federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

FOCUS TMT – 27 FEBBRAIO 2015

Il Quarto emendamento della Costituzione americana tra terrorismo internazionale e *datagate*: Security v. Privacy

di Luca Pietro Vanoni
Ricercatore di Diritto costituzionale
Università di Milano

Il Quarto emendamento della Costituzione americana tra terrorismo internazionale e *datagate*: Security v. Privacy*

di Luca Pietro Vanoni
Ricercatore di Diritto costituzionale
Università di Milano

Sommario: 1. Il Datagate e la Costituzione: Iron Man v. Capitain America. **2.** Il diritto privacy e le sfide del nuovo secolo: i termini del problema. **3.** Security vs. Privacy: le norme sulla sorveglianza elettronica dall'epoca del proibizionismo all'avvento del terrorismo internazionale. **4.** La Sezione 215 e il Bulk Metadata Surveillance Program: profili di costituzionalità. **5.** Il Bulk Metadata Surveillance Program di fronte ai giudici federali: «an almost-Orwelian tecnology» o «a legitimate tool to interdict terrorist threats»? **6.** Tra Security e Privacy. Conclusioni.

1. Il Datagate e la Costituzione: Iron Man v. Capitain America.

In un famoso fumetto di qualche anno fa, gli scrittori Mark Millard e Brian Bendis immaginavano che il Governo americano, spaventato dall'uso incontrollato dei loro superpoteri, avesse imposto a tutti gli eroi mascherati del paese di registrarsi presso le autorità rinunciando alla loro identità segreta. Di fronte a questa richiesta, il mondo dei supereroi si è diviso in due fazioni, la prima capitanata da Iron Man, fiero sostenitore delle ragioni del Governo e della necessità di sacrificare la propria riservatezza sull'altare della sicurezza della nazione, la seconda guidata da Captain America, strenuo difensore del sogno americano e del diritto alla segretezza della propria persona e identità.

L'epico duello tra i due supereroi immaginato da Millard e Bendis non fa che riproporre sulla carta lo scontro ideale e politico tra la necessità di difendere la nazione dagli attacchi del terrorismo internazionale e l'esigenza di tutelare la vita privata dei cittadini americani dal

* Articolo sottoposto a referaggio.

controllo invasivo dei servizi di intelligence in atto oggi negli Stati Uniti. In altri termini, il fumetto *Civil War* racconta bene il delicato intreccio tra security e privacy che, soprattutto a seguito degli attentati dell'11 settembre, condiziona la vita della democrazia americana e che può essere sintetizzato dalla domanda che Captain America rivolge ad Iron Man e al Governo americano nel corso di tutto il fumetto: fino a che punto è possibile comprimere i diritti dei cittadini per tutelare la sicurezza nazionale senza che ciò comprometta, definitivamente, quei valori di libertà e giustizia che l'America è nata per difendere?

Negli Stati Uniti la risposta a questo quesito non può essere data una volta per tutte, ma è invece il frutto di un costante e faticoso equilibrio che tiene conto delle circostanze concrete, dei fatti, delle sfide che il sistema costituzionale è chiamato a affrontare. Si capisce pertanto perché ultimamente il dibattito sul rapporto tra privacy e security sia stato rilanciato con forza dal c.d. *Datagate*, ovvero dalle rivelazioni con cui, a partire dal giugno 2013, l'ex consulente della National Security Agency (NSA) Eric Snowden ha cominciato a denunciare l'esistenza di programmi segreti di sorveglianza e di intercettazione delle comunicazioni telefoniche e digitali interne ed esterne alla nazione americana[1]. Nell'opinione pubblica internazionale particolare scalpore ha suscitato la predisposizione di programmi quali PRISM, o TEMPORA attraverso cui le agenzie di intelligence americane come l'NSA e l'FBI (ma anche la britannica GCHQ o la francese DGSE) hanno acquisito ed immagazzinato negli ultimi anni miliardi di informazioni digitali raccolte con la collaborazione delle principali aziende informatiche quali Apple, Google, Microsoft, e Facebook, o intercettate direttamente dai cavi sottomarini atlantici utilizzati per la trasmissione dei dati[2]. Ma a livello interno, altrettanto clamore ha suscitato la notizia delle autorizzazioni concesse al Governo americano dalle Corti speciali americane al fine di ottenere dalle principali compagni telefoniche i registri e i tabulati degli ultimi otto anni contenenti i c.d. metadati telefonici dei loro clienti.

Non appena pubblicata, la notizia ha sollevato molteplici proteste tra i cittadini, che si sono sentiti violati nella riservatezza delle loro comunicazioni; se infatti è vero che i metadati telefonici

[1] Il primo articolo sull'inchiesta *Datagate* è G. GREENWALD, *NSA collecting phone records of millions of Verizon customers daily*, Guardian, 5 giugno 2013, in http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[2] Il programma PRISM, in particolare, ha suscitato grosse polemiche in Europa. A riguardo cfr. (in lingua italiana) F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *Federalismi.it*, 26 giugno 2013; M. NINO, *Il caso* Datagate*: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privay*, in *Dir. Um. E Dir. Inter.*, 2013, p. 727 ss. Sulle implicazioni relative ai programmi di sorveglianza elettronica attuati dalla NSA all'estero, v. anche P. MARGULIES, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 Fordham L. Rev, 2014, p. 2137 ss.

non riguardano il contenuto delle telefonate, ma solo informazioni digitali legate al momento, alla durata e al luogo delle comunicazioni, è altrettanto vero che molti sono i fatti sensibili riguardanti la vita dei cittadini che possono essere ricavate dallo studio dei metadati[3]. E così, in America, le rivelazioni di Snowden hanno presto spinto cittadini singoli o associati a ricorrere presso i giudici federali e statali per far valere il loro diritto alla privacy e alla riservatezza sancito dal Quarto emendamento della Costituzione.

Non sempre, in realtà, la risposta dei giudici a tali pretese è stata univoca, perché i casi loro sottoposti toccano il delicatissimo equilibrio esistente tra il diritto alla privacy dei cittadini da un lato, e l'esigenza governativa di proteggere i confini nazionali dall'altro. Per questo le Corti americane hanno proposto interpretazioni della Costituzione tra loro radicalmente diverse, arrivando recentemente a dichiarare l'incostituzionalità del programma governativo di raccolta dei metadati telefonici nel distretto di Columbia (*Klayman v. Obama*) ma ammettendone la piena legittimità poche settimane più tardi in quello di New York (*ACLU v. Clapper*). Le differenti soluzioni a cui sono giunti i due giudici federali testimoniano la delicatezza del problema, e le difficoltà interpretative legate alla applicazione di una clausola costituzionale (il Quarto emendamento) il cui ambito è stato fortemente condizionato dall'avvento dell'era digitale: come vedremo, infatti, l'inadeguatezza della giurisprudenza in materia rende complicato definire precisamente l'ambito di applicazione del diritto alla privacy nei casi in esame, e non è impossibile che – anche in ragione delle opposte interpretazioni recentemente fornite dai giudici federali – la Corte suprema sarà chiamata presto a pronunciarsi. I giudici americani, pertanto, si sono trovati di fronte al quesito efficacemente sintetizzato nel fumetto di Millar e Bendis: fino a che punto è possibile per un ordinamento democratico sacrificare sull'altare della sicurezza nazionale quelle libertà che esso è nato per garantire e difendere?

2. Il diritto privacy e le sfide del nuovo secolo: i termini del problema.

Fin dai tempi della rivoluzione, la tutela della privacy ha rappresentato un tema fondamentale per i cittadini delle colonie americane, che detestavano l'arroganza con cui gli ufficiali inglesi perquisivano senza mandato le loro proprietà e controllavano la loro posta e le loro

[3] Come ricordato da F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, cit., p. 5 gli ordinamenti si sono trovati di fronte a «nodi e problemi di enorme rilevanza», che vanno «dalla facilità con la quale gli Stati fanno carta straccia dei valori democratici che essi proclamano alla difficolta di trovare punti di equilibrio chiari e conclamati tra sicurezza e diritti fondamentali».

comunicazioni[4]. Già prima dell'indipendenza, del resto, il diritto alla riservatezza personale era garantito in alcune colonie[5], e patrioti del calibro di Patrick Henry o Benjamin Franklin enfatizzarono pubblicamente – anche a fini propagandistici – la sua importanza come diritto fondamentale ed inalienabile dell'uomo[6].

Una volta sconfitti gli inglesi, questo diffuso sentimento di diffidenza per l'eccessivo controllo da parte dello Stato fu codificato nel Quarto emendamento della Costituzione, che ancora oggi sancisce il diritto dei cittadini «to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures»[7]. Liberatisi dell'oppressione dell'impero britannico, i Framers americani vollero, infatti, circoscrivere i limiti del Governo federale, ovvero di quel nuovo potere che – soprattutto al tempo della approvazione del Bill of Rights – era visto con sospetto dai singoli Stati. Dal punto di vista storico, pertanto, il Quarto emendamento «non scaturisce da

[4] Le origini del Quarto emendamento sono profondamente legate alle ragioni che condussero alla guerra d'indipendenza americana, perché sebbene il sistema della Common Law inglese riconoscesse una parziale protezione delle abitazioni e del domicilio dei cittadini (c.d. *castle doctine*), spesso tale pur minima tutela non era applicata nei territori delle colonie di fine diciottesimo secolo. Nella seconda metà del diciottesimo secolo, in particolare, i coloni inglesi, contrari alla eccessiva pressione fiscale imposta dal Re, cominciarono ad aggirare i controlli doganali sulla importazione/esportazione delle merci attraverso la predisposizione di efficaci reti di contrabbando. Proprio per combattere questo fenomeno, il Parlamento inglese approvò l'Exercise Act del 1754, attribuendo agli ufficiali inglesi (e in particolare a quelli doganali) ampi poteri di ispezione dei carichi e di sequestro dei beni. Gli americani considerarono particolarmente sgradevole questo atteggiamento imperialista della corona inglese, e provarono anche ad opporsi a tale legge ricorrendo senza fortuna presso le Corti inglesi eccependo il divieto di general warrants. La perseveranza del Governo britannico nell'adozione di tale misure liberticide giocò così un ruolo chiave nella rivoluzione americana. Sulle origini storiche del Quarto emendamento v. (tra gli altri) T.Y. DAVIES, *Recovering the Original Fourth Amendment* , in MICH. L. REV., 1999, p. 547 ss.; W. J. CUDDIHY, *The Fourth Amendment: Origins and Original Meaning*, Oxford, 2008.

[5] Vedi, ad esempio, la Costituzione del Massachusetts redatta da John Adams nel 1780, che ha per certi aspetti anticipato la formulazione del Quarto emendamento, sancendo espressamente il diritto di ogni individuo «to be secure from all the unreasonable search and seizure of his person, his house, his papers, and all his possessions». Cfr. T.K. CLANCY, *The Framers Intent: John Adams, His Era, and the Fourth Amendment*, IND. L. J., 2011, p. 979 ss.

[6] Ad esempio Patrik Henry, opponendosi agli inglesi, ricordava che «They may (…) go into your cellars and rooms, and search, rasack, and measure, everything you eat, drink, and wear. They ought to be restrained within proper bounds» (cfr. J. ELLIOT, *The Debate on Several Conventions on the Adoption of the Federal Constitution, 1974*, p. 448-449), mentre per Benjamin Franklin «They who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety» (cfr. Benjamin Franklin, *Pennsylvania Assembly: Reply to the Governor*, *FranklinPapers.Org*, http://franklinpapers.org/franklin/framedVolumes.jsp?vol=6&page=238a)

[7] Così il Quarto emendamento della Costituzione americana: «The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized».

precedenti coloniali, ma nasce per distaccarsene»[8], e testimonia il geloso attaccamento del popolo americano per la propria libertà, e la conseguente diffidenza verso il potere statale, da qualunque parte esso provenga. Esso nel definire i confini tracciati dalla Costituzione per proteggere i cittadini da ogni «unreasonable search and seizure» del Governo, costituisce uno dei pilasti attorno a cui si è poi sviluppato il sistema di Criminal Law and Procedures in America.

Al tempo della sua introduzione nel Bill of Rights, il diritto costituzionale alla privacy proteggeva i cittadini unicamente da violazioni fisiche della loro riservatezza da parte della pubblica autorità, tutelando dunque la loro casa e la loro corrispondenza da indebite ingerenze[9]. Oggi il suo significato all'interno del sistema costituzionale americano è profondamente cambiato per l'insorgere di almeno due fattori.

In primo luogo, lo sviluppo tecnologico ha inciso sull'interpretazione e sul ruolo di tale clausola nel sistema costituzionale americano, non solo perché, com'è ovvio, al tempo della approvazione del Bill of Rights i Framers non potevano immaginare le implicazioni e l'incidenza della rivoluzione elettronica e digitale sulla vita dei cittadini, ma anche perché tale rivoluzione ha cambiato il modo con cui ognuno di noi oggi immagina il proprio diritto «*to be secure* in their persons, houses, papers, and effects». Tale problematica, in realtà, non è neppure così recente, se è vero che già nel 1928 la Corte suprema americana si è trovata a dover ridiscutere il significato della clausola costituzionale rispetto alle intercettazioni telefoniche, ovvero ad una tecnologia la cui disciplina non è – almeno nominalmente – ricompresa nella definizione di «search and seizure» della Costituzione americana[10]. In alcuni casi le difficolta interpretative legate all'avvento di nuove tecnologie sono state superate da specifici interventi normativi che hanno regolato,

[8] L.W. LEVY, *Original Intent and the Framers' Constitution*, 1998, p. 224. Come ricordato da W. CUDDIHY - B. C. HARDY, *A Man's House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution*, 37 in WM. & MARY Q., 1980, p. 398, e riportato da Y. MACLIN, *When The Cure For The Fourth Amendment Is Worse Than The Disease*, in *Sou. Cal. L. Rev.*, 1994, p. 11 nota 45: «The adoption of the Fourth Amendment signaled that "old ways" of thinking should no longer be accepted. The Fourth Amendment represented an American extension of the English tradition that a man's house was his castle. Governmental interests in Great Britain and the colonies remained largely outside that tradition. Specific warrants were not the orthodox method by which English and colonial law restrained official powers of search. Indeed, no single dominant theme or restraint existed. The requirement that all search warrants be specific, the heart of the Fourth Amendment, accordingly enlarged the tradition's scope, for it controlled searches by the government to a degree never previously attempted. Although aged British precedents supported an undefined right against unreasonable searches, the particular mechanism by which the Fourth Amendment defined and enforced that right was neither ancient nor British».

