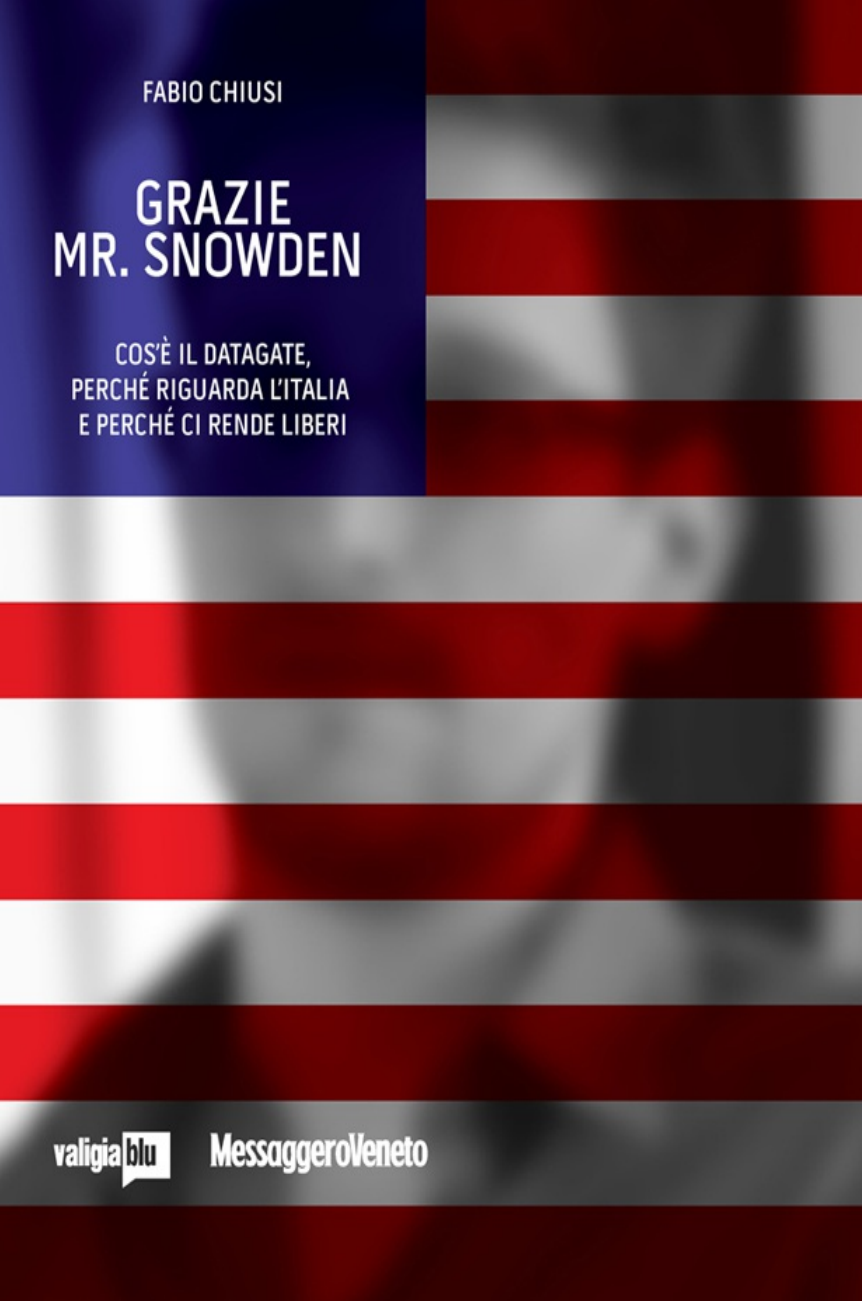
FABIO CHIUSI
GRAZIE
MR. SNOWDEN
COS'È IL DATAGATE,
PERCHÉ RIGUARDA L'ITALIA
E PERCHÉ CI RENDE LIBERI
valigia blu
MessaggeroVeneto

Fabio Chiusi

Grazie Mr. Snowden

Cos'è il Datagate,
perché riguarda l'Italia
e perché ci rende liberi

Un'iniziativa editoriale di Messaggero Veneto in collaborazione con Valigia Blu

http://messaggeroveneto.gelocal.it/
http://chiusinellarete-messaggeroveneto.blogautore.repubblica.it/
http://www.valigiablu.it/

Editing: Matteo Pascoletti e Vincenzo Marino
Copertina: Marco Tonus
Realizzazione tecnica: Fabio Di Donna

Fabio Chiusi

Classe 1980, udinese, dopo un master in Storia e filosofia della scienza presso la London School of Economics ha aperto il blog ilnichilista.com e cominciato a lavorare come giornalista freelance. Attualmente collabora con le testate locali del gruppo Espresso, il settimanale l'Espresso, Wired Italia e La Lettura del Corriere della Sera, oltre a gestire un blog sul sito del Messaggero Veneto (chiusinellarete-messaggeroveneto.blogautore.repubblica.it). È autore di diversi saggi sul rapporto tra tecnologia e società, tra cui "Critica della democrazia digitale" (Codice, marzo 2014).

INTRODUZIONE

Milioni di cittadini trattati come sospetti terroristi e spiati senza riguardo della legge. Capi di Stato, leader politici, uomini d'affari intercettati al telefono o violati nelle loro comunicazioni private. Accordi segreti per l'accesso alle banche dati dei principali colossi *web*, costretti a obbedire alle richieste governative senza poterne rivelare l'esatta estensione, o direttamente a loro insaputa. Il traffico internet copiato direttamente dai cavi sottomarini che trasportano le connessioni e immagazzinato, analizzato, dall'India al Brasile, passando per Germania, Spagna, Francia e Italia. Ma anche il deliberato indebolimento degli standard crittografici che rendono possibile mantenere sicure le nostre transazioni finanziarie online così come le comunicazioni in chat, i contenuti pubblicati sui social network, gli scambi via mail. E le intrusioni informatiche a danno dell'Onu e dei partner europei, lo spionaggio commerciale del gigante petrolifero Petrobras, l'intrusione ai danni di Al Jazeera, il controllo delle abitudini sessuali online dei diffusori di «idee radicali» (così da poterne compromettere la reputazione) e delle *community online* di giochi come *World of Warcraft*. Il tutto affogato da una massa di bugie, silenzi, promesse elettorali infrante, minacce a giornalisti. E tanta, tantissima opacità in luogo della sbandierata trasparenza.

Tutto questo, e molto altro, è lo scandalo che in Italia

abbiamo definito «Datagate». Ossia, ciò che è emerso e continua a emergere dai documenti *top secret* sottratti all'*intelligence* statunitense dell'Nsa (National Security Agency) dal suo ex analista, Edward Snowden, e pubblicati a partire da giugno da *Guardian*, *Der Spiegel*, *Washington Post* e in seguito *New York Times*, *El Mundo*, *Le Monde* e *L'Espresso*. Una vicenda già esplosiva, che ha scatenato incidenti diplomatici a ripetizione, reazioni indignate (ma ipocrite) dei capi di Stato europei, un mutato atteggiamento dell'opinione pubblica nei confronti del rapporto tra sicurezza e privacy (oggi, a prescindere dal colore politico, la bilancia pende molto meno dalla parte della prima). Senza contare i timidi e meno timidi propositi di riforma, della cui opportunità si sono finalmente accorti anche il presidente Barack Obama e i vertici dell'*intelligence*.

Resta ancora molto da sapere e capire, se è vero che ciò che conosciamo non rappresenta che una minima parte di quanto contenuto nel materiale prelevato dall'ex *contractor* dell'Nsa. Eppure qualcosa si può già dire. Prima di tutto, le accuse mosse all'*intelligence* appaiono molto più solide delle sue smentite. Da un lato ci sono prove documentali e testimonianze dirette, dall'altro la parola di vertici di istituzioni incapaci di replicare nel merito, scoperte a mentire (e ad ammetterlo, più o meno velatamente) o, più semplicemente, intente a porre la questione della sorveglianza digitale di massa in termini talmente vaghi da risultare imperscrutabili, sottraendole così al vaglio della ragione. Finora non risultano pubblicazioni indiscriminate di masse di documenti tali da mettere a

repentaglio le operazioni dell'*intelligence* nel mondo o addirittura la «sicurezza nazionale» degli Stati Uniti. A fronte delle affermazioni dell'Nsa, che vorrebbero oltre 50 piani terroristici sventati grazie all'imponente apparato di controllo impiegato, risultano molte più smentite (dati alla mano, questa volta) che conferme, come ha scritto *Pro Publica*. E come ha confermato, dopo un'accurata analisi caso per caso, il think tank "New America Foundation".[1]

Anzi, uno dei messaggi principali da trarre dalla vicenda è una domanda seria e articolata sull'efficacia dell'idea che per tutelare la sicurezza dei propri cittadini si debba mettere sotto sorveglianza il mondo intero, per giunta senza badare alle regole (proprie o di altri paesi). Domanda che, tuttavia, discende da una ancora più radicale sull'opportunità del progetto dell'Nsa, sulla sua compatibilità stessa con l'idea di un paese libero nel senso in cui intendiamo la parola «libertà» nelle più avanzate democrazie occidentali. Perché scorrendo i documenti di Snowden ci si trova di fronte a un ecosistema composto da due gambe, una costituita da colossi privati, l'altra da programmi dell'*intelligence*, che reggono entrambe sullo stesso presupposto: la loro sussistenza si fonda su una raccolta sempre più bulimica e al contempo mirata di dati, il petrolio della nostra era. È un modo per conciliare l'equilibrio economico e quello politico. Ma ciò che entrambe queste gambe reggono è un sistema che non differisce di molto rispetto a quello in atto nei regimi autoritari che gli Stati Uniti, in questi anni, hanno condannato come «nemici del libero *web*» e delle libertà civili. O almeno, questa è la spiacevole sensazione: che le differenze siano molto più sfumate

rispetto a prima dello scandalo. Cambiano gli acronimi, ma tra il Sorm russo e il Prism statunitense (insieme a tutti gli altri programmi di sorveglianza), tutto sommato, non c'è una differenza qualitativa: si registra tutto, e la legge troppo spesso finisce per diventare una formalità che in qualche modo si può sempre sbrigare prima che diventi un intralcio.

Un altro insegnamento che già possiamo trarre dal Datagate è che la reazione di larghi settori dell'opinione pubblica soffre di due pericolose premesse concettuali, derivanti in parte dal trattamento mediatico del caso e in parte dal clima culturale in cui siamo immersi. La prima è il determinismo tecnologico, l'idea arrendevole che siccome una tecnologia può fare *x*, allora *x* si dovrà necessariamente verificare nella storia. Nel caso Nsa, se l'*intelligence* dispone di abbastanza capacità di raccolta, immagazzinamento e analisi dei dati da registrare e computare ogni comunicazione al telefono o in rete, allora è normale, scontato lo faccia. Può, quindi deve. È un'idea avversata anche dallo stesso Snowden nel suo *Manifesto per la verità* pubblicato da *Der Spiegel*: «il fatto che le tecnologie di spionaggio esistano non basta a determinare che siano utilizzate, né tantomeno come». Altrimenti dal piano descrittivo si passa al normativo, e dalla cronaca si finisce per giungere a una giustificazione politica, addirittura *morale*, di quanto accade.

Le tecnologie sono costrutti umani, non dati di natura: contengono la metafisica di chi le ha create, le premesse concettuali, le convinzioni, gli scopi degli ingegneri informatici che le hanno predisposte. Accettare il determinismo tecnologico significa mettere

il futuro della democrazia nelle mani di tecnici del tutto svincolati dal controllo degli elettori e molto spesso perfino degli eletti. E si giunge alla seconda pericolosa premessa: il riduzionismo tecnologico. Perché la politica a questo modo si riduce ad algoritmo, a scelta obbligata. E se il calcolo restituisce il risultato per cui la privacy individuale è solamente un intralcio nel cammino della storia, non stupisce che siano così tanti ad accettarne la dipartita prima ancora che esali l'ultimo respiro. Senza rendersi conto, oltretutto, che il prossimo ostacolo da rimuovere in quel percorso è la politica stessa.

Lo scandalo Nsa dovrebbe costringere a fermarci e riflettere sul modo acritico con cui abbiamo accettato il predominio di così tante tecnologie in così tanti aspetti delle nostre vite. Se accettando i termini di utilizzo di servizi come Facebook, Google e Apple non siamo in grado di metterci al riparo da intrusioni di qualunque tipo (e in qualunque tempo, dato che non sappiamo in che modo i dati raccolti oggi potranno essere usati contro di noi tra dieci o vent'anni) da parte dei governi, anche di quelli democratici, è forse giunto il momento di ripensare il contratto sociale su cui l'uso di questi servizi si fonda. Se il «tutto gratis» si tramuta in un incubo di controllo e insensatezza, forse è il caso di ridiscuterlo. Se l'architettura di Internet così come la conosciamo non porta inevitabilmente alla libertà, alla condivisione egualitaria, alla partecipazione, all'inclusione come ci hanno raccontato presunti «guru» per decenni, ma consente al contrario una sorveglianza invisibile, pervasiva e potenzialmente totalitaria forse è il caso di cambiarla – non a caso si inizia a parlare di infrastrutture di rete a codice aperto, di utilizzo diffuso

delle più avanzate tecniche di cifratura, di modalità per scomparire dalla rete, più che di essere sempre visibili, presenti.

Lo hanno scritto in molti, in questi mesi, ma credo valga la pena ribadirlo: la rete così come la conosciamo è a un punto di svolta con il Datagate. Perché il Big Data e il *cloud computing* si basano sulla fiducia: che quei dati raccolti in massa, e immagazzinati nei server delle aziende per liberare i nostri hard disk e renderli ubiqui, siano computati nel rispetto delle regole che le società democratiche si sono date *offline* come *online*, non in base all'inutile tautologia per cui «le spie spiano» (quindi tutto è lecito?) o a una presunta (ma mai esplicitata) differenza tra i diritti di un uomo quando è un utente di Internet e quando è un cittadino del mondo «reale». Oggi quella fiducia per molti si è rotta, con conseguenze in termini di *governance* globale di Internet, di geopolitica ma anche di puri e semplici affari: già diversi studi sostengono, per esempio, che il danno all'industria della «nuvola informatica» nei soli Stati Uniti sia stimabile tra i 35 e gli oltre 100 miliardi di dollari.

Ciò che va ridisegnato non è solo l'equilibrio tra sicurezza e libertà – compito già di per sé arduo. È anche l'economia basata sui nostri dati, che produce al contempo pubblicità personalizzate (Amazon che ci consiglia proprio il libro che ci interessa, per esempio) e sorveglianza di massa. Due lati di una stessa medaglia, per una moneta che ha accontentato tutti: i consumatori, che fruiscono di servizi gratuiti e focalizzati proprio su *ciascuno di loro*; le aziende, che ne

ricavano copiosi introiti; i governi, che possono controllare i loro cittadini, sempre. Ma si è scoperto nel dettaglio, anche e soprattutto grazie al Datagate, quanto entrambi i lati costringano al pensiero spiacevole che la vera cifra della nostra epoca non sia la liberazione tramite la tecnologia, ma un punto di equilibrio retto su una servitù volontaria e in molti casi inconsapevole dei cittadini nei confronti dei loro nuovi sovrani digitali. Mi auguro che il racconto delle pagine seguenti sia letto come il tentativo di aumentare questa consapevolezza, per iniziare una riflessione collettiva e critica su come invertire la rotta prima che sia troppo tardi. Di certo è il modo in cui l'ho inteso.

CAPITOLO I: GIUGNO

Sorveglianza di massa delle comunicazioni telefoniche

Il Datagate inizia ufficialmente il 6 giugno 2013 con lo scoop del *Guardian* firmato da Glenn Greenwald: «la National Security Agency sta attualmente raccogliendo le documentazioni telefoniche di milioni di utenti Verizon sulla base di una ingiunzione top secret emanata in aprile». La richiesta della Foreign Intelligence Surveillance Court all'operatore è di fornire i «metadati» sulle utenze per chiamate all'interno degli Stati Uniti o dagli Usa all'estero per il periodo dal 25 aprile 2013 al 19 luglio 2013, «su base quotidiana e senza interruzioni». Scrive Greenwald:[2]

> Il documento dimostra per la prima volta che sotto l'amministrazione Obama i dati delle comunicazioni di milioni di cittadini statunitensi vengono raccolti indiscriminatamente in massa – indipendentemente dal loro essere sospettati di alcun illecito.

Secondo Greenwald, l'Nsa registra il numero di telefono di chi chiama e di chi risponde, da dove chiamino e ricevano la telefonata, la durata e l'ora della chiamata, i numeri di serie che identificano i telefoni coinvolti; non il contenuto delle telefonate né l'identità delle persone al telefono.

