come principio generale il rispetto assoluto all'intimità della vita privata e tanto meno come limite alla libertà dell'arte » , ricollegando la tutelabilità dell'interesse in questione esclusivamente al fatto che «[…] la conoscenza delle vicende della vita altrui non sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto […]», attraverso cioè comportamenti che integrassero gli estremi del fatto illecito. Secondo la Cassazione quindi «il tema ben poteva trovare la sua soluzione, senza il bisogno di inventare istituti nuovi, nel precetto generale del *neminem laedere*, come specificato per l'appunto nell'art. 2043 c.c.»[52]. Dopo questo primo indirizzo, la Cassazione torna a pronunciarsi sulla materia nel 1963, con la sentenza del 20 aprile n. 990, con la quale riconosce fondata la pretesa dei familiari di Claretta Petacci a non raccontare in un libro vicende private in assenza di interesse pubblico. La sentenza può considerarsi decisiva in quanto segna il mutamento della rigida posizione iniziale. Dalla suddetta pronuncia non scaturisce ancora il riconoscimento incondizionato del diritto alla riservatezza, dato che la Corte ribadisce la mancanza di una norma che espressamente la contempli, respingendo inoltre la praticabilità dello strumento analogico. Tuttavia essa afferma l'esistenza di un «diritto *erga omnes* alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo»[53]. La formula richiama l'art. 2 Cost.

[52] E. Graziadei, *Privatezza: rimedi vecchi e offese nuove*, in www.Giur.it., 1971.

[53] Cass. 20 aprile 1963 n. 990, in www.Foro.it, 1963, I, p. 877.

che è posto quindi a fondamento del diritto in questione, dimostrando di accogliere, sulla scorta di autorevole dottrina, la configurazione monistica del diritto unico della personalità. Da tale costruzione giuridica deriva il divieto di divulgare notizie attinenti alla vita privata dell'individuo «a meno che non sussista un consenso anche implicito della persona, desunto dall'attività in concreto svolta, o, data la natura dell'attività medesima o del fatto divulgato, non sussista un prevalente interesse pubblico di conoscenza»[54].

La successiva tappa dell'iter evolutivo della giurisprudenza della Suprema Corte è rappresentata da una sentenza del 1975[55] con la quale si tutelava il diritto alla riservatezza della moglie dello Scià di Persia. La Corte porta in rilievo l'esistenza di un duplice fondamento, implicito ed esplicito, del diritto alla riservatezza: il primo viene individuato «in quel complesso di norme ordinarie e costituzionali che, tutelando aspetti peculiari della persona, nel sistema dell'ordinamento sostanziale, non possono non riferirsi anche alla sfera privata di essa»[56]. Il fondamento definito esplicito è fissato « in tutte quelle norme, contenute in modo particolare in leggi speciali, nelle quali si richiama espressamente la "vita privata del soggetto" o addirittura la riservatezza»[57]. La sentenza opera inoltre un espresso richiamo degli artt. 2, 3, 27, 29 e 41 Cost. quali norme da cui ricavare principi di «tutela della sfera privata del soggetto con conseguenti limitazioni ad altre garanzie costituzionali quali, per esempio, il diritto all'informazione»[58]. Con sentenze successive[59], la Cassazione è arrivata a riconoscere pienamente l'esistenza, nel nostro ordinamento, di un diritto alla riservatezza. In conclusione si riscontra, tra la prima e l'ultima rilevante decisione in materia, un vero e proprio capovolgimento dell'orientamento della Suprema Corte sulla questione dell'esistenza di un autonomo diritto alla riservatezza, risultante da una complessa attività interpretativa delle norme positive, attraverso le fasi che si è cercato di schematizzare. Su tale cambiamento hanno senza dubbio inciso anche le crescenti

---

[54] Ibidem.

[55] Cass. 27 maggio 1975, n. 2129,1975.

[56] G. Giacobbe, *Il diritto alla riservatezza nella prospettiva degli strumenti di tutela*, in AAVV, Il riserbo e la notizia, p. 113.

[57] Ibidem.

[58] Ibidem.

[59] Cfr., ad esempio, Cass. 21 febbraio 1994, n. 1652, in Giur. it., 1995, I, 1, p. 298.

esigenze di tutela avvertite in seguito ai mutamenti della realtà sociale. In Italia era quindi per lo più tutelata la riservatezza delle persone famose piuttosto che di ogni cittadino. Occorre aspettare la legge 675 del 1996 e il Codice in materia di protezione dei dati personali (Codice della privacy) cioè il Decreto legislativo 30 giugno 2003, n.196, per avere una tutela della privacy estesa a tutti. In tale decreto si afferma chiaramente il diritto di privacy come diritto non solo a non trattare i propri dati senza consenso, ma anche come diritto all'adozione di garanzie tecniche ed organizzative, che tutti devono rispettare per procedere in maniera lecita al trattamento dei dati altrui[60]. Il nostro legislatore ha quindi introdotto nel nostro ordinamento, accanto al diritto alla riservatezza, un autonomo diritto alla protezione dei dati personali, come diritto avente ad oggetto la protezione del dato personale, a prescindere dalla tutela della sfera intima della persona e della famiglia, nonché della sua immagine sociale. La prima legge organica in materia di protezione dei dati personali è quindi stata la legge del 31 Dicembre 1996, n. 675. Questa ha introdotto nell'ordinamento il nuovo diritto relativo alla protezione dei dati personali, distinto dal diritto alla riservatezza già da tempo riconosciuto nell'ordinamento giuridico italiano. Tale diritto ha un oggetto estremamente vasto che è conseguenza della stessa definizione di "dato personale"[61]. Costituisce dato personale "qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale[62] ". Il dato personale è quindi qualunque informazione riferibile ad una persona fisica, per cui sono escluse le persone giuridiche, gli enti o le associazioni. Riguarda quindi tutte quelle informazioni che configurano il modo di essere del soggetto nella società; sono invece esclusi dall'ambito di applicazione i dati anonimi, intendendo per tali quei dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile. Il diritto alla protezione dei dati personali si colloca nell'ambito dei diritti della personalità, e come tale assoluto,

---

[60] C. Canale, *Internet e le nuove frontiere di tutela della privacy alla luce delle ultime sentenze della Corte di Cassazione e della Corte di Giustizia Europea,* www.temiromana.it.

[61] G. Finocchiaro, P*rivacy e protezione dei dati personali, Bologna, 2012.*

[62]D.lgs 30 Giugno 2003 n.196, Art. 4. b) "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

indisponibile e imprescrittibile, il cui fondamento si rinviene nell'art. 2 della Costituzione[63]. Il diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata (diritto alla riservatezza) costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle informazioni sul proprio conto. L' art. 2 della Costituzione inteso come clausola generale di protezione del libero e completo svolgimento della persona umana, traduce in linguaggio giuridico tre principi: il principio personalista che riconosce e garantisce i diritti individuali dell'uomo come singolo; il principio pluralista che riconosce e garantisce i diritti inviolabili dell'uomo nell'ambito delle formazioni sociali; il principio di solidarietà che richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica, e sociale. La norma ha la funzione di tutelare e garantire quei diritti naturali e quei valori di libertà che emergono e si affermano con l'evoluzione del costume sociale (diritto alla riservatezza, diritto all'identità sessuale etc). In questo modo l'art. 2 Cost. si qualifica come norma a fattispecie aperta per cui qualsiasi nuova generazione dei diritti di libertà può entrare a far parte dell'ordinamento giuridico acquistando rilevanza costituzionale. Il diritto in questione e i diritti della personalità ad esso limitrofi, quali il diritto alla riservatezza, il diritto all'immagine, il diritto alla reputazione. sono tutti volti a tutelare un unico bene giuridico: l'identità, nelle sue molteplici forme. La reputazione che è la considerazione in cui si è tenuti dagli altri, i dati personali e cioè le informazioni su un soggetto, l'identità personale ovvero la proiezione di sé nel sociale, il nome che caratterizza l'identità anagrafica, tutti questi diversi elementi formano l'immagine sociale di un soggetto, la sua identità. E' vero che la persona è ciò che è in un determinato momento storico e l'identità muta col tempo. Eventi avvenuti in una certa epoca possono non corrispondere più alla personalità del soggetto in un diverso momento storico. E' proprio sulla base del potenziale conflitto tra la verità della storia e l'identità attuale, nasce il diritto all'oblio. Con tale diritto si fa riferimento al diritto di un soggetto a non vedere ripubblicate alcune notizie relative a vicende, già legittimamente pubblicate, rispetto all'accadimento delle quali è trascorso un notevole periodo di tempo. La

[63] Art. 2 Cost. << La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale>>.

giurisprudenza ha avuto modo di affermare che il tempo gioca un ruolo importante anche qualora non si tratti di eventi di cronaca, ma di qualsivoglia evento in relazione al quale un periodo significativo sia ormai trascorso e manchino elementi di constestualizzazione. In questi casi la giurisprudenza ha ravvisato la violazione del diritto all'identità personale. Come quest'ultimo, così il diritto all'oblio nella sua prima formulazione nasce come diritto riferito ai fatti di cronaca, trova una diversa declinazione nel contesto online. Infatti, la ripubblicazione non è più necessaria, dal momento che la rete non dimentica. Ciò comporta un archivio storico di dimensioni globali, nel quale sono del tutto assenti i criteri essenziali dell'archiviazione, relativi alla qualità dell'informazione, alla contestualizzazzione della stessa, che è il fulcro della costruzione del diritto dell'identità personale e di quello all'oblio.