[9] V. (da ultimo e per tutti) O.S. KERR, *The Curious History of the Fourth Amendments Search*, GWU Legal Studies Research Paper No. 2012-107, 2013, disponibile in SSRN http://ssrn.com/abstract=2154611.

[10] Si tratta del famoso caso *Olmstead v. United States*, 277 U.S. 438 (1928), su cui vedi *infra* § 4.

autorizzato, limitato il loro utilizzo a fini investigativi[11], estendendo per via legislativa la protezione garantita dal Quarto emendamento. Ma, nella sua natura, il problema è rimasto e rimane ancora oggi vivo nell'ordinamento costituzionale americano.

In secondo luogo, la lotta al terrorismo ha recentemente ampliato la portata e i limiti della protezione della privacy, perché l'avvento dell'era digitale non ha solo moltiplicato in modo esponenziale le tecniche di controllo dei governi sui dati sensibili dei propri cittadini, ma ha altresì fornito a tutti (e quindi anche ai terroristi) nuove modalità di comunicazione che necessitano di essere controllate preventivamente. Soprattutto a seguito degli attentati dell'11 settembre, il Governo americano ha così rafforzato i meccanismi di sorveglianza nazionale al fine di raccogliere, all'interno dei propri confini, il maggior numero di informazioni utili a prevenire la minaccia terroristica[12]. Per perseguire tale scopo, il Governo federale ha spesso utilizzato strumenti tipici del sistema penale quali intercettazioni, ispezioni e perquisizioni. L'utilizzo di tali tecniche persegue in realtà uno scopo diverso da quello previsto dal sistema penale, perché mentre i pubblici ufficiali che indagano sulla commissione di un delitto si avvalgono di tali strumenti per ricostruire la verità processuale e punire i colpevoli di un fatto già avvenuto, le indagini compiute dagli agenti dell'NSA cercano piuttosto di acquisire in anticipo tutti gli elementi utili a prevenire una minaccia non ancora concretizzatasi, e seguono dunque uno schema investigativo preventivo diffuso che è potenzialmente molto più invasivo della privacy dei cittadini.

Tali meccanismi di controllo, inoltre, sollevano fondati dubbi di legittimità quando sono condotti a partire da sospetti vaghi e generici, o addirittura in mancanza di elementi circostanziati sulla natura delle future minacce. E così, mentre generalmente nessuno metterebbe mai in dubbio che

[11] Così, ad esempio, in riferimento al tema delle intercettazioni telefoniche sei anni dopo la sentenza *Olmstead v. United States* il Congresso americano approvò una legge che vietava le intercettazioni telefoniche (cfr. Communication Act, 1934, Ch. 652, 48 Stat. 1064), anche se esso è rimasto spesso inattuato. Sotto il profilo costituzionale, pertanto, la problematica sulla costituzionalità delle intercettazioni telefoniche è stata risolta solo anni più tardi con la sentenza della Corte Suprema *United States v. Katz* del 1967, che ha definitivamente stabilito come tale strumento investigativo rientra nella copertura offerta ai cittadini dal Quarto emendamento.

[12] Come ricordato nella hearing tenuta presso il Congresso pochi mesi dopo l'attacco alle torri gemelle dall'Attorney General John Ashcroft «it was without saying that the paramount objective of U.S. counterterrorism policy is the prevention of terrorist acts» e «this objective of preventing terrorist acts before they occur requires the collection and effective use of foreign intelligence and foreign counterintelligence to detect and react to terrorist threat before they occur». Cfr. S. DYCUS, A.L. BERNEY, W.C. BANKS, P. RAVEN-HANSEN, *National Security Law*, Wolters Kluwer, 2008, p. 479. Analogamente, già il 14 settembre 2001, il direttore della NSA «approved the targeting of terrorist-associated foreign telephone numbers on communication links between the United States and foreign countries where terrorists were known to be operating». Cfr. P.M. SHANE, *The NSA and the Legal Regime for Foreign Intelligence Surveillance*, in Jour. L. and Pol. for Infor. Soc., 2014, p. 273.

di fronte al fondato sospetto del compimento di un crimine la polizia possa predisporre un sistema di sorveglianza dell'indagato, nei i casi riguardanti la prevenzione della minaccia terroristica ci si trova spesso di fronte a sospetti meno definiti, il che rende più complicata l'identificazione degli standard probatori[13]. Per questo la dottrina americana ha cominciato a domandarsi quale sia il ruolo del Quarto emendamento nell'epoca della guerra digitale globale, posto che, come facilmente intuibile, «the current criminal laws and traditional enforcement process cannot provide absolute protection against terrorist acts» ed anzi «traditional Fourth Amendment requirements may thwart many investigations of terrorism, which depend on stealth to prevent terrorist plans before they are carried out»[14].

In definitiva, dunque, la disciplina e l'operato della NSA deve oggi tenere conto di obiettivi specifici connessi ai compiti istituzionali (che riguardano azioni predisposte al fine di sventare attentati terroristici sul suolo americano e le attività controspionaggio e prevenzione dei crimini internazionali all'estero) ma anche del rispetto del sistema democratico e della rule of law americana. Nella tradizione costituzionale americana, del resto, lo stesso termine *security* (che è oggi prevalentemente usato come sinonimo di *national* o *homeland security*) si riferisce, in realtà anche alla sicurezza dei cittadini di essere protetti (*to be secure*) dagli abusi del potere governativo; per questo come ricordato da un recente rapporto commissionato dalla Casa bianca «the United States Government must protect, at once, two different forms of security: *national* security and *personal* privacy»[15].

Seguendo questa prospettiva, l'interrogativo di fondo è dunque: le investigazioni condotte per garantire la sicurezza nazionale sono soggette agli stessi limiti previsti dal Quarto emendamento della Costituzione o devono invece essere trattate in modo differente data la particolare natura e

[13] Come ricordato da S. DYCUS, A.L. BERNEY, W.C. BANKS, P. RAVEN-HANSEN, *National Security Law*, cit., p. 477, «no one argues that a mere hunch about anticipated violent acts or subversion will justify surveillance of potential target», mentre i casi sulla sicurezza nazionale riguardano «something less than a completed illegal act must suffice», e pertanto «the development of standard of approval of investigations into national security threat is a critical legal issue».

[14] Cfr. W.C. BANKS, M.E. BOWMAN, *Executive Autority for National Security Surveillance*, 50 Am. U. L. Rev., 2001, p. 92.

[15] Cfr. Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies pubblicato il 12 dicembre 2013 con il titolo Liberty and Security In a Changing World, in http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, p. 14-15: «In the American tradition, the word "security" has had multiple meanings. In contemporary parlance, it often refers to national security or homeland security. One of the government's most fundamental responsibilities is to protect this form of security, broadly understood. At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: "The right of the people *to be secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated (…)" (emphasis added). Both forms of security must be protected».

finalità da esse perseguite? E, in subordine, le limitazioni previste da tale clausola costituzionale trovano applicazione anche alle attività di spionaggio condotte all'interno del territorio americano? Due domande non semplici a cui anche la Corte suprema, in passato, non ha dato risposte univoche, essendosi limitata a ricordare sinteticamente che il Quarto emendamento trova applicazione nei confronti della sorveglianza governativa finalizzata alla sicurezza nazionale, ma che, in tale materia, le regole possono differire da quelle generalmente utilizzate per i crimini ordinari[16].

3. Security vs. Privacy: le norme sulla sorveglianza elettronica dall'epoca del proibizionismo all'avvento del terrorismo internazionale.

Al pari del diritto costituzionale alla riservatezza, anche la sicurezza nazionale costituisce un valore riconosciuto da tutte le democrazie occidentali. In America, storicamente, tale compito fu fin dall'origine attribuito alle autorità statali per prevenire le minacce interne, e al potere esecutivo federale per affrontare i conflitti esteri con le altre nazioni. Nel primo secolo della storia americana, pertanto, la sicurezza nazionale fu sostanzialmente intesa come sinonimo di ordine pubblico garantito localmente dalle polizie dei singoli Stati, e solo a seguito del proliferare della criminalità organizzata nell'epoca del proibizionismo nacque l'esigenza di predisporre un'agenzia investigativa a livello federale.

A testimonianza della diffidenza e ritrosia degli americani verso il potere federale, la nascita del Bureau of Investigation (poi rinominato Federal Bureau of Investigation - FBI) nel 1908 suscitò fin da subito non pochi timori tra i membri del Congresso, preoccupati delle conseguenze che la creazione di una polizia governativa non istituita per legge avrebbe potuto produrre nei confronti delle libertà dei cittadini[17]. Ma queste iniziali perplessità non frenarono la rapida ascesa del Bureau, che nel corso del ventesimo secolo ha visto crescere in modo esponenziale le sue risorse e mansioni[18]. Tale crescita ha seguito di pari passo lo sviluppo tecnologico, fornendo agli agenti federali nuovi strumenti d'investigazione, anche se – a dispetto dell'importanza assunta

[16] Così la sentenza United States v. U.S. District Court, 407 U.S. 207 (1972).

[17] Cfr. a tal riguardo, la dichiarazione del deputato J. Swagar Sherley riportata in D.J. SOLOVE, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, Yale Un. Press, 2011, p. 5: «In my reading of history I recall no instance where a government perished because of the absence of a secret-service force, but many there are that perished as a result of spy system».

[18] Si calcola che se nel 1933 gli agenti dell'FBI erano 355, nel 1954 essi avevano già raggiunto il consistente numero di 4,380 e ai giorni nostri (2008) superano le 12.000 unità. Cfr. a riguardo C. GENTRY, *J. Edgar Hoover: The Man and the Secrets*, 1991, p. 113.

dall'organo investigativo – i poteri e le mansioni continuarono a non essere regolate da una legge del Congresso, come invece è avvenuto per molte altre agenzie.

Nel frattempo, l'entrata degli Stati Uniti nel secondo conflitto mondiale amplificò enormemente il dibattito sulla sicurezza nazionale, facendo emergere l'esigenza di controllare non solo il proprio territorio, ma anche le minacce provenienti dall'estero. L'insorgere della guerra fredda e i timori legati al controllo sovietico di una parte del mondo portarono poi all'approvazione di leggi specifiche sulla sicurezza nazionale quale il National Security Act del 1947, e alla creazione di agenzie permanenti preposte a tale compito quali la Central Intelligence Agency (CIA) e la National Security Agency (NSA).

Quest'ultima, in particolare, fu istituita dal Presidente Truman nel 1952 al fine di raccogliere, analizzare, elaborare, decriptare tutte le informazioni segrete estere, e a trasmetterle alle altre agency. Data la natura prevalentemente tecnica delle sue mansioni, l'NSA fu a lungo considerata un organismo minore, tanto che per molto tempo l'acronimo NSA fu ironicamente utilizzato dagli americani per descrivere "No Such Agency". Ma in realtà lo sviluppo degli strumenti tecnologici e la silenziosa espansione delle tecniche investigative degli agenti dell'NSA hanno oggi trasformato tale agenzia in una delle più importanti risorse dell'intelligence americana.

Pur essendo prevalentemente rivolto allo spionaggio estero, l'azione capillare delle agency americane non tardò a produrre effetti anche all'interno del territorio americano. Già durante gli anni cinquanta, infatti, il crescente timore della diffusione del comunismo all'interno e all'esterno del territorio americano aveva portato alla creazione del Counter Intelligence Program (COINTERPRO), ovvero di un programma di controllo dei cittadini americani che autorizzò gli agenti dell'FBI a raccogliere e catalogare informazioni sui componenti di gruppi politici anarchici o socialisti dichiaratamente violenti, ma anche sugli oppositori pacifici della guerra in Vietnam o sui membri del movimento per i diritti civili (come, ad esempio, il reverendo Martin L. King). Sotto il controllo del direttore J. Edgar Hoover, l'FBI predispose una ramificata azione di sorveglianza investigativa con cui, non sempre per fini legati alla sicurezza nazionale, mise sotto controllo le comunicazioni di centinaia di attori, scrittori, professori, politici e cittadini americani più o meno famosi[19]. Al di là del giudizio storico sull'operato di Hoover che rimane ancor oggi

[19] Si tratta della famosa creazione dei c.d. files segreti di J. Edgar Hoover, la cui storia controversa non è ancora oggi del tutto conosciuta. Membro del Bureau per oltre cinquant'anni sotto otto diversi presidenti, Hoover si mise il luce inizialmente per i suoi successi conseguiti contro la criminalità organizzata, ma fu poi coinvolto in una brutale guerra investigativa contro i dissidenti politici che, secondo alcuni, ha portato alla creazione di numerosi e cospicui dossiers con cui egli avrebbe ricattato deputati o senatori americani per fini personali o politici. Sulla discussa figura di Hoover v. (tra gli altri) il già citato C. GENTRY, *J. Edgar*

controverso, lo sviluppo tecnologico delle agenzie federali negli anni cinquanta portò ad una rapidissima espansione degli strumenti di controllo delle comunicazioni interne, suscitando più di un dubbio sulla sua legittimità; pur nascendo per fini legittimi e ragioni legate alla sicurezza degli Stati Uniti, la crescita per lo più non regolamentata di agency dotate di un potere tanto esteso portò ad abusi e prevaricazioni da parte del Governo federale, come testimoniano le dimissioni del presidente Nixon a seguito del notissimo scandalo Watergate.