I risvolti per la privacy, argomenta il quotidiano londinese, si possono facilmente ricavare:

> L'amministrazione [Obama, *ndr*] sottolinea che l'ingiunzione ottenuta dal *Guardian* riguarda i dati delle chiamate, e non consente al governo di ascoltare le telefonate. Tuttavia, nel 2013, i metadati ottenuti forniscono alle autorità una ampia conoscenza dell'identità del chiamante. In particolare, una volta incrociati con gli archivi pubblici, i metadati possono rivelare nome, indirizzo, patente di guida, storia creditizia, numero di sicurezza sociale e altro. Gli analisti del governo sarebbero in grado di determinare se la relazione tra le due persone sia abituale, occasionale o un evento unico.

Come spiega James Ball (*Guardian*) per l'amministrazione Usa la privacy non ha niente a che vedere con questi metadati,[3] non più di leggere mittente e destinatario su un pacco postale o una lettera. Una concezione criticata dagli attivisti per la tutela della riservatezza personale, in testa Eff[4] e Aclu:[5] quest'ultima ha definito la sorveglianza dell'Nsa «oltre l'orwelliano». Mentre il giudizio della Corte d'Appello sul caso Stati Uniti vs Maynard aveva evidenziato in precedenza:

> Una persona che sappia tutto degli spostamenti di un altro individuo può dedurre se va in Chiesa ogni settimana, se è un forte bevitore, se va regolarmente in palestra, se è un marito infedele, se è un paziente sottoposto a cure mediche, se è coinvolto in qualche gruppo politico e non solo uno di questi fatti personali, ma tutti questi fatti personali.

Il giudizio è coerente con il risultato di uno studio,[6] pubblicato a marzo e condotto dal Mit e dall'Università di Louvain, in Belgio, sulla difficoltà di mantenere

anonimi i metadati prodotti da cellulari. Il *data journalist* del *Guardian* (ed ex membro del team di Wikileaks) ricorda che lo scopo dell'Nsa è, più dell'identificazione del singolo individuo, il «*data mining*»: usare algoritmi che, sfruttando l'imponente mole di dati raccolti, siano in grado di dedurre comportamenti «inusuali» o sospetti e dunque prevenire attacchi terroristici o smantellare organizzazioni criminali. Possedere tutte queste informazioni, tuttavia, fornisce al governo «un potere di cui in precedenza era sprovvisto: sorveglianza facile e retroattiva», che consente alle autorità di percorrere storie individuali in qualunque momento. «In sostanza, siete osservati; il governo non sa solamente il vostro nome, mentre lo fa».

Bruce Schneier, tra i massimi esperti di sicurezza informatica e privacy al mondo, commentando su *The Atlantic* è allarmato da ciò che ancora non è stato scoperto: «non sappiamo se anche altre compagnie telefoniche [oltre a Verizon, *ndr*] hanno consegnato i loro dati all'Nsa. Non sappiamo se è stata una richiesta unica o continuamente reiterata». Ancora, non sappiamo quali dati esattamente maneggi l'agenzia per la sicurezza, a livello nazionale e internazionale; se abbia stretto degli accordi con i colossi del *web* o li sfrutti a loro insaputa, magari inserendo deliberatamente delle vie d'accesso nascoste («*backdoor*») negli strumenti di comunicazione (perfino senza che i rivenditori lo sappiano). Non sappiamo se questa sorveglianza si interfacci con quella operata da droni e videocamere (anche «intelligenti») e in che modo, per quanto vengano trattenuti questi dati e come

vengano trattati e utilizzati. E «c'è molto altro che non sappiamo, e spesso ciò che sappiamo è obsoleto». Per questo, conclude Schneier, abbiamo bisogno dei *whistleblower*, a cui Obama, e a questo punto non può certo essere un caso, dà una caccia senza precedenti.

Almeno una domanda di Schneier sembra trovare risposta: secondo il *Wall Street Journal*, infatti, le compagnie telefoniche coinvolte sarebbero tre, non una. Oltre a Verizon, la sorveglianza dell'Nsa riguarderebbe anche At&T e Sprint Nextel. Di mezzo ci sarebbero non solo le telefonate, ma anche le mail, le navigazioni online dei cittadini e le transazioni compiute secondo i dati forniti da tre compagnie di carte di credito, secondo le fonti del *Wall Street Journal*.

Se l'opinione pubblica ignora i fatti rivelati dal *Guardian*, la politica, invece, sapeva? «Tutti ne erano consapevoli da anni», riporta *The Hill*, «ogni membro del Senato». *Usa Today* ne aveva scritto già nel 2006, ma citando fonti coperte dall'anonimato e nessun documento. Visto alla radice, il problema è aver continuato lungo il solco tracciato dall'amministrazione di George W. Bush e dall'impostazione, dopo l'11 settembre, sulla sicurezza nazionale in funzione anti-terroristica.

Il 7 giugno, il giorno dopo lo *scoop* di Greenwald, il *Wall Street Journal* ripercorre le tappe fondamentali di questo processo a partire dal Patriot Act del 2001, con cui le autorità si arrogavano il diritto di registrare dati telefonici senza passare dal giudice; il *New York Times* fornisce una cronologia in forma di infografica della sorveglianza elettronica durante le amministrazioni Bush e Obama. Lo stesso giorno, il *Daily Beast* rivela che

i metadati sono condivisi con l'*intelligence* britannica: «in pochi e discreti casi», scrive riportando le parole di ufficiali presenti e passati dell'*intelligence* statunitense, «l'Nsa ha condiviso analisi non redatte della documentazione ottenuta con la sua controparte britannica», il Gchq.[7]

Sorveglianza di massa delle comunicazioni online

Per capire quale ruolo giochi Prism nel Datagate, occorre fare un passo indietro, allo scoop del *Washington Post* (anch'esso del 6 giugno):

> La National Security Agency e l'Fbi si inseriscono direttamente nei server centrali di nove colossi statunitensi del web, estraendone chat audio e video, fotografie, e-mail, documenti e log di connessione che consentono agli analisti di tracciare bersagli stranieri.

Lo rivela un documento «*top secret*» consistente in quarantuno *slide*, datate aprile 2013, a uso dell'*intelligence*; fonti dell'Nbc confermano. Il programma Prism, fino a questo momento segreto, è in corso dal 2007 e da allora ha conosciuto «sei anni di rapida crescita nella raccolta dei dati». Le aziende coinvolte sono: Microsoft, Yahoo, Google, Facebook, Pal Talk, Aol, Skype, YouTube e Apple. Tutte le compagnie che hanno deciso di rispondere pubblicamente negano di sapere di che si tratti e respingono qualunque coinvolgimento. Come nota David Meyer su *Gigaom*, tuttavia, è il governo a non aver negato l'esistenza di questo canale diretto segreto.[8] Siamo in presenza di una sorveglianza elettronica effettuata senza passare da un giudice? Ne scrivono anche Greenwald ed Ewen MacAskill sul *Guardian*, rivelando particolari inquietanti:

> Diversamente dalla raccolta delle documentazioni telefoniche, questa sorveglianza può includere il contenuto delle comunicazioni e non solo i metadati. […] Prism […] apre la possibilità che le comunicazioni fatte interamente in

> suolo statunitense siano tracciate senza ordinanza giudiziaria.

Anche il consenso dei colossi *web* non sembra necessario: «il programma Prism», si legge infatti, «consente all'agenzia di impadronirsi direttamente e unilateralmente delle comunicazioni contenute sui server delle aziende». Riassumendo cosa cambi dal punto di vista operativo nella lotta al terrorismo per comunicazioni anche fuori dal territorio statunitense (ma avvenute tramite cavi americani), i due giornalisti scrivono:

> Se in precedenza l'Nsa aveva bisogno di autorizzazioni individuali, e della conferma che tutte le parti in causa si trovassero fuori dagli Stati Uniti, ora hanno solamente bisogno del ragionevole sospetto che una delle parti sia fuori dal Paese quando i dati sono stati raccolti dall'Nsa.

Gli autori dettagliano anche l'incremento nel numero di comunicazioni ottenute nel 2012: del 248% per Skype, del 131% per i dati di Facebook e del 63% per quelli di Google.

Su *Gigaom*, è ancora David Meyer a sottolineare la mancanza di credibilità degli Stati Uniti verso la promozione delle libertà civili *online*. Se già fino a ieri gli Stati Uniti potevano essere accusati di ipocrisia rispetto alla loro politica di promozione dei *social media* e delle tecnologie di rete come strumenti di democrazia e libertà, oggi sarà ancora più difficile per l'amministrazione Obama condannare censura e sorveglianza di massa nei regimi autoritari. Del resto, mentre l'ex vicepresidente Al Gore definisce i programmi di sorveglianza di massa appena rivelati

«oscenamente offensivi», l'amministrazione Obama li difende a spada tratta. Il direttore dell'Nsa, James Clapper, li definisce «importanti e totalmente legali», affermando che i resoconti di *Guardian* e *Washington Post* sarebbero pieni di errori, anche se Clapper non entra nello specifico. Giudica addirittura le pubblicazioni «riprovevoli», poiché rischiano di procurare «danni irreversibili» alla capacità degli Stati Uniti di «identificare e rispondere» alle tante minacce cui è sottoposto il Paese. Come già nel caso delle rivelazioni di Wikileaks, il problema è chi le pubblica, non il loro contenuto.

Risulta debole la difesa di Obama: ribadisce che «nessuno ascolta le vostre telefonate» e che il governo Usa non detiene l'identità di chi chiama e riceve le chiamate controllate. Prism «non si applica ai cittadini statunitensi», ha aggiunto (le inchieste giornalistiche dicono il contrario), ricordando come il contestato programma abbia ricevuto più volte lo scrutinio e il via libera del Congresso (ma non dell'opinione pubblica).[9] Il paragone con il Grande Fratello, dice Obama, regge solo «in astratto»; il sacrificio della privacy sarebbe «modesto» secondo il presidente (difficile usare un aggettivo simile per una sorveglianza indiscriminata e di massa di un'intera popolazione). Particolarmente infelice poi l'uscita sulle fughe di notizie: «*I don't welcome leaks*», non sono benvenute, ha detto Obama, forse dimenticando che il processo a Chelsea Manning, fonte di Wikileaks, è in quel momento in corso di svolgimento.[10]

Per quanto riguarda le implicazioni di quanto emerso finora, un primo bilancio può essere affidato a

Cindy Cohn, direttore legale dell'Eff, che dichiara a *The Verge*:

> Ci sono tre modi per fermare tutto questo [...]. L'esecutivo potrebbe dire «basta, lo fermiamo». Il Congresso potrebbe costringerlo a fermarsi in un modo o nell'altro, o passando una legge contro (il programma di sorveglianza) o definanziandolo. Un terzo modo è che le corti emanino un'ingiunzione stabilendo che è illegale o incostituzionale.

La fonte è Edward Snowden

È il 9 giugno quando il *Guardian*, su decisione del diretto interessato, rivela la propria fonte degli *scoop* sull'Nsa. Si tratta del ventinovenne Edward Snowden: ex assistente tecnico della Cia, un passato alla stessa agenzia dell'*intelligence* e un presente alla Booz Allen Hamilton e altri *contractor* della difesa. «Non ho intenzione di nascondermi perché non ho fatto niente di male», dice al quotidiano londinese, che già lo annovera tra i *whistleblower* più importanti della storia statunitense insieme a Daniel Ellsberg (cui dobbiamo la conoscenza dei *Pentagon Papers*) e lo stesso Manning. Snowden sostiene di averlo fatto unicamente per «informare il pubblico», di essere conscio che i media lo «demonizzeranno» e cercheranno di «personalizzare» il dibattito e di non desiderare alcuna attenzione mediatica. Avrebbe copiato i documenti tre settimane fa, dall'ufficio Nsa delle Hawaii, dove lavorava. Da allora si trova a Hong Kong, in una stanza d'albergo in cui cerca di proteggersi dal rischio di essere spiato. Come visto, il suo timore per una reazione da parte delle autorità Usa è più che giustificato.

Emerge un forte attaccamento di Snowden al valore della libertà della Rete e in particolare al preservare la privacy degli utenti *online*:

> Afferma che un tempo vedeva Internet come «la più importante invenzione di tutta la storia umana». Da adolescente, ha trascorso giornate intere «parlando con persone di ogni tipo di vedute che non avrei mai incontrato da me». Ma crede che il valore di Internet, insieme con la privacy di base, stia venendo rapidamente distrutto dalla

> sorveglianza ubiqua. «Non mi vedo come un eroe», dice, «perché ciò che faccio è auto-interessato: non voglio vivere in un mondo in cui non c'è alcuna privacy e quindi nessuno spazio per l'esplorazione intellettuale e la creatività».

«Ciò che stanno facendo», dice dell'Nsa e del governo Usa, «pone un rischio esistenziale alla democrazia».

Da Prism a Boundless Informant

Il *Guardian*, intanto, continua le rivelazioni:

> La National Security Agency ha sviluppato un potente strumento per registrare e analizzare da dove provenga la sua *intelligence*, sollevando dubbi sulle sue ripetute rassicurazioni fornite al Congresso circa il non tenere traccia di tutta la sorveglianza che opera sulle comunicazioni americane.

Il «potente strumento» si chiama Boundless Informant. Il suo funzionamento è descritto in un documento *top secret* analizzato e pubblicato dal quotidiano londinese: permetterebbe di «dettagliare e mappare paese per paese l'enorme massa di informazioni raccolte da computer e reti telefoniche». A marzo 2013, Boundless Informant ha raccolto 97 miliardi di «elementi di *intelligence*» dalle reti informatiche globali, scrivono Glenn Greenwald ed Ewen MacAskill, tre da quelle statunitensi. Gli autori ricordano come il direttore dell'*intelligence* Usa, James Clapper, avesse negato di fronte alla commissione per l'*intelligence* del Senato di raccogliere «milioni di informazioni su cittadini americani». Ed è ancora così, risponde una portavoce dell'Nsa in relazione alla rivelazione di Boundless Informant.

Sviluppi sul caso Prism

Fonti interpellate da *Cnet*, che contraddicono quelle della Nbc, e un'analisi di *Business Insider* (che segnala anche alcune modifiche nello *scoop* del *Washington Post* su Prism, che ne annacquerebbero la portata), negano che l'*intelligence* statunitense abbia accesso diretto ai server delle aziende inizialmente menzionate nello scandalo, da Facebook a Google passando per Microsoft e Apple. Tutte, come visto, hanno ripetutamente negato alcun coinvolgimento nel programma di sorveglianza di massa Prism. Tuttavia, il *New York Times* sostiene che «almeno un po'» abbiano collaborato, a eccezione di Twitter. In particolare, a seguito di un incontro con esponenti del governo Usa in visita nella Silicon Valley, alcune avrebbero concesso «modifiche» per rendere più semplice il passaggio dei dati in loro possesso nelle mani della autorità; Google e Facebook avrebbero discusso un piano per costruire «portali sicuri» appositamente dedicati allo scopo.[11] Le aziende sono in ogni caso obbligate ad adempiere a tali richieste secondo il Foreign Intelligence Surveillance Act (Fisa): si tratterebbe solo di rendere più semplice il trasferimento dei dati.[12] *Zdnet* formula un'ipotesi sul funzionamento di Prism:

> Crediamo che l'ingiunzione Fisa [di cui il Transparency Report di Google, pur potenziato con i dati delle National Security Letters, non può recare traccia, *ndr*] abbia autorizzato l'Nsa a piazzare uno strumento di intercettazione della rete Tier 1 di Verizon, che ha aspirato efficacemente ogni bit e byte di dati transitati nei suoi *network*. Se fosse così, Verizon sarebbe stato costretto ad ottemperare, senza

> possibilità di appello. La chiave è cosa faccia davvero un Tier 1, come funzioni, e quali compagnie lo usino. Dato che tutte le compagnie [coinvolte nello scandalo, *ndr*] usano reti Tier 1, ciò che potrebbe essere accaduto è che i dati dei loro utenti siano stati sottratti a loro insaputa per il semplice fatto di essere connessi a Internet.

Le autorità statunitensi continuano intanto a difendere il proprio operato, e non solo. Secondo la *Reuters*, l'8 giugno un'agenzia dell'*intelligence* avrebbe chiesto l'apertura di un'inchiesta penale sulla fuga di notizie che ha portato agli scoop di *Guardian* e *Washington Post*. La richiesta è nelle mani del Dipartimento di Giustizia, si legge, che dovrà decidere se ci siano i presupposti per l'avvio dell'indagine giudiziaria. Il numero uno dell'*intelligence*, Clapper attacca nuovamente gli autori degli scoop e le loro fonti: le pubblicazioni sarebbero «incaute» e fuorvianti; impossibile dettagliare in che modo, ha argomentato, senza rivelare ulteriori informazioni riservate. Prism, contrariamente a quanto si è letto, non sarebbe un «programma di *data mining*», rispetterebbe le leggi vigenti e soprattutto «continua a essere uno dei nostri strumenti più importanti per la difesa della sicurezza nazionale».