Sembrano due le innovazioni più importanti introdotte dal codice della privacy[64]: la valorizzazione del bene informazione e l'attribuzione di un ruolo centrale al soggetto cui si riferiscono i dati personali nel sistema di protezione. Infatti, valorizzando il bene informazione il legislatore ha formalizzato, sotto il profilo giuridico, quanto già ampiamente noto in campo economico: che i dati e le informazioni hanno un valore economico. Ponendo al centro il soggetto al quale i dati si riferiscono, e non il soggetto che li ha raccolti, il legislatore ha ribaltato la prospettiva, che era stata essenzialmente incentrata sulla protezione delle banche di dati. Inoltre, prima della legge n.675 del 1996 le informazioni erano oggetto di considerazione giuridica solo se la loro diffusione poteva cagionare la lesione del diritto alla riservatezza o comunque un danno ingiusto *ex* art. 2043 c.c.. La legge n.675 ha introdotto, invece, la tutela dell'informazione in quanto tale, a prescindere dal contenuto: ciò che prima appariva senza valore, una volta divenuto oggetto di specifica informativa e sottoposto a consenso, ha assunto rilevanza sempre più evidente. La seconda delle innovazioni, cioè quella relativa all'attribuzione di un ruolo centrale all'interessato, è collegata alla natura dell'informazione che in questo caso viene in rilievo. Il dato personale, infatti, non è solo un bene economicamente rilevante, ma anche un elemento che contribuisce a definire l'identità di un soggetto. Dunque, vi è un aspetto più

[64] D. lgs 196/2003, Codice in materia di protezione dei dati personali.

strettamente personale nell'informazione, riguardo al quale la legge pone al centro del sistema l'interessato attribuendogli il controllo sui suoi dati personali attraverso i diritti di accesso, rettifica, integrazione, opposizione, nonché ove è previsto, condizionando il trattamento all'espressione del consenso[65].

Tornando alle previsioni Costituzionali, all'art. 15 sancisce che la libertà e la segretezza delle comunicazioni sono inviolabili e la loro limitazione può avvenire solo per atto motivato del giudice e nel rispetto delle garanzie previste dalla legge. Secondo la giurisprudenza consolidata, sono comunicazioni tutelate dall'articolo in esame sia il messaggio di posta elettronica inviato ad un destinatario determinato oppure ad una *mailing list* chiusa, o ancora ad una chat tra due soggetti o ad una videoconferenza *one to one.* Al contrario, rientrano nel novero della libertà di manifestazione di pensiero (art. 21 Cost.) tutte quelle comunicazioni che si realizzano in forme che consentono la partecipazione di un numero indeterminato di soggetti (Chat-room, Mailing list aperte, etc.). Oggetto della garanzia costituzionale, quindi ,non sono né la cosa che incorpora materialmente il pensiero o la notizia trasmessi, né la forma in cui vengono espressi, bensì l'atto del corrispondere o del comunicare in maniera non conoscibile dalla generalità e quindi ad avere rilievo è il rapporto di comunicazione che si instaura tra due soggetti determinati. Tutte le limitazioni devono essere accompagnate da apposite garanzie previste dalla legge che dovrà quindi individuare gli scopi della misura limitativa, la durata massima della stessa, i casi e i modi in cui la restrizione può essere adottata, la sindacabilità del provvedimento assunto. Inoltre, tutte le limitazioni devono essere adottate mediante un atto necessario motivato di un giudice su richiesta del pubblico ministero. Tale previsione ha maggiore forza nelle ipotesi delle intercettazioni, consentite dal codice di procedura penale solo per talune categorie di reati e come assolutamente indispensabili al proseguimento delle indagini. La l. del 20 novembre 2016, n.281 ha inoltre stabilito che i documenti, i supporti e gli atti concernenti dati e contenuti di conversazioni e comunicazioni, relativi al traffico telefonico e telematico, illegalmente formati o acquisiti, vengono secretati e custoditi in luogo protetto dal pubblico ministero, in attesa delle determinazioni

[65] G. Finocchiaro, P*rivacy e protezione dei dati personali, Bologna, 2012.*

del GIP in merito alla loro distruzione. Ai sensi del D.lgs. 196/2003 i dati estrinseci per finalità di accertamento devono essere mantenuti dal gestore telefonico per due anni, mentre quelli riguardanti il traffico telematico per un anno[66]. Il pubblico ministero può, con decreto motivato, acquisirli.

Par. 4: *Fonti dell'ordinamento statunitense in materia di privacy e accordo EU-US privacy shield del luglio 2016*

La tutela della privacy nel contesto statunitense è attuata sia in rapporto alla vita pubblica delle persone, sia alla loro sfera privata, sulla base del primo e del quarto emendamento della Costituzione. Mentre nel primo caso la privacy è garantita in nome dei principi di libertà di espressione e di associazione, nel secondo caso, invece, si tratta del diritto alla sicurezza per la propria persona, abitazione, documenti ed effetti, contro ogni ragionevole intrusione dello stato o del Governo. Oltre al riferimento costituzionale (primo e quarto emendamento), il diritto alla privacy trova tutela a livello di legislazione ordinaria sia nella legge federale, sia nelle normative dei singoli stati. Senza analizzare a fondo il problema di definire i rapporti tra i due, basti affermare che i provvedimenti presi dai parlamentari di Washington lasciano ampio spazio di manovra e discrezionalità alle azioni dei singoli stati federati. La tutela costituzionale della privacy negli USA presenta, infatti, una particolarità rispetto al modello europeo: essa riconosce una zona franca per la quale è proibito l'intervento del Governo federale negli affari personali degli individui; spetta agli stati federati garantire, eventualmente, tramite azioni "positive", una maggiore sfera di tutela della privacy rispetto al minimo previsto costituzionalmente.

La legge di riferimento negli Stati Uniti fino ad oggi, era il *Privacy Act*, approvato dal Congresso il 31 dicembre 1974. Tale normativa si componeva di un articolo, il 552 del titolo quinto del Codice degli Stati Uniti[67], suddiviso in ventuno sottoparagrafi rubricati con le lettere dell'alfabeto. Inizialmente concepita come uno strumento operativo per rafforzare le garanzie previste dal quarto

[66] Art. 132 D.lgs. 196/2003.

[67] *Public Law* No. 93-579, 88 Stat. 1897, in 5 U.S.C. (*United States Code),* § 552.

emendamento, la legge stabiliva che nessun ente pubblico potesse trasmettere a persone o a organizzazioni terze, dati relativi ad un soggetto senza averne ottenuto il previo consenso o la richiesta scritta. Eccezione a tale divieto era prevista nei casi che riguardavano l'utilizzo statistico o d'archivio dei dati, gli atti delle agenzie governative, le investigazioni condotte dal Congresso. Inoltre, essa prevedeva che chiunque avesse diritto a ottenere copia dei documenti relativi ai dati che lo riguardavano, ed eventualmente, esigere la modifica o la correzione degli stessi. Il *Privacy Act* prevedeva poi una serie di esenzioni, generali e specifiche, per le quali l'individuo non aveva il diritto di far valere la propria privacy nei confronti delle Corti nell'esercizio dell'azione penale. Si trattava ancora una volta del limite posto al diritto dalle esigenze di sicurezza nazionale e di ordine pubblico, che, per via del progresso tecnologico, portò il Congresso, nel 1988, ad approvare il *Computer Matching and Privacy Protection Act*, con cui emendò parte del *Privacy Act.* L'obiettivo fu quello di assicurare l'uniformità procedurale nella elaborazione dei dati e il principio costituzionale del giusto processo, attraverso specifici *boards* o comitati a salvaguardia dell'integrità dei dati trattati. Inoltre, nel 2008, il legislatore americano approvò il *Genetics Information Non-Discrimination Act* (GINA) che, tra le altre previsioni, vieta espressamente e severamente l'uso dell'informazione genetica da parte delle compagnie di assicurazione, e che è stato presentato come << la prima legislazione a tutela dei diritti civili varata dal Congresso negli ultimi vent'anni[68] >>. Tuttavia, non si può dire che tutte le leggi approvate dal Congresso americano siano state in favore della privacy. Basta tornare all'articolo 552 del Codice, e in particolare ai due punti in cui vengono disciplinati i rapporti contrattuali del governo con terzi e la gestione degli indirizzari. Con l'introduzione dei programmi di sicurezza nazionale, si è diffusa progressivamente la convinzione che alcuni di questi progetti di sicurezza siano in palese contrasto con le disposizioni del *Privacy Act.*

La crescente interdipendenza mondiale che si delinea tra globalizzazione, legislazione di emergenza e nuovi strumenti tecnologici, ha portato gli USA e l'Unione Europea a cercare degli accordi in materia, soprattutto per tutelare il

[68] Parere di J. Gruber, direttore del National Workrights Institute, in *La tutela della privacy negli Stati Uniti D'America e in Europa,* di U. Pagallo, Milano, 2008.