Proprio le enormi polemiche suscitate da tale caso sensibilizzarono l'opinione pubblica sui pericoli e sugli eccessi della sorveglianza federale, costringendo il Congresso a regolare e limitare il potere riservato all'FBI e alle altre agency americane. A partire dal 1975, il Congresso istituì così una speciale commissione d'inchiesta presieduta dal senatore Frank Church, che accertò numerosi abusi perpetuati dalle agenzie governative sotto il controllo di quasi tutti presidenti americani da Roosevelt a Nixon[20], e approvò misure legislative volte a controllare l'attività di

Hoover: The Man and the Secrets, 1991 e (più recentemente) R. KESSLER, *The Bureau: The Secret History of the FBI*, 2002.

[20] I lavori del Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (comunemente chiamato Church Commitee) si conclusero nel 1976 con la pubblicazione di quattordici volumi contenenti report, dossiers e documenti probatori che accertarono un capillare controllo delle comunicazioni dei cittadini americani messa in atto da CIA, FBI e NSA. L'NSA, in particolare, fu coinvolta nelle hearings della Commissione Church per due differenti programmi investigativi: il progetto MINARET, introdotto al fine di raccogliere e immagazzinare informazioni delle intelligence straniere, e per controllare in particolare i rapporti tra dissidenti americani e il Governo di Cuba, e l'operazione SHAMROCK, con cui il Governo aveva obbligato le tre compagnie private di telecomunicazione (RCA Global, ITT World Communications, and Western Union International) ad inoltrare il traffico telegrafico internazionale al dipartimento della Difesa. Nate per fini connessi alla sicurezza nazionale, entrambe queste operazioni avevano finito per raccogliere ed immagazzinare conversazioni di centinaia di cittadini americani per fini non connessi alla sicurezza della nazione; si calcola ad esempio che attraverso i programmi MINARET e SHAMROCK l'NSA predispose numerosi files su circa 75.000 cittadini americani tra il 1952 e il 1974: come ricordato «persons included in these files included civil rights leaders, antiwar activists and Members of Congress. For at least 13 years, CIA employees were given unrestricted access to this files, and one or more worked full time retrieving information that presumably was contributed to the CIA's domestic intelligence program which exsisted from 1967 to 1974» (cfr. House Comm. On Gov't Operations, Interception Of International Telecommunications by the National Security Agency (Draft Report) 2, in http://www.maryferrell.org/mffweb/archive/viewer/showDoc.do?docId=145022&relPageId=4. Per considerazioni sul Church Committee in particolare rispetto all'attività della NSA v., da ultimo, L. K. DONOHUE, *Bulk Metadata Collection: Statutory and Constitutional Consideration*, in *Harv. J.L. & Pol'y* (in corso di pubblicazione), disponibile anche in www.http://ssrn.com/abstract=2344774. In termini generali, in ogni caso, le conclusioni del Church Committee misero in ogni caso in luce come «too many people have been spied upon too many Government Agencies and too much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of hostile foreign power». Cfr. Church Committee Report, Vol. 5, Intelligence Activities: Hearings on S. Res. 21 Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States, 94th Cong. 9, 1975p. 5).

vigilanza governativa. La più importante di queste misure è certamente rappresentata dal Foreign Intelligence Surveillance Act (FISA) del 1978, finalizzato a definire «a secure framework by which the executive branch could conduct legitimate electronic surveillance for foreign intelligence purpose within the context of this Nation's commitment to privacy and individual rights», e a riportare così i programmi federali di sorverglianza elettronica «under the rule of law»[21].

La legge predispone una serie di misure volte a limitare l'azione della NSA nella raccolta dei dati sensibili ottenuti mediante sorveglianza elettronica, restringendo ad esempio la nozione di «foreign power or agent thereof»[22] e stabilendo che il Governo è tenuto a dimostrare che esistono fondati motivi («probable cause») per ritenere che il sorvegliato sia realmente un agente straniero[23]. In questo modo il Congresso tentò di differenziare il trattamento riservato agli stranieri sospettati di spionaggio da quello riservato ai cittadini anche quando ritenuti colpevoli di tenere relazioni con agenti stranieri, fornendo un grado di protezione maggiore a questi ultimi.

Al fine di regolare e monitorare il processo di sorveglianza elettronica, infine, la legge del 1978 ha previsto la creazione di tribunali speciali chiamati in segreto a valutare, autorizzare o respingere le richieste governative. Il Congresso ha così istituito la Foreign Intelligence Surveillance Court (FISC) composta da undici giudici federali «which shall have jurisdiction to hear applicants for and grant orders approving such surveillance»[24], e la Foreign Intelligence Surveillance Court of Review (FISCR) composta da tre giudici delle U.S. District Court of Appeal «which shall have jurisdiction to review the denial of any application made under [FISA]»[25]. Entrambi i tribunali sono istituiti al fine di introdurre all'interno del processo un soggetto terzo e neutrale chiamato a giudicare la ragionevolezza e la legittimità delle richieste governative di sorveglianza; i giudici del FISC e del FISCR hanno infatti il compito di verificare se il Governo abbia o meno rispettato i requisiti di legge nel predisporre un certo programma di sorveglianza investigativa[26] e, nel caso

[21] Cfr. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783. La citazione è tratta da S. Rep. No. 95-604, p. 7 (1977).
[22] Cfr. 50 U.S.C. § 1801 (a).
[23] Cfr. 50 U.S.C. § 1805 (a)(3).
[24] Cfr. 50 U.S.C. § 1803 (a)(1).
[25] Cfr. 50 U.SC. § 1803 (b).
[26] Come precisato dal FISA (50 U.S.C. § 1804) «Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include— (1) the identity of the Federal officer making the application; (2) the identity, if known, or a description of the specific target of the electronic surveillance; (3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that— (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

l'accertamento dia esito positivo, sono tenuti ad autorizzarlo. Il controllo delle Corti di sorveglianza, tuttavia, è molto più circoscritto di quello dei giudici ordinari, e si limita ad una valutazione formale dei requisiti di legge; come ricordato dalla dottrina, infatti, «FISA regulations are much looser than those for ordinary crime» poichè, mentre nel sistema penale americano «surveillance is authorized only if there is a showing of probable cause that the surveillance will uncover evidence of criminal activities» il meccanismo di controllo istituito dal FISA prevede che «orders are granted if there is a probable cause to believe that monitored party is "foreign power" or "an agent of a foreign power"»[27].

Inizialmente le operazioni regolate dal FISA (e il controllo operato dai giudici) riguardarono esclusivamente la sorveglianza elettronica. Ma nel corso degli anni numerosi emendamenti hanno ampliato l'ambito della legge, disponendo ad esempio la possibilità per il Governo di predisporre *physical search*, o utilizzare dispositivi di registrazione dati quali i *pen register* e i *trap-and-trace device*[28]. Nel 1998, inoltre, il Congresso ha introdotto all'interno del FISA la c.d. *business record provision*, che consente all'FBI di ottenere (previa autorizzazione dei giudici del FISC) da soggetti privati che forniscono alcuni servizi (e segnatamente i «common carries, public accommodations service, storage facilities, rental vehicle facilities»[29]) copia dei registri commerciali ogni volta che si sia in presenza di «specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power»[30]. In definitiva, dunque, nel corso degli anni le disposizioni contenute nel FISA sono sensibilmente mutate, adattandosi allo sviluppo tecnologico e alla nascita delle nuove minacce alla sicurezza nazionale.

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power; (4) a statement of the proposed minimization procedures; (5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance».

[27] Così D.J. SOLOVE, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, cit., p. 74-75. È opportuno peraltro ricordare che nel sistema americano la distinzione tra investigazioni penali e spionaggio terroristico è sancita anche a livello legislativo, in quanto se per queste ultime si utilizzano le norme contenute nel FISA, la disciplina della sorveglianza elettronica concernente il perseguimento di crimini federali segue le regole contenute nell'Elecronic Comminication Privacy Act (ECPA) che stabilisce più ampie garanzie di tutela della privacy.

[28] Si tratta di dispositivi tecnologici in grado di registrare i dati elettronici sensibili riguardanti una comunicazione telefonica quali ad esempio il numero chiamato, l'orario della comunicazione, i dispositivi connessi, il titolare dell'utenza. La possibilità di utilizzare tali strumenti è stata introdotta a metà degli anni Novanta, ed è oggi contenuta nel 50 U.S.C. § 1821-1824 (physical search) e § 1841-1842 (trap and trace device).

[29] Cfr. la previsione introdotta dal Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, §602, 112 Stat. 2396, 2410.

[30] Cfr. 50 U.S.C. § 1862 (b)(2)(B).

Non è un caso, a questo riguardo, che l'introduzione della *business records provision* sia avvenuta, a fine anni novanta, sull'onda della reazione emotiva generata dall'attentato terroristico di Oklahoma city, in cui un veterano della guerra del golfo fece esplodere un edificio federale causando la morte di 168 persone. In sostanza, dunque, il verificarsi di impreviste minacce alla sicurezza nazionale accresce il bisogno di predisporre nuove misure di controllo che, inevitabilmente, finiscono con il comprimere il diritto alla riservatezza.

Quest'ultima considerazione spiega le ragioni delle corpose modifiche operate al FISA nel nuovo millennio, che – unitamente ad altri interventi normativi – hanno ampliato in modo significativo le modalità di controllo, sorveglianza, immagazzinamento dei dati elettronici e digitali delle agencies governative americane. Gli attentati dell'11 settembre 2001, infatti, hanno mostrato la pericolosità delle minacce terroristiche e l'inadeguatezza dei tradizionali sistemi di spionaggio, tanto che, nei mesi successivi all'attacco terroristico, molti analisti hanno criticato l'organizzazione burocratizzata dei sistemi di Intelligence, rilevando come il sistema disegnato dal FISA intralciasse una rapida trasmissione dei dati tra le diverse agenzie chiamate a difendere la sicurezza nazionale[31]. Per far fronte a questi problemi il Congresso ha così approvato il USA PATRIOT Act, ovvero una normativa finalizzata a rafforzare il potere dei corpi di polizia statunitensi e ad estendere l'ambito di applicazione delle regole sullo spionaggio internazionale[32].

Tra le numerose modifiche operate dal PATRIOT Act, particolarmente interessante ai fini della nostra indagine appare quella contenuta nella sezione 215 della legge, che ha ampliato l'ambito

[31] Cfr. ad esempio, le considerazioni di J. YOO, *War by Other Means: An Insider's Account of the War of Terror*, Atlantic Press, 2006. Del resto, come riportato dal 9/11 Commission Report del 2004, uno dei principali problemi registrati circa l'ineffettiva sorveglianza del terrorismo internazionale riguarda esattamente l'eccessiva frammentarietà delle agencies americane chiamate, in diversa misura, a difendere i confini nazionali dipendenti da diversi rami della amministrazione. E a queste ragioni si deve, del resto, l'istituzione del Department of Homeland Security (DHS) prevista dall' Homeland Security Act del 2002 (Public Law 107-296), che ha profondamente modificato la struttura della macchina amministrativa americana, riunendo 22 agencies e uffici separati sotto il controllo di un unico Cabinet-level departmen.

[32] In particolare il PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) amplia gli scopi del sistema di controllo della Intelligence Community americana, rendendo meno definiti i confini che limitano il potere delle agencies di richiedere la sorveglianza dei sospettati. Così, mentre prima delle modifiche del 2001, le regole sullo spionaggio internazionale contenute nel FISA erano applicabili solo quando «the purpose» dell'indagine riguardava esclusivamente la racconta di informazioni relative a «foreign intelligence», l'approvazione del PATRIOT Act ha ampliato l'ambito delle misure contenute nel FISA, prevedendo la loro applicazione anche quando la raccolta di informazioni relative alle intelligence straniere è «a significant purpose» dell'investigazione. Cfr. USA PATRIOT Act, Pub. L. No. 107-56, § 204, che modifica 50 U.S.C. § 1804(a)(7)(B). Come osservato da D.J. SOLOVE, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, cit. p. 76, «this seemingly subtle change has dramatic ramifications. With the change in language from "*the* purpose" to "*a significant* purpose", foreign intelligence gathering no longer needs to be the primary purpose of the surveillance» perché «the government can now rely on loose FISA protections even when foreign intelligence gathering is only one of many goals».

della *business provision* sopra ricordata, sostituendola con una norma maggiormente estensiva riguardante l'acquisizione delle c.d. *tangible things*. Codificata nel paragrafo 1861 del FISA, essa autorizza l'FBI «[to] make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items)» ogni volta che ciò sia necessario per condurre «an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities (…)»[33].

Analogamente a quanto previsto nel 1998 dalla *business provision*, anche la sezione 215 consente quindi al Governo di costringere soggetti privati che erogano servizi pubblici (come ad esempio le compagnie telefoniche che operano sul territorio nazionale) a consegnare i registri, i tabulati e ogni altro documento od oggetto utile ai fini delle investigazioni terroristiche. Ma a differenza della previsione del 1998, la sezione 215 estende il potere governativo in due rilevantissimi profili: in primo luogo, ampliando l'ambito soggettivo ed oggettivo di indagine, essa ha rimosso le limitazioni riguardanti la tipologia dei soggetti obbligati a presentare i loro documenti, e degli oggetti che possono essere acquisiti previa autorizzazione dei giudici del FISC[34]. In secondo luogo, essa ha modificato in modo significativo gli standard richiesti per tale autorizzazione, al punto che mentre in precedenza il Governo era tenuto a fornire «specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power»[35], dopo il 2001 le norme del FISA consentono ai giudici di rilasciare l'autorizzazione ogniqualvolta il Governo ritenga che l'acquisizione dei documenti sia *genericamente* connessa ad una indagine relativa ad attività terroristiche o di intelligence clandestina[36].