La difesa delle autorità non convince l'organizzazione per i diritti umani Freedom House che, come anticipato dal *blog* *Future Tense* di *Slate*, ha penalizzato gli Stati Uniti nella classifica 2013 sulla libertà della rete. Nel frattempo si moltiplicano le analisi che inseriscono lo scandalo nell'ottica della perdita di credibilità dell'amministrazione Obama rispetto alla difesa del libero *web* e sull'assottigliarsi dei confini con democrazie immature e regimi autoritari (quanto al controllo della

rete). *The Atlantic* è durissimo: l'infrastruttura tecnica e giuridica messa in piedi da Bush e Obama costituisce esattamente l'apparato materiale e concettuale di cui abbisogna un tiranno. Non si può fondare uno Stato di diritto sulla presunzione che gli elettori non ne eleggano mai uno pronto a tramutare strumenti per la difesa della sicurezza nazionale in strumenti di dominio e repressione indiscriminata. La Cnn riassume i tre scenari possibili:

1. *Le cose non stanno come dicono i giornali*. Non c'è accesso diretto ai server delle aziende, non c'è sorveglianza indiscriminata e di massa, le informazioni vengono solamente trasferite sulla base di richieste specifiche e dopo un'ingiunzione apposita. È l'ipotesi di Declan McCullagh su *Cnet* e della stessa Nsa: Prism è un semplice strumento per processare dati dell'*intelligence*, come dice il nome stesso: «Planning Tool for Resource Integration, Synchronization, and Management». Non uno strumento di raccolta di informazioni, ma di organizzazione interna di informazioni già precedentemente ottenute, dunque. Chi dice il contrario ha male interpretato le *slide top secret* di cui sono entrati in possesso *Guardian* e *Washington Post*;[13]
2. *Le cose stanno come dicono i giornali, e le aziende, almeno alcune, sapevano*. Del resto che l'Nsa si stesse dotando del più grande (e preoccupante) *data center* per la sorveglianza al mondo è cosa nota almeno dalla storia di copertina di *Wired* del marzo 2012. È improbabile che le compagnie

ignorassero tutto, e non siano mai state chiamate a collaborare. Ma i dati in possesso delle aziende non sono crittati? Nessun problema, dice un esperto alla Cnn: il governo sarebbe in grado di decrittarli (accedendo ai loro server). La versione ritenuta più probabile dell'ipotesi è che all'interno delle singole aziende fossero in pochi a sapere, e che fosse richiesta massima segretezza;

3. Le aziende non sapevano, ma l'Nsa è entrata in possesso dei loro dati comunque. È lo scenario ipotizzato anche da *Zdnet*, e – precisa la Cnn – qualcosa di simile è già accaduto nel 2003. Tuttavia in caso di intrusione dell'*intelligence* «le aziende lo avrebbero scoperto in poco tempo».

Secondo il *Guardian*, una *slide* precedentemente non pubblicata ed estratta dal materiale *top secret* visionato contraddice la prima e la terza ipotesi. Nel documento Prism è distinto da «programmi che riguardano la "raccolta di dati durante passaggio su cavi in fibra ottica e infrastrutture"», concerne invece la raccolta «diretta» dai server delle aziende coinvolte. Per i sostenitori della versione dell'Nsa, insomma, non resta che aggrapparsi alla possibilità che le *slide* non siano corrette o particolarmente rilevanti, dovendo però spiegare, come detto, la ragione della loro massima segretezza.

Uno scandalo sempre più internazionale

A poco più di una settimana dall'articolo di Greenwald, il Datagate estende ulteriormente la portata degli attori e degli scenari coinvolti (consapevoli o no). Il 16 giugno il *Guardian*, servendosi ancora del materiale fornito da Edward Snowden, rivela che l'*intelligence* britannica (il Gchq), in collaborazione con quella statunitense, ha spiato le comunicazioni telefoniche e via Internet dei delegati agli incontri del G20 tenuti a Londra nell'aprile e settembre 2009. Secondo il quotidiano londinese l'*intelligence* è in grado di:

> - Predisporre Internet cafè dove ha utilizzato un programma di intercettazione delle email e un software di *key-logging* per spiare l'uso dei computer da parte dei delegati;
>
> - Fare breccia nella sicurezza dei BlackBerry dei delegati per controllarne messaggi via mail e telefonate;
>
> - Fornire a quarantacinque analisti resoconti in tempo reale ventiquattr'ore su ventiquattro su chi stesse telefonando e a quale destinatario durante il summit;
>
> - Sorvegliare il ministro delle finanze turco e potenzialmente quindici altri;
>
> - Ricevere rapporti da un tentativo dell'Nsa di intercettare il leader russo, Dmitry Medvedev.

Sempre lo stesso giorno, il *Guardian* scrive che l'*intelligence* britannica ha anche cercato di spiare i delegati di un incontro tra i vertici dei governi di membri del Commonwealth tenutosi a Trinidad nel 2009.

Il giorno prima, invece, *Cnet* ha spostato il dibattito

negli Stati Uniti sui livelli interni di autorizzazione: «la National Security Agency», scrive *Cnet*, «ha ammesso in un nuovo *briefing* riservato che non ha bisogno di un'autorizzazione giudiziaria per ascoltare le telefonate all'interno del paese». Il democratico Jerrold Nadler, si legge, ha rivelato in settimana, durante una sessione informativa segreta con i membri del Congresso che «gli è stato detto» che per accedere ai contenuti delle telefonate basterebbe «semplicemente» la decisione al riguardo di un «analista» dell'intelligence. «Nessun'altra autorizzazione di legge è richiesta», riporta il sito di notizie tecnologiche, citando ciò che ha appreso Nadler, che commenta: «ero piuttosto sorpreso». I funzionari anche «di basso rango» che possono ascoltare le telefonate dei cittadini sarebbero «migliaia». Ma non ci sono di mezzo solo le telefonate:

> La rivelazione di Nadler indica che gli analisti dell'Nsa potrebbero avere accesso ai contenuti delle comunicazioni via Internet senza precedentemente chiedere l'autorizzazione del giudice.

L'Nsa non ha inizialmente risposto alle richieste di *Cnet* di commentare le affermazioni di Nadler, che contraddicono l'idea del direttore dell'Fbi, Robert Mueller, secondo cui nessuna intercettazione sarebbe possibile senza autorizzazione specifica (per l'individuo e la singola telefonata) della Foreign Intelligence Surveillance Court.[14] Nelle ore successive alla pubblicazione, James Clapper, direttore dell'Nsa, smentisce ufficialmente *Cnet*: «l'affermazione per cui un singolo analista possa intercettare comunicazioni domestiche senza adeguata autorizzazione legale è

scorretta e non è stata comunicata al Congresso». Il democratico Nadler si dice «soddisfatto» che l'amministrazione abbia ribadito ciò che aveva «sempre creduto», ossia appunto che l'*intelligence* non possa ascoltare cittadini statunitensi senza autorizzazione. Come racconta l'*Huffington Post*, il pezzo di *Cnet*, in seguito aggiornato con un nuovo titolo per meglio rispecchiarne il contenuto, scrive Declan McCullagh, era stato accolto con scetticismo da alcuni commentatori.

Sul fronte dei livelli di autorizzazione, il 20 giugno il *Guardian* pubblica due documenti (di cui uno *top secret*) che mettono però in dubbio la smentita di Clapper:

> Documenti *top secret* inviati alla corte che supervisiona la sorveglianza dell'intelligence USA mostrano che i giudici hanno autorizzato ordini non specifici che consentono all'NSA di utilizzare informazioni 'inavvertitamente' registrate da comunicazioni interne agli Stati Uniti senza autorizzazione giudiziaria.

Il primo documento riguarda le procedure usate per sorvegliare cittadini non statunitensi, il secondo la minimizzazione della raccolta dati sugli statunitensi. Entrambi sono stati inviati alla corte segreta che ha il compito di valutare le richieste dell'*intelligence* prima che possa controllare un soggetto bersaglio. Scrive il *Guardian*:

> I documenti mostrano che perfino se sottoposte al giudizio delle autorità che governano la raccolta di *intelligence* straniera su bersagli stranieri, le comunicazioni degli statunitensi possono essere registrate, immagazzinate e usate, si legge.

In particolare, nonostante il regime legale del Fisa, l'Nsa può:

- Mantenere fino a cinque anni dati che possono potenzialmente contenere dettagli su cittadini statunitensi;

- Conservare e utilizzare comunicazioni domestiche «acquisite inavvertitamente» se contengono informazioni di *intelligence* utili, informazioni su attività criminali, minacce all'incolumità di persone o cose, informazioni crittate o che si ritiene contengano informazioni rilevanti per la *cybersecurity*;

- Preservare «informazioni di intelligence straniera» contenute in comunicazioni tra legali e clienti;

- Accedere al contenuto di comunicazioni raccolte da «macchine con sede negli Stati Uniti» o utenze telefoniche per stabilire se i bersagli si trovino negli Usa, con lo scopo di cessare ulteriore sorveglianza.[15]

Prism è solo la punta dell'iceberg

Sebbene l'attenzione si sia concentrata su Prism, tra le rivelazioni del *Washington Post*, come ricorda *Think Progress*, si menzionava un altro programma di sorveglianza: Blarney. Di che si tratta?

> Secondo il *Washington Post*, Blarney raccoglie metadati dai colli di bottiglia [«*choke point*», *ndr*] distribuiti lungo la dorsale [«*backbone*» , *ndr*] di Internet come parte di un «programma di raccolta in corso che fa leva sulla comunità dell'intelligence e le partnership commerciali per ottenere accesso e sfruttare intelligence straniera ottenuta dalle reti globali».

Nella *slide* pubblicata dal *Guardian*, Blarney figura, in opposizione a Prism, tra i sistemi di raccolta che si basano sull'intercettazione del flusso di dati mentre vengono trasmessi (*«Upstream»*). Un analogo per il traffico *online* di quanto rivelato sulla sorveglianza delle utenze Verizon nello scandalo Datagate nei giorni scorsi.[16] Di nuovo, il tutto è perfettamente coerente con i documenti e le ricostruzioni prodotte da Klein anni fa. Alla luce di quanto ha scritto *Cnet*, Blarney potrebbe essere uno degli strumenti tecnici attraverso cui si realizza la raccolta delle comunicazioni telefoniche senza autorizzazione giudiziaria.

Sono però le inchieste di *Bloomberg*, *Washington Post* e *Associated Press* a mettere Prism e Blarney nella più ampia prospettiva del funzionamento complessivo della macchina della sorveglianza di massa dell'Nsa. Come visto, nei giorni dello scoppio dello scandalo i colossi *web* coinvolti hanno ripetutamente negato di

essere alla conoscenza del programma Prism; Facebook e Microsoft hanno rivelato il numero di richieste mirate da parte del governo di dati degli utenti in loro possesso. Dati che tuttavia non dettagliano quali richieste siano dovute alla preoccupazione di tutelare la sicurezza nazionale (a norma del Fisa), come invece chiedono di poter comunicare Google, Facebook, Microsoft e Twitter. Così, mentre l'affermazione del direttore dell'Nsa Keith Alexander, secondo cui questi dati avrebbero consentito di sventare «dozzine» di piani terroristici, non trova sostegno empirico, *Bloomberg* rivela come sarebbero «migliaia» le aziende (del settore tecnologico, ma anche finanziario e manufatturiero) a collaborare con l'*intelligence* fornendo dettagli tecnici delle loro infrastrutture (anche in funzione di intrusione in computer "nemici"), ricevendone in cambio dei «benefici, tra cui l'accesso a *intelligence* riservata».

Si va a questo modo «molto oltre» quanto rivelato da Snowden, continua *Bloomberg*. Microsoft, per esempio, «fornisce alle agenzie di intelligence informazioni sui bug al proprio popolare software prima di rilasciarne in pubblico la risoluzione (*fix*)». Si torna inoltre a parlare di raccolta di dati senza passare dalle richieste del Fisa. Racconta *Bloomberg*, menzionando una delle fonti interpellate:

> Alcune compagnie di telecomunicazione statunitensi forniscono alle agenzie di intelligence accesso a infrastrutture e dati all'estero che richiederebbero un ordine del giudice se consentito all'interno degli Stati Uniti […]. In questi casi, non è necessario alcun controllo a norma del Fisa, e le aziende forniscono le informazioni su base volontaria.[17]

Gli accordi in questione, precisa *Bloomberg*, sono «legali» ma «vasti». E, soprattutto, sono conosciuti solo da pochi dirigenti all'interno di ogni singola azienda. In cambio della cooperazione, le compagnie otterrebbero la garanzia di essere tenute al riparo da cause civili riguardanti il passaggio delle informazioni.

Il tutto si aggiunge alla raccolta sui dati delle carte di credito e, come ha rivelato il *New York Times*, del Dna dei cittadini anche solo «potenziali sospetti» di crimini, così come al programma di catalogazione della sorveglianza globale Boundless Informant, e allo spionaggio elettronico di Cina e Hong Kong da parte degli Stati Uniti di cui Snowden ha finora solo parlato a voce in una intervista al *South China Morning Post*.

Anche per *Associated Press* siamo in presenza della punta dell'iceberg:

> Interviste con oltre una dozzina di attuali e precedenti ufficiali governativi, del settore tecnologico e di esperti mostrano che, se Prism ha attratto l'attenzione di recente, il programma in realtà non è che una parte relativamente piccola di un progetto di controllo molto più esteso e intrusivo.

Mentre Prism sarebbe un modo per «dare senso alla cacofonia del traffico Internet grezzo», il vero motivo di preoccupazione dovrebbe essere che l'intelligence si allacci al *backbone* della struttura della Rete per intercettare tutto il traffico in entrata e uscita dal Paese. Secondo le fonti di *Associated Press* sono due le «componenti vitali del successo di Prism»: la collaborazione delle aziende e, soprattutto, il suo inserirsi in un progetto di sorveglianza complessivo più ampio che «dura da anni». Il responsabile sarebbe

George W. Bush:

> Poco dopo gli attacchi terroristici dell'11 settembre [...] ha segretamente autorizzato l'Nsa ad allacciarsi ai cavi in fibra ottica che entrano ed escono dagli Stati Uniti, conscio del fatto che ciò avrebbe dato al governo un accesso senza precedenti e senza bisogno di ricorso all'autorità giudiziaria alle conversazioni private degli americani.

Nonostante la legge lo vieti, senza previa autorizzazione giudiziaria, l'Nsa a questo modo ha da allora accesso a «email, telefonate, video chat, navigazioni, transazioni bancarie e altro». «Servono computer potenti per decrittare, immagazzinare e analizzare tutte queste informazioni, ma i dati sono tutti lì, a sfrecciare alla velocità della luce». Dati che, in più, restano a tempo indeterminato a disposizione delle autorità per future indagini:

> Ciò che non è chiaro al pubblico è per quanto il governo trattenga i suoi dati. E questo è importante, perché gli Stati Uniti un giorno avranno un nuovo nemico. Tra due decenni, il governo potrebbe avere una raccolta di mail e documentazione telefonica degli statunitensi cui fare ricorso per indagare su qualunque cosa il Congresso dichiari costituire una minaccia alla sicurezza nazionale.

A dettagliare ulteriormente il sistema complessivo della sorveglianza telefonica e digitale prodotto da Bush è il *Washington Post*, che rivela aspetti inediti del programma Stellar Wind[18] e dei suoi quattro successori che «hanno portato gli americani e il territorio americano sotto il dominio dell'Nsa per la prima volta in decadi». Prism sarebbe uno di questi quattro programmi insieme a Nucleon (per intercettare il

contenuto delle telefonate) e ai sistemi di raccolta dei metadati telefonici e prodotti via *web* chiamati Marina e Mainway.

Sul funzionamento di Prism e sulla responsabilità di chi ridimensiona

Il punto più controverso resta il funzionamento di Prism.[19] Fanno discutere, in particolare, alcune correzioni da più parti evidenziate al resoconto iniziale del *Washington Post*, oltre che diverse fonti interpellate, che smentirebbero l'accesso «diretto» dell'intelligence ai *server* delle aziende menzionate nelle slide passate da Snowden ai giornalisti. Una posizione che si riassume nel ridimensionamento della portata dello scandalo Prism verso un travisamento scandalistico. Questo scetticismo si scontra però con le conferme fornite dalle fonti interpellate dalla Nbc, e più in generale con le affermazioni riportate dal democratico Nadler e da *Cnet*, con il quadro dipinto dalle dodici fonti ascoltate da *Associated Press*, con le informazioni diffuse al pubblico negli anni passati dal *whistleblower* Klein, con le parole di Snowden. E con il parere di uno dei massimi esperti di sicurezza informatica al mondo, Bruce Schneier: «dovete assumere che tutto sia intercettato». Se l'Nsa ha accesso indiscriminato a tutto il traffico Internet, la disputa sull'accesso «diretto» o meno ai server dei colossi *web* non muta nella sostanza l'entità della sorveglianza dell'intelligence sui cittadini Usa e non. Muta, questo di certo, rispetto alla responsabilità delle aziende coinvolte.