trasferimento e lo scambio dei dati. Tra questi, l'accordo quadro sui PNR, che dovrebbe garantire standard elevati di protezione dei dati all'atto dello scambio, tra autorità giudiziarie e di polizia; si tratta di dati personali quali fedine penali, nomi o indirizzi da scambiare tra le due sponde dell'Atlantico per combattere il crimine e il terrorismo. Quando il 24 febbraio 2016 il Presidente Obama ha firmato la legge sul ricorso giudiziario, si è aperta la strada alla firma dell'accordo, che istituirà un quadro completo di alto livello di protezione dei dati per la cooperazione tra UE e USA. La legge sul ricorso giudiziario (*Judicial Redress Act*) sancisce infatti il diritto per tutti i cittadini dell'UE di adire i tribunali statunitensi per far applicare i propri diritti di tutela dei dati, un diritto di cui godono già i cittadini statunitensi in Europa. La *Judicial Redress Act bill*, approvata grazie a un largo sostegno delle camere del Congresso, è stata considerata come un gesto che dimostra la volontà di ricostruire il rapporto di fiducia con gli alleati europei in seguito allo scandalo del Datagate, nato dalle rivelazioni di Edward Snowden sui controlli di massa operati dalla NSA sulle comunicazioni degli utenti europei. Già con l'Us *Freedom Act*[69], la legge che ha sottratto alla NSA la possibilità di raccogliere e archiviare indistintamente i dati telefonici di milioni di americani, era stato compiuto un primo passo formale per riaffermare il dovere di tutelare i diritti dei cittadini. Con il *Judicial Redress Act*, il presidente americano mira ora a ripristinare il rapporto di reciproco rispetto tra Europa e Stati Uniti. Obama ha definito la legge una misura chiave per la tutela dei dati dei consumatori che contribuirà a incrementare il mercato del paese. Molti osservatori hanno accolto il *Judicial Redress Act* come un passo necessario per ristabilire un clima di effettiva collaborazione per la lotta al terrorismo e la condivisione dei dati raccolti dalle rispettive forze di sicurezza e di intelligence. Durante la cerimonia formale del *Judicial Redress Act,* Obama si è soffermato sul tema del rapporto tra privacy e sicurezza, dichiarando che opererà per << Garantire che anche se proteggiamo la sicurezza del popolo americano, siamo pure consapevoli della privacy che amiamo così tanto>>. Washington starebbe già studiando una nuova proposta di legge per la creazione di una commissione sulla

[69] Legge degli Stati Uniti emanata il 2 giugno 2015 che ha restituito in forma modificata diverse disposizioni scadute del Patriot Act.

sicurezza digitale, volta a favorire l'approvazione di una nuova legge definitiva in materia di privacy e crittografia entro la fine dell'anno.

Nel 2000, l'Unione Europea e gli Stati Uniti D'America avevano concluso un accordo che regolava le modalità attraverso cui le società statunitensi potevano esportare e gestire i dati personali dei cittadini dell'Unione europea: un "approdo sicuro", questa la sua traduzione letterale, per le imprese americane che fino a oggi potevano considerarsi automaticamente in regola nel trattamento della privacy dei cittadini europei[70].

L'accordo, o meglio la decisione della Commissione che ne ha riconosciuto validità, era in linea con quanto disposto dall'art. 25 della Direttiva 95/46/CE, il quale dispone a livello generale il divieto di trasferimento dei dati al di fuori del territorio dell'Unione, a meno che lo stato terzo non garantisca "un livello adeguato" e al di là delle deroghe poste a tale divieto nell'articolo successivo. Si trattava di uno strumento volontario, che si configurava come una sorta di autoregolamentazione a cui si sottoponevano le aziende americane, base per riconoscere quell'adeguatezza nel trattamento dei dati richiesta dalla normativa europea. Riguardava le società che immagazzinavano i dati dei clienti e dunque in prima battuta quelle attive nel business di Internet come Facebook e Google, ma non solo: sono infatti 4.500 le aziende americane che hanno sottoscritto il *Safe Harbor*. Lo scopo dell'accordo era quello di impedire la perdita accidentale o la rivelazione di dati personali.

Per poter aderire al programma le società americane dovevano rispettare sette principi: 1) gli utenti dovevano essere avvertiti sulla raccolta e l'utilizzo dei propri dati personali; 2) ciascuno doveva essere libero di rifiutare la raccolta dei dati e il loro trasferimento a terzi; 3) i dati potevano essere trasferiti solo a organizzazioni che seguivano principi adeguati di protezione dei dati; 4) le aziende dovevano fornire garanzie contro il rischio che i dati venissero smarriti; 5) dovevano essere raccolti solo i dati rilevanti ai fini della rilevazione; 6) gli utenti avevano il diritto di accedere ai dati raccolti ed eventualmente a correggerli o cancellarli se inesatti; 7) dovevano essere previsti meccanismi atti a garantire l'effettiva attuazione dei

[70] L. Castagneri, *Cos'è il Safe Harbor e perché ti riguarda da vicino,* Gennaio 2016. Si tratta del Safe Harbor, la cui validità è stata riconosciuta in Europa con la Decisione della Commissione 2000/520/CE del 26 luglio 2000, c.d Approdo sicuro.

principi dell'approdo sicuro. Una volta che l'impresa aderiva al programma, doveva rinnovare la certificazione ogni 12 mesi[71]. La Corte di giustizia dell'Unione Europea ha annullato la Decisione 2000/520/CE[72]. La Corte ha dichiarato invalida questa decisione con cui la Commissione Europea aveva accertato l'adeguatezza della protezione dei dati personali offerta dal cosiddetto *Safe Harbour*, quale condizione per il trasferimento di dati personali dall'Unione Europea verso gli Stati Uniti. La vicenda nasce dal ricorso presentato da un cittadino austriaco, Maximillian Schrems, verso il *Data Protection Commissioner* irlandese. Il ricorrente, utente di Facebook, denunciava che i dati personali forniti al social network e trasferiti dalla filiale irlandese di Facebook alla sede principale della stessa negli Stati Uniti, fossero sottoposti ad intensa attività di sorveglianza di massa da parte del governo statunitense. Il ricorrente chiedeva quindi al DPC irlandese di vietare tale trasferimento vista l'inadeguatezza degli Stati Uniti di impedire una sorveglianza indiscriminata sui dati. Il ricorso inizialmente veniva respinto sia perché non era certo che i dati personali del ricorrente fossero stati oggetto di sorveglianza da parte delle autorità pubbliche statunitensi, sia perchè l'adeguatezza del trasferimento dati verso gli Usa era già stata determinata sulla base della decisione 2000/520/CE. Il provvedimento impugnato dal ricorrente finisce innanzi alla Corte di Giustizia quest'ultima dopo aver precisato che è esclusiva competenza della Corte di Giustizia decidere sulla validità di una decisione della Commissione, invalidò la decisione sul *Safe Harbour*[73]. Sulla decisione della CGUE hanno influito senza dubbio le rivelazioni di Edward Snowden e il venire alla luce di un vero e proprio sistema di sorveglianza di massa, alla luce del quale sono sorti dubbi sulla tutela garantita ai dati dei cittadini europei una volta trasferiti oltreoceano.

Se negoziati per un nuovo accordo tra Usa e Ue erano stati aperti già da due anni, in seguito alla pronuncia del giudice di Lussemburgo si è avvertita più che mai la necessità di arrivare a un nuovo accordo in materia. E' nato quindi un nuovo accordo politico battezzato "*Eu-Us Privacy Shield*", lo "Scudo per la privacy Stati

---

[71] *Protezione dei dati, che cos'è il "Safe Harbor",* www.ilsole24ore.it Luglio 2016.

[72] Lussemburgo, 6 ottobre 2015, Sentenza nella causa C-362/14 Maximillian Schrems/Data Protection Commissioner.

[73] Da www.curia.europa.eu, documents, 6 Ottobre 2015.

Uniti-Ue", adottato il 12 luglio 2016. Tale accordo politico tutela i diritti fondamentali di qualsiasi persona nell'Unione Europea i cui dati personali sono trasferiti verso gli Stati Uniti; e prevede obblighi rigorosi per le imprese che operano sui dati al fine di assicurare il rispetto delle regole a cui hanno aderito, pena sanzioni molto gravose; gli Stati Uniti hanno assicurato ufficialmente all'Unione Europea che l'accesso della pubblica autorità ai dati, per applicazione della legge o per esigenze di sicurezza nazionale, è limitato, garantito e puntualmente vigilato. Qualsiasi persona nell'Unione Europea potrà ricorrere in questo settore. Inoltre gli Stati Uniti hanno escluso attività indiscriminate di sorveglianza di massa sui dati personali trasferiti negli Usa nell'ambito dello scudo. L'eventuale raccolta di dati in blocco è prevista solo in presenza di determinati presupposti e sarà comunque più mirata e concentrata possibile. In tali circostanze, ritenute eccezionali, sono previste una serie di dettagliate garanzie riguardo all'uso dei dati. Inoltre viene previsto un meccanismo di mediazione: chiunque si ritenga leso nei suoi diritti, nell'ambito dello scudo, ha a disposizione meccanismi di ricorso di facile accesso e di costo contenuto. Sarà l'impresa stessa a risolvere il caso di reclamo o un organo ad hoc ADR[74]. L'individui potranno rivolgersi anche alle rispettive autorità nazionali di protezione dati nonché ad arbitrato. In quei casi che implicano la sicurezza nazionale potranno rivolgersi al Mediatore che è organo indipendente dai servizi di intelligence degli Stati Uniti. Lo scudo verrà annualmente sottoposto ad analisi comune da parte della Commissione Europea e del Dipartimento del Commercio degli Stati Uniti, che consulteranno esperti dell'intelligence statunitense e autorità europee di protezione dei dati[75]. Erano infatti sorti dubbi sul *Privacy Shield* sollevati dallo stesso Parlamento Europeo che, con una risoluzione non legislativa, aveva chiesto alla Commissione Europea di continuare le negoziazioni con gli Stati Uniti al fine di rimediare alle carenze del *Privacy Shield.* Infatti, se da un lato il nuovo accordo presentava dei sostanziali miglioramenti rispetto al precedente *Safe Harbour*, dall'altro ci sarebbero stati ancora dei nodi problematici da sciogliere: l'accesso da parte delle autorità di pubblica sicurezza ai dati trasferiti, la complessità del

[74] *Alternative Dispute Resolution.*

[75] F. De Benedetti, *Addio a Safe harbor, ecco lo "scudo per la privacy": sì all'accordo Usa-Ue sui dati personali,* in www.LaRepubblica.it, Febbraio 2016.