---

[33] Cfr. PATRIOT Act of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) oggi codificata in 50 U.S.C. § 1861(a)(1).

[34] Come già ricordato in precedenza, il Business Provision Act del 1998 stabiliva una lista ristretta di soggetti privati che erano tenuti a presentare i loro documenti (e segnatamente « common carries, pubblic accomodations service, storage facilities, rental vehicle facilities»), limitando inoltre anche la acquisizione dei soli business records di tali compagnie private. La previsione introdotta dal PATRIOT Act, invece, oltre a non definire in alcun modo i soggetti terzi obbligati a produrre tali documenti, prevede espressamente che il FISC possa autorizzare il sequestro di «any tangible things including books, records, papers, documents, and other items», e quindi – potenzialmente – di ogni oggetto (fisico, elettronico o digitale) utile.

[35] Così il tenore letterale della disposizione contenuta nell'Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, § 602, 112 Stat. 2396, 2410 (1998).

[36] Come riportato *supra* (nota 29) l'attuale disposizione del FISA dopo le modifiche operate dal PATRIOT Act stabilisce infatti che l'aquisizione delle c.d. tangible things possa avvenire ogni volta che essa risulti necessaria per condurre «an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities».

In altri termini, l'estensione dell'ambito di applicazione della norma e la assenza di specifici standard necessari per la sua applicazione hanno portato ad un significativo aumento dei poteri concessi alle agencies governative, agitando il sospetto che il sequestro di beni e dati sensibili riguardanti la privacy degli americani possa oggi essere prevista senza un mandato specifico, e dunque aggirando il divieto di general warrant contenuto nel Quarto emendamento della Costituzione. La pericolosità della norma in esame, del resto, fu probabilmente riconosciuta dallo stesso Congresso, che al momento della sua approvazione stabilì che essa avrebbe dovuto rimanere in vigore solo per un periodo limitato di tempo, e in ragione della straordinaria emergenza terroristica a cui il Governo era chiamato a far fronte. In realtà la previsione è stata poi più volte riconfermata negli anni fino a costituire, di fatto, una norma pressoché permanente all'interno dell'ordinamento americano[37], anche se – almeno in un caso – il Congresso ha tentato di ridurne la portata[38]. Tale disposizione, infine, costituisce il fondamento normativo attraverso cui il Governo americano ha avviato i programmi di sorveglianza rivelati al mondo da Eric Snowden. Uno di questi programmi, in particolare, «involves the use of court orders under FISA's business records authority to collect transactional information about every telephone call placed over the networks of domestic telecommunications carriers – i.e., numbers dialed and call duration, but not content or location data»[39].

[37] In un primo momento, la sezione 215 del PATRIOT Act avrebbe dovuto rimanere in vigore fino al 31 dicembre 2005, ma essa è stata riconfermata sette volte dal Congresso con interventi normativi specifici, e attualmente il PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011) ha esteso la validità della norma fino al 1 giugno 2015. Sulle problematiche politiche relative alla riconferma di tale norma v. Paul Kane & Felicia Sonmez, *Congress Extends Patriot Act Provisions*, in Wash. Post, May 27, 2011.

[38] Come ricordato dal Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies *"Liberty and Security In a Changing World"*, cit., p. 81, la formulazione originaria della sezione 215 del Patriot act « was criticized as being too open-ended, and Congress thereafter amended section 215 in the USA PATRIOT Improvement and Reauthorization Act of 2005, which authorized the FISC to issue such orders only if the government provides "a statement of facts showing that there are reasonable grounds to believe that the tangible objects sought are relevant" to an authorized investigation intended to protect "against international terrorism or clandestine intelligence activities"». (Cfr. USA PATRIOT Improvement and Reauthorization Act of 2005 § 106, 120 Stat. 196 oggi contenuto in 50 U.S.C. § 1861(b)(2)(A)). La Sezione 215 attualmente vigente prevede inoltre che le investigazioni sui cittadini americani debbano essere condotte «solely on the basis of activities protected by the first amendment to the Constitution» e che per alcuni tipi di tangible thigs (come «library records, book sales records, firearms sales records, tax return records, educational records, and medical records with information identifying an individual») solo le più alte autorità dell'FBI (segnatamente: Director of the FBI, the Deputy Director of the FBI, or the Executive Assistant for National Security) possano richiedere la relativa autorizzazione. Cfr. 50 U.S.C. § 1863(a)(3) (2006). A commento di tali disposizioni, v. tra gli altri D.J. SOLOVE, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, cit.

[39] N.A. SALES, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy* , 10 ISJLP, 2014, p. 525.

4. La Sezione 215 e il Bulk Metadata Surveillance Program: profili di costituzionalità

Come già ricordato, le problematiche relative alla costituzionalità della sezione 215, e più in generale dei poteri federali di sorveglianza elettronica, sono sorte a seguito delle rivelazioni di due specifici programmi segreti della NSA, l'uno riguardante l'intercettazione e il controllo delle e-mail di cittadini non americani al di fuori dei confini nazionali, l'altro relativo alla raccolta dei dati telefonici ottenuti sia all'interno che all'esterno degli Stati Uniti. Per quanto entrambi i programmi abbiano suscitato più di un imbarazzo all'amministrazione Obama minandone la credibilità internazionale[40], sotto il profilo di costituzionalità interna i maggiori problemi riguardano la applicazione interna del National Security Agency's Bulk Metadata Surveillance Program. Avviato a partire dal maggio del 2006 in applicazione della sezione 1861 del FISA, tale programma obbliga le principali compagnie telefoniche americane a consegnare alla NSA i registri dei metadati in loro possesso[41]; in questo modo, il Governo americano ha ottenuto negli ultimi sette anni trentaquattro autorizzazioni dai giudici del FISC, raccogliendo in segreto un numero considerevole di dati sul traffico telefonico e digitale dei suoi cittadini[42].

I registri consegnati all'NSA riguardano in particolare i c.d. telephony metadata, ovverosia ogni informazione relativa al luogo, al momento e alla durata delle telefonate, ma non il loro contenuto (registrato o trascritto) che rimane sconosciuto agli agenti federali[43]. I metadati

[40] Si tratta, in particolare, delle polemiche suscitate a seguito delle intercettazioni della corrispondenza elettronica e telefonica privata del cancelliere tedesco Angela Merkel e del presidente francese Hollande. Cfr. Intercettato il telefonino di Angela Merkel. Berlino convoca ambasciatore Usa, in Il Sole 24 Ore, ed. on-line, 24 ottobre 2013 http://www.ilsole24ore.com/art/servizio/2013-10-23/berlino-intercettato-usa-anche-telefonino-merkel-cancelliera-obama-inaccettabile-194805.shtml?uuid=ABcyLnY.

[41] In particolare, il primo ordine rilasciato dai giudici del FISC in relazione a tale programma è datato 24 maggio 2006; cfr. In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Telecommunications Providers] Relating to [REDACTED], Order, No. BR 0605 (FISA Ct. May 24, 2006), disponibile in https://www.eff.org/sites/default/files/filenode/docket_06-05_1dec201_redacted.ex_-_ocr_0.pdf.

[42] È quanto emerge dal documento *Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act 2* (Aug. 9, 2013) disponibile in https://www.documentcloud.org/documents/750211-administration-white-paper-section-215.html, redatto dalla Casa bianca nell'agosto del 2013, a seguito delle pressanti richieste dell'opinione pubblica e della stampa circa il programma di sorveglianza elettronica rivelato da Erick Snowden. Tale documento (p. 3) «explains the Government's legal basis for an intelligence collection program under which the Federal Bureau of Investigation (FBI) obtains court orders directing certain telecommunications service providers to produce telephony metadata in bulk» che sono «stored, queried and analyzed by the National Security Agency (NSA) for counterterrorism purposes» su autorizzazione delle Corti del FISC «under the "business records" provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861, enacted as section 215 of the USA PATRIOT Act (Section 215). The Court first authorized the program in 2006, and it has since been renewed thirty-four times under orders issued by fourteen different FISC judges».

[43] Cfr. il già citato Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things del 24 maggio 2004, che precisa al p.to 2 che «The tangible things to be produced are all

acquisiti sono organizzati in database che possono essere consultati al fine di scoprire eventuali contatti tra le cellule terroristiche all'interno e all'esterno del territorio americano; gli analisti dell'NSA, in particolare possono servirsi di tale database a partire da un c.d. "identifier", cioè dal "contatto" – generalmente un numero di telefono ma non solo – che si presume essere associato ad attività terroristiche, e che costituisce il punto di partenza ("seed") della ricerca. Una volta ottenuta l'autorizzazione ad indagare[44], gli analisti informatici possono quindi analizzare i dati per individuare i contatti di primo, secondo e terzo livello del seed originale, seguendo un procedimento chiamato "three-hop": in termini pratici, ciò comporta che le indagini coinvolgano non solo i numeri telefonici direttamente contattati dal seed (c.d. "first hop"), ma anche tutte le utenze che siano entrate in comunicazione con gli identifiers del primo livello (c.d. "second hop") e con quelli del secondo livello (c.d. "third hop")[45]. Ciò significa che, attraverso tale procedimento, l'NSA è in grado di acquisire un numero impressionante di dati, estendendo in modo indefinito la sua ricerca ad utenze che – nella maggior parte dei casi – non hanno nulla a che vedere con quel "reasonable articulate suspicion" che costituisce lo standard per indagare su potenziali terroristi[46].

Secondo il Governo americano, il Bulk Metadata Surveillance Program rappresenta uno strumento fondamentale per la prevenzione del terrorismo, ed è utilizzato con modalità che tutelano la privacy dei cittadini americani. Esso, infatti, sarebbe soggetto a controlli accurati da

---

call-detail records or "telephony metadata" created by (omissis). Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, communications device identifier, etc), trunk identifier, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.1 [50 U.S.C. § 186l(c)(2)(A)]».

[44] Tale autorizzazione è rilasciata da uno dei ventidue designati Officials facenti parte dell'NSA's Homeland Security Analysis Center, o connessi all'NSA's Signal Intelligence Directorate. La ricerca dei metadati a partire da un particolare seed è generalmente rilasciata a seguito di un generale e ragionevole sospetto ("reasonable, articulate suspicion") che l'utenza in esame sia connessa ad una associazione terroristica.

[45] Come ricordato dal già menzionato Section 215 White Paper, p. 3-4. «The first "hop" refers to the set of numbers directly in contact with the seed identifier. The second "hop" refers to the set of numbers found to be in direct contact with the first "hop" numbers, and the third "hop" refers to the set of numbers found to be in direct contact with the second "hop" numbers».

[46] Come paventato dal giudice Richard J. Leon nella sentenza *Klayman v. Obama* (su cui v. *infra*), infatti, «the actual number of telephone numbers and their associated metadata captured in any given query varies, of course, but in absence of any specific representations from the Government about typical query results, it is likely that the quantity of phone numbers captured in any given query would be very large». Anche se è impossibile contare con esattezza il numero di contatti su cui gli analisti hanno svolto indagini informatiche, il direttore dell'NSA Signal Intelligence Theresa H. Shea ha recentemente ammesso che «the number of metadata responsive to such queries is substantially larger than 300, but is still a very small percentage of the total volume of metadata records» (cfr. *Klayman v. Obama*, nota 21).

parte non solo dei giudici del FISC, ma anche del Department of Justice (DOJ) e degli stessi uffici dell'NSA, che sono chiamati a ponderare con grande attenzione i sospetti che rendono necessario l'utilizzo dei dati informatici[47]. Al di là delle rassicurazioni governative, il numero dei dati in possesso degli agenti dell'NSA e la portata generale dei parametri contenuti nella sezione 215 ha sollevato più di un dubbio (e ben più di qualche polemica) circa la costituzionalità della azione governativa.

Se da un lato, infatti, l'utilizzo delle nuove tecnologie è oggi considerato una necessità imprescindibile per prevenire concretamente le possibili minacce terroristiche, è d'altro canto facile comprendere come la raccolta indiscriminata di dati sensibili possa ingenerare potenziali rischi alla libertà dei cittadini americani[48]. I metadati telefonici non riguardano il contenuto delle comunicazioni ma solo la traccia delle comunicazioni avvenute tra utenti e già in possesso delle compagnie telefoniche. Al contempo, però, si tratta pur sempre di informazioni connesse a scelte, abitudini ed inclinazioni che sono in grado di rivelare, se adeguatamente analizzate, pezzi rilevanti della vita personale. Per questo occorre chiedersi se il Quarto emendamento trovi applicazione anche nel caso della raccolta di metadati telefonici, e analizzare la disciplina normativa relativa al Bulk Metadata Surveillance Program a partire dal quadro complessivo della interpretazione fornita negli anni dalla Corte suprema al diritto alla privacy, per capire se tale programma governativo costituisca o meno «a digital trespass on the private lives of American citizens»[49].

---

47 Vedi, ad esempio, le considerazioni espresse dal Governo nel già citato White Paper, p. 4-5 secondo cui «the telephony metadata collection program is subject to an extensive regime of oversight and internal checks and is monitored by the Department of Justice (DOJ), the FISC, and Congress, as well as the Intelligence Community. No more than twenty-two designated NSA officials can make a finding that there is "reasonable, articulable suspicion" that a seed identifier proposed for query is associated with a specific foreign terrorist organization, and NSA's Office of General Counsel must review and approve any such findings for numbers believed to be used by U.S. persons (…)In addition to internal oversight, any compliance matters in this program that are identified by the NSA, DOJ, or ODNI are reported to the FISC. The FISC's orders to produce records under the program must be renewed every 90 days, and applications for renewals must report information about how the authority has been implemented under the prior authorization. Significant compliance incidents are also reported to the Intelligence and Judiciary Committees of both houses of Congress».