Riassume *Il Post*:

> L'espressione «accesso diretto», scrive il *Washington Post*, nel suo significato tecnico significa esattamente ciò che è stato scritto alla pubblicazione delle due inchieste, cioè che la Nsa avrebbe potuto entrare direttamente nei *server* delle aziende. Nel contesto può voler dire però un'altra cosa:

> «diretto» può significare che la Nsa riceve i dati che gli sono inviati direttamente dalle società informatiche, e quindi che non deve «intercettarli» come fa con altri sistemi di sorveglianza. Le inesattezze sono state corrette dal *Washington Post* dopo che era arrivata la smentita da parte delle aziende interessate [...]: con parole diverse, le aziende sono andate oltre i toni rituali di queste circostanze e hanno detto di non avere mai sentito parlare di Prism, di non avere mai concesso l'autorizzazione alla Nsa per accedere direttamente ai loro server, ma di avere collaborato solo in presenza di specifiche ordinanze di un tribunale federale, e solo caso per caso. Questo ha ridimensionato anche un'altra informazione che si è rivelata poi inesatta, cioè che le società di Internet «partecipassero consapevolmente» al progetto.

Scrive invece l'*Associated Press*:

> Ciò che l'Nsa chiamava Prism era conosciuto dalle aziende come un sistema semplificato che automatizzava e rendeva più facile l'*hoovering* [cioè la raccolta di dati, *nda*] degli anni precedenti [...]. Le compagnie [...] volevano ridurre il loro carico di lavoro. Il governo voleva dati in un formato strutturato, coerente che fosse semplice da navigare.

Se le richieste di cui le aziende erano a conoscenza a norma di legge erano tutto sommato poche migliaia e mirate (come pare di capire dai dati pubblicati), le fonti che raccontano di una sorveglianza indiscriminata senza previa autorizzazione giudiziaria fanno pensare che la differenza tra accesso «diretto» e intercettazione di massa sia più funzionale a una presentazione in Power Point[20] che a un ridimensionamento del tema complessivo agli occhi dell'opinione pubblica Ma, se fosse confermato il non accesso «diretto», non è detto che le aziende ne escano meglio. Prima di tutto l'ampiezza della collaborazione fornita e l'accettazione di benefici

come contropartita ipotizzate da *Bloomberg* dovrebbero essere oggetto di scrutinio pubblico, non di accordi segreti tra pochi dirigenti di multinazionali e ufficiali dell'*intelligence*. Dovrebbero esserlo di certo per chi fa del «*do no evil*» la propria missione aziendale. Inoltre le smentite delle aziende potrebbero essere vere formalmente, ma produrre un sistema che, di fatto, le priva di significato. Scrive Michael Arrington, che in proposito ha una teoria ben strutturata (e corroborata dal parere di diversi esperti): «le aziende hanno formulato attentamente le loro risposte, in modo da non stare tecnicamente mentendo». Ovvero:

> La mia ipotesi è che Google e le altre abbiano acconsentito a ricevere richieste Fisa in modo automatico, processarle in modo automatico, e inviare i dati in modo automatico. L'intero processo potrebbe richiedere un lasso di tempo molto limitato. Millisecondi per piccoli set di dati.

Molto raramente, scrive Arrington, ci sarebbe un intervento umano per rifiutare la trasmissione dei dati. Il problema di tutta questa automazione (che, come dicono le fonti di *Associated Press*, risponde all'idea di ridurre il carico di lavoro – e le possibili lagnanze del governo) è che:

> L'Nsa può iniziare la sorveglianza su un tema specifico una intera settimana prima di rivolgersi alla corte segreta per ottenere un ordine Fisa. Nell'ultimo anno, ogni singolo ordine emanato è stato rispettato, per cui è solo una formalità.

Per ottenere dati tramite Prism basterebbe che un analista dell'*intelligence* lo decida: il sistema automatizzato fa il resto. Il tutto a norma di legge,

anche se la legge diventa in sostanza superflua. Il punto che mette in crisi l'innocenza delle aziende[21] è, nell'ipotesi di Arrington, il non essersi opposti (come ha fatto solamente Twitter) a questo grado di automazione, pur rendendo possibile nei fatti un sistema di raccolta indiscriminata dei dati degli utenti.[22]

C'è infine un argomento teorico contro l'ipotesi del ridimensionamento (in Italia e all'estero). Lo espone splendidamente Hamilton Nowlan su Gawker:[23]

> Noterete alcune somiglianze tra le posizioni [di chi vorrebbe ridimensionare l'impatto dello scandalo, o giustificarlo, *ndr*]. Tutti questi membri dei *media*, che apparentemente lavorano per conto del pubblico, preferirebbero credere alle parole completamente non verificabili di un'agenzia governativa *top secret* che sostiene che non ci sia niente di scorretto, piuttosto che vedere qualunque tipo di materiale riservato fuoriuscire nel regno del pubblico dominio. Amano ritenersi capaci di dedurre le motivazioni e la mentalità di Edward Snowden sulla base del più insignificante degli aneddoti. Tutti mostrano sdegno all'idea che il pubblico abbia il diritto di sapere cosa stia facendo il suo governo, a meno che tale conoscenza non sia specificamente approvata dai censori governativi.

Ecco il passaggio chiave, sulla responsabilità dei «cinici dei *media*»:

> E tutti, in un modo o nell'altro, esprimono l'idea che queste cose non meritino le nostre preoccupazioni perché, ehi, persone intelligenti come loro sapevano già (ehm, assumevano) che cosa stava succedendo. Prestarci troppa attenzione ora danneggerebbe dunque la loro reputazione di esperti. Questa è l'idea più pericolosa di tutte. Quando i *media* stessi non si possono permettere di appassionarsi a un enorme programma segreto di spionaggio governativo, siamo tutti nei guai. Nessuno saprebbe alcunché di nulla, se qualcuno non si prendesse la briga di scriverne.

Circa un mese dopo, il 10 luglio, il *Washington Post* pubblica quattro nuove *slide* delle quarantuno complessive che dettagliano il programma Prism, fornite da Snowden al quotidiano statunitense e al *Guardian*. Le *slide* illustrano, rispettivamente:

1. La raccolta dati da un nuovo bersaglio;
2. Come siano processate e analizzate le informazioni ottenute da compagnie private;
3. Il sistema di notazione utilizzato, che dimostra che la sorveglianza di massa di Prism è effettivamente «in tempo reale»;[24]
4. La ricerca nel database di Prism, che avrebbe «117.675 bersagli di sorveglianza attivi».

Per *Business Insider* le nuove *slide* sembrano contraddire l'affermazione iniziale degli autori dello *scoop*, secondo cui Prism fornirebbe all'intelligence «accesso diretto» ai *server* delle aziende spiate. Per *Read Write*, le nuove *slide* mostrano l'esatto contrario. Nel frattempo, gli *scoop* continuano.

Spiate le rappresentanze Ue a Washington e diverse ambasciate

Dopo le rivelazioni del *Guardian* sullo spionaggio effettuato da Nsa e Gchq durante i *summit* del G20 tenuti a Londra nell'aprile e settembre 2009, alla fine di giugno arrivano quelle di *Der Spiegel*. Documenti riservati datati 2010, ottenuti da *Der Spiegel* grazie a Edward Snowden, mostrano che l'Nsa «non solo ha condotto sorveglianza *online* dei cittadini europei, ma sembra anche avere specificamente preso a bersaglio gli edifici che ospitano le istituzioni europee», in particolare le loro rappresentanze a Washington. La sorveglianza sarebbe stata condotta con intercettazioni telefoniche e l'intrusione nelle loro reti informatiche. «A questo modo», si legge, «gli americani sono stati in grado di accedere alle discussioni nelle stanze dell'Ue, così come alle mail e a documenti a uso interno sui loro computer». Le rappresentanze dell'Onu avrebbero subito lo stesso trattamento, secondo i documenti «parzialmente» consultati da *Der Spiegel*. La reazione del presidente del Parlamento Europeo, Martin Schulz, è durissima:

> Sono molto preoccupato e scioccato dalle accuse alle autorità Usa di spionaggio degli uffici Ue. Se dovessero rivelarsi vere, sarebbe una questione estremamente seria che avrebbe un duro impatto sulle relazioni Ue-Usa. In nome del Parlamento Europeo, chiedo un pieno chiarimento e richiedo immediatamente ulteriori informazioni alle autorità Usa riguardo a queste accuse.

In una mail alla Cnn, la portavoce Marlene Holzner

precisa che l'Ue si è «immediatamente» messa in contatto con le autorità Usa a Washington e Bruxelles, le quali hanno risposto di stare verificando l'accuratezza delle informazioni diffuse dallo *Spiegel*, promettendo di rispondere nel merito quanto prima. Nel frattempo, il *Guardian* fornisce ulteriori dettagli sull'operazione rivelata da *Der Spiegel*: le missioni e ambasciate spiate, secondo i documenti forniti da Snowden, sono trentotto. Tra i paesi bersaglio, insieme a Francia, Grecia, Giappone, Messico e Corea del Sud, c'è anche l'Italia.[25] Non è chiaro se la sorveglianza sia compiuta dalla sola Nsa o di concerto con Fbi e Cia. Scrive il *Guardian*:

> I documenti suggeriscono che lo scopo della prassi d'intercettazione contro l'ambasciata Ue a Washington sia di raccogliere informazioni riservate sui motivi di disaccordo a livello delle politiche su questioni di rilievo globale o su altre ragioni di dissenso tra gli stati membri.

In precedenza, il 29 giugno, il *Guardian* ha pubblicato[26] in esclusiva un'intervista a un ex tenente della Marina, Wayne Madsen, in cui si sostiene che «almeno sei paesi dell'Unione Europea oltre alla Gran Bretagna», Italia compresa, avrebbero «collaborato» con l'Nsa; in particolare, i paesi coinvolti avrebbero stipulato accordi per consegnare, su richiesta, i dati telefonici e delle comunicazioni via Internet all'*intelligence* statunitense. Il pezzo è poi rimosso dal sito del quotidiano, come spiegano *Telegraph* e *Business Insider*: quest'ultimo elenca anche i molti motivi per cui Madsen risulta una fonte tutt'altro che affidabile. Ragione ufficiale della rimozione? Un'indagine in corso. In seguito il contenuto delle affermazioni di Madsen è

stato confermato dal *Guardian*, che a supporto cita rapporti dell'intelligence Usa a cui è stato tolto il velo di segretezza e documenti parlamentari Ue. Si legge nella versione attualmente disponibile *online* del pezzo:

> [Il contraente, *ndr*] continuerà a rendere disponibile all'altro, di continuo e senza richiesta, tutto il traffico grezzo, le comunicazioni di *intelligence* (Comint) e il materiale tecnico acquisito o prodotto, e tutte le informazioni rilevanti riguardo alle sue attività, priorità e strutture.

Non sono tuttavia spiegate la temporanea rimozione e la scomparsa di ogni menzione a Madsen. È servita un'intervista del *Corriere* all'autore dell'articolo originario per confermare le ricostruzioni delle testate rivali: il problema era effettivamente l'affidabilità della fonte.

Gchq e Nsa spiano innocenti e sospettati

Senza che il pubblico ne fosse a conoscenza, il Gchq ha intercettato, allacciandosi ai cavi in fibra ottica che trasportano i dati, il traffico telefonico, il contenuto di email, post su Facebook e la storia delle navigazioni di persone «innocenti, così come di sospetti», scrive il *Guardian*. Informazioni che l'intelligence britannica condivide con l'Nsa secondo il programma di sorveglianza Tempora. I dati, processati da trecento analisti del Gchq e duecentocinquanta dell'Nsa (ma sarebbero ben 850 mila i suoi dipendenti e *contractor* che vi hanno avuto accesso), sono mantenuti nei registri dell'intelligence per trenta giorni. Il programma è in corso da diciotto mesi, scrive il quotidiano, e porta alla raccolta di seicento milioni di «eventi telefonici» al giorno, ottenuti da circa duecento cavi in fibra ottica (fino a quarantasei alla volta). Tempora ha la capacità teorica di registrare oltre ventuno petabyte (cioè migliaia di terabyte, o migliaia di miliardi di byte) di dati al giorno, «l'equivalente di inviare tutte le informazioni contenute in tutti i libri della British Library centonovantadue volte al giorno». Una fonte informata del programma interpellata dal *Guardian* afferma che il tutto avviene nel rispetto della legge, e che gran parte dei dati non sia nemmeno presa in considerazione: sarebbero analizzati solo quelli potenzialmente relazionati a una minaccia per la sicurezza nazionale, sulla base di alcuni indicatori capaci di riconoscere elementi di pericolo nelle comunicazioni intercettate.

Analogo trattamento sembra essere toccato ai cittadini statunitensi. A fine giugno il *Guardian* si occupa anche dell'amministrazione Obama. Secondo il quotidiano londinese, l'Nsa ha avuto il via libera dall'attuale presidente degli Stati Uniti per registrare «in massa» i metadati della posta elettronica per «comunicazioni con almeno un parlante al di fuori degli Stati Uniti o per cui nessuno dei parlanti fosse riconosciuto come cittadino degli Stati Uniti». Secondo un memo segreto del 2007, pubblicato dal quotidiano londinese, ciò si è tradotto nel tempo nella possibilità per l'*intelligence* di «analizzare i metadati delle comunicazioni associate a cittadini degli Stati Uniti e persone ritenute essere negli Stati Uniti». Il programma, prosecuzione dello Stellar Wind lanciato da George W. Bush nel 2001, si sarebbe interrotto nel 2011 «per ragioni operative e di risorse». Che significa? Che fino ad allora l'Nsa, scrivono Glenn Greenwald e Spencer Ackermann, ha potuto registrare account e indirizzo Ip del mittente, e account del destinatario – anche se non il contenuto delle mail. Il tutto per cittadini statunitensi. Per il *Guardian*, la distinzione tra contenuto e metadati, nel caso delle comunicazioni elettroniche, è tuttavia più sfumata di quanto sostenga l'amministrazione Obama, che usa la distinzione per giustificare la sorveglianza e attestare il rispetto della privacy dei cittadini. Per esempio, bastano i metadati per sapere cosa stiamo leggendo, su cosa siamo curiosi, con quali persone interagiamo, a che tipo di conversazioni prendiamo parte, spiega al *Guardian* Julian Sanchez del Cato Institute: «è un modo per entrarti nella testa per molti versi equivalente alla

lettura di un diario personale», afferma ancora, parlando di una «mappa in tempo reale del nostro cervello». Si tratta di un'integrazione decisiva – perché proveniente dalle comunicazioni private – rispetto alla mole già sterminata di dati che immettiamo quotidianamente (e pubblicamente) in rete, da noi e su noi stessi, tramite le navigazioni *online* e i contenuti pubblicati sui *social media*. In un secondo articolo del 27 giugno, il *Guardian* contraddice i proclami dell'amministrazione Obama, secondo cui il programma iniziato con Bush sarebbe finito nel 2011:

> È chiaro che l'agenzia [l'Nsa, *ndr*] raccolga e analizzi quantità significative di dati da sistemi di comunicazione statunitensi durante il monitoraggio di bersagli stranieri.

A supporto dell'affermazione il quotidiano porta «documenti *top secret*» visionati dai propri giornalisti. In particolare, a dicembre 2012 l'*intelligence* ha annunciato «l'ampliamento» delle capacità di intercettazione del traffico *online* tramite il programma Evil Olive, che consentirebbe all'agenzia di immagazzinarne il 75%. È menzionato un altro programma di sorveglianza, Shell Trumpet, che avrebbe raggiunto il triliardo di metadati acquisiti: non è chiaro in che misura riguardino cittadini stranieri o americani e quale ne sia la legittimazione legale. Nonostante il programma sia in corso da cinque anni, solo nel 2012 avrebbe registrato metà dei dati ottenuti. Due ulteriori programmi di sorveglianza, Moonlight Path e Spinneret, sono stati annunciati a febbraio 2013 e pianificati per il lancio a settembre di quest'anno.

CAPITOLO II: LUGLIO

Gli abusi della corte segreta sulla sorveglianza

Dallo scoppio dello scandalo, il passaggio delle richieste di sorveglianza per la corte segreta Fisa è stato richiamato dai difensori della National Security Agency come garanzia che lo spionaggio di massa delle comunicazioni telefoniche e *online* avvenisse sempre e comunque a norma di legge. Alle rivelazioni di *Cnet*, smentite dal direttore dell'Nsa James Clapper, e ai documenti pubblicati successivamente dal *Guardian*, che mostrano la fragilità della smentita, si unisce un'inchiesta del *New York Times*. Ai dubbi già visti il *New York Times* aggiunge «una dozzina di sentenze riservate» che dimostra come in realtà la corte abbia creato «un corpo legislativo segreto che fornisce all'Nsa il potere di accumulare immense raccolte di dati sui cittadini americani». E non solo sospetti terroristi, «ma anche persone potenzialmente coinvolte in casi di proliferazione nucleare, spionaggio e attacchi informatici», secondo gli esperti interpellati dal quotidiano. Nelle 100 pagine di documentazione visionate dal *Times* è dimostrato come la corte abbia stabilito dei precedenti legali «senza quasi alcuno scrutinio pubblico» e sulla base di una interpretazione del corpo normativo ampia abbastanza da rendere

compatibile la sorveglianza di massa col Quarto Emendamento della Costituzione Usa.[27]

Decade così la tesi delle richieste specifiche per soli bersagli già ragionevolmente sospettati di terrorismo:

> In un caso recente per esempio gli ufficiali dell'*intelligence* sono stati in grado di accedere all'allegato a una mail inviata all'interno degli Stati Uniti perché avevano sostenuto di essere preoccupati che la mail contenesse uno schema o un diagramma potenzialmente connesso al programma nucleare iraniano.