meccanismo di ricorso, l'assenza di poteri effettivi in capo alla nuova figura del Mediatore nel Dipartimento di Stato, nonché la possibilità di raccogliere grandi quantità di dati, che in alcuni casi non sarebbe conforme ai principi di necessità e proporzionalità. Dubbi, inoltre, furono posti dal Gruppo di lavoro ex art. 29[76]. Secondo tale organismo i testi della Commissione oltre ad essere estremamente complessi e a volte incoerenti, non tutelavano adeguatamente i cittadini europei perché lasciavano ampio margine di azione alle autorità di pubblica sicurezza americane. In ogni caso sempre secondo il gruppo, i testi dell'accordo dovevano essere revisionati in modo da assicurare un livello di protezione in linea con quello assicurato dal Regolamento[77]. La Commissione basandosi sui pareri espressi da queste autorità che avevano sollevato i dubbi in proposito, ha inserito varie precisazioni e ulteriori miglioramenti, concordando ulteriori elementi riguardanti la raccolta dei dati in blocco, rafforzando il meccanismo del Mediatore, esprimendo con maggiore chiarezza gli obblighi delle imprese. Notificata agli stati membri la decisione di adeguatezza il 12 luglio 2016 è entrata in vigore immediatamente. Vera Jurova, commissaria per la giustizia ha così commentato: << Lo scudo UE-USA per la privacy è un sistema nuovo e solido che offre agli europei la protezione dei dati personali e alle imprese la certezza del diritto. Rafforza le norme sulla protezione dei dati, che saranno fatte rispettare più rigorosamente, offre garanzie riguardo all'accesso da parte delle autorità pubbliche e semplifica per le singole persone le possibilità di ricorso in caso di reclamo. Il nuovo regime reinfonderà fiducia tra i consumatori i cui dati sono trasferiti verso l'altra sponda dell'Atlantico. Assieme alle autorità europee di protezione dei dati, al Parlamento europeo, agli Stati membri e alle controparti statunitensi abbiamo lavorato per mettere a punto un sistema che garantisse agli europei gli standard più elevati di protezione dei dati personali >>[78].

---

[76] Il Gruppo è stato istituito dall'art. 29 della direttiva 95/46 è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta. Il Gruppo adotta le sue decisioni a maggioranza semplice dei rappresentanti delle autorità di controllo.

[77] WP238, Opinion 01/2016 on the EU- U.S. Privacy Schield draft adequacy decision, 13 April 2016.

[78] Comunicato stampa, Commissione Europea, *La Commissione europea lancia lo scudo UE-USA per la privacy: più tutele per i flussi transatlantici di dati,* Bruxelles, 12 Luglio 2016.

Par. 5: *Differenze e affinità tra modello americano e quello europeo della privacy*

Risulta a questo punto chiaro, alla luce della ricostruzione normativa svolta, la distanza che intercorre tra il contesto europeo e quello statunitense in materia di privacy.

L'impostazione americana ed europea non sono perfettamente allineate. La prima, infatti, si concentra più sul valore economico e negoziabile dei dati personali che possono quindi essere ceduti agli utenti senza alcuna limitazione; esempio particolarmente eloquente è il caso Sorrell vs IMS Health del 2011[79]. L'approccio europeo, invece, muove dalla centralità della persona e dal diritto in capo ad essa di intervenire per tutelare il corretto trattamento dei dati personali. In Europa infatti la protezione dei dati è riconosciuta come diritto fondamentale, mentre negli USA l'approccio è più focalizzato sugli aspetti commerciali e sui diritti dei consumatori. Esistono dei punti di convergenza tra i due ordinamenti che riguardano la tutela dei diritti degli utenti sulla rete e la necessità di migliorare l'applicazione concreta di norme favorendo la cooperazione. Negli USA la legislazione si esime dall'imporre limitazioni relative alla privacy in materia di trasferimento dei dati personali verso altri paesi. Non esiste nessuna autorità federale che regolamenti il tutto, o che abbia poteri e funzioni che siano affini a quelle delle autorità europee di protezione dei dati. Il modello americano della privacy si presenta fondamentalmente come un sistema di tipo settoriale; manca cioè un quadro normativo generale che orienta e disciplina il settore in esame, che quindi risulta frammentato nelle disposizioni dei cinquanta stati federati. Da più parti è stata sollevata la necessità di introdurre una legislazione federale a vocazione generale per la tutela della privacy, ma questa tutela è invece ricondotta sostanzialmente alle decisioni della Corte Suprema. Il modello europeo della privacy, invece, si presenta come un sistema a vocazione "generale" con alcuni tratti tipici degli assetti giuridici federali. Vi è quindi un quadro normativo

[79] La Corte Suprema degli Stati Uniti ha annullato una legge dello stato del Vermont che limitava la possibilità per le società farmaceutiche di acquistare prescrizioni mediche senza il consenso dei medici, sulla base del fatto che la legge violava la libertà di espressione. E' un esempio di quanto sia forte l'enfasi posta sulla libertà di espressione dal sistema giuridico statunitense. Infatti secondo il diritto americano il trattamento dei dati personali è generalmente consentito; al contrario, ai sensi del diritto UE, tale trattamento è vietato se non ha un solido ancoraggio normativo.

generale (diritto comunitario) che orienta la materia. La rivoluzione tecnologica, la lotta al terrorismo e la globalizzazione ripropongono per entrambi i modelli le stesse questioni.

Non è difficile comprendere perché nel 2007 Bill Gates ha chiesto a gran voce una nuova legislazione federale sulla privacy. *L'Act* del 1974 con le successive modifiche copre solo una parte dell'ambito operativo dell'istituto, lasciando in sostanza alle leggi dei singoli stati ampio margine nella disciplina relativa ai rapporti tra privati. Così, alla specializzazione per materia tipica dell'ordinamento statunitense va ad aggiungersi quella per territorio, nel senso che, in materia di privacy, esistono almeno cinquanta normative diverse, che si intrecciano con ambiti così diversi dell'ordinamento come possono essere, la quiete familiare, la tutela del domicilio, la protezione della proprietà privata. A differenza della tutela costituzionale e federale della privacy, che s'interessa prevalentemente dei rapporti tra governo e individui, la legislazione ordinaria degli stati federati ha soprattutto a che fare con l'ambito delle relazioni tra privati cittadini. Essa incontra quindi come limite alla propria attività di promozione e di sviluppo, quello di non restringere in forma indebita l'altrui sfera, oltre ad altri eventuali diritti costituzionali in gioco[80].

[80] U. Pagallo, *La tutela della privacy negli Stati Uniti D'America e in Europa,* Varese, 2008, capitolo II.

Capitolo 3

Apple vs FBI: sicurezza nazionale o tutela della privacy?

Premessa

Quanto fin qui esposto dimostra come la tutela della privacy sia diventata una delle garanzie essenziali offerte ai cittadini delle società democratiche. Quello che ci si chiede oggi è se la lotta al terrorismo possa mettere, e fino a che punto, in discussione tale tutela. Il dibattito che si svolge intorno a tale questione è sintomatico del fatto che tutto il sistema è in equilibrio precario. Infatti dall'11 settembre ad oggi gli eventi terroristici che si sono susseguiti hanno sempre di più posto in luce la necessità di una più puntuale regolamentazione. L'evento terroristico che si prende in esame in questa trattazione è la strage di San Bernardino del 2 dicembre 2015 in California. Quest'ultima infatti porta alla luce la questione relativa alla composizione dei due interessi, privacy e sicurezza nazionale che in una società democratica possono apparire inconciliabili ma che è necessario portare in equilibrio.

Par. 1: Il caso

Durante le indagini sulla strage di San Bernardino, del 2 Dicembre 2015, in California, in cui furono uccise 14 persone e i due autori dell'attacco, fu rinvenuto un iPhone 5C appartenuto a Syed Rizwan Farook, uno dei due terroristi. L'Fbi ottenne da Apple i backup del telefono tramite il servizio iCloud, ma scoprì che non erano abbastanza recenti per ottenere informazioni sulle attività dei terroristi nelle settimane precedenti all'attacco. Infatti, dopo aver recuperato l'Iphone 5C, l'Fbi aveva chiesto ai tecnici della Contea di resettare la password del servizio iCloud da remoto, cioè da un altro dispositivo, pensando così di ottenere i dati dal backup di iCloud, senza l'aiuto della Apple. Questa procedura però bloccò i successivi backup dei file più recenti verso iCloud, perché quando si modifica la password da un altro dispositivo è necessario sbloccare l'iPhone inserendo il codice deciso dalla persona che lo utilizza. Il codice impostato da

Farook non era noto e dal momento che il sistema iOS prevede l'autocancellazione dei dati dopo dieci tentativi di sblocco, l'Fbi non poteva procedere con il metodo solitamente utilizzato per penetrare i dispositivi elettronici, provando cioè tutte le possibili password fino all'individuazione di quella corretta. Il *Secure Enclave,* questo è il nome del meccanismo di sicurezza previsto dalla Apple, doveva quindi , secondo l'Fbi, essere disabilitato per permettere all'agenzia di tentare ogni tipo di combinazione possibile. Gli agenti chiesero quindi a Apple – tramite un'ordinanza del giudice Sheri Pym del tribunale distruttale federale della California centrale – di creare una versione modificata ad hoc del suo sistema operativo iOS da installare su quel telefono, in modo da fornire un accesso secondario agli investigatori e permettere loro di ottenere i dati più recenti dall'iPhone di Farook, che erano criptati. Il giudice impose alla Apple di realizzare il software per disabilitare il sistema crittografico. Apple si oppose, sostenendo che una soluzione di questo tipo avrebbe creato un precedente molto pericoloso, perché l'FBI avrebbe potuto accedere a qualsiasi altro iPhone in suo possesso e che comunque una modifica di questo tipo a iOS sarebbe stata tecnicamente molto difficile. Intervenne a tal proposito, Tim Cook che in una lunga lettera[81] e in una intervista alla *Abc news* spiegò che quello che l'Fbi richiedeva avrebbe fornito una chiave universale, appetibile per qualunque organizzazione criminale o governo e che quindi avrebbe posto chiunque la custodisse in una posizione molto scomoda, suscettibile infatti di continui attacchi informatici. Di conseguenza prima o poi tale chiave si sarebbe persa <<Compromettendo centinaia di milioni di utenti onesti che ai propri telefoni o palmari consegnano informazioni sensibili riguardanti ad esempio, dati di lavoro, messaggi confidenziali o addirittura luoghi dove si trovano i loro figli >>[82]. Per questo motivo sarebbe stato opportuno quindi non creare affatto tale chiave universale. La posizione di Tim Cook al riguardo ricevette il sostegno di tutte le grandi aziende statunitensi del web – come Facebook e Google – e alimentò il dibattito relativo alla tutela dei dati online.