48 I rischi legati ad un controllo di massa dei metadati dei cittadini sono molteplici; come ricordato da S. KADIDAL, *NSA Surveillance: The Implications for Civil Liberties*, 10 ISJLP, 2014, p. 463 «To what extent are judges, members of Congress and other elected officials exempted from NSA surveillance? If they are not, the chilling effect that afflicts attorneys and journalists applies here as well and has similarly enormous potential to corrupt the political process. Imagine Anthony Weiner [deputato americano coinvolto nel 2011 in uno scandalo sessuale n.d.r.] hadn't accidentally mass-tweeted that fateful photograph, and had remained in the House, but knew that the NSA knew about his habits – and was casting the deciding vote on a bill limiting the powers of the NSA?»

49 L. K. DONOHUE, *Bulk Metadata Collection: Statutory and Constitutional Consideration*, cit., p. 64-65, afferma che «The telephony metadata program amounts to a general warrant, the prohibition of which gave rise to the Fourth Amendment. The reason such warrants were rejected is because they amounted to granting the

Come noto, il contenuto originario del Quarto emendamento si riferisce primariamente alla protezione dei confini *fisici* della privacy dei cittadini, difendendoli da illegittime perquisizioni della loro persona e delle loro abitazioni. Al momento dell'approvazione della Costituzione i Framers non potevano certo immaginare che con l'avvento dell'era digitale i confini della privacy si sarebbero trasformati in luoghi non solo materiali ma anche virtuali; la stessa Corte suprema, del resto, ha inizialmente interpretato tale clausola a partire dalla c.d. *physical trespass doctrine*, sostenendo che il diritto costituzionale alla privacy trovasse applicazione nei soli casi di intrusione fisica del Governo nelle proprietà e nella corrispondenza dei cittadini senza uno specifico mandato[50].

Così, ad esempio, nel famoso caso *Olmstead v. United States* del 1928, chiamata per la prima volta a pronunciarsi sulla costituzionalità di intercettazioni disposte senza mandato dagli agenti federali per frenare l'importazione illegale di alcolici nella costa pacifica, la Corte ha stabilito che «the [Fourth] Amendment does not prohibit what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing, and that only. There was no entry of the houses or offices of the defendants»[51]. Una volta accertato che le microspie erano state installate al di fuori di abitazioni private, la Corte ha risolto il caso a partire da una interpretazione restrittiva della privacy personale, ritenendo legittime intercettazioni federali senza mandato perché non ottenute attraverso il "physical trespass" della proprietà del ricorrente.

L'irragionevolezza di tale soluzione fu da subito ben chiara al giudice Brandeis, che (nella dissenting opinion del caso *Olmstead*) definì miope ed antiquato l'approccio della Corte, sostenendo invece la necessità di una interpretazione più moderna e flessibile del Quarto emendamento, perché «subtler and more far-reaching means of invading privacy had become available to the government», e «discovery and invention have made possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet»[52]. Per quasi quarant'anni, il suggerimento del giudice Brandeis è rimasto per lo più inascoltato, benché – sotto il profilo legislativo – il Congresso sia intervenuto diverse volte per regolare le zone grigie del Quarto emendamento. È stato l'insorgere dell'era

government an indefinite right of trespass, for which redress (because of their execution with legal sanction) could not be sought. Beyond the general warrant concern, the bulk telephony metadata program is digital trespass on the private lives of American citizens».

[50] Cfr. ad esempio, *Boyd v. United States*, 116 U.S. 616 (1886) sulla protezione dei «personal papers and documents», e *Ex Parte Jackson*, 96 U.S. 717 (1877) sull'invio delle lettere sigillate.

[51] *Olmstead v. United States*, 277 U.S. 438, 465 (1928).

[52] Id., 473 (J. Brandeis dissenting).

tecnologica a mostrare l'inadeguatezza di un approccio esclusivamente basato sulla difesa della proprietà materiale, costringendo la Corte suprema a rivedere la propria posizione[53].

Nel caso *Katz v. United States* del 1967, i giudici hanno dovuto pronunciarsi sul ricorso di un cittadino di Los Angeles, condannato per violazione di una legge federale che vietava le scommesse telefoniche. Al fine raccogliere le prove di tale reato, l'FBI aveva messo sotto controllo i telefoni pubblici in prossimità dell'appartamento del ricorrente, cogliendolo in flagrante ed arrestandolo; secondo Katz tale azione era da considerarsi illegittima perché condotta senza mandato, e di conseguenza suscettibile di inficiare la regolarità delle prove acquisite. Se interpretato alla luce della giurisprudenza precedente, il caso *Katz* avrebbe dovuto risolversi con il riconoscimento della regolarità delle intercettazioni che, condotte al di fuori della abitazione privata del ricorrente, erano pienamente conformi a quanto sostenuto in precedenza dalla *physical trespass doctrine*. Inaspettatamente, la Corte suprema decise invece di rivedere tale dottrina, sostenendo che il Quarto emendamento «protects people, not places» e pertanto «what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection»; al contrario, «what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected»[54]. Per la Corte, in sostanza, il diritto alla privacy non riguarda più esclusivamente i luoghi e i confini fisici elencati in Costituzione, ma anche la percezione che i cittadini hanno della loro riservatezza, sia essa esercitata in pubblico che in privato; come ricordato dalla concurring opinion del giudice Harlan, il Quarto emendamento dovrebbe quindi proteggere «an actual (subjective) expectation of privacy» quando la società «is prepared to recognize [it] as "reasonable"»[55].

Con l'elaborazione del *reasonable expectation of privacy* test, l'attenzione dei giudici si è così spostata da un criterio prevalentemente fondato su dati oggettivi (l'invasione fisica della proprietà dei cittadini) ad uno maggiormente legato al contesto e agli elementi soggettivi (il grado di privacy

[53] Come ricordato da E. ATKINS, *Spying on Americans: At What Point Does the NSA Collection and Searching of Metadata Violate the Fourth Amendment* , 10 Wash. J. L. Tech. & Arts 51, 2014, «as people increasingly relied on the telephone for conducting their private affairs, Olmstead's reasoning became more difficult to maintain», e pertanto «Justice Louis Brandeis' dissent in Olmstead has become the flagship of privacy rights arguments in post Olmstead cases».

[54] Cfr. *Katz v. United States*, 389 U.S. 351-352 (1967).

[55] Cfr. *Id.*, 361 (Harlan J. concurring): «As the Court's opinion states, "the Fourth Amendment protects people, not places." The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a "place." My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable"».

ragionevolmente atteso dai cittadini nei vari contesti)[56]. Lo scopo della Corte era probabilmente quello di estendere il controllo di costituzionalità ad ipotesi non specificamente contemplate nella Costituzione, introducendo – attraverso il principio di ragionevolezza – un controllo meno rigido dei parametri del Quarto emendamento e quindi maggiormente adattabile alle esigenze riguardanti le nuove tecnologie[57]. Il suo utilizzo non sempre però ha portato ad una reale estensione del diritto alla riservatezza anche perché, pochi anni più tardi, esso è stato affiancato dalla c.d. *third party doctrine*, ovverosia dal principio elaborato dalla Corte suprema per cui «a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties»[58]. Le origini di tale dottrina risalgono ad una serie di casi degli anni sessanta in cui la Corte suprema ha ammesso le prove acquisite da informatori segreti sostenendo come il diritto costituzionale alla privacy non si estenda a quelle informazioni che, volontariamente e liberamente, sono rivelate a terze persone[59], e ha trovato una applicazione chiara e definita a partire dalle sentenze *United States v. Miller* (1976) e *Smith v. Maryland* (1979).

In *Miller*, in particolare, i giudici hanno ritenuto legittima l'acquisizione forzata di documenti contabili prelevati dalle banche del convenuto sostenendo che il Quarto emendamento «does not prohibit the obtain of information revealed to a third party and conveyed by him to Government authority», in quanto «all the documents obtained, including financial statements and deposit slips, contain only information voluntary conveyed to banks and exposed to their employees in the ordinary course of business»[60]. Analogamente, nella sentenza *Smith*, la Corte Suprema ha

---

[56] Così, infatti, la Corte nella sentenza *Katz*, id. p. 353: [I]t is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable search and seizures[; therefore,] it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure». In modo non dissimile anche *Kyllo v. United States, 533 U.S. 27, 34–35 (2001),* sull'utilizzo di scanner termici, *United States v Karo* 468 U.S. 705 (1984) e , *United States v. Karo, 468 U.S. 705, 707–10 (1984)* sulle modalità di controllo attraverso rilevatori (beeper).

[57] Questo in risposta anche a quanto sostenuto da Brandeis nella dissenting opinion del caso *Olmstead*; come osservato da C. Steiker e riportato da D.J. SOLOVE, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, cit., p. 99 «Brandeis could have felt vindicated by Court's replecement of trespass doctrine whit one more oriented toward right of privacy».

[58] Cfr. *Smith v. Maryland* 422 U.S. 743-744 (1979).

[59] V., in particolare, i casi *Lopez v. United States*, 373 U.S. 427 (1963); *United States v. White*, 385 U.S. 206 (1966); *Hoffa v. United States*, 385 U.S. 293 (1966).

[60] *United States v. Miller* 425 U.S. 435 (1976). Mitch Miller era stato indagato per importazione illegale di alcolici, e per frode fiscale sul traffico; per ottenere le prove necessarie a dimostrare la sua colpevolezza, il Bureau of Alcohol, Tobacco, and Firearms (ATF) aveva ordinato forzatamente a due banche di consegnargli tutti i registri contabili riguardanti i depositi di Miller. Secondo la Majority opinion del giudice Powell, «the documents soubpoenaed are not [Miller's] "private papers"», quanto piuttosto documenti riguardanti l'attività economica della banca; i diritti di Miller dunque non sono stati violati in quanto, avendo egli stesso inoltrato le informazioni contenute in tali documenti ad un terzo soggetto (la Banca), questi ultimi devono pertanto essere considerati pubblici.

ritenuto che una cimice (pen register) installata nella linea telefonica non costituisse una perquisizione (search) ai sensi del Quarto emendamento, dal momento che i cittadini, quando effettuano telefonate, non si aspettato che i numeri da loro composti rimangano sconosciuti, in quanto «people know that they must convey numerical information to the telephone company» e quindi «cannot harbour any general expectation that the numbers they dial will remain secret»[61]. In particolare con *Smith*, la Corte suprema ha compiuto un passo importante nella delimitazione del diritto alla riservatezza dei cittadini americani: applicando la *third party doctrine* anche alle informazioni raccolte attraverso l'ausilio automatico e ripetitivo di una macchina, i giudici hanno costruito il fondamento normativo per l'espansione di tale teoria all'utilizzo e al trattamento dei dati informatici nell'era digitale[62].

In questa prospettiva è facile capire perché il Governo abbia sostenuto la costituzionalità del Bulk Metadata Surveillance Program statuendo che i metadati acquisiti dagli agenti dell'NSA, al pari dei numeri telefonici registrati dal pen register nel caso *Smith*, costituiscono informazioni raccolte giornalmente dai provider telefonici e dunque rientrano nell'ambito della *third party doctrine*. Secondo il Governo, inoltre, lo scopo finale del programma autorizzato ai sensi della Sezione 215

61 *Smith v. Maryland* 422 U.S. 743 (1979). Smith era stato indagato per furto e per molestie telefoniche ai danni di Patricia McDonough, che aveva sporto denuncia indicando una sommaria descrizione del possibile colpevole e la targa del suo veicolo. Durante le indagini, la polizia, che aveva cominciato a sospettare di Smith, solo attraverso l'utilizzo del pen register device istallato senza mandato presso la compagnia telefonica della vittima era riuscita a risalire alla utenza di Smith, e, quindi, ad incriminarlo formalmente. Secondo il giudice Blackmun, le previsioni contenute nel Quarto emendamento sono infrante dagli atti del Governo che acquisiscono, senza mandato, le informazioni che siano all'interno del reasonable expectation privacy test. Ma all'interno di tale categoria non possono evidentemente essere ricomprese tutte le informazioni che sono volontariamente affidate alle compagnie telefoniche, e che sono ad esse necessarie per svolgere la propria attività commerciale: i numeri telefonici delle utenze chiamate, che risultano a disposizione di tali compagnie, non sono dunque dati sensibili coperti dalla protezione costituzionale garantita dal Quarto emendamento.

62 Sebbene la protezione della privacy digitale sia oggi regolata negli Stati Uniti da numerose leggi ordinarie (tra cui, ad esempio, il Privacy Act del 1974, poi emendato dal Computer and Privacy Act del 1988, e – più recentemente - Electronic Communications Privacy Act del 2008) colpisce in ogni caso come, secondo la dottrina della *third party*, i cittadini americani sembrano non godere della tutela *costituzionale* rispetto a una serie di azioni quotidiane (che vanno dal pagamenti elettronici, alla corrispondenza e alle comunicazioni digitali, e all'uso di reti informatiche) che per loro natura implicano la trasmissione di informazioni a soggetti terzi. Come ricordato da M. TOKSON, *Autonomation and the Fourth Amendment*, 96 IOWA L. REV., 2011, p. 585 ss., infatti, «The Third Party Doctrine precedents, and Smith in particular, are problematic in an age where an ever-growing proportion of personal communications and transactions are carried out over the Internet. Internet users, now comprising eighty percent of U.S. citizens, generate enormous amounts of personal data online, virtually all of it accessible to third-party Internet service providers ("ISPs") or websites. E-mails, web-surfing histories, credit card and address information, and search term records are all routinely stored by online entities and are potentially available to the government, or even to private parties that purchase customer information for marketing purposes. With the Fourth Amendment inapplicable to this mass of easily obtainable personal information, government investigators could monitor the communications of individuals and organizations on an unprecedented scale».