Un tempo sarebbe servita probabilmente l'autorizzazione giudiziaria, nota il *Times,* perché di mezzo ci sono comunicazioni cittadini americani. Dal 2008 non più. La corte segreta, inoltre, ascolta il solo parere del governo (che dunque manca di contraddittorio) e non ha mai opposto un rifiuto alle richieste di intercettazione. Un singolo giudice, addirittura, ha totalizzato circa milleottocento autorizzazioni solo lo scorso anno. Il potere della corte, continua il *Times*, è impressionante:

> È diventato quasi il parallelo della Corte Suprema, ricoprendo il ruolo di arbitro ultimo delle questioni riguardanti la sorveglianza e producendo sentenze che molto probabilmente costituiranno la base delle prassi di *intelligence* per gli anni a venire.

L'Nsa collabora con altri paesi

Edward Snowden ritorna a parlare in un'intervista concessa a *Der Spiegel* in cui accusa l'*intelligence* statunitense di «collaborare con i tedeschi». Secondo Snowden, il Foreign Affairs Directorate dell'agenzia sarebbe «responsabile di collaborazioni con altri paesi». Non solo:

> Le collaborazioni sono organizzate in modo da consentire alle autorità di «mettere al riparo i *leader* politici» degli altri paesi da «contraccolpi negativi» nel caso dovesse diventare di pubblico dominio «quanto gravemente abbiano violato la privacy globale».

La scelta dei partner avverrebbe sulla base dei loro «contenuti su Facebook o via mail». In particolare, la collaborazione tra Nsa e il Bnd tedesco (il servizio di *intelligence* per minacce dall'estero) è «molto più intensa di quanto sapessimo in precedenza». L'Nsa fornirebbe al Bnd «strumenti di analisi» per il monitoraggio di flussi di dati stranieri che attraversano la Germania. I dati sarebbero prelevati da «cinque differenti nodi» e analizzati a Pullach, vicino a Monaco di Baviera. «Il capo del Bnd, Gerhard Schindler, ha confermato la collaborazione con l'Nsa durante un incontro con membri del comitato di controllo dell'intelligence del Parlamento tedesco», si legge. Ma non è tutto. *Der Spiegel* pubblica inoltre un resoconto basato su documenti «segreti» forniti da Snowden. I documenti «rivelano che l'Nsa ha sistematicamente monitorato e raccolto gran parte dei dati telefonici e delle connessioni Internet» in Germania. Scrive il settimanale tedesco:

> Statistiche interne all'Nsa indicano che l'agenzia immagazzina all'incirca mezzo miliardo di comunicazioni in Germania al mese. Sono incluse telefonate, email, messaggi su cellulare e trascrizioni delle chat. I metadati [...] sono poi immagazzinati nel quartier generale dell'Nsa di Fort Meade, vicino a Washington, Dc.

L'intensità della sorveglianza che investe la Germania è alla pari con Cina, Iraq e Arabia Saudita – scrive *Der Spiegel* ricordando i dati ottenuti da Boundless Informant (la mappa della sorveglianza globale dell'Nsa rivelata dal *Guardian*).[28]

Scorrendo le statistiche fornite da *Der Spiegel*, si scopre che di mezzo ci sono anche Francia e Italia:

> I dati raccolti sulla Germania nei giorni qualunque sono fino a venti milioni di chiamate e dieci milioni di scambi di dati via Internet. Durante l'ultima vigilia di Natale, i dati raccolti sono stati di circa tredici milioni di telefonate e circa la metà di scambi online. Nei giorni più trafficati, come il 7 gennaio di quest'anno, le informazioni raccolte hanno avuto un picco di quasi sessanta milioni di comunicazioni sorvegliate. Si scopre che l'Nsa è più attiva in Germania che in qualunque altro paese dell'Ue. Per fare un paragone, durante gli stessi giorni, gli statunitensi hanno registrato soltanto una media di due milioni di dati al giorno in Francia.

Una media, quest'ultima, che la Francia condivide con l'Italia. Non a caso è anche su questi dati che si svolge, il 2 luglio, un'audizione dell'ambasciatore Giampiero Massolo al Copasir. Di cui il presidente, il leghista Giacomo Stucchi, e il segretario, il senatore Pd Felice Casson, danno interpretazioni radicalmente opposte: «tutte le domande hanno avuto una risposta», secondo il primo; «le risposte non sono state

assolutamente sufficienti», ribatte il secondo. Nel frattempo, buona parte degli organi di stampa italiani si è accontentata delle (non) spiegazioni dell'amministrazione Obama, spesso nascondendosi dietro l'argomento per cui sarebbero solo metadati, e quindi niente di preoccupante. Una tesi insostenibile, alla luce di quanto visto finora.[29] A rendere ancora più insufficienti le risposte dell'audizione al Copasir, giungono il 28 agosto le rivelazioni dell'*Espresso*, in un articolo firmato da Stefania Maurizi. Si legge, tra l'altro:

> Dalle informazioni in possesso dell'*Espresso* risulta che i documenti dell'ex *contractor* [Snowden, *ndr*] lasciano emergere una serie di nomi dei cavi sottomarini a fibra ottica intercettati dai servizi inglesi del Gchq, [...] omologo britannico della Nsa e che con la Nsa ha una relazione speciale di collaborazione e condivisione dei dati. Tra i cavi intercettati dal Gchq ce ne sono tre che interessano l'Italia e che permettono quindi di accedere ad alcuni dei dati più personali degli italiani: quelli delle loro interazioni sociali attraverso le comunicazioni telefoniche e via Internet.

Sono inevitabili due domande: Londra e Washington ci spiano (a nostra insaputa o meno)? Se sì, come e con quali regole?

Quanto alla Francia, ci sono anche le rivelazioni di *Le Monde*, secondo cui il paese, al netto dell'indignazione di Francois Hollande per lo spionaggio dell'ambasciata a Washington, ha il suo «Prism», indipendente dall'Nsa. Affermazioni analoghe si leggono in Spagna. In Svezia, invece, Rick Falkvinge, fondatore del primo Partito Pirata, sostiene che «la Svezia intercetta la Russia per conto dell'Nsa». E lo sta facendo dall'entrata in vigore di una controversa legge sulla

sorveglianza:

> L'agenzia Fra sta continuamente intercettando la Russia sulla base di un accordo firmato nell'aprile del 2007, e condividendone i dati con l'Nsa. In questo contesto, non è una coincidenza che la Svezia e la Gran Bretagna, unici due Paesi europei, abbiano recentemente scelto di bloccare le inchieste dell'Ue sulle intercettazioni da parte degli Stati Uniti di ufficiali e imprese europee.

Nel corso del mese *Der Spiegel*, ancora grazie a Snowden e a documenti riservati forniti dal *whistleblower*, torna sulla situazione tedesca, facendo emergere un quadro ancora più preoccupante che chiama in causa Angela Merkel. «A fine aprile», scrive *Der Spiegel*, «un team di dodici ufficiali di alto rango della Bnd si è recato negli Stati Uniti, dove ha visitato il cuore dell'impero americano globale della sorveglianza». Lì il presidente della Bnd, Gerhard Schindler, ha espresso ripetutamente il desiderio di collaborare più strettamente con l'Nsa; una richiesta esaudita, scrive ancora *Der Spiegel*. Gli agenti, compresi quelli della Ssi (i «gioielli della corona» dell'*intelligence* statunitense, secondo Snowden), istruiscono i colleghi tedeschi sulle modalità di raccolta di dati all'interno dei programmi di sorveglianza. Secondo i documenti in possesso del settimanale non si tratterebbe né del primo né dell'ultimo viaggio di questo tipo. I rapporti tra le agenzie dei due paesi, sviluppati a partire dal 2007 per sventare un piano terroristico in Germania, si sarebbero intensificati durante l'era di Angela Merkel, portando a sessioni di addestramento degli agenti tedeschi da parte dei colleghi Usa e, già dal 2008, alla fornitura ai tedeschi del programma XKeyscore,[30]

capace di intercettare dati grezzi. Essendo in grado di monitorare in tempo reale le attività *online* dei bersagli, secondo *Der Spiegel*, XKeyscore rende possibile una «sorveglianza digitale quasi totale».[31]

In conferenza stampa Merkel ha ribadito di non essere assolutamente al corrente dei rapporti tra Nsa e intelligence tedesca. I documenti, tuttavia, la contraddicono. La Germania è considerata dagli americani un «partner chiave». Un partner, tra l'altro, che nel 2012 avrebbe mostrato più volte la sua volontà di aumentare la capacità di sorveglianza, addirittura giungendo a modificare l'interpretazione di una legge sulla privacy (G-10) «per consentire al Bnd di condividere con maggiore facilità le informazioni riservate con i partner stranieri». Si comprende dunque come quella di Merkel sia una posizione sempre più insostenibile. Le rivelazioni di *Der Spiegel* si sommano a quelle sul mezzo miliardo di comunicazioni immagazzinate ogni mese – telefonate, email, sms, trascrizioni di chat – tramite XKeyscore – dall'*intelligence* statunitense e quindi trasferite a Fort Meade, nella sede dell'Nsa; alle infrastrutture di spionaggio imbastite dagli statunitensi in suolo tedesco, e oggi utilizzate da entrambi. Lo spiato è dunque diventato a sua volta spia. Non solo per i documenti di Snowden che provano i rapporti tra le intelligence dei due Paesi. Ci sono anche le rivelazioni di *Bild*, secondo cui i servizi segreti e il governo tedesco sapevano da anni di un programma chiamato Prism a conduzione statunitense per spiare la Germania. La prova è un documento Nato del 2011 ottenuto dal *tabloid*. Anche in questo caso la reazione delle autorità tedesche è stata a

dir poco bizzarra: hanno sostenuto si trattasse non del Prism che ha originato il Datagate, ma di un altro programma omonimo, specifico per la Nato, tutt'altro che segreto e a cui comunque avrebbero avuto accesso solamente statunitensi. La *Bild* ha replicato colpo su colpo, al punto che David Meyer, su *Gigaom*, si è chiesto se esistano davvero due Prism, per «folle coincidenza» sostanzialmente identici, oppure uno solo, nel qual caso è Angela Merkel che mente al riguardo.

Il programma XKeyscore

Sul *Guardian* Glenn Greenwald approfondisce il funzionamento di XKeyscore, «un programma *top secret* della National Security Agency», che «consente agli analisti di compiere ricerche, senza alcuna autorizzazione, all'interno di vasti database contenenti email, *chat online* e lo storico delle navigazioni di milioni di individui». Secondo i documenti forniti da Snowden a Greenwald, XKeyscore è il programma di sorveglianza di massa più esteso in possesso dell'*intelligence* statunitense, al punto che una *slide* di presentazione vanta che possa registrare «quasi tutto ciò che un utente tipo fa su Internet», per giunta sulla base della semplice compilazione di un formulario generico a schermo, senza alcuna autorizzazione giudiziaria o controllo di un ufficiale dell'Nsa. Il *Guardian*, inoltre, pubblica integralmente una presentazione di XKeyscore risalente al 25 febbraio 2008, da cui si deduce, come segnala Chris Soghoian dell'Aclu, che nemmeno l'utilizzo di sistemi di cifratura delle comunicazioni (Vpn, Pgp) è sufficiente a sfuggire allo spionaggio dell'Nsa. La sorveglianza compiuta attraverso XKeyscore si spinge, secondo le slide pubblicate dal *Guardian* (e in alcuni casi già dal brasiliano *O Globo*), al «contenuto delle email, i siti visitati e le ricerche compiute, così come i relativi metadati». Basta essere in possesso di un indirizzo Ip o mail, e si applica anche ai cittadini statunitensi, scrive Greenwald, sempre senza autorizzazione di alcuna autorità giudiziaria. L'attività sui *social media* è inclusa

grazie all'utilizzo di uno strumento chiamato «Dni Presenter», che consente agli analisti che utilizzano XKeyscore di «leggere i contenuti delle *chat* e dei messaggi privati su Facebook». Il tutto in tempo reale. Stando a un documento del 2007, gli elementi di *intelligence* raccolti in questo modo sarebbero tra gli uno e i due miliardi al giorno, per un totale di 850 miliardi relativi a conversazioni telefoniche e centocinquanta miliardi per comunicazioni via Internet. Nel 2012, la capacità di raccogliere elementi di intelligence ha raggiunto i quarantuno miliardi nell'arco di trenta giorni; talmente tanti dati da poter essere immagazzinati solo per tre-cinque giorni, per quanto riguarda i contenuti, e trenta per i metadati. Ma, come ha spiegato *Der Spiegel*, XKeyscore ha la capacità di intervenire retroattivamente, rivelando «qualunque termine l'utente bersaglio abbia inserito in un motore di ricerca». Secondo *Slate* il programma consentirebbe agli agenti dell'Nsa di spiare le ricerche compiute su Google Maps, mentre per *O Globo*, XKeyscore utilizza 700 server dislocati in 150 località sparse in tutto il mondo.

L'Nsa ha replicato al *Guardian* sostenendo che l'attività dell'agenzia riguarda solamente «bersagli stranieri legittimi», che XKeyscore rientra nei programmi legalmente predisposti, e che «le affermazioni riguardanti un accesso diffuso e senza verifiche da parte degli analisti dell'Nsa» al programma «sono semplicemente non vere». Sempre secondo l'Nsa, XKeyscore avrebbe contribuito a catturare trecento terroristi. L'affermazione è però senza riscontri.[32]

L'Nsa spia l'America Latina

Tra i bersagli in America latina della sorveglianza di massa della National Security Agency non c'è solo il Brasile, come già rivelato da *O Globo*. Stando a una nuova inchiesta, pubblicata ancora da *O Globo*[33] e firmata da Glenn Greenwald con Roberto Kaz e José Casado, i metadati delle conversazioni telefoniche e via Internet vengono registrati a milioni anche in «Messico, Venezuela, Argentina, Colombia ed Ecuador, tra gli altri». Secondo i documenti riservati consultati dai giornalisti, il monitoraggio di questi paesi si spingerebbe oltre la prevenzione del terrorismo, comprendendo anche «segreti commerciali» come «dati sul petrolio e gli acquisti militari in Venezuela, il settore energetico e il traffico di sostanze stupefacenti in Messico», e una mappatura dei movimenti delle forze rivoluzionarie colombiane (Farc); In Colombia la raccolta dei dati da parte dell'*intelligence* avrebbe avuto luogo dal 2008 a marzo 2013.

Nel primo semestre del 2013 i programmi di sorveglianza adoperati sono, secondo *O Globo*, Prism (con cui sarebbero stati ottenuti i «segreti commerciali» menzionati in precedenza) e Boundless Informant. Colombia, Brasile e Messico sarebbero dunque gli obiettivi prioritari dello spionaggio dell'Nsa nel continente, mentre sarebbero stati oggetto di minori attenzioni Venezuela, Argentina, Panama, Costa Rica, Nicaragua, Honduras, Paraguay, Cile, Perù ed El Salvador.[34] Il sito della *Reuters* sottolinea come le reazioni istituzionali non si siano fatte attendere. «Un

brivido mi è corso sulla schiena quando ho scoperto che siamo tutti spiati», dichiara il presidente argentino Cristina Fernandez de Kirchner, chiedendo anche una forte risposta formale da parte degli aderenti al Mercosur, incontratisi nei giorni seguenti; anche i presidenti di Perù e Bolivia esprimono preoccupazione dopo le rivelazioni di *O Globo*. Il governo brasiliano, invece, oltre a chiedere spiegazioni ha predisposto una «task force» composta dai ministeri della Difesa, delle Comunicazioni, della Giustizia e degli Esteri per «indagare sul presunto spionaggio e stabilire se la privacy dei cittadini brasiliani sia stata violata», scrive la *Reuters*.

Come precisa il *Washington Post*, l'*intelligence* non ha voluto rispondere alle accuse del quotidiano brasiliano, se non con un breve comunicato, che recita: «siamo stati chiari sul fatto che gli Stati Uniti raccolgono *intelligence* straniera del tipo raccolto da tutti i paesi». Sempre secondo il *Washington Post*, l'ambasciatore statunitense in Brasile, Thomas Shannon, ha negato le accuse rivolte all'Nsa (il resoconto di *O Globo* sarebbe «scorretto»), aggiungendo che gli Stati Uniti non collaborano con operatori delle telecomunicazioni brasiliani.