---

[81] T. Cook, *A Message to Our Customers*, February 16, 2016.

[82] T. Cook, *Apple vs. FBI: perché Apple si rifiuta di sbloccare l'iPhone di un terrorista?,* intervista in Abc news, febbraio 2016.

Il Dipartimento di Giustizia (DOJ) emise una mozione molto dura nei confronti di Apple: <<Il governo e il paese hanno bisogno di sapere cosa c'è sul telefono del terrorista, e il governo ha bisogno dell'assistenza di Apple per farlo >>, si legge nella mozione. << La retorica di Apple non è solo falsa, ma anche dannosa per le istituzioni che sono in grado di salvaguardare la nostra libertà e i nostri diritti >>[83]. Inoltre, << La preoccupazione di Apple riguarda il suo modello di business e il suo brand. Si tratta solo di una strategia di marketing >>. Queste le parole di un portavoce del DoJ. E ancora: << Apple deve adempiere alle responsabilità civiche di base. Per questioni di marketing, l'azienda non può preferire la tutela dalla privacy rispetto ai mandati di un tribunale. Questo ordine non apre una porta su ogni iPhone come sostiene Apple, e non consente agli hacker di accedere agli iPhone. Non si sta chiedendo ad Apple di decifrare gli iPhone di tutti gli utenti, visto che questa richiesta non dà al governo la possibilità di accedere ai dati presenti su un dispositivo senza il mandato di una corte >>[84].

La corte diede ad Apple altri tre giorni (rispetto al 26 febbraio) per rispondere a questa richiesta. Per opporsi alla richiesta dei giudici Apple presentò a sua volta in tribunale una mozione che metteva in evidenza i temi già affrontati da Tim Cook prima nella lettera e poi nell'intervista: << Non si tratta di un caso isolato di un iPhone. Piuttosto, questo è un caso sul Dipartimento di Giustizia (DOJ) e sull'Fbi che stanno cercando di avere, attraverso i tribunali, un potere pericoloso che il Congresso e il popolo americano hanno finora negato: la possibilità di obbligare aziende come Apple a mettere a rischio la sicurezza e la privacy di centinaia di milioni di individui in tutto il mondo >>[85]. Infatti, a tal proposito, si fa riferimento al 2015 anno in cui il Congresso non approvò una serie di aggiornamenti al *Communications Assistance for Law Enforcement Act* (CALEA), normativa che regola, tra l'altro, i rapporti tra stati federali e aziende di telecomunicazione. Di conseguenza non emendando la legge, il Congresso e il Governo, non hanno riconosciuto all' Fbi i poteri aggiuntivi che adesso essa cerca di ottenere tramite i tribunali. Da ciò si evince la necessità, per la Apple, di coinvolgere il potere

[83] Mozione ufficiale, Department of Justice vs Apple.

[84] P. Carr, portavoce del *Department Of Justice.*

[85] Mozione ufficiale di Apple vs Fbi.

legislativo del Congresso per affrontare il tema privacy e non le aule dei tribunali[86].

La vicenda sarebbe arrivata alla Corte Suprema, se l'Fbi non avesse, ad un certo punto, dichiarato di essere riuscita a sbloccare l'iPhone. - Secondo fonti ufficiose sarebbero stati gli *hacker* di un'azienda di sicurezza israeliana (la Celebrite) ad operare in tal senso - . L'Fbi è quindi riuscita a superare il blocco del cellulare dell'attentatore di San Bernardino senza l'aiuto della Apple. Questa circostanza ha consentito al Dipartimento della Giustizia americano di non procedere con una azione legale nei confronti della Apple per avere accesso alle informazioni contenute nel cellulare, considerate indispensabili per l'inchiesta. Secondo Esha Bhandari: << Non e' detto che la battaglia sia finita, il governo potrebbe rifiutare di condividere le scoperte con la Apple, decidendo che l'informazione è top secret >>[87]. Apple tramite i suoi legali aveva dichiarato di non conoscere gli strumenti che l'Fbi intendeva usare per sbloccare l'iPhone e di non sapere quale soluzione avesse trovato il governo. D'altra parte, se le indagini fossero proseguite su questa strada, auspicava una condivisione delle informazioni sulle criticità dell'iPhone[88]. Il fatto che Apple abbia deciso di non citare l'Fbi e che ques'utlimo non abbia più alcuna pretesa nel caso San Bernardino fa pensare che la questione sia definitivamente chiusa, almeno per ora.

Par. 2: Analisi critica della vicenda

Considerate le numerose manifestazioni pubbliche presso gli *Apple Store* statunitensi che seguirono a tali fatti, si stava sostanzialmente rischiando di allontanare i cittadini dalla convinzione di poter dialogare con le istituzioni in materia di privacy, e di avviarsi verso un mondo in cui i diritti sono garantiti dai mercati e non dai governi. Infatti al di là dell'interesse alla protezione della privacy, la posizione di Apple nella vicenda fa si che essa si presenti al mondo come garante ultimo del diritto alla privacy degli utenti che usufruiscono dei loro

[86] *Apple ha fatto ricorso in tribunale contro l'Fbi,* www.ilpost.it, febbraio 2016.

[87] E. Bhandari, avvocato della American Civil Liberties Union (Aclu), New York Times, marzo 2016.

[88] F. Rampini, *L'Fbi sblocca l'iPhone di San Bernardino senza l'aiuto di Apple,* www.repubblica.it, 29 marzo 2016.

dispositivi, proponendo quindi l'immagine di un governo non attento ai diritti fondamentali e pronto a violarli almeno in nome della sicurezza interna e internazionale. Le aziende private diventano portatori delle libertà fondamentali dei cittadini contro gli stati e i governi. È evidente che vi sono almeno due ragioni per le quali i colossi di mercato non dovrebbero assumere il ruolo di difensori e garanti delle libertà fondamentali dei cittadini: in primo luogo le società di capitali assumono posizioni che variano a seconda delle congiunture di mercato e come tali molto volubili. Di conseguenza se i diritti e le libertà fondamentali restassero affidati alla volontà o meno di queste società di difenderli, la democrazia, sulla quale si basano gli stessi, a fatica guadagnata, risulterebbe fragile. La seconda ragione anche più importante della precedente è che la Apple si è opposta ad un governo che ha sostenuto l'economia del suo business e ha potuto farlo contando proprio sulla forza economica raggiunta nel cyberspazio; se fosse stata una società più piccola avrebbe dovuto sottostare all'ordine della autorità senza potere di replica. Queste considerazioni dimostrano come il diritto alla privacy, così come i diritti e le libertà fondamentali in genere, sarebbero estremamente fragili se la loro tutela fosse garantita solo da alcuni colossi dell'economia digitale, e soprattutto se la loro tutela diventasse terreno di competizione sui mercati: i concorrenti più piccoli non avrebbero infatti nessuna possibilità contro i giganti dell'economia digitale[89]. << L'Fbi sta creando un mondo in cui i cittadini devono affidarsi ad Apple per difendere i loro diritti >>, questo è il primo pensiero pubblicato da Edward Snowden, il *whistleblower* ("informatore") americano, il giorno successivo alla pubblicazione della lettera di Tim Cook[90]. Per questo motivo consentire alle grandi aziende di esercitare un ruolo così pregnante nella società contemporanea è uno sbaglio di cui sono responsabili i governi e i parlamenti se ritardano ad adeguare le normative ai nuovi tempi[91]. D'altra parte bisogna considerare, come evidenziato da Zygmunt Bauman a proposito della globalizzazione, che la grande mole di dati che aumenta ogni volta che si utilizzano i nuovi strumenti tecnologici, per esempio carte di credito, fa si che il cittadino, fornendo i dati da immagazzinare, sia il primo e volontario fattore che

[89] G.Scorza, *Un errore trasformare i giganti del web in eroi e martiri della libertà,* L'Espresso, 2 marzo 2016.

[90] R.Luna, *La benedizione di Edward Snowden,* in www.laRepubblica.it, 20 febbraio 2016.