è compatibile con il quadro generale delle libertà garantite dal Quarto emendamento, in virtù del fatto che la raccolta di metadati telefonici «does not involve searching the property of persons making telephone calls», e «the volume of records does not convert that activity into a search»[63]. Infine, anche a voler ritenere che la raccolta dei metadati costituisca una perquisizione ai sensi del Quarto emendamento, essa incontrerebbe gli standard di ragionevolezza elaborati dalla Corte, perché a fronte del legittimo interesse del Governo a garantire la sicurezza del suo territorio, la riservatezza dei cittadini appare intaccata in modo minimo e marginale[64].

Nonostante tali affermazioni si fondino su un precedente giurisprudenziale, i dubbi sulla legittimità del Bulk Metadata Surveillance Program non sono stati completamente dissipati. In primo luogo, pur non essendo assimilabili alla registrazione del contenuto delle telefonate, la straordinaria quantità di metadati immagazzinati dall'NSA nei sette anni di vita del programma è in grado di rivelare informazioni sensibili di un vasto numero di cittadini americani. Inoltre, sotto il profilo giuridico, sebbene il caso *Smith* costituisca sicuramente un precedente vincolante per il controllo di costituzionalità del Bulk Metadata Surveillance Program, è importante ricordare che i due casi presentano differenze sostanziali circa la finalità delle indagini: se in *Smith* lo scopo delle indagini riguarda l'accertamento della verità processuale nel caso di un delitto già commesso, il fine del programma NSA è quello di prevenire attentati terroristici.

5. Il Bulk Metadata Surveillance Program di fronte ai giudici federali: «an almost-Orwelian tecnology» o «a legitimate tool to interdict terrorist threats»?

Le difficoltà interpretative sulla costituzionalità del Bulk Metadata Surveillance Program sono emerse in tutta la loro evidenza in due recenti decisioni delle Corti federali dei distretti di Columbia e New York, che, pur chiamate a risolvere casi analoghi, sono giunte a conclusioni opposte.

In entrambi i casi, i ricorrenti avevano eccepito l'illegittimità del programma governativo, chiedendo – in qualità di clienti delle compagnie telefoniche intercettate, che l'NSA sospendesse

[63] Cfr. Section 215 White Paper, cit., p. 20.

[64] Secondo il Governo, infatti, l'indagine condotta nell'ambito del programma contestato «would satisfy the reasonableness standard that the Supreme Court has established in its cases authorizing the Government to conduct large-scale, but minimally intrusive, suspicionless searches», in quanto, secondo quanto sostenuto dalla Corte nel caso *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013), tale standard richiede un bilanciamento tra «the promotion of legitimate Governmental interests against the degree to which [the search] intrudes upon an individual's privacy». In questo caso, prosegue il Governo, « Such a balance of interests overwhelmingly favors the Government in this context» perché «if any Fourth Amendment privacy interest were implicated by collection of telephony metadata, which does not include the content of any conversations, it would be minimal». Cfr. Section 215 White Paper, cit., p. 20.

la racconta dei metadati associati alle loro utenze, e distruggesse le informazioni già raccolte. Pur fondandosi su ricorsi del tutto speculari i due casi sono stati decisi in modo diverso: mentre in *Klayman v. Obama* il giudice R. Leon ha accolto le ragioni dei ricorrenti ordinando all'NSA di interrompere il programma, in *ACLU v. Clapper* il giudice W.J. Pauley III lo ha ritenuto costituzionalmente legittimo. Dalle differenti letture emerge tutta la tensione esistente tra la necessità di tutelare la liberà dei cittadini da un lato e la loro sicurezza dall'altro.

In *Klayman v. Obama*[65], la Corte federale del Distretto di Columbia ha deciso che l'indiscriminata e arbitraria raccolta di metadati telefonici disposta dall'NSA costituisce a tutti gli effetti una illegittima perquisizione ("search") vietata dal Quarto emendamento. Nel dichiarare l'incostituzionalità del programma, il giudice Leon ha innanzitutto dovuto distanziarsi dai parametri delineati dalla Corte nel caso *Smith*, precisando che sarebbe irragionevole giudicare le abitudini telefoniche dei cittadini di oggi con i criteri di trentaquattro anni fa[66], perché la rivoluzione digitale ha stravolto il nostro rapporto con la tecnologia e moltiplicato le capacità del Governo di acquisire ed immagazzinare dati sensibili informatizzati[67]. Sebbene infatti il tipo di informazioni ricavabili dai metadati odierni non sia troppo dissimile a quello che era possibile acquisire con i pen register devices[68], «the ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly*, what that information can tell the Government about people's lives»[69]. Per il giudice Leon, in definitiva, non è possibile solcare le acque inesplorate del Quarto emendamento utilizzando come stella polare un caso che è stato deciso prima dell'invenzione dei telefoni cellulari[70], perché «the almost-Orwellian technology»[71]

---

[65] *Klayman v. Obama*, Civ. Us. Colu. Dist. Court, n. 13-0851, decisa il 16 dicembre 2013 e disponibile in http://sensenbrenner.house.gov/uploadedfiles/klayman_v._obama.pdf

[66] Id., p. 53: «people in 2013 have an entirely different relationship with phones than they did thirty-four years ago».

[67] Così, ad esempio, il giudice Leon ricorda che «Cell phones have also morphed into multi-purpose devices. They are now maps and music players (…) They are cameras (…) They are even lighters that people hold up at rock concerts (…) They are ubiquitous as well. Count the phones at the bus stop, in a restaurant, or around the table at a work meeting or any given occasion. Thirty-four years ago [when *Smith* was decided], *none* of those phones would have been there … [instead], city streets were lined with pay phones … when people wanted to send "text messages," they wrote letters and attached postage stamps» (cfr. *Klayman v. Obama*, p. 51)

[68] La sentenza afferma (p. 52) «what metadata *is* has not changed over time. As in *Smith*, the *types* of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like», anche se, come osservato nella nota 57 della sentenza, i metadati possono oggi «unlike thirty-four years ago, reveal the user's location».

[69] Id., p. 52.

[70] Id., p. 55: «I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones»

oggi a disposizione del Governo americano pone i giudici di fronte ad uno scenario che, nel 1979, «was, at best, stuff of science fiction»[72].

Escludendo l'applicazione della *third party doctrine* elaborata in *Smith*, pertanto, la Corte federale si è trovata a dover risolvere il caso a partire dal *reasonable expectation privacy test*, verificando concretamente la ragionevolezza delle pretese dei ricorrenti. Anche sotto questo profilo, la sentenza fonda le proprie argomentazioni sull'impatto che l'era digitale e l'utilizzo quotidiano e costante dei telefoni cellulari ha avuto sulla società; l'avvento della c.d. "cell phone-centric culture" e il rapido mutare delle nostre abitudini hanno drasticamente accresciuto l'importanza che i metadati rivestono nelle nostre vite, perché «records that once would have revealed few scattered tiles of information about a person, now revealed an entire mosaic – a vibrant and constantly updating picture of person's life»[73].

A sostegno di tali argomentazioni, il giudice Leon ha utilizzato le argomentazioni sviluppate in *United States v. Jones* (2012) in cui la Corte suprema ha disposto l'incostituzionalità dell'utilizzo da parte dell'FBI di dispositivi GPS a lungo raggio per tracciare i movimenti dei veicoli sospetti. In quel caso la maggioranza dei giudici aveva osservato che l'impatto straordinario delle nuove tecnologie sulla privacy dei cittadini chiedeva ai giudici di ponderare attentamente le violazioni della loro riservatezza non solo alla luce di precedenti test giurisprudenziali, ma prestando anche attenzione al mutato contesto sociale e tecnologico; e così, pur non superando espressamente la giurisprudenza *Smith*, alcuni giudici hanno sostenuto che la *third party doctrine* meriterebbe forse di essere ripensata alla luce dell'era digitale, perché non tutte le informazioni che i cittadini/utenti rivelano a terzi soggetti devono essere, per questa sola ragione, escluse dalla protezione del Quarto emendamento[74]. Appoggiandosi a tali osservazioni[75], il giudice Leon fonda le proprie

---

[71] Id., p. 49: «the almost-Orwellian technology that enables the Government to store and analyze the phone data of every telephone user in United States is unlike anything that could have been conceived in 1979».

[72] Id. p. Il giudice precisa così che (p. 55) «When do present-day circumstances — the evolution of the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies — become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like Smith simply does not apply? The answer, unfortunately for the Government, is now».

[73] Id. p. 54.

[74] In *United States v. Jones*, 132 S. Ct. 945 (2012), cinque giudici hanno riconosciuto come l'espansione delle nuove tecnologie impone di ripensare alle modalità di applicazione del Quarto emendamento. In questo senso, il giudice Alito nella sua concurring opinion ha specificamente ricordato che «the daily business of living one's life creates a digital record with privacy implications» e che – ad esempio - «cell phones and other wireless devices now permit wireless carriers to track and record the location of users — and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States» (Id. 963, J. Alito concurring). Ancora più specificamente, il giudice Sotomayor precisa che «in light

argomentazioni sulla specificità del caso di specie, rilevando che se il compito dei giudici è quello «di difendere la privacy e la sicurezza degli individui dall'arbitraria ed indiscriminata ingerenza dei pubblici ufficiali governativi»[76], non vi è dubbio che «il sistematico controllo e registrazione dei metadati costituisca una indiscriminata ed arbitraria invasione della privacy dei cittadini americani» contraria al grado di riservatezza immaginato dagli padri costituenti del Quarto emendamento[77].

Del tutto opposta è la conclusione raggiunta, poche settimane più tardi, dalla Corte del secondo distretto di New York in *ACLU v. Clapper*, che ha respinto un ricorso presentato dalla ACLU sostenendo la piena legittimità del Bulk Metadata Surveillance Program[78]. La differente

---

of the level of intrusiveness represented by modern technology, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties» perché « "I would not assume that all information voluntarily disclosed to some member of the public (third party) for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection» (Id. 957 J. Sotomayor concurring). Infine lo stesso giudice Leon ricorda nella sentenza *Klayman* che i giudici in *Jones* hanno rilevato l'incostituzionalità dell'utilizzo di sensori GPS a lungo termine per monitorare i movimenti di Jones «without questioning the validity of the Court's 1983 decision in United States v. Knotts, that the use of a tracking beeper does not constitute a search because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another"», e osservando piuttosto come «they emphasized the many significant ways in whitch the short the short-range, short-term tracking device used in Knotts differed from the constant month-long surveillance achieved with the GPS device attached to Jones's car» (cfr. *Klayman*, p. 45). In questo modo il giudice Leon giustifica, anche alla luce di un analogo caso deciso dalla Corte suprema, il suo distinguishing dal caso *Smith*.

[75] Dubbi sull'incostituzionalità del Bulk Metadata Surveillance Program in forza delle considerazioni sviluppate dalla Corte suprema nel caso *Jones* erano già state avanzate da J.D. MORNIN, *NSA Metadata Collection and the Fourth Amendment*, 29 Berkeley Tech. L.J. 2014, p. 1005: «The NSA metadata collection program falls within the area of concern that the five Justices in Jones identified. As explained above, metadata collection - particularly on a large scale and over long periods of time - can be equally or more revealing than the content of conversations. The Justices stopped short of calling into question the rationale underlying the third-party doctrine, although Justice Sotomayor argued strongly that the doctrine should receive especially close judicial scrutiny given, the types of data and tools for analysis now available to law enforcement».

[76] Così il giudice Leon ricorda che «in reaching this decision, I find comfort in the statement in the Supreme Court's recent majority opinion in *Jones* that "[a]t bottom, we must assur[e] preservation of the degree of privacy and security of individuals against government that existed when Fourth Amendment was adopted". Indeed as the Supreme Court noted more than a decade before *Smith* "the basic purpose of th[e Forth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against *arbitrary invasions by governmental officials*"» (cfr. *Klayman v. Obama*, p. 63).

[77] Id. p. 64: «I cannot imagine a more "indiscriminate" and "arbitrary invasion" of privacy than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on "that degree of privacy" that the Founders enshirined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware "the abridgement of freedom of the people by gradual and silent encroachments by those power", would aghast».

[78] V. *ACLU v. Clapper*, Us. NY South Dist. Court,. 13 Civ. 3994 del 27 12 2013, disponibile in http://www.nysd.uscourts.gov/cases/show.php?db=special&id=364..

impostazione risulta evidente fin dall'incipit della decisione, la quale, soffermandosi con una certa enfasi sulle drammatiche conseguenze dell'attentato dell'11 settembre del 2001, osserva che un più efficiente utilizzo dei sistemi informatici da parte delle agencies federali avrebbe potuto forse evitare la tragedia e prevenire l'attacco, in quanto «telephony metadata would have furnished the missing information and might have permitted the NSA to notify the FBI of the fact that Al Mihdhar [ovvero uno dei responsabili dell'attentato n.d.r.] was calling the Yemeni safe house from and inside the United States»[79]. Fin da subito, pertanto, il giudice Pauley poggia la sua decisione sul pilastro costituzionale della sicurezza nazionale, puntando l'attenzione sulla necessità per il Governo di imparare dai propri errori e di ricorrere ad ogni misura necessaria a prevenire futuri attacchi.