La bocciatura dell'emendamento anti-sorveglianza

Negli Stati Uniti, intanto, il primo tentativo in Parlamento di fermare la sorveglianza di massa dell'Nsa subisce una battuta d'arresto. Anche se per poco, solamente dodici voti, la Camera degli Stati Uniti boccia infatti l'emendamento Amash (dal nome del repubblicano Justin Amash) che si proponeva per l'appunto di «fermare la sorveglianza generalizzata degli americani» da parte dell'*intelligence*: nello specifico, di limitare la raccolta dei dati da parte del governo secondo la sezione 215 del Patriot Act (riguardante questioni di sicurezza nazionale) a «persone soggette a un'indagine secondo quella norma»; l'emendamento prevedeva inoltre una supervisione giudiziaria del monitoraggio più accurata rispetto a quella attuale, di fatto inesistente. Amash aveva motivato la sua proposta con l'obiettivo ideale di «difendere il Quarto Emendamento», lo stesso di chi ha protestato[35] proprio il 4 luglio 2013,[36] e «la privacy di ogni cittadino statunitense», oltre a voler evitare, più pragmaticamente, il ripetersi di registrazioni indiscriminate di milioni di metadati telefonici – come avvenuto per le utenze Verizon, e non solo.

Il voto si è concluso con duecentocinque favorevoli e duecentodiciassette contrari. Il *Guardian* li dettaglia nome per nome, mostrando anche come la proposta abbia incontrato il favore di più democratici (111 contro i 94 dei repubblicani), mentre nel Partito Repubblicano (Gop) hanno prevalso i no (134, cui si sommano 83

democratici). Una questione dunque che, scrive il *New York Times*, «ha messo democratico contro democratico e repubblicano contro repubblicano». Come ha scritto *The Atlantic*, indipendentemente dall'esito del voto c'è di buono che ora sappiamo come la pensano i singoli membri del Congresso rispetto ai programmi condotti dall'Nsa e svelati da Edward Snowden. Un'operazione di elementare trasparenza finora inedita. È singolare, tuttavia, che la Casa Bianca abbia espresso netta contrarietà all'emendamento proposto da Amash citando la mancanza di un «processo informato, aperto e deliberativo»: non solo perché si tratta di programmi di *intelligence* considerati *top secret*, ma perché la loro approvazione non è stata affatto il risultato di un processo trasparente né di un dibattito con l'opinione pubblica. Non a caso, la prima reazione di Barack Obama allo scoppio del Datagate è stata di auspicarsi che una simile discussione potesse svilupparsi: significa che prima non c'era.

Secondo diversi analisti il margine tra favorevoli e contrari è stato molto più ristretto del previsto. Per il *Guardian*, la spaccatura trasversale nel Congresso è un «chiaro segnale» al presidente: qualcosa, rispetto alle prassi dell'Nsa, deve cambiare. A maggior ragione dopo l'opposizione della Casa Bianca e gli «incontri segreti» tenuti dall'*intelligence* Usa per fare pressioni su singoli membri della Camera e convincerli a votare contro l'emendamento. «Che il margine sia stato così ristretto», nota tuttavia *Tech Crunch*, «non garantisce affatto che i programmi di sorveglianza domestica dell'Nsa saranno sfidati di nuovo, e con successo».

CAPITOLO III: AGOSTO

La sorveglianza dell'Nsa usata per combattere crimini domestici

Uno dei principali argomenti usati dalle autorità statunitensi a difesa dei programmi di sorveglianza di massa è stato quello sicurezza nazionale, anche se finora non è stato dimostrato il legame tra l'impiego dei primi ed eventuali attentati sventati. L'argomento subisce un duro colpo dopo quanto scoperto dalla *Reuters* a inizio mese, ponendo l'attenzione su quali siano gli scopi effettivi della sorveglianza di massa. Secondo *Reuters*, il governo statunitense sta nascondendo infatti l'uso dei programmi di sorveglianza dell'*intelligence*, avviando casi giudiziari e costruendo prove contro cittadini americani su questioni che nulla hanno a che vedere con il contrasto del terrorismo. *Reuters* cita a sostegno documenti riservati di cui è entrata in possesso. In particolare, scrive:

> Un'unità segreta della Drug Enforcement Administration (Dea) degli Stati Uniti sta incanalando informazioni ottenute da intercettazioni di *intelligence*, cimici, informatori e un consistente database di documentazione telefonica da diverse agenzie nel paese che le aiutano a lanciare indagini su cittadini americani.

L'unità menzionata è la Special Operations Division (Sod), che include tra i partner Fbi, Cia e Nsa; il programma della Sod riguarda criminali comuni, in particolare spacciatori. Non solo: l'unità copre le sue mosse, ricostruendo in maniera artefatta il modo in cui ha ottenuto le prove. *Reuters* cita un caso di spaccio in Florida, in cui un giudice afferma di aver prima appreso di una dritta essenziale per far partire le indagini da un informatore, e poi, dopo aver pressato la fonte, che quella dritta proveniva da dati raccolti dall'Nsa. Coprire il modo in cui nasce un'inchiesta, spiega *Reuters*, è secondo diversi esperti contrario al diritto a un giusto processo, perché potrebbe impedire alla difesa la produzione di prove a suo vantaggio. Alcuni ufficiali della Sod hanno tuttavia replicato che si tratta di un metodo in uso da decenni, perfettamente legale e utile. L'idea su cui si basa è quella della «costruzione parallela». In un esempio: se si deve fermare un camion sospetto di contenere un carico di droga, l'agenzia può imbeccare gli agenti sul posto e far credere che il fermo avvenga per un controllo di rito; invece, è informato dalle informazioni precedentemente ottenute dai programmi di raccolta dati dell'*intelligence*.

Secondo *Tech Crunch*, questa scoperta rende l'idea che «l'attività dell'Nsa riguardi solamente terroristi e cittadini non statunitensi totalmente pretestuosa». Ancora: «C'è una connessione diretta tra la sorveglianza dell'Nsa e la persecuzione di crimini ordinari nel paese».

Il *Washington Post* pone invece una domanda:

> I sondaggi mostrano un forte supporto popolare per i programmi di sorveglianza di massa dell'Nsa quando le parole «terrorismo» e «corti» sono incluse nella domanda.

> Quando i sondaggisti non fanno alcuna connessione col terrorismo, il supporto tende a svanire. Che accadrà quando la domanda renderà chiaro che l'*intelligence* non solo non è utilizzata per indagini terroristiche contro bersagli stranieri, ma che sta venendo impiegata attivamente per indagare contro cittadini americani?

Soltanto 24 ore prima il *New York Times* aveva scritto che l'utilizzo dei dati prodotti dall'Nsa è stato di frequente motivo di scontro tra le varie agenzie governative che potrebbero mettere a frutto i risultati prodotti dai programmi di sorveglianza di massa per le loro indagini; non ultime, proprio quelle citate da *Reuters*. Il problema per gli ufficiali governativi sembra non, come denuncia parte dell'opinione pubblica, che quei programmi siano troppo vasti, ma che non lo siano abbastanza. Nel frattempo, il dato incontestabile è che prosegue l'effetto Snowden (ovvero, come da definizione di Jay Rosen, il moltiplicarsi di inchieste sulla sorveglianza Nsa *indipendenti* dai suoi documenti).

Chiudono Lavabit e Silent Mail

Il *New York Times* l'8 agosto fornisce l'ennesima smentita dell'idea, sostenuta dalle autorità statunitensi, per cui la sorveglianza delle comunicazioni telefoniche e via Internet della National Security Agency non riguardi i contenuti, avvenga solo previa autorizzazione giudiziaria e comunque solo per sospetti terroristi stranieri (e mai per cittadini statunitensi). Il quotidiano, citando «ufficiali dell'*intelligence*», afferma che l'Nsa compie ricerche proprio tra i contenuti di email e comunicazioni testuali di cittadini americani da e per il paese, in «vaste quantità» e a caccia di «quelle persone che menzionino informazioni circa stranieri sotto sorveglianza». Tradotto:

> L'Nsa non solo intercetta le comunicazioni degli americani che sono in diretto contatto con bersagli stranieri oltreoceano, una prassi che le autorità hanno apertamente riconosciuto. Sta anche tessendo una tela ben più ampia per includere soggetti che citino informazioni collegate a quegli stranieri, come un indirizzo email poco usato.

La rivelazione del *New York Times* porta a reazioni senza precedenti da parte di due fornitori di servizi mail «sicuri», Lavabit e Silent Circle. Lavabit, che sarebbe stato utilizzato anche da Edward Snowden, chiude i battenti il 9 agosto con un durissimo comunicato. Nel breve testo il proprietario, Ladar Levison, spiega di aver preso questa decisione per evitare di diventare «complice di crimini contro i cittadini americani». Levison avrebbe ricevuto l'ingiunzione di consegnare dati sui propri utenti, circa 350 mila, al governo Usa, e

senza poter informare gli utenti coinvolti; secondo la Bbc, Lavabit avrebbe intrapreso una battaglia legale per opporsi. La chiusa del comunicato è nettamente critica. Scrive Levison:

> Senza un intervento del Congresso o un chiaro precedente giudiziario, suggerisco caldamente di non affidare i propri dati personali a un'azienda con legami fisici agli Stati Uniti.

La decisione di Levison spinge il Ceo di Silent Circle, Michael Janke, a chiudere il servizio di mail criptata, Silent Mail, fornito dalla sua azienda. Troppe le possibilità di intercettazione dei dati scambiati da parte del governo Usa che, tuttavia, finora non aveva raggiunto Silent Circle con l'ordine di consegnare dati degli utenti, come per Lavabit. Meglio in ogni caso cessare il servizio che comprometterne la privacy, è il ragionamento di Janke.[37] Janke ha anche risposto a una richiesta di chiarimento da parte sempre di *Techrunch*. In ballo non c'è solo la minaccia alla sicurezza del servizio mail fornito, quanto piuttosto il fatto che Silent Mail fosse utilizzato da gruppi per i diritti umani, reporter e capi di Stato. Bersagli di altro profilo che hanno dato da riflettere al Ceo dell'azienda: meglio prevenire che trovarsi di fronte alle richieste del governo e combattere una battaglia persa per proteggerne la privacy. Del resto, scrive Janke, «sapevamo che il governo Usa ci avrebbe perseguito». Era solo questione di tempo, e il caso Lavabit deve avere confermato le preoccupazioni di Janke.

La detenzione di Miranda, le intimidazioni del governo al Guardian

Il compagno di Glenn Greenwald, David Miranda, il 18 agosto è trattenuto per più di nove ore dalle autorità britanniche. Ne dà notizia il *Guardian* il giorno seguente il fermo, scrivendo che il provvedimento è scattato mentre Miranda si trovava all'aeroporto londinese di Heathrow, in transito in un viaggio da Berlino al Brasile, dove vive. Le reazioni sono, comprensibilmente, dure: Dan Gilmor, su Twitter, denuncia la «la dichiarazione di guerra al *Guardian* e per estensione al giornalismo»; lo stesso Greenwald sul *Guardian* parla di «fallito tentativo di intimidazione». Amnesty International condanna la detenzione, il governo brasiliano «manifesta grave preoccupazione».

Stando alla versione del *Guardian*, Miranda è fermato in base al Terrorism Act del 2000. Eppure le autorità britanniche si limitano (per modo di dire) a informarsi dell'eventuale possesso di materiale riservato, interferendo così in un'inchiesta giornalistica. Il fermo di nove ore appare eccessivo; Miranda subisce inoltre il sequestro di portatile, *smarthpone* e altri dispositivi senza sapere se e quando gli saranno restituiti.

In seguito è lo stesso Miranda[38] a parlare al *Guardian* della detenzione, che definisce «totale abuso di potere». «Mi hanno minacciato per tutto il tempo, dicendo che se non avessi collaborato mi avrebbero sbattuto in galera» afferma. Lo scenario delineato è da regime autoritario, con sette agenti che lo interrogano alternandosi l'un

l'altro, senza avvocato né interprete, nonostante Miranda abbia manifestato disagio non potendosi esprimere nella propria lingua madre, tra minacce e intimidazioni. Miranda conferma che il terrorismo non ha nulla a che vedere con le ragioni del fermo.[39]

Le parole di Gilmor sulla «guerra al *Guardian* e per estensione al giornalismo» sembrano riscontrate da quanto riporta successivamente il direttore del quotidiano, Alan Rusbridger:

> Poco più di due mesi fa sono stato contattato da un alto ufficiale del governo che affermava di rappresentare il punto di vista del primo ministro. Vi hanno fatto seguito due incontri in cui ha richiesto la restituzione o la distruzione di tutto il materiale su cui stavamo lavorando. Il tono era gelido, pur se cordiale, ma c'era l'implicita minaccia che altri ufficiali all'interno del governo e di Whitehall [sede del ministero della Difesa e quartier generale dell'esercito, *ndr*] erano a favore di un approccio ben più draconiano. L'umore si è inasprito poco più di un mese fa, quando ho ricevuto una telefonata dal centro del governo che diceva: «Vi siete divertiti. Ora vogliamo il materiale». Ci sono stati altri incontri, poi, con ombrose figure di Whitehall. La richiesta era la stessa: ridateci il materiale di Snowden o distruggetelo. Ho spiegato che non potevamo proseguire il nostro lavoro di ricerca e giornalistico sul tema se avessimo acconsentito. L'uomo di Whitehall è apparso perplesso: «Avete avuto il vostro dibattito. Non c'è bisogno di scriverne ancora». Durante uno di questi incontri ho chiesto direttamente se il governo si sarebbe mosso per fermare il lavoro d'inchiesta del *Guardian* per vie legali – rivolgendosi a una Corte per costringerci a consegnare il materiale su cui stavamo lavorando. L'ufficiale ha confermato che, in assenza di una restituzione o della sua distruzione, questa era proprio l'intenzione del governo.

Che in effetti si realizza:

> E così si è verificato uno dei momenti più bizzarri della

> lunga storia del *Guardian* – con due esperti di sicurezza del Gchq a supervisionare la distruzione degli hard disk nel seminterrato del *Guardian* solo per assicurarsi che non ci fosse nulla di interessante nei pezzi di metallo maciullati da passare ad agenti cinesi.

Rusbridger dice che il lavoro giornalistico del *Guardian* sui documenti di Snowden proseguirà, a ogni modo. Solo «non da Londra». Il punto è che potrebbe non essere lontano il giorno in cui «sarà impossibile per i giornalisti avere fonti riservate».

Ci sono tuttavia delle contraddizioni nella versione del *Guardian* del fermo. Le evidenziano gli articoli di Louise Mensch[40] e Joshua Foust. Prima di tutto, a Miranda è stato offerto un avvocato (in principio era stato scritto il contrario): è stato lui a rifiutarlo. Ancora, Miranda, inizialmente presentato come completamente estraneo alla vicenda, è coinvolto esplicitamente, dietro compenso del *Guardian*, nel lavoro giornalistico sul Datagate. Non si tratterebbe semplicemente del «compagno di Greenwald», dunque, ma di una figura direttamente coinvolta, in questo caso, nel trasporto di materiale riservato da Berlino al Brasile, cioè da Laura Poitras a Greenwald stesso. Sono aspetti che però non alterano la sostanza della vicenda: l'offerta di un avvocato di ufficio, specie in circostanze simili, non equivale alla possibilità di disporre di un proprio avvocato; e il fermo è più grave (e non meno) se riguarda non un semplice cittadino ma un «giornalista» (o qualcosa di affine). In ogni caso, il *Guardian* avrebbe comunque il dovere di chiarire alla luce di questi nuovi elementi, per tutelare oltre ogni sospetto la propria credibilità in un momento così delicato.

Nei pezzi citati è invece molto debole la difesa della legalità (ma non dell'opportunità) del fermo. Come spiega questa analisi legale,[41] «se l'interrogatorio, la detenzione e la perquisizione di Miranda sono stati condotti con qualunque altro scopo rispetto a determinare se fosse un terrorista, allora sono stati condotti in modo illegale». Qui tutti gli indizi sembrano portare a una pericolosissima identificazione del lavoro giornalistico con l'attività terroristica, se si vuole mantenere la *ratio* della legge. Per non parlare del fatto che il criterio stabilito dalla legge contro il terrorismo alla Parte 1, Sezione 1 (e), la detenzione per la «seria» minaccia di «interferire con o manomettere un sistema elettronico», è talmente vago da rendere possibili gli abusi di cui il caso Miranda ha offerto testimonianza oltre ogni pur lecito dubbio sui dettagli del suo resoconto.

Il costo della sorveglianza digitale

La sorveglianza dell'Nsa ha un costo, e salato, per il contribuente. Secondo il *Guardian* si tratterebbe di milioni di dollari, che l'*intelligence* Usa avrebbe sborsato per coprire le spese dei colossi *web* coinvolti nel discusso programma di sorveglianza Prism. In particolare, l'esborso di denaro è avvenuto a carico dello Special Source Operations, il «fiore all'occhiello» dell'Nsa, come sostiene Edward Snowden.