[91] Ibidem.

facilita la sua sorveglianza. Secondo l'autore, avendo lo stato nazione quasi come unica prerogativa, quella di mantenere l'ordine garantendo ad alcuni una vita sicura ed ordinata e utilizzando per questo scopo sugli altri la forza della legge, la banca dati, generata dal mercato stesso e costituita dalla rete mondiale dell'iPhone di Apple è quasi un sogno che si avvera per lo stato impegnato, com'è, nella sorveglianza dei cittadini[92]. E' singolare che le trattative su un diritto fondamentale, quale quello della privacy, si siano svolte tra un'autorità nazionale e un'azienda privata, ponendo in secondo piano di fatto coloro che dovrebbero essere i beneficiari del diritto messo in pericolo: i cittadini. Queste dinamiche fanno emergere probabilmente il fatto che si voleva ottenere un risultato senza un dibattito politico concreto sull'argomento. Inoltre considerando quanto il diritto alla privacy sarà sottoposto ad attacchi vista la mole di dati e di informazioni che ormai circolano in rete, diventa urgente prevenire errori anche più importanti. Bisogna capire quali dati stiamo producendo, quando e perché, chi li sta utilizzando per trarvi guadagno. Per farlo bisognerà sensibilizzare i cittadini e avvicinarli alle istituzioni chiamate a legiferare sulla questione. In questo modo si potrà forse evitare sia la sorveglianza che l'Fbi sta cercando di imporre sotto forma di tutela della sicurezza nazionale, sia la sorveglianza commerciale, attuata per trarre guadagno grazie allo smercio dei dati dei cittadini. Lo stesso Antonello Soro, Presidente del Garante per la protezione dei dati personali italiana è intervenuto chiedendosi se << […] Rendere i nostri telefoni sicuri rispetto ad eccessi abusivi, implica necessariamente - come farebbe intendere Apple - renderli inaccessibili alla giustizia? Si sta davvero chiedendo - come sostiene Tim Cook - agli stessi ingegneri che hanno progettato queste straordinarie casseforti di scassinarle? O si sta, chiedendo agli ingegneri di aprirne una, per accertare ragioni e responsabilità di una strage per prevenirne altre?[…] Quando si tratta di modulare il rapporto tra libertà e sicurezza non esistono soluzioni facili. Mai come su questo terreno, in cui devono comporsi libertà e sicurezza, diritto e tecnologia, privacy e prevenzione, è necessario rigore nelle scelte e attenzione a tutti i valori in gioco. Perché nessuno di essi può essere ritenuto mai recessivo o, peggio, ostativo agli altri; come spesso invece si sente dire a proposito della privacy. Che

[92] Z. Bauman, *Dentro la globalizzazione. Le conseguenze sulle persone,* Bari, 2002, p.152.

sarebbe bene riconoscere come presupposto di libertà e democrazia sempre, non soltanto quando favorisce il profitto individuale >>[93]. Le questioni poste dal Garante per la privacy sono questioni fondamentali per capire il dibattito in corso senza assumere posizioni a favore di una parte piuttosto che a favore dell'altra, basandosi solo su semplificazioni mediatiche derivanti da un insufficiente approfondimento della questione o da una volontà di esasperare un confronto già portato al limite. E' sintomatico che il presidente di un *authority* che ha come obiettivo quello di preservare la privacy dei cittadini, in questo caso non si ponga dalla parte di Apple, ma piuttosto inviti alla calma, alla ponderazione e all'approfondimento. L'obiettivo quindi del Garante è quello di eliminare l'idea ormai radicalizzata che non possa esservi in futuro un mondo in cui privacy e sicurezza nazionale e internazionale possano convivere senza che la ricerca di una comporti l'annullamento dell'altra.

Par. 3: Riflessioni conclusive

Abbiamo cercato di ripercorrere la vicenda passo dopo passo per cercare di capire meglio quello che da quasi tutti i media è stato definito " il grande rifiuto di Apple al giudice californiano". Abbiamo cercato di evidenziare le ragioni tanto di chi ha sostenuto la società di Cupertino, tanto di chi invece ha contestato alla società di mettersi dalla parte dei terroristi e di volere impedire il corso della giustizia. A questo punto se riflettiamo sul fatto che proprio un'azienda come la Apple, sostenuta e cresciuta grazie alle politiche commerciali statunitensi si è rifiutata di sbloccare quell'unico cellulare, ci rendiamo conto che il rifiuto non può essere ricondotto né ad una mera questione di marketing, né ad un mero confronto tra parti opposte, piuttosto può forse ricollegarsi a quella massiccia e indiscriminata sorveglianza di massa attuata dal governo americano e venuta alla luce con lo scandalo del Datagate[94]. Infatti, secondo le rivelazioni di Edward Snowden, la NSA sembra aver spiato chiunque per finalità anche diverse dalla lotta al

[93] Intervento di A. Soro, Presidente del Garante per la protezione dei dati personali, Huffington Post, 20 febbraio 2016.

[94] M. Pratellesi, *Privacy e sicurezza: la sfida Apple-Fbi non è solo questione di leggi,* L'Espresso, 21 Febbraio 2016.

terrorismo, al di là dei propri confini nazionali e in violazione di tutti i trattati internazionali. Inoltre bisogna considerare che qualora la Apple avesse sbloccato il cellulare avrebbe di fatto creato un precedente per richieste analoghe da parte della Francia, visto le stragi terroristiche del 2015, o comunque di qualunque altro governo che in futuro lo avesse richiesto, per esempio anche per il governo egiziano di Al- Sisi se le richiedesse di sbloccare il cellulare di Giulio Regeni[95]. Piuttosto forse la Apple avrebbe potuto proporre una soluzione per facilitare l'Fbi nell'accesso ai dati presenti nel telefono di Farook, avrebbe cioè dovuto instaurare una collaborazione per cercare di contemperare i due interessi. Non bisogna dimenticare però che, nel caso di specie, vi era un'ordinanza del giudice riguardante quello specifico caso, vale a dire l'accesso ai dati di un singolo iPhone appartenuto ad un presunto terrorista, e in qualsiasi democrazia gli ordini dei giudici devono essere rispettati o quantomeno impugnati, sicuramente non "rifiutati". In sede di impugnazione, e solo in questa, si sarebbe forse potuto trovare un'equilibrio tra il diritto alla privacy del singolo e la sua violazione in nome della sicurezza nazionale. Il punto è che tale equilibrio non deve essere stabilito né da Apple, né da altre aziende private, né dai legislatori nazionali o dai singoli giudici quanto piuttosto dall'intera comunità internazionale attraverso un concreto dibattito politico. Infatti bisogna considerare che il cyberspazio è quella vita parallela, sebbene virtuale, fatta di consultazione di servizi online, scambio di messaggi, socializzazione a distanza e archiviazione di dati personali. Gli utenti, all'interno di esso, allettati da offerte di ogni tipo si lasciano trasportare senza considerare i rischi e un certo tipo di aziende private non perde l'occasione di sfruttare l'opportunità: i servizi gratuiti offerti in cambio di copia dei loro contratti. Nel cyberspazio molti si muovono convinti di godere dell'anonimato assoluto, da qui nasce una forte aspettativa di tutela della privacy che contrasta però, con la circostanza non considerata dai più, che non ci sono confini ben definiti: se chiudo il computer lascio aperti varchi attraverso cui si può spiare la mia vita, rubare l'identità digitale e quant'altro. Non essendoci confini spaziali poi, il luogo fisico in cui è possibile intercettare le comunicazioni, può essere così lontano da far parte addirittura di un'altra giurisdizione: qui sorgono i problemi

[95] Ibidem.

sia per l'utente (come ottenere la tutela del segreto delle comunicazioni), sia per gli investigatori (come ricevere assistenza per l'intercettazione e legittimità dell'eventuale utilizzo, come prova, del materiale intercettato). Per questi motivi il cyberspazio è diventato terreno fertile per chi intende compiere reati visto che vi sono infrastrutture di servizi e contenuti su internet posti fuori dalla nostra giurisdizione che diventano zone franche per vari tipi di attività illecite. E' quindi evidente la necessità di trovare una soluzione a livello internazionale per prevenire tutto ciò garantendo nello stesso tempo le libertà individuali. Per presidiare il cyberspazio viene attuata con diverse metodologie la sorveglianza elettronica, che tra i vari metodi prevede anche la mera osservazione del traffico del cyberspazio. Quest'ultima può diventare uno strumento molto importante in grado di fornire un'allerta precoce in caso di pericolo imminente, ad esempio nel caso di un *cyberstorm* che miri ad attaccare le infrastrutture critiche del paese. Tuttavia da una parte, gli operatori che gestiscono le reti di comunicazione sono molto restii a farsi strumento di tale osservazione per il timore di censure dell'autorità giudiziaria e/o del Garante per la protezione dei dati personali, dall'altra l'autorità giudiziaria teme eccezioni di proporzionalità in quanto l'attività svolta potrebbe essere scambiata per sorveglianza indiscriminata di massa. Detto ciò la sicurezza dei cittadini e delle infrastrutture nel cyberspazio richiede tanto la consapevolezza dei rischi da parte degli utenti quanto la loro fiducia sia nei servizi di comunicazione offerti dagli operatori che si sono impegnati a rispettare la privacy, sia nelle istituzioni governative che sempre di più stanno comprendendo che il cyberspazio è una realtà parallela dove servono garanzie per i cittadini e strumenti efficaci per la sicurezza nazionale e per la giustizia. Tutto questo riguarda l'intera Comunità Internazionale perché le comunicazioni, così come le minacce, sono globali, per cui non possono che essere globali anche gli strumenti di contrasto.