Partendo da questa prospettiva, il giudice Pauley ha innanzitutto analizzato il programma di raccolta dei metadati telefonici sotto il profilo legislativo, ritenendolo legittimo perché condotto in conformità ai limiti e agli standard probatori contenuti dalla sezione 215 del Patriot Act. In secondo luogo, dal punto di vista generale, la Corte ha fatto notare che il controllo del Congresso e delle sue commissioni sull'operato del Governo dimostrano una unità di intenti degli organi costituzionali nella guerra al terrorismo internazionale; il fatto che il ramo legislativo abbia ripetutamente prorogato la validità della sezione 215 del Patriot Act, ad esempio, testimonia la comune valutazione dei poteri federali nel considerare ancora attuale la minaccia terroristica, e giustifica quindi anche l'adozione di misure straordinarie (tra cui appunto la creazione di database digitali) che sono necessarie agli agenti dell'NSA per ricostruire quelle relazioni segrete tra organizzazioni terroristiche che altrimenti non sarebbe stato possibile rintracciare. Se è vero infatti che la raccolta dei metadati disposta dal Governo è particolarmente ampia, occorre ricordare che ciò è giustificato dal fatto che le indagini contro-terroristiche si discostano profondamente dalle investigazioni criminali, in quanto – a differenza di queste ultime – sono necessariamente preventive e dunque scontano un grado di imprecisione strutturale perché vi è modo di conoscere con esattezza metadati saranno utili a tali investigazioni prima di averli concretamente raccolti[80]. L'ampiezza delle intercettazioni è dunque strutturalmente legata alla

[79] Id., p. 2.

[80] Id. p. 35-36: «The new ability to query aggregated telephony metadata significantly increases the NSA's capability to detect the faintest patterns left behind by individuals affiliated with foreign terrorist organizations. Armed with all the metadata, NSA can draw connections it might otherwise never be able to find. The collection is broad, but the scope of counterterrorism investigations is unprecedented. National security investigations are fundamentally different from criminal investigations. They are prospective – focused on preventing attacks – as opposed to the retrospective investigation of crimes».

loro utilità concreta; per questo, conclude la Corte, «Congress was clearly aware of the need for breadth and provided the Government with the tools to interdict terrorist threats»[81].

Quanto ai profili di costituzionalità, il giudice Pauley rileva innanzitutto che, secondo la Corte suprema, i cittadini non hanno una legittima aspettativa di privacy sui numeri telefonici che compongono. Diversamente da quanto deciso dal giudice Leon, Pauley ricava dunque da *Smith v. Maryland* i parametri costituzionali per risolvere il caso; gli utenti telefonici, infatti, sono tutti a conoscenza del fatto che le compagnie di telecomunicazione registrano i metadati relativi alle loro comunicazioni, che vengono immagazzinati per ragioni commerciali e di sicurezza del sistema. Tale circostanza annulla la pretesa di privacy dei cittadini su tali informazioni, perché – come già ricordato in *Smith* – «when a person voluntary gives information to a third party, he forfeits his right to privacy in the information»[82]. A nulla vale, in questo senso, la considerazione per cui il database dei metadati possa costituire «un ricco mosaico di informazioni personali» sulla vita dei cittadini[83]; il fatto stesso i metadati siano raccolti in registri di proprietà delle compagni telefoniche dimostra come essi abbiano in realtà già rinunciato alla privacy su tali informazioni. Del resto, ricorda il giudice Pauley, ogni giorno la gente consegna volontariamente dati personali alle multinazionali che li utilizzano per scopi commerciali, ma nonostante il fatto che tali informazioni siano ben più rilevanti ed invasive dei metadati telefonici, solo pochissime persone sembrano preoccuparsene[84].

Seguendo questa interpretazione, pertanto, la Corte si discosta dalla decisione *Klayman*, sostenendo che, sebbene l'uso moderno dei telefoni cellulari abbia drasticamente cambiato le abitudini dei cittadini, il caso in esame riguarda esclusivamente l'utilizzo di metadati che – come riconosciuto dallo stesso giudice Leon[85] – non sono cambiati nel corso degli anni, e che racchiudono lo stesso tipo di informazioni che la Corte suprema si era trovata a giudicare nel

[81] Id., p. 36.
[82] Id., p. 42.
[83] Secondo la ricorrente ACLU, infatti, «the analysis of bulk telephony metadata allows the creation of a rich mosaic: it can "reveal a person's religion, political associations, use of a telephone-sex hotline, contemplation of suicide, addiction to gambling or drugs, experience with rape, grappling with sexuality, or support for particular political causes"» (cfr. Id. p. 40).
[84] Id., p. 51.
[85] Come ricodato anche *supra*, nota 64.

caso *Smith v. Maryland*[86]. Per questo, conclude il giudice Pauley, «because Smith controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment»[87].

6. Tra Security e Privacy. Conclusioni

Le rivelazioni di Snowden sui programmi di controllo della NSA hanno riacceso in America il dibattito sulla protezione della privacy nell'era digitale e sui limiti della c.d. guerra tecnologica, mettendo in discussione l'opportunità di tecniche investigative che possono certo risultare fortemente invasive della riservatezza dei cittadini, ma che allo stesso tempo potrebbero rivelarsi come l'unico strumento idoneo a garantire la loro sicurezza. L'eco internazionale del *Datagate*, peraltro, ha generato più di un imbarazzo all'amministrazione Obama, che si è a lungo prodigata nel rassicurare i cittadini americani circa la necessità di tali operazioni autorizzate e condotte nell'esclusivo interesse della nazione.

Nonostante tali rassicurazioni, le preoccupazioni sollevate dai media hanno interrogato anche l'esecutivo che – pur riaffermando con forza la necessità di predisporre sistemi di controllo delle comunicazioni – ha recentemente ricordato in una direttiva esecutiva i rischi connessi ad un utilizzo indiscriminato di tale controllo, invitando gli operatori ad agire con il massimo rispetto possibile dei diritti di riservatezza e privacy[88]. In questa prospettiva, lo stesso Presidente Obama ha annunciato possibili modifiche nella procedura di raccolta ed immagazzinamento dei metadati, ipotizzando che i database siano in futuro conservati da non ancora identificate "terze parti" invece che da agenzie governative, e disponendo un rafforzamento i poteri ispettivi dell'Attorney

[86] Del resto, ricorda il giudice Pauley, (p. 42) «The collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search».

[87] Id., p. 44.

[88] Cfr. Presidential Policy Directive/Ppd-28 - Signals Intelligence Activities, 17 gennaio 2014, in http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities, adottata a seguito delle conclusioni raggiunte dal già citato Report Liberty and Security In a Changing World (cfr. *supra*): «Advanced technologies can increase risks, as well as opportunities, however, and we must consider these risks when deploying our signals intelligence capabilities. The IC conducts signals intelligence activities with care and precision to ensure that its collection, retention, use, and dissemination of signals intelligence account for these risks. In light of the evolving technological and geopolitical environment, we must continue to ensure that our signals intelligence policies and practices appropriately take into account our alliances and other partnerships; the leadership role that the United States plays in upholding democratic principles and universal human rights; the increased globalization of trade, investment, and information flows; our commitment to an open, interoperable and secure global Internet; and the legitimate privacy and civil liberties concerns of U.S. citizens and citizens of other nations».

General sulle richieste presentate dall'Intelligence americana ai giudici del FISC[89]. Più di recente, il Presidente americano ha ufficialmente riaffermato la necessità di sospendere l'acquisizione automatica dei metadati telefonici e la creazione di database governativi, invitando a rivedere quanto prima le procedure in esame[90]. Il Congresso, infine, sta discutendo una serie di modifiche del FISA e del PATRIOT Act volte a rendere più stringente il controllo sull'operato delle agencies governative[91], ma è troppo presto per prevedere quale sarà l'esito e gli effetti di questa riforma legislativa[92].

---

89 Vedi il discorso presidenziale del 17 gennaio 2014, riportato da http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

90 Cfr. *Statement by the President on the Section 215 Bulk Metadata Program*, 27 marzo 2014, in http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program. Tale documento è stato salutato dalla stampa come una precisa presa di posizione del Presidente contro il Bulk metadata collection program, in quanto egli ha ricordato che «having carefully considered the available options, I have decided that the best path forward is that the government should not collect or hold this data in bulk. Instead, the data should remain at the telephone companies for the length of time it currently does today. The government would obtain the data pursuant to individual orders from the Foreign Intelligence Surveillance Court (FISC) approving the use of specific numbers for such queries, if a judge agrees based on national security concerns». Tuttavia, nello stesso documento, il Presidente Obama ha anche statuito che «Given that legislation has not yet been enacted, and given the importance of maintaining the capabilities of the Section 215 telephony metadata program, the government has sought a 90-day reauthorization of the existing program». Con tale richiesta Obama ha dunque di fatto avvallato la richiesta ai giudici del FISC di prorogare di ulteriori novanta giorni la validità del Bulk Metadata Program, e analoghe richieste sono state ulteriormente presentate il 20 giugno (http://www.justice.gov/opa/pr/joint-statement-office-director-national-intelligence-and-department-justice-declassification) e il 13 settembre (http://thehill.com/policy/technology/ 217618-spy-court-renews-nsa-program).

91 Esigenza, questa, messa in luce anche dalla dottrina, che ha osservato come «the NSA may well have good reasons to analyze large troves of telephony metadata, but section 215 seems like an awkward way to do it. Congress should enact new legislation that specifically authorizes the program and describes the limits under which it may operate. In fact, Congress is on the verge of making substantial changes to the metadata program as this article goes to press. The legislation would effectively transform it from a programmatic surveillance initiative that involves bulk collection to a more familiar individualized surveillance tool that only allows the NSA to obtain call records from phone companies if the FISA court concludes that they are associated with a "specific selection term" (such as an individual phone number)». Cfr. N.A. SALES, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*, 10 ISJLP, 2014, p. 550.

92 Cfr, in particolare, la discussione del progetto di legge Sen. 1599 presentato dal Senatore Patrick Leahy (USA Freedom Act) che modificherebbe il PATRIOT Act e il FISA ridefinendo confini molto più stretti per le intercettazione governative. Cfr. https://beta.congress.gov/bill/113th-congress/senate-bill/1599. Come osservato tuttavia, l'approvazione di tale progetto è oggetto di uno scontro politico/istituzionale particolarmente acceso, e mentre la versione votata alla Camera sembra tradire le attese di chi si aspettava un deciso cambio di rotta (cfr. *The NSA bill got to the House at warp speed. Senators are our only hope*, in *Guardian*, 22 maggio 2014, http://www.theguardian.com/commentisfree/2014/may/22/nsa-reform-bill-passed-house-usa-freedom-act-senators-only-hope), la recente versione discussa al Senato pare maggiormente restrittiva per il Governo (Privacy-Boosted Freedom Act Introduced in Senate, in USnews,29 luglio 2014, *http://www.usnews.com/news/articles/2014/07/29/patrick-leahy-introduces-privacy-boosted-*

Se sul piano politico le future implicazioni del *Datagate* sono ancora tutte da verificare, sotto il profilo costituzionale il dibattito sui metadati telefonici ha già interrogato gli interpreti sulla portata del Quarto emendamento. Analogamente a quanto avvenuto nelle Corti federali, anche la dottrina si è così divisa tra i difensori della sicurezza nazionale, la cui tutela giustifica una parziale compressione dei diritti dei cittadini[93], e quelli della privacy, che hanno invece enfatizzato i rischi legati alla creazione illimitata di database indefiniti[94].

Dal punto di vista dell'interpretazione costituzionale, il caso *Smith* (e la *third party doctrine*) pare costituire il precedente più simile al caso in esame, perché certamente i metadati raccolti dal Governo contengono informazioni in già possesso delle compagnie telefoniche. D'altro canto, però, tale giurisprudenza appare troppo risalente per costituire un precedente completamente vincolate, e se pure è vero che le informazioni contenute oggi nei metadati sono analoghe a quelle registrate nel 1979 dai *pen register devices*, è quanto meno logicamente bizzarro risolvere un caso giuridico sulla base di argomentazioni che sono antecedenti la stessa invenzione del telefoni cellulari. Del resto, in termini generali, anche i giudici della Corte suprema paiono ultimamente più orientati a ripensare ai parametri di applicazione del Quarto emendamento: come ricordava il

usa-freedom-act). In ogni caso, data la complessità e la delicatezza politica della materia, è improbabile che la riforma sia effettivamente discussa e votata prima delle elezioni di midterm del novembre 2014.

93 Così, ad esempio, ad avviso di J. YOO, *The Legality of the National Security Agency's Bulk Metadata Surveillance Programs* (Dicembre 2013), Harv. J. of Law and Pub. Pol. (in corso di pubblicazione), disponibile su http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2369192 p. 2, il programma di sorveglianza NSA «does not fall within the Congress's autorization for foreign intelligence and couter terrorism surveillance», e quindi «it would most likely rest within President' Commander in Chief autority». In ogni caso, conclude l'A., anche a voler considerare il programma NSA sottoposto al controllo del Congresso secondo le disposizione di FISA, esso «does not violate the Forth Amendment as currently interpreted by the federal courts». In modo non dissimile anche R. DE, *The NSA and Accountability in an Era of Big Data*, 7 J. Nat'l Sec. L. &Pol'y, 2014, p. 310: «Big data is transforming the world in which NSA carries out its mission, but NSA is constantly evolving in terms of the mix of technology, resources, skills, and authorities necessary to take advantage of its opportunities and meet its challenges. What remains constant is NSA's commitment to the law; to the notion that how the Agency conducts its activities is just as important as whether it is authorized to conduct them. Although much of the detail by necessity must remain secret, a great deal gets lost in the public discourse about the legal framework within which NSA conducts its mission, its requirement for specifically tailored and externally approved minimization procedures, and the robust oversight structures in place across all three branches of government. These features are as much a part of the reality in which NSA operates today as is the reality of big data».