I costi sono stati sostenuti per coprire le uscite necessarie a ottemperare alle richieste governative, ma anche e soprattutto per ottenere «ripetute» proroghe nelle «certificazioni» annuali richieste dalla Fisc (la corte deputata a giudicare l'operato dell'Nsa). Atti che stabiliscono il rispetto della legge nella sorveglianza condotta; più volte, proprio a causa delle violazioni commesse, è stato necessario chiedere estensioni del termine ultimo, che si pagano a caro prezzo. Queste violazioni, aggiunge il *Wall Street Journal*, nell'Nsa sono avvenute anche per questioni affettive personali (denominate Loveint) che nulla hanno a che vedere con il contrasto del terrorismo. A beneficiare dei «rimborsi», le aziende che secondo il materiale fornito da Snowden all'origine del Datagate hanno partecipato a Prism: tra loro, Apple, Facebook, Yahoo e Google. I pagamenti sarebbero avvenuti dopo il severo giudizio della Fisc del 2011 reso pubblico dalla stessa Nsa, dietro richiesta dell'Electronic Frontier Foundation, in quegli stessi giorni. Le proroghe dimostrano i problemi incontrati dall'*intelligence* nel rendere a norma di legge la

sorveglianza condotta insieme alle aziende in questione. Il legame tra Silicon Valley e intelligence, dunque, va oltre i semplici accordi di cui hanno già scritto il *Guardian* e il *New York Times*, da ora peraltro impegnati in una *partnership* per i documenti riguardanti l'agenzia britannica Gchq, così da sfuggire alle pressioni del governo britannico ordinate dallo stesso David Cameron.

Il *Guardian* ha chiesto alle aziende coinvolte di precisare natura, entità e forme del «rimborso». Yahoo ha risposto che i rimborsi ottenuti sono stati sempre a norma di legge. Facebook ha negato ogni compenso legato a richieste governative di dati. Google ha evaso la domanda, ribadendo più in generale che le affermazioni reperite sulla stampa sul grado di sorveglianza esercitato sono esagerate. Le risposte non convincono gli esperti: alcuni sostengono si tratti di "legalese" per nascondere la verità. Per il guru della sicurezza informatica, Bruce Schneier, le aziende sono addirittura «legalmente obbligate a mentire». Non a caso alcune chiedono un quadro normativo che consenta loro di poter fornire maggiore trasparenza al pubblico. Il sospetto, poi, è che le aziende abbiano sfruttato l'obbligo del governo di rimborsare le spese sostenute per la sorveglianza per realizzare veri e propri guadagni. Come spiega la consulente dell'Aclu, Michelle Richardson, a *The Hill*, gli attivisti per la privacy temono che le compagnie traggano profitto dal consentire al governo di spiare i loro utenti. Sarebbe proprio la differenza tra rimborso e profitto, in altre parole, a incentivare le aziende a supportare la sorveglianza dell'Nsa.

Non sono gli unici costi. Grazie a Snowden e al *Washington Post*, che pubblica un documento di 178 pagine, emerge per la prima volta il *black budget* dell'*intelligence*: nel 2013 ammonta a 52,6 miliardi di dollari. Con questo *scoop* ora sappiamo come sono spesi i soldi dei contribuenti e se i risultati ottenuti dalle sedici agenzie che compongono l'intelligence Usa soddisfino gli obiettivi posti dal presidente e dal Congresso.

Tra le rivelazioni contenute nel documento:

1. L'esplosione dei costi della Cia, saliti a 14,7 miliardi nel 2013, ben oltre le stime e superiore del 50% a quelli dell'Nsa, considerata finora «il gigante» del settore;
2. La conferma delle intrusioni informatiche dell'Nsa in sistemi informatici stranieri per carpire informazioni e in funzione di sabotaggio (offensive *cyber-operations*);
3. L'esistenza di indagini nel 2013 su oltre 4 mila impiegati in possesso di informazioni altamente riservate per scongiurare il rischio che le compromettano;
4. L'interesse dell'*intelligence* per paesi amici e nemici, mettendo insieme tra le priorità Cina, Russia, Cuba, Iran e Israele;
5. Il contrasto del terrorismo è solo il primo di cinque obiettivi dell'intelligence Usa;
6. La Corea del Nord è il Paese più difficile da penetrare. Gli analisti, in particolare, non sanno nulla delle intenzioni del leader Kim Jong Un.

Dagli attacchi subiti nel 2001 a oggi, scrive il *Post*,

le spese in *intelligence* hanno raggiunto i 500 miliardi di dollari:

> Un impero dello spionaggio con risorse e una portata superiore a quella di qualunque avversario, e sostenuto perfino ora con spese che rivaleggiano con o superano i livelli del culmine della Guerra Fredda.

Per il 2013, l'Nsa è costata 10,5 miliardi di dollari, denaro indispensabile per dotarsi dei sofisticati strumenti tecnologici di sorveglianza da cui è sempre più dipendente «per colmare i gap nella *human intelligence*».

Quanto alla sorveglianza del traffico Internet (Sigint, o Signals Intelligence), i fondi sono 48,6 milioni di dollari, destinati a «far fronte al sovraccarico informativo» prodotto dai dati ricevuti intercettando i cavi in fibra ottica che trasportano le connessioni e i provider di Silicon Valley. Un altro miliardo e 700 milioni di dollari è dedicato poi dalla Cia a soluzioni tecniche per la raccolta di dati, tra cui un programma condotto insieme all'Nsa per l'intercettazione di comunicazioni telefoniche e radio da territori ostili e chiamato Clansig. Il personale impiegato nella categoria Consolidated Cryptologic Program, dedicato a decifrare comunicazioni cifrate, ammonta invece a 35 mila unità. Somma le forze dell'Nsa, della marina e dell'esercito.

In un secondo articolo il *Washington Post* dettaglia un nuovo aspetto del *black budget*:

> L'Nsa sta pagando centinaia di milioni di dollari l'anno ad aziende statunitensi per accedere clandestinamente alle loro reti di comunicazione, filtrando vasti flussi di traffico alla

> ricerca di bersagli stranieri in un procedimento che finisce per coinvolgere grossi volumi di chiamate telefoniche, email e messaggi istantanei.

Il denaro, 278 milioni di dollari (meno dei 394 del 2011) nell'anno fiscale corrente, finisce nelle casse dei partecipanti del programma Corporate Partner Access. Una cooperazione riguardante la spina dorsale delle comunicazioni globali (*backbone*) che nasce addirittura negli anni Settanta con il programma Blarney, secondo i documenti di Snowden visionati dal quotidiano.

Il *Washington Post* rivela inoltre l'esistenza di Genie, un programma *top secret* il cui scopo è infiltrare sistemi informatici stranieri per porli sotto il controllo degli Stati Uniti.[42] Con un budget di 652 milioni di dollari, ha piazzato *malware*[43] in remoto all'interno di «decine di migliaia di macchine ogni anno, con la previsione di raggiungerne milioni» in futuro tramite il programma automatizzato Turbine. Così da rallentarle o mandarle in tilt. Entro la fine del 2013 Genie avrà effettuato almeno 85 mila infiltrazioni in macchine «strategiche in tutto il mondo», il quadruplo del numero disponibile nel 2008. Lo staff impiegato è di 1.870 persone.[44]

L'Nsa ha hackerato l'Onu

Nell'estate del 2012, la National Security Agency ha violato i sistemi crittografici a protezione della riservatezza dei sistemi interni di videoconferenza delle Nazioni Unite. Lo scrive il settimanale tedesco *Der Spiegel*, che documenta come in tre settimane l'intelligence statunitense abbia aumentato il numero di comunicazioni decifrate da 12 a 458. In un caso, intercettando un tentativo analogo da parte della controparte cinese. Come ricorda *Gigaom*, lo spionaggio a danno dell'Onu è illegale secondo la normativa internazionale. I documenti forniti da Edward Snowden e analizzati da *Der Spiegel*, inoltre, sostengono che gli Stati Uniti abbiano spiato oltre 80 ambasciate e consolati, l'Unione Europea e la International Atomic Energy Agency (Iaea), con sede a Vienna.[45]

Entrambe le operazioni rientrano tra le direttive di un programma di sorveglianza chiamato Special Collection Service. Un programma «intensivo e ben organizzato che nulla ha a che vedere con il contrasto del terrorismo», scrive il settimanale. *The Verge* ricorda come lo spionaggio degli uffici Onu da parte degli Usa, secondo molti osservatori, sia prassi da decenni. Per esempio, sarebbe avvenuto prima della guerra in Iraq, come sostiene il giornalista James Bamford, autore di diversi volumi sull'Nsa dal 2001 a oggi. Secondo il *New York Times*, le nuove rivelazioni fornite da *Der Spiegel*, insieme alle altre che coinvolgono cittadini tedeschi, potrebbero avere conseguenze sui rapporti tra Stati Uniti e Germania. In particolare, ufficiali tedeschi di

alto rango avrebbero fatto visita a Washington di recente per «negoziare un nuovo accordo formale» con gli Usa che stabilisca che nessuna delle due parti in causa può spiare l'altra.

L'intelligence britannica copia tutto il traffico Internet in Medio Oriente

L'*Independent* sostiene che il Regno Unito abbia una base segreta in Medio Oriente per la sorveglianza digitale; in particolare «per intercettare e processare vaste quantità di email, telefonate e traffico *web* per conto delle agenzie di *intelligence* occidentali». I dati sono estratti direttamente dai cavi in fibra ottica che attraversano la regione. Più precisamente, tutto il traffico che vi transita viene «copiato» e immagazzinato per l'analisi nei magazzini informatici della base. Le informazioni rilevanti ai fini di intelligence così ottenute sono trasmesse al Gchq britannico e quindi all'Nsa; è l'ennesima conferma del grado di collaborazione tra l'agenzia britannica e quella statunitense. *The Independent* scrive che non intende rivelare l'esatta ubicazione della base operativa, ma che la struttura è parte del più vasto progetto di sorveglianza digitale da un miliardo di sterline ancora in fase di realizzazione, e del programma Tempora rivelato a giugno dal *Guardian*. Ma chi è la fonte dello *scoop*? Tutte le informazioni sulla base segreta in Medio Oriente provengono dai documenti prelevati e diffusi da Edward Snowden, dice l'*Independent*. Glenn Greenwald, tuttavia, riporta la smentita di Snowden. La fonte sarebbe dunque il governo stesso, si legge nel pezzo di Greenwald, che si inserisce in una polemica tra i due quotidiani circa l'esistenza o meno di accordi tra il *Guardian* e le autorità britanniche su cosa pubblicare e cosa no. Secondo

Snowden e Greenwald, in sostanza, il governo starebbe lasciando fuoriuscire informazioni riservate che lo riguardano, dandole in pasto ai rivali per far apparire realmente pericolose le pubblicazioni di *Guardian* e *Washington Post*. L'accusa all'*Independent*, in altre parole, è di essere stato ingannato, o peggio imbeccato, dal governo. L'*Independent* smentisce a sua volta su Twitter, per bocca di Oliver Wright.[46]

Il comitato indipendente non è indipendente

Intanto negli Stati Uniti prende forma il comitato indipendente di esperti che dovrebbe valutare le operazioni di sorveglianza dell'Nsa, previsto da Barack Obama all'interno del suo proposito di riforma complessiva dell'operato dell'agenzia. Non mancano le polemiche. I quattro selezionati, scrive Abc, sono Michael Morrell (ex Cia e consulente per l'*intelligence* durante l'11 settembre), Richard Clarke (già consulente di alto profilo per la Casa Bianca durante le ultime tre presidenze, in particolare già coordinatore nazionale per sicurezza e lotta al terrorismo), Peter Swire (consulente per la privacy di Bill Clinton e per l'economia sotto Obama) e Cass Sunstein (di cui *Esquire* ricorda un *paper* del 2008 in cui consiglia al governo di infiltrare «*chat room*, *social network* e gruppi in carne e ossa» per smontare «complottismi» avversi, e anche di stipendiare segretamente voci «indipendenti» perché promuovano le sue posizioni *online*).

Come scrive *Ars Technica*, le polemiche sul reale grado di indipendenza del comitato, che fanno seguito a quelle sulla supervisione di James Clapper, non possono di conseguenza sorprendere. Chi ne difende l'autorevolezza sostiene che individui più addentro le stanze del potere abbiano maggiori probabilità di intervenire con successo e cambiare realmente le prassi dell'agenzia. Altri sostengono al contrario che le loro posizioni pregresse siano, appunto, un deterrente alla loro indipendenza.

Le polemiche non sono certo attutite da nuove

rivelazioni che estendono la portata conosciuta della sorveglianza di massa, mostrando anche come sia stata violata la Costituzione americana. Il 20 agosto, infatti, il *Wall Street Journal* scrive che l'Nsa ha la capacità di controllare fino al 75% del traffico Internet negli Stati Uniti. «In alcuni casi», precisa il quotidiano, l'agenzia legge anche il contenuto delle mail «inviate tra cittadini degli Stati Uniti»; è inoltre in grado di «filtrare le chiamate effettuate via Internet». L'Nsa ci riesce grazie a programmi di cui in parte si è già parlato: Blarney, Fairview, Oakstar, Lithium e Stormbrew, «tra gli altri», capaci di «filtrare e raccogliere informazioni» da colossi come At&T (che non ha voluto commentare). Mentre fino a ora si riteneva si allacciassero ai cavi in fibra ottica che scorrono sotto l'oceano laddove entrano nel paese, le fonti del *Wall Street Journal* sostengono che invece l'intercettazione avvenga in 12 diverse giunture della rete Internet all'interno degli Stati Uniti. Il sistema di raccolta dati, sempre secondo le fonti, funziona in due passaggi. Nel primo l'Nsa chiede alle aziende di telecomunicazione di inviarle «vari flussi di traffico» in cui ritiene sia più probabile reperire «*intelligence* straniera». Poi, nel secondo, è l'Nsa a intervenire copiando il traffico e decidendo quali comunicazioni trattenere sulla base di «indicatori forti» (*strong selectors*), come indirizzi mail o di computer appartenenti a organizzazioni o individui di suo interesse. Dettaglio interessante rivelato è che gli apparati di sorveglianza sono prodotti da Narus, Cisco e Juniper, gli stessi coinvolti nella produzione e vendita di strumenti simili a regimi autoritari. L'apparato tecnico di cui dispongono democrazie e dittature, in altre

parole, sembra essere in larga parte lo stesso.

Un altro colpo all'immagine del governo e dell'Nsa arriva dal *Washington Post*, che pubblica documento cui è stato tolto il velo di segretezza dalla stessa *intelligence* statunitense, dopo una battaglia di oltre un anno dell'Electronic Frontier Foundation. Si tratta di un *memorandum* segreto del Fisc, la corte adibita a valutare la sorveglianza dell'Nsa di 85 pagine del 2011, da cui si evince che «per molti anni», scrive il *Post*, «l'Nsa ha illegalmente raccolto decine di migliaia di email e altre comunicazioni elettroniche tra americani, come parte di un metodo di collezione dei dati oggi rivisto».

La corte, in questa circostanza, sembra preoccupata delle menzogne che l'Nsa ha raccontato perfino alla giustizia. «Per la prima volta», si legge, «il governo ha informato la corte che il volume e la natura delle informazioni che stava raccogliendo sono sostanzialmente differenti da ciò che la corte era stata indotta a credere».

In particolare, precisa *The Verge*, secondo i dati del 2011 l'Nsa ha raccolto oltre 250 milioni di «comunicazioni via Internet», la gran parte grazie al discusso programma Prism. Che la raccolta dei dati dell'Nsa fosse «incostituzionale» già dal 2008, del resto, il *Post* l'aveva sostenuto qualche giorno prima, pubblicando un *audit* interno della stessa agenzia che lo dimostrerebbe. Da aprile 2011 a marzo 2012, cioè dopo il parere del Fisc pubblicato in seguito, le violazioni della privacy o delle indicazioni della corte sono state ben 2.776.

Per Barack Obama, intervistato in esclusiva

alla Cnn, le rivelazioni in questione dimostrano che le salvaguardie, le garanzie, i controlli previsti dalla legge ai programmi di sorveglianza «funzionano». Si dice fiducioso che nessuno alla Nsa stia cercando di commettere abusi alle libertà civili dei cittadini. La stessa Nsa, in una dichiarazione a *Bloomberg*, ha ammesso casi «molto rari» di violazioni «intenzionali» dei suoi poteri negli ultimi dieci anni. Per eccesso di zelo, secondo l'agenzia. Per *Bloomberg* l'ammissione è sufficiente per mostrare una contraddizione rispetto a quanto sostenuto dall'Nsa dall'inizio dello scandalo.