Conclusioni

L'obbiettivo che si è cercato di raggiungere in questa trattazione è trovare un equilibrio stabile tra due esigenze apparentemente in contrasto ma in realtà sinergiche: il diritto alla privacy e la sicurezza nazionale. Attraverso l'analisi dei due concetti così come si sono evoluti nel tempo, attraverso l'individuazione delle fonti su cui tali diritti si basano, si è preso spunto dalla contesa tra Apple ed Fbi per rilevare quanto sia attuale e in parte ancora aperto il dibattito su tale questione. Innanzitutto è emerso che la ricerca di questo equilibrio non può essere affidata né ad Apple né a nessun altro soggetto privato. Non è un'azienda privata, sebbene di dimensioni colossali, che deve assurgere a garante della privacy globale, né tantomeno può imporre la sua personale idea di equilibrio tra privacy e sicurezza. Non può infatti una società democratica, affidare la difesa dei diritti fondamentali come quello della privacy, a scelte di singoli soggetti di mercato. Si è cercato di spiegare sufficientemente le ragioni di ciò nella trattazione. La conclusione della vicenda Apple vs Fbi ha evidenziato, a mio avviso, come la lotta al terrorismo si debba fare con la cooperazione e lo scambio di informazioni tra le agenzie della sicurezza e le polizie, molto più che con la sorveglianza di massa. L'apertura standardizzata degli strumenti di comunicazione che l'Fbi chiedeva alla Apple appare infatti meno legittima della soluzione di vagliare caso per caso. Si è riportato come lo stesso Garante Italiano, Antonello Soro, è intervenuto sostenendo la necessità di comporre i due interessi perché nessuno di essi deve essere ritenuto ostativo per l'altro[96]. Per cui il Presidente di un *authority* che ha come obbiettivo quello di preservare la privacy dei cittadini, invita alla calma e alla ponderazione piuttosto che schierarsi dalla parte di Apple, a dimostrazione che vi può essere in futuro un mondo in cui privacy e sicurezza nazionale ed internazionale, possono convivere senza che la ricerca di una comporti l'annullamento dell'altra. Si è cercato di individuare questo equilibrio nel senso di responsabilità che caratterizza i diritti di libertà tra i quali rientrano appunto, tanto il diritto alla privacy quanto il diritto dei cittadini alla sicurezza nazionale. Senso di responsabilità che si traduce per i cittadini nell'essere consapevoli dei rischi

[96] Rif. interno, pg. 45

derivanti dalla navigazione nel *cyberspazio,* e nella fiducia degli stessi, sia nei servizi di comunicazione offerti dagli operatori che si sono impegnati a rispettare la privacy sia nelle istituzioni governative che devono approntare garanzie e strumenti efficaci per la sicurezza nazionale e per la giustizia. È risultato evidente che il *cyberspazio* è terreno fertile per chi intende compiere attività illecite ed è emersa la necessità di trovare una soluzione a livello internazionale per prevenire ciò garantendo nello stesso tempo le libertà individuali. Come si è avuto modo di evidenziare, la tutela del diritto alla privacy a livello europeo sembra oggi maggiormente garantita dalla recente approvazione del Regolamento Europeo sulla protezione dei dati, che almeno garantirà una uniformità di disciplina in materia, negli stati membri. Con la recente approvazione poi, del *Privacy Shield,* accordo per la privacy tra Unione Europea e USA, sembrano rafforzate le norme sulla protezione dei dati trasferiti dai cittadini europei nel territorio americano. Emerge quindi a mio avviso la necessità di un equilibrio tra queste due esigenze a livello internazionale, che sia frutto soprattutto di un dibattito politico concreto.

La crisi internazionale scaturita dai sempre più frequenti attacchi terroristici ha posto in evidenza la necessità di garantire la sicurezza nazionale. Questa ha imposto decisioni serie che dovranno però essere assunte con la cautela data dalla consapevolezza che ogni libertà che subisce un limite diventa, in una società democratica, e superata l'emergenza, una libertà da riconquistare.

Bibliografia

- BASSU C., *La legislazione antiterrorismo e la limitazione della libertà personale in Canada e negli Stati Uniti,* in *Diritti fondamentali e sicurezza dopo l'11 settembre 2001,* Napoli, 2006.
- BAUMAN Z., *Dentro la globalizzazione. Le conseguenze sulle persone,* Bari, 2002.
- CARR N., *Il lato oscuro della Rete: libertà, sicurezza, privacy,* Milano, 2008.
- DI MARTINO A., *Protezione dati personali,* in *I diritti fondamentali e le Corti in Europa, (*a cura di) PANUNZIO P., 2005.
- FINOCCHIARO G., *Privacy e protezione dei dati personali, disciplina e strumenti operativi,* Bologna, 2012.
- GIACOBBE G., *Il diritto alla riservatezza nella prospettiva degli strumenti di tutela,* Napoli, 1983.
- GORI U., LISI S., *Information warfare 2015. Manovre cybernetiche:impatto sulla sicurezza nazionale,* Milano, 2015.
- GRANIERI M.,, *La tutela della privacy,* in *Manuale di commercio elettronico, (a cura di) E.M. TRIPODI, F. SANTORO, S. MISSINEO,* Milano, 2000.
- GREENWALD G., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State,* New York 2014.
- LÈVY. P., *L'intelligenza collettiva. Per un antropologia del cyberspazio,* Milano, 2002.
- MENSI M., *Il caso "Datagate". Alcune riflessioni, in Diritto, economia e tecnologia della privacy,* 1, Milano, 2013.
- MENSI M., FALLETTA P., *Il diritto del web, casi e materiali,* Padova, 2015.
- NINO M., *Terrorismo internazionale, privacy e protezione dei dati personali,* Napoli, 2012.
- 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,* Napoli, 2013.
- PAGALLO U., *La tutela della privacy negli Stati Uniti e in Europa,* Milano, 2014.

- PERRI P., *Protezione dei dati e nuove tecnologie, aspetti nazionali, europei e statunitensi,* Milano, 2007.
- POLDELMENGO L., *Nel posto sbagliato,* Roma, 2014.
- RAPETTO U., *Le sfide alla sicurezza nell'era digitale,* Roma, 2013.
- RESCIGNO P., *Manuale di diritto privato italiano,* Napoli, 1992.
- RODOTÀ, S., *Intorno alla privacy. Ipotesi e prospettive,* in *Studi in memoria di Franco Piga,* V.2, Milano, 1992.
- RODOTÀ, S., *Privacy*, in *Sinistra senza sinistra*, Milano, 2008.
- RODOTÀ, S., *Il Diritto di avere Diritti*, Bari, 2012.
- SARTRE J.P., *L'essere e il nulla,* Milano, 1943.
- VALENSISE M., *In difesa della privacy, in Media 2.0 Potere e libertà, Aspenia,* Milano, n. 54/2011.
- VAN HOBOKEN J.V.J., RUBINSTEIN I.S., *Privacy and Security in the Cloud: some realism about technical solutions to transnational surveillance in the post-Snowden era, Maine Low Review,* Vol. 66, n.2, New York, 2014.
- WARREN S., BRANDEIS L., *The right to privacy,* vol.IV, in *Harvard law review,* Harvard, 1980.

Sitografia

- www.utetgiuridica.it
- www.gnosis.aisi.gov.it
- www.altrodiritto.unifi.it
- www.foroitaliano.it
- www.temiromana.it
- www.camera.it
- www.senato.it
- www.gazzettaufficiale.it
- www.consilium.europa.eu
- www.eur-lex.europa.eu
- www.pharmasoft-fea.com
- www.assodpo.it
- www.uscode.house.gov

- www.curia.europa.eu
- www.ec.europa.eu

Abstract

With this work we intend to verify how much freedom you are willing to sacrifice for our safety since terrorism on the web, one of the worst nightmares of recent times, has prompted Governments to increasingly pervasive surveillance of privacy at the expense of privacy rights of every citizen.

Analyzing the recent contest between Apple and Fbi which has focused attention on the issue, we tried to focus our attention on the two concepts privacy and national security; European, Italian and American sources found that out of this law and what is meant by "national security"; the affair has pithily between Apple and Fbi and various dissertations on the issue. We will after drawn conclusions on the dichotomy between privacy and national security, by supporting the apparent contradiction, and highlighting so a possible reconciliation between the two based on the one hand, on the "sense of responsibility", inherent in every right to freedom, on the other hand the hope that this dichotomy could lead to a democratic State, evolution, evolution related to the changed conditions of life after Sept. 11, and due to the fact that the democratic State, seriously threatened, are trying to defend themselves without putting into play its achievements and its values. It is also recognised that the desirable balance between privacy and national security, must take place within the international community as a whole, since they are global communications and global threats and must be also the instruments.

First, we must consider that the right to privacy was drafted by the US doctrine at the end of the 800 and has gradually modelled in relation to the evolution of customs and to the rapid technological progress. Born as "right to be alone" became "one theme that pervades the entire constitutional structure" not only in the USA but in all democratic countries. In the ' 70 legally the right to privacy, was played as an instrument for protecting a dual need of individuals: firstly, the protection of privacy by the curiosity of others; on the other hand, the "control" of the information flow out of the private realm. However the rapid technological advances of the Internet and the media, are undermining the various regulatory

instruments people protection of personal data. Understood in this way, the right to privacy did not raise particular problems of protection because, by referring to the fundamental rights of the person, fall under articles 13, 14, 15 and dictation 21 of the Constitution, within the broader recognition to the inviolable rights of man in article 2. Already in the mid-1980s, the notion of confidentiality no longer coincides with the concepts of privacy of domestic intimacy, of decorum or reputation, but covers all the events related to the private life, personal and family without social relevance. In fact, according to the ruling of the Court of Cassation 1975 # 2199, the right to privacy is identified with the interest to steal others ' private affairs knowledge, occurring both inside and outside the household and not having domicile for third parties a socially important interest. Also with the ruling # 38 of 1973 the Constitutional Court has the case under the inviolable rights of man. Over time, the confidentiality requirements change significantly since the individual performs actions and choices in cyberspace, virtual reality that connects computers around the world into a single network and allowing those who use to interact, leaving a "track" that could allow the reconstruction of the identikit of a person. In such a situation, the protection of the home is totally unfit to ensure individual privacy. It is stated then, the need for the organized collection of personal information disseminated in the environment does not happen without the knowledge of the person concerned and does not lend itself to use damaging to the rights and dignity of the human person. It is in the light of what emerges the concept of "privacy" which law including the "power of control over the movement of personal information" in addition to the right to be "left alone", intended as a requirement of protection of the individual from interference in his life for commercial purposes. Privacy becomes, by instrument of isolation from others, ("right to be left alone") in a communication tool, in that, while guaranteeing the protection of anonymity, will allow for example to denounce abuses, to avoid discrimination and whatnot. Privacy becomes a right to control the use that the others make of information pertaining to an individual. In the planetary circulation system of information privacy is the fulcrum around which revolves the correct usage of the network and its potential development; efficient protection of privacy can be guaranteed recognising the existence of a right to

privacy that has that is rooted in international treaties and intensifying regulatory interventions in the field of protection of personal data.