94 V. L. K. DONOHUE, *Bulk Metadata Collection: Statutory and Constitutional Consideration*, cit., che anticipando la decisione del giudice Leon ha messo in luce le differenze tra il caso Smith e l'attuale programma di controllo ed immagazzinamento dati dell'NSA, ricordando peraltro il parziale cambiamento di argomentazioni operato dalla Corte Suprema nei casi *Jones* e *Killo*. Analogamente, E. ATKINS, *Spying on Americans: At What Point Does the NSA's Collection and Searching of Metadata Violate the Fourth Amendment*, cit., p. 87: «The metadata information the Government is able to collect, store, and search on a massive scale makes Section 215 a violation of the Fourth Amendment. The Fourth Amendment is clear: to search a constitutionally protected area, one must have probable cause and obtain a warrant from a detached and neutral judge. That is not being done under the metadata program».

giudice Sotomayor nel caso *Jones*, infatti «it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties» poiché «this approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks»[95]. Pur non costituendo parte vincolante della decisione, le parole del giudice Sotomayor riecheggiano quelle ormai famose con cui il giudice Brandeis quasi cento anni fa ammoniva la Corte ad aprire gli occhi di fronte all'insorgere delle nuove tecnologie[96]. Come già avvenuto in passato, quindi, la Corte sarà probabilmente chiamata a ridiscutere la propria giurisprudenza alla luce delle nuove tecnologie, e i casi nati a seguito del *Datagate* potrebbero costituire in futuro l'occasione per chiarire l'ambito e la portata del Quarto emendamento nell'era digitale.

Anche l'eventuale superamento della giurisprudenza *Smith*, tuttavia, non sarebbe sufficiente a risolvere tutti i problemi legati al difficile bilanciamento tra sicurezza e privacy nell'era del terrorismo globale. È vero infatti che l'evolversi della tecnologia è in grado di fornire al Governo formidabili strumenti di controllo della popolazione, e che le rivelazioni di Snowden hanno riportato alla memoria degli americani episodi della loro storia che, dal caso Watergate ai dossier di Hoover, testimoniano la pericolosità intrinseca nell' utilizzo incontrollato di tali strumenti. D'altro canto, tecnologie sempre più sofisticate sono oggi a disposizione non solo dei governi ma anche di larga parte della popolazione mondiale, e il loro utilizzo ha reso possibili operazioni terroristiche su larga scala. Detto altrimenti, è proprio la diffusione globale della tecnologia digitale a rendere necessario il controllo stringente delle reti di comunicazione da parte dei governi, perché per individuare ed isolare una comunicazione terrorista dalle moltissime altre occorre innanzitutto raccogliere un volume significativo di informazioni; come efficacemente ricordato, «per trovare il proverbiale ago occorre prima raccogliere il pagliaio che gli sta attorno»[97].

---

[95] *United States v. Jones*, cit., J. Sotomayor concurring.

[96] Cfr. la dissenting opinion del caso *Olmstead* su cui vedi *supra* in particolare nota 49.

[97] Così J. ROBINSON JR., *The Snowden Disconnect: When The Ends Justify The Means*, 21 aprile 2014, diponibile in http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427412, p. 7: «U.S. government maintains that collecting metadata is not invasive and also that it is not protected under the third party doctrine from Smith v. Maryland. Also, claims the government, mass collection of metadata is necessary because the government does not always know beforehand which communications involve foreign terrorists. That is, "identify[ing] potential terrorist communications ... requires collecting and storing a large volume and high percentage of information about unrelated communications." Therefore, the argument goes, the government must collect everything so that they can find what they are looking for after the fact. According to the NSA, collecting Americans' metadata in this way is legal because there are "reasonable grounds to believe" that such collection is relevant to international terrorism investigations. To find the needle, you must collect the haystack around it».

In definitiva, dunque, pur essendo innegabile la pericolosità intrinseca nella raccolta indiscriminata dei metadati telefonici da parte dei Governi, è vero anche che, come ricordato dal giudice Pauley, il diritto di privacy non può essere assoluto perchè «the Bill of Right is not a suicide-pact»[98].

Alla luce di tutto ciò, come è possibile trovare il giusto equilibrio tra privacy e security nell'era del terrorismo digitale? In che modo proteggere la riservatezza dei cittadini senza compromettere con eccessive limitazioni la sicurezza loro e della nazione? Come testimonia la storia americana, la risposta a queste domande non è univoca, e segue un andamento costante che vede ampliarsi considerevolmente i poteri del Governo ogni volta che la minaccia terroristica è più pressante, per comprimersi a vantaggio della privacy una volta che essa diventa meno attuale. Inoltre, l'adozione di strumenti di controllo invasivi è tanto più tollerata quanto più è stringente il nesso tra essa e la sua funzione, e il loro utilizzo è dunque spesso commisurato alla loro concreta efficacia. In questa prospettiva, anche la legittimità del Bulk Metadata Surveillance Program è stata in parte misurata dai giudici federali a partire dalla sua *funzionalità* e alla luce del principio di *ragionevolezza* che rappresenta «the ultimate touchstone of the Fourth Amandment»[99].

Proprio sotto questo profilo si riscontrano, a ben guardare, le principali differenze tra le sentenze *Klayman* e *Clapper*; al di là dalle divergenti ricostruzioni dei precedenti giurisprudenziali, infatti, ciò che più colpisce è il differente parere delle due Corti circa l'utilità pratica del programma governativo rispetto alla lotta al terrorismo, da cui deriva – inevitabilmente – un diverso giudizio di ragionevolezza circa la pertinenza di tale programma rispetto allo scopo a cui è preposto.

In *Clapper*, infatti, il giudice Pauley ha ricordato che la raccolta dei metadati telefonici costituisce uno strumento «importante e irrinunciabile» per combattere la guerra al terrorismo, finalizzato a rintracciare comunicazioni altrimenti irrintracciabili e a prevenire i tragici eventi del passato[100]. Dal momento che non vi sono prove che il Governo utilizzi il programma per fini diversi da quello dichiarato[101], e poiché è realmente funzionale a proteggere la sicurezza dei cittadini

[98] Come osservato dal giudice Jackson nella sentenza *Terminiello v. City of Chicago* 337 U.S. 1 (1949) e riportato dal giudice Pauley nelle conclusioni della sentenza *ACLU v. Clapper*, p. 51.

[99] Così le conclusioni di *Aclu v. Clapper* (p. 51): «whether the Fourth Amendment protects bulk telephony metadata is ultimately a question of reasonableness. *Missouri v. McNeely*, 133 S. Ct. 1552, 1569-70 (2013) ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness")».

[100] Cfr. *Aclu v. Clapper*, cit., p. 52: «No doubt, the Bulk Metadata collection program vacuums up information about virtually every telephone call to, from, or within the United States. That is by design, as it allows the NSA to detect relationships so attenuated and ephemeral they would otherwise escape notice. As September 11th attacks demonstrate, the cost of missing such a thread can be horrific».

[101] Id., (p. 50-51) «there is no evidence that the Government has used any of the bulk telephony metadata it collected for any other purpose other than investigating and disrupting terrorist attacks».

americani[102], esso deve essere dichiarato legittimo dalle Corti, il cui compito è «to reject as false, claims in the name of civil liberty which, if granted, would paralyze or impair authority to defend [the] existence of our society, and to reject, as false, claims in the name of security which would undermine our freedoms as open the way to oppression»[103].

Profondamente diverso è invece, nel merito, il giudizio della Corte di Columbia nel caso *Klayman*. A dispetto di quanto sostenuto dal Governo, per cui la raccolta di metadati è indispensabile per prevenire futuri attacchi, il giudice Leon ha ritenuto che, ad una più attenta analisi, il ricorso a tale strumento sia in realtà funzionale ad ottenere *più rapidamente* informazioni che potrebbero essere acquisite ugualmente con gli strumenti investigativi tradizionali[104]. Il Governo, inoltre, non è riuscito a spiegare *in che modo* la raccolta, l'immagazzinamento e l'analisi dei metadati telefonici sia servita *concretamente* a sventare un attentato terroristico; al contrario, secondo il giudice, permangono seri dubbi «about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in case involving imminent threats of terrorism», e pertanto «the NSA's bulk collection program is indeed an *unreasonable* search under the Fourth Amendment»[105].

Per entrambi i giudici l'argomento cardine delle rispettive decisioni si fonda quindi sulla (*ir*)*ragionevolezza* del Bulk Metadata Surveillance Program rispetto alla sua ratio. Prima ancora che in una diversa interpretazione *astratta* delle norme sulla privacy, la discordanza tra le due Corti sembra così poggiare su una differente valutazione *concreta* dell'efficacia dell'azione dell'NSA. Per il giudice Pauley non vi sono dubbi che il programma contestato sia funzionale allo scopo per cui è stato istituito; al contrario per il giudice Leon la raccolta indiscriminata, generalizzata e vastissima di metadati personali dei cittadini costituisce una prova tangibile della sproporzione dell'azione governativa. Partendo da una diversa valutazione sull'utilità del programma, le due Corti giungono quindi a risultati diversi circa la sua (ir)ragionevolezza, e dunque rispetto alla sua (in)costituzionalità.

---

[102] Id., p. 52: «Technology allowed al-Qaeda to operate decentralized and plot international terrorist attack remotely. The bulk telephony metadata collection program represents the Government's counter-punch».
[103] Id., p. 52-53.
[104] Cfr. *Klayman v. Obama*, cit., p. 59: «the Government asserts that the Bulk Telephony Metadata Program serves the "programmatic purpose" of identifying unknown terrorist operatives and preventing terrorist attacks"(…). A closer examination of record, however, reveals that the Government's interest is a bit more nuanced – it is not merely to investigate potential terrorists, but rather, to do so *faster* than other investigative methods might allow».
[105] Id., p. 62.

Sotto il profilo contenutistico è difficile stabilire con esattezza quale dei due giudizi sia più pertinente alla realtà. Da un lato il Governo americano ha ripetutamente assicurato ai suoi cittadini che l'utilizzo dei loro metadati è strettamente finalizzato alla loro protezione, che il controllo dei giudici del FISC è sufficiente ad impedire ogni abuso, che grazie a questo programma l'Intelligence è stata capace di sventare numerosi attacchi terroristici in patria e nel mondo[106]. Il Bulk Metadata Surveillance Program, in particolare, è nato per correggere gli errori di comunicazione tra agenzie federali messi in luce dalla Commissione 9/11, ed è quindi uno strumento indispensabile per assicurare la sicurezza nazionale, perché, come ricordato dal direttore della NSA Keith Alexander, «there is no other way we know of to connect the dots»[107].
D'altra parte, però, l'utilità e l'importanza del Bulk Metadata Surveillance Program è stata recentemente contestata da un'indagine commissionata dalla New American Foundation, i cui risultati hanno ridimensionato moltissimo il ruolo giocato dalla raccolta dei metadati telefonici nella prevenzione delle attività terroristiche, evidenziando invece come i metodi di investigazione tradizionale si siano rivelati decisamente più efficaci[108]. La mole di dati raccolti preventivamente dalla NSA, inoltre, è certamente imponente e forse sproporzionata rispetto all'identificazione di

[106] Come ricordato dal Presidente nel discorso alla nazione del 17 gennaio 2014 l'Intelligence americana «Relationships with foreign intelligence services have expanded and our capacity to repel cyber attacks have been strengthened. And taken together, these efforts have prevented multiple attacks and saved innocent lives – not just here in the United States, but around the globe» http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html. Analogamente, il direttore dell'NSA Keith Alexander ha testimoniato presso il Congresso americano lo scorso 13 dicembre sostenendo che «the information gathered from these programs provided the US Government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world».

[107] Come riportato da *NSA chief on spying programs: "There is no other way to connect the dots"*, in *The Guardian – on line*, 13 dicembre 2013, http://www.theguardian.com/world/2013/dec/11/nsa-chiefs-keith-alexander-senate-surveillance, il Gen. Alexander ha espresso la necessità di avere un numero sufficiente di informazioni immagazzinate per poi essere in grado di ricercare e ricostruire i nessi tra i sospettati e i nuclei terroristici prima che essi compliscano gli obiettivi.

[108] Cfr. I risultati sono raccolti nel report P. BERGEN, D. STERMAN, E SCHEIDER, B. CAHAL, *Do NSA's Bulk Surveillace Programs Stop Terrorism?*, New American Foudation Report, Gennaio 2014, in http://www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists, «However, our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, (…) appears to have played an identifiable role in initiating, at most, 1.8 per cent of these cases».

comunicazioni tra terroristi, e nulla impedisce oggi che – come già avvenuto in passato nella storia americana – una volta raccolti ed immagazzinati i metadati acquisiti, essi siano segretamente impiegati per fini diversi da quello di tutelare la sicurezza nazionale.

In definitiva, dunque, l'equilibrio costituzionale tra privacy e security in America non sembra definibile una volta per tutte da regole astratte, ma dipende invece da circostanze concrete legate a diversi fattori. Più che nella Costituzione questo equilibrio va quindi cercato nella realtà, analizzando cioè elementi quali la funzionalità dei programmi di intelligence, la loro efficacia nel contesto del terrorismo tecnologico, la loro concreta invadenza delle libertà dei cittadini, soppesando le ragioni del Governo alla luce dei principi di proporzionalità e ragionevolezza.

Ancora una volta il diritto americano sembra insegnarci a guardare i fatti prima che le norme perché – come ricordava un grande studioso di questo sistema giuridico – «corrisponde ad una concezione mitologica del diritto pensare che le parole di documenti giuridici quali i testi degli articoli della Costituzione degli Stati Uniti posseggano un loro significato intrinseco»[109]. È seguendo tale insegnamento che occorre studiare i limiti e il significato del Quarto emendamento nell'era digitale, verificando cioè non nelle norme astratte ma nella realtà giuridica vivente quale equilibrio tra security e privacy sia possibile garantire concretamente.

[109] G. BOGNETTI, *Lo spirito del costituzionalismo americano*, *vol. I. La Costituzione liberale*, Torino, 2000, p. 112.