CAPITOLO IV: SETTEMBRE

L'Nsa ha spiato Al Jazeera e diplomatici francesi

Per la prima volta dallo scoppio dello scandalo Datagate, è accertato lo spionaggio dei media da parte dell'Nsa. Secondo uno dei documenti (datato 23 marzo 2006) passati al settimanale *Der Spiegel* da Edward Snowden, il bersaglio è Al Jazeera. Lo spionaggio dell'emittente del Qatar è avvenuto hackerando le comunicazioni internet protette. Tra i soggetti intercettati ci sarebbero stati «bersagli interessanti» che Al Jazeera intendeva tenere al sicuro in modo particolare. L'Nsa, aggiunge *Der Spiegel*, ha considerato la riuscita dell'operazione un «successo ragguardevole», e i bersagli intercettati «ad alto potenziale come fonti di *intelligence*». Sempre *Der Spiegel*, dopo aver dettagliato le modalità di spionaggio di Unione Europea e Onu da parte dell'intelligence Usa di cui abbiamo già detto, ha inoltre documentato la sorveglianza condotta ai danni di diplomatici francesi. Anche qui il materiale, risalente al giugno 2010, parla dell'intrusione nei sistemi criptati di comunicazione del ministero degli Esteri di Parigi come di una «storia di successo». Controllati anche i rappresentanti francesi a Washington e alle Nazioni Unite, si legge in una lista risalente a settembre dello stesso anno. L'Nsa, scrive il settimanale, era

interessata agli «obiettivi di politica estera francese, specialmente nel commercio di armi, e alla sua stabilità economica».

Il progetto Hemisphere: oltre la sorveglianza dell'Nsa

Il *New York Times* rivela che l'accesso ai *log* delle telefonate dei cittadini statunitensi non è avvenuto solo in funzione di contrasto del terrorismo e all'interno degli accordi con operatori come Verizon di cui ha scritto il *Guardian* a giugno.[47] Vi accedono anche gli agenti della narcotici, in particolare ai database di At&T, ottenendo informazioni molto più lontane nel tempo. In particolare, secondo il progetto Hemisphere, il governo paga i dipendenti del colosso delle telecomunicazioni affinché prendano parte alle operazioni antidroga fornendo agli agenti accesso a un insieme di dati telefonici che risalgono fino al 1987. «La portata e la longevità dell'immagazzinamento dei dati», scrive il *Times*, «sembra non avere paragoni con altri programmi governativi», potendo attingere a telefonate effettuate 26 anni fa. E aggiungendo quattro miliardi di registrazioni al database ogni giorno, come sostengono le *slide* di presentazione del programma pubblicate sempre dal quotidiano newyorkese. Il programma è stato lanciato, in gran segreto, nel 2007. Secondo l'amministrazione Obama ci sarebbe tuttavia una differenza chiave tra Hemisphere e i programmi di sorveglianza dell'NSA: i dati sarebbero immagazzinati da AT&T, non dal governo, che li richiederebbe tramite *administrative subpoenas*. Il portavoce di AT&T, Mark A. Siegel, tuttavia, si è rifiutato di rispondere alle dettagliate domande del *Times*, che includevano richieste di chiarimento circa la

percentuale di telefonate all'interno degli Stati Uniti registrate da Hemisphere, la dimensione del suo database, e le modalità di accesso dei suoi impiegati ai dati.

La guerra dell'Nsa alle comunicazioni protette

Guardian, *New York Times* e *Pro Publica*, in una collaborazione per descrivere e comprendere il significato dei documenti *top secret* forniti da Edward Snowden (cinquantamila, in totale, alle tre testate), rivelano che la National Security Agency, insieme alla sua controparte britannica, il Gchq, è in grado di decifrare buona parte dei sistemi di comunicazione protetti su cui fanno affidamento centinaia di milioni di utenti Internet nel mondo per mettere al sicuro i propri dati personali, le transazioni *online*, i rapporti bancari, i dati sensibili di natura medica, e anche mail, le *chat*, ricerche in rete e telefonate. Come si legge sul quotidiano newyorkese, è intaccato uno dei segreti più gelosamente custoditi dalle agenzie dei due paesi: la capacità di leggere messaggi cifrati mentre l'utente che li invia è convinto della loro cifratura. Tutte e tre le testate sono state contattate da «ufficiali dell'*intelligence*» che hanno chiesto di non pubblicare gli articoli che dettagliano le rivelazioni, sostenendo che potrebbero indurre i «bersagli stranieri» (definizione di comodo, come visto e come vedremo subito) a mutare sistemi di cifratura e dunque sparire dallo sguardo dell'Nsa. I tre giornali hanno comunque deciso di pubblicare la notizia, e *Pro Publica* ha anche scritto un editoriale per spiegare perché:

> Crediamo che questa storia sia importante. Mostra che le aspettative di milioni di utenti su Internet circa la privacy delle loro comunicazioni elettroniche sono errate.

Per il *Times* il nemico dell'*intelligence* è «l'utilizzo onnipresente della crittografia in rete». Così, dopo che negli anni Novanta si è tentata con scarsa fortuna la strada di inserire una via d'accesso privilegiata (*backdoor*) nei sistemi di cifratura attraverso una battaglia pubblica (quella dell'amministrazione Clinton per il Clipper Chip), si è dedicata a realizzare lo stesso scopo di nascosto. È uno stesso memo dell'agenzia a sostenere che «lo sforzo nell'ultimo decennio», definito come «aggressivo» e condotto su diversi fronti, è stato proprio «violare le tecnologie di cifratura di diffuso utilizzo su Internet».[48] Riuscendoci, questa volta. Perché l'Nsa non utilizza solo il *brute force*, cioè il puro calcolo reso possibile dai suoi «supercomputer», per violare la riservatezza delle comunicazioni degli utenti. L'agenzia di *intelligence* detiene un database interno di chiavi crittografiche di prodotti commerciali specifici, un Key Provisioning Service, che le garantisce di «decifrare automaticamente molti messaggi». Se una chiave fosse mancante, c'è un Key Recovery Service che si preoccupa di ottenerla. L'*intelligence* ha anche e soprattutto stretto accordi segreti, dicono i documenti, con compagnie tecnologiche e gli stessi produttori di servizi Internet proprio per inserire di nascosto «vulnerabilità», cioè appunto *backdoor*, nei *software* commerciali per la cifratura. Il materiale e le interviste condotte per corroborarne i contenuti non specificano quali aziende siano coinvolte.

Si legge su *Pro Publica*:

> Per almeno tre anni, dice un documento, il Gchq, quasi certamente in stretta collaborazione con l'Nsa, ha cercato di avere accesso al traffico protetto dei più popolari colossi

> web: Google, Yahoo, Facebook e Microsoft Hotmail. Nel 2012 l'intelligence britannica avrebbe ottenuto «nuove opportunità di accesso» ai sistemi di Google.[49]

A prescindere dalle aziende interessate, scrive il Times:

> l'Nsa si è introdotta nei computer bersaglio per catturare i messaggi prima che venissero cifrati. In alcuni casi, le aziende sostengono di essere state obbligate dal governo a fornire le loro chiavi crittografiche o a creare *backdoor*.

Il *Guardian*, infine, pubblica due documenti: come l'Nsa collabora con le compagnie tecnologiche e la guida alla criptoanalisi. In particolare, il primo dettaglia il *budget* dell'*intelligence*, mostrando come le operazioni proseguano a tutto spiano con un investimento per il 2013 di 254,9 milioni di dollari (a fronte dei 20 spesi per Prism), previsti all'interno di un programma decennale (con picchi di investimenti per 800 milioni) di «Sigint (cioè Signals Intelligence, in sostanza raccolta del traffico Internet) Enabling». Lo scopo? Coinvolgere «attivamente» aziende tecnologiche statunitensi e straniere per «influenzare di nascosto e/o sfruttare apertamente i design dei loro prodotti commerciali». E inserirvi, come detto, vie d'accesso conosciute all'intelligence ma non ai consumatori. Definiti significativamente, dice il *Guardian*, «avversari». Altro obiettivo è influenzare gli standard crittografici in uso a livello internazionale. Il programma si chiama, in codice, Bullrun[50] per l'Nsa e Edgehill per il Gchq; entrambi i nomi fanno riferimento ad avvenimenti delle rispettive guerre civili. Tra i protocolli di cifratura di popolare utilizzo cui le agenzie hanno segretamente

accesso ci sono l'Https, il voice-over-Ip e l'Ssl. Una infografica dettagliata è reperibile sul sito del *New York Times*.

Non tutti i sistemi di protezione sono ancora stati decifrati, si legge nei documenti. E del resto, ricordano tutte le testate coinvolte nelle rivelazioni, lo stesso Snowden lo aveva affermato lo scorso giugno nel Q&A con i lettori del *Guardian*. Lo stesso guru della sicurezza informatica Bruce Schneier, che anche nell'intervista concessami per *L'Espresso* ha mostrato scetticismo, concorda: è ancora possibile proteggersi dallo sguardo dell'*intelligence*. Ma come? In cinque punti, dice:

1. Usando servizi come Tor[51] per «nascondersi nella rete». Non che l'Nsa non prenda di mira gli utenti del servizio, come detto anche nella nostra intervista, ma richiede lavoro. E non sempre quel lavoro viene fatto;
2. Cifrando le proprie comunicazioni. Sarà comunque più sicuro che non farlo;
3. Utilizzando un computer mai connesso a Internet, servendosene per cifrare il file desiderato e solo allora trasferendolo – meglio se tramite una chiavetta Usb sicura – sul nostro computer abituale;
4. Diventando sospettosi circa qualunque soluzione commerciale, specie se da grossi rivenditori;
5. Sfruttando servizi di crittografia a chiave pubblica «che devono essere compatibili con altre implementazioni», perché rendono più difficile per l'Nsa intrufolarsi di nascosto e imporre modifiche a suo uso e consumo.

Anche l'Eff ha i suoi suggerimenti, di natura più politica: firmare la petizione per fermare lo spionaggio dell'Nsa, contattare direttamente i membri del Congresso, spronare gli ingegneri informatici (come quelli dello Ietf, già al lavoro per cifrare tutto il traffico Internet) a reagire a queste indebite intrusioni nel loro lavoro. Scrive poi *Reuters* che il Brasile sta cercando una soluzione più radicale allo spionaggio dell'Nsa, di cui è stata vittima perfino la sua presidente Dilma Rousseff: costruire un proprio cavo in fibra ottica sicuro per le comunicazioni con i governi di paesi vicini. Ironia della sorte, proprio nelle stesse ore il Pew Research Center riportava i dati di un sondaggio secondo cui gli utenti desiderano fortemente l'anonimato *online*. Poco dopo si è scoperto quanto sia davvero complicato mantenerlo. Ancora, solo due giorni prima Wikileaks pubblicava la terza parte degli *Spy files*, dettagliando ulteriori aziende che hanno fornito strumenti di sorveglianza digitale utilizzati per scopi non legittimi. La soluzione adottata da Wikileaks per combattere gli abusi è stata tracciare gli spostamenti dei manager di alcune delle compagnie coinvolte.

Gli abusi dell'Nsa sulle utenze telefoniche

Secondo documenti in passato coperti da segreto e resi pubblici dalla National Security Agency in risposta a una richiesta di trasparenza (Foia) dell'Eff, l'*intelligence* statunitense ha abusato dei suoi poteri di indagine sulle utenze telefoniche presenti nei suoi database. Come si legge sul sito dell'organizzazione per i diritti in Rete, la corte deputata a controllare l'operato dell'Nsa, la Fisa, aveva richiesto che si potessero svolgere solo per utenze gravate, previa dimostrazione, dal ragionevole sospetto («*reasonable articulable suspcion*») di un coinvolgimento in attività terroristiche. Ma i numeri della lista (*alert list*) delle utenze di interesse parlano di 19 mila unità nel 2009: solo per 1.800 l'Nsa disponeva di un ragionevole sospetto. Il programma che giustificava la raccolta dei metadati telefonici era partito nel 2006, quando la *alert list* era composta da 4 mila numeri, scrive la Cnn.

Che significa in concreto? Che l'*intelligence* conduceva indagini senza ragionevole sospetto, e usava i dati così ottenuti per garantirsi l'autorizzazione a compiere indagini sui sospetti. Nelle parole di Trevor Timm, dell'Eff: «stavano conducendo ricerche in assenza di sospetto per ottenere il sospetto che la corte Fisa richiedeva per condurre ricerche». Una chiara violazione delle regole, dato che, come scrive *Reuters*, il criterio per condurre ricerche sui metadati telefonici si è tradotto di fatto, tra il 2006 e il 2009, nella semplice convinzione che l'utenza bersaglio potesse avere qualche tipo di valore in termini di intelligence straniera. Molto

più vago e permissivo, dunque, rispetto a un Ras.

Quanto alle ricerche, consentivano di ottenere i contatti chiamati dall'utenza bersaglio, oltre a quelli di chi riceveva la chiamata. A questo modo, circa 600 utenze di cittadini statunitensi sono state passate «impropriamente», scrive sempre *Reuters*, a Cia e Fbi come «sospette».

Incredibile la giustificazione dell'intelligence, che sostiene di non aver compreso del tutto come funzionasse il suo sistema di sorveglianza dell'epoca, al punto da non essere in grado di spiegarlo nemmeno alla corte, corsa ai ripari dal 2009, chiedendo l'autorizzazione alle ricerche utenza per utenza.

Per il *Washington Post* l'ammissione rivela una preoccupante accoppiata di estensione dei poteri di sorveglianza e mancanza di competenza tecnica nell'esercitarli, per non parlare dei ripetuti inganni orditi ai danni della corte, che tra l'altro avrebbe dovuto controllarne l'operato proprio sulla base dei dati forniti dall'Nsa.

Del resto, è stato proprio il *Post*, l'8 settembre, a raccontare come nel 2011 l'amministrazione Obama sia riuscita a strappare alla corte la rimozione dei limiti alla raccolta dei metadati telefonici e delle mail da parte dell'Nsa, estendendo da cinque a sei anni (e oltre, in casi eccezionali) il periodo in cui è legittimo detenere le intercettazioni delle comunicazioni statunitensi. Il tutto «senza dibattito pubblico o autorizzazione del Congresso». Nel 2008, in particolare, la corte aveva ottenuto il divieto di compiere ricerche su vasti database di mail e utenze telefoniche di cittadini statunitensi «senza autorizzazione giudiziaria»: bastava

fosse «ragionevolmente probabile» si producessero «elementi di intelligence straniera». Divieto rimosso nel 2011, alterando radicalmente la logica di fondo della sorveglianza governativa: prima raccogli i dati, poi curati della privacy dei cittadini. Secondo l'Nsa, ciò è necessario per garantire l'identificazione tempestiva di potenziali bersagli.

Il social network dell'Nsa

Se ci fosse di che scherzare, si potrebbe dire con Ryan Singel che l'Nsa ha aperto il suo *social network*, che non è richiesto login e che ne siamo tutti membri da anni. Il problema è che la realtà non è molto diversa. Scrive infatti il *New York Times*, sulla base delle interviste a ufficiali condotte dal quotidiano e dei documenti forniti da Edward Snowden:

> Dal 2010, la National Security Agency sfrutta le sue enormi raccolte di dati per creare sofisticati grafici di alcune delle connessioni sociali degli americani, che possono identificare chi frequentano, dove si trovano in un preciso momento, i loro compagni di viaggio e altre informazioni personali.

Per esempio, si legge ancora, preferenze religiose e politiche, se si ha una relazione extraconiugale o uno psichiatra. L'*intelligence* Usa può aiutarsi nell'analisi dei metadati telefonici e via mail raccolti con i dati provenienti da altre fonti pubbliche e commerciali, si legge sul *Times*, tra cui:

> Codici bancari, informazioni assicurative, profili Facebook, liste di passeggeri o votanti, informazioni di localizzazione Gps, così come registri di proprietà e non specificati dati fiscali, secondo i documenti.

Si tratta, secondo gli esperti, della profilazione individuale più completa e «*predittiva*» che si possa ottenere da conversazioni telefoniche e via Internet. A compierla, uno strumento di nome Mainway:

> Un deposito in cui affluiscono quotidianamente le enormi

> moli di dati che scorrono nei cavi in fibra ottica dell'agenzia, delle aziende che ne sono partner e delle reti informatiche straniere che sono state hackerate.

Nel 2011, si trattava di 700 milioni di metadati telefonici al giorno; nel budget del 2013, è scritto che la capacità è di 20 miliardi di *record events* al giorno, disponibili all'Nsa entro 60 minuti. A mettere in relazione i dati e scoprirvi potenziali intrecci e pattern di interesse per l'*intelligence* è un sistema chiamato Enterprise Knowledge System (costo: 394 milioni di dollari), che computa in automatico informazioni prelevate da 94 «tipologie di entità» (numeri di telefono, email, indirizzi Ip) e 164 «tipologie di relazioni». E costruisce a questo modo un vero e proprio social network in cui vengono messe in mostra le «comunità di interesse» dei profili bersaglio.

In precedenza, ciò era possibile solo per bersagli stranieri. Ma, come spiega Kevin Gosztola su *Firedoglake*, la restrizione è stata eliminata sotto la presidenza di Bush Jr, mentre Barack Obama e la sua amministrazione «non hanno avuto apparentemente problemi a