We must also point out that the protection of personal data applies to both consumer data processing in order to study its behaviour for marketing needs, both the processing and storage of data for purposes of prevention, repression of crimes and/or national security. The fast technological progress, making it easier for surveillance and entry into the privacy of citizens, decreased more and more the area qualifies as a policy. If as regards the first aspect of privacy "guilty" of the breach of law are the same users who refuse to read or underestimate the terms just to get in return for their services, as far as the second aspect we have witnessed over the last fifteen years in positions ranging from periods of large claims of the "right to privacy in the world" and "disaster terrorism" periods , where the risk of calling into question the democratic guarantees conquered, was very high. The two needs privacy and national security appear to some irreconcilable, for others accord on the grounds that national security is one of many expressions of the right to freedom. For this reason, national security and the right to privacy can find balance in reference to the sense of responsibility that the concept of freedom is closely connected. National security and the privacy rights reflect the phenomena occurring in the world from September 11, 2001 until today, namely the terrorist acts and the ever-faster technological progress. The latter has allowed us to easily store and low cost information relating to an individual terrorist acts require more and more a struggle to ensure preventive and repressive national security. Prevention and suppression which results in more control, made possible by the new technologies, now is part of individual’s lives. The relationship between privacy and national security before September 11 and was characterized by considering important the question of privacy, fragile as it was, due to the ever increasing technology. After 11 September the consideration moves on national security as it imposes the need to give appropriate response to terrorist threats but, for this loss to the fundamental principles of a democratic State. A little over a month after the attack in the United States was passed the Usa Patriot Act, a federal law aimed at fighting terrorism, by strengthening security measures. This law by insisting on the sphere of personal freedom and interfered deeply in the lives of Americans (removal of impronterebbe libraries, monitoring

of telephone communications and computer systems etc.). The consequence of this new regulatory framework in the United States is looking at the impact that the emergence of terrorism exerts on the hierarchical ladder of priorities and shared values under the rule of law: the public security becomes fundamental right and sets itself as the source of the tendency to compress the guarantees of individual rights. The anti-terrorism legislation complements the ordinary regulatory system not as instrumental to the passing of a State of exception, but has an impact on domestic law and integrate permanently with sorting and undermining the fundamental guarantees that forms the basis of modern democracies and that should be indisputable and intangible. In Italy, after 11 September, having also experienced the terrorism in 70's, there are no special modifications to introduce instruments or special restrictions to personal freedoms. Rather has felt the need to feed the public's confidence in the institutions, to stimulate collaborative strategies been-Consultatio citizen to constant vigilance or they will be attacked democratic principles. Your privacy remains a characteristic of liberal and democratic State, but also an achievement that can be prone to shrinkage, due to adverse economic trends that, without diminishing the powers of the individual, will defend the community.

Regarding the sources related to the affirmation of the right to privacy as a fundamental right, have contributed essential international human rights conventions that have recognized "the right to respect for private life, home and correspondence", that the public authority cannot interfere with the exercise of this right except in the cases provided for by law and provided that it is to safeguard national security [article 8 first and second paragraphs]. From these documents has emerged as the "right to privacy consists essentially in living their lives with as little interference necessary", expanding progressively the meaning to be given to the concept of private life and correspondence, are the foundations for the recognition of the right to conscious control on the circulation of personal information. The right to privacy was born in Italy at the level of case-law, first with the judgment of the Court of Cassation # 44/87/1956, later with the judgment of the Court of Cassation # 990/1963. The latter affirms the existence of a "right

erga omnes to freedom of self-determination in the performance of the personality of man as an individual." From this legal construction, based on art. 2 of the Constitution, comes the prohibition of disclosure of information about the private life without the express consent or even implied. With subsequent rulings, the Supreme Court coming to fully recognise the existence, in the Italian legal system, of a right to privacy even though it will extend to all, since the judgments concerned until then only celebrities, only with the law 675/1956 and by Legislative Decree n. 196/2003 (privacy code). The new law has a very extensive because wide is the definition of personal information. The latter is to be understood as any information relating to an individual, and is placed in the context of personal rights and therefore, unavailable, imprescriptible. The right to protection of personal data is not to be construed as negative freedom not to suffer interference in private life (right to privacy) but positive freedom to exercise control on the circulation of information about us. In this way the legislature has formalized, in legal terms, that data and information have an economic value, since it is introduced the protection of information as such, regardless of the contents. For more on the personal becomes element that helps to define the identity of a subject, that the law focuses on giving him control over your data. Directive 95/46/EC "mother" was repealed on April 14, 2016 with the approval of a new European regulation in this regard. The need to issue a regulation stems from the continuous evolution of the same concepts of privacy and protection of personal data and its protection from change, given the diffusion of technological progress. Also as far as the matrix was the same, each country had declined and applied in their own way the Directive 95/46. The new regulation will give the most common provisions to ensure citizens instead, and easier to apply those protections for construction companies in the industry. Among the most important in the regulation include: the concept of privacy by design, meaning that the protection of the rights of the persons concerned with regard to the processing of personal data, should be incorporated from the early design phase to the final elimination; the concept of privacy by default which means that privacy settings must comply with the General principles of data protection, such as data minimisation and the limitation of the purposes for which they were collected. Whatever doubts or critical points highlighted within the regulation, Member

States will have 24 months to adapt to the new regulatory framework. U.s. ordering sources regarding privacy are found in the first and fourth amendment to the Constitution which respectively, privacy is guaranteed in the name of the principles of freedom of expression and Association, and that this is the right to security of person, House, papers and effects against any intrusion of the State and Government. Quoting constitutional right of privacy is grounded in ordinary legislation, both in federal law, both in the legislation of individual States. The latter have ample discretionary. The Constitution of the United States in fact recognize an enclave in which prohibits Federal Government intervention in personal affairs of individuals, it is therefore the Federal States ensure greater sphere of privacy protection than the minimum provided for constitutionally. The reference in the US law is the Privacy Act, approved by Congress on December 31, 1974 amended in 1988 by the Computer Matching and Privacy Protection Act to ensure procedural uniformity in the data processing and the constitutional principle of due process. In 2008 Congress passed the Genetics Information Non-Discrimantion Act considered as "the first civil rights legislation enacted by Congress over the past 20 years. The growing global interdependence that has emerged between globalization, emergency legislation and new technological tools, he then ported the US and the European Union, to seek agreements to protect data transfer and Exchange. Remember the PNR framework agreement which should guarantee high standards of data protection at the time of the Exchange, between judicial and police authorities in order to combat crimes and terrorism. After the scandal of Datagate, born by the revelations of Edward Snowden mass controls operated by the NSA on communications of European users, was approved on 24 February 2016 from the USA the law on judicial (Judical Redress Act), which lays down the right for all EU citizens to sue in u.s. courts to enforce their data protection rights already, right enjoyed by u.s. citizens in Europe. On July 12, 2016 came into force on Privacy Shield, the "United States-EU privacy Shield": is a political agreement that safeguards the fundamental rights of any person in the European Union whose personal data are transferred to the United States. In this agreement were expected obligations for companies working in the field in order to ensure compliance with the rules which has been adhered to. It is officially guaranteed that public authorities access to the

data is limited, guaranteed and monitored by excluding indiscriminate mass surveillance activities concerning personal information transferred to the USA under the shield. Any bulk data collection will only be possible under certain circumstances and still more targeted and focused as possible. Anyone who wronged his rights, as part of the shield will have easy access to redress mechanisms and inexpensive. From all this is that while the American model of privacy is focused more on the economic value and negotiable personal data, which may then be transferred to users without any restrictions, the European model of privacy moves instead from the centrality of the person and the right to it control of the processing of personal data is recognized as a fundamental right. Also as the American system of privacy comes basically sectoral type, so it lacks a general regulatory framework and is then fragmented in the provisions of the fifty Federal States, the European system of privacy, however, is presented as a general vocation that is there is a general regulatory framework, Community law, which directs the material.

Finally, having demonstrated that the protection of privacy is a fundamental right and a priority guarantee offered to citizens of democratic societies, what is asked in this complex, is if the fight against terrorism may pose, and to what extent, questioning such protection, placing behind this reflection the recent terrorist event of the massacre of San Bernardino of December 2, 2015 in California that he saw as opposed the two interests : privacy and national security. During the investigation, the Fbi found an iPhone 5 c belonged to one of the two terrorists died in the attack. To get the data from the backup to iCloud the Fbi asked the County engineers reset the password of iCloud service remotely, IE from another device. This procedure stopped the next most recent file backup to iCloud, because when you change your password from another device you must unlock the iPhone by entering code decided by the person using it. Not having known the Code adopted by terrorist and since the iOS system foresees the auto deletion of data after 10 attempts to unlock, the Fbi could not proceed to add all possible passwords until the correct one, as it usually does. Whereby by a court order Apple was asked to find an ad hoc solution for secondary investigators access to

the latest data from the iPhone of the terrorist. Apple basically opposed for reasons relating to the protection of privacy. It was a debate between those who supported the position of Apple and those who challenged the company to put itself on the side of terrorists and would impede the course of Justice.

In conclusion, by analyzing the story step by step it was concluded that the refusal of Apple to the courts cannot be traced back to a mere question of marketing talking to a simple comparison of opposite sides, but rather can be linked to the massive and indiscriminate mass surveillance carried out by the American Government coming forth with the scandal of datagate as well as to the fact of not wanting to create precedents for similar requests from other Governments. But it is true that, in the present case there was a court order, for more on one device belonged to a alleged terrorist, and in any democratic society, judges ' orders are to be respected or enforced. In an appeal would have been able to strike a balance between the right to privacy of the individual and its violation in the name of national security. The point is that this balance cannot be established either by private companies, no matter how great they are, nor by the national legislature or by individual judges, but rather by the entire international community, by then a concrete political debate. This is because being communications, as well as threats, global, even contrast tools they need to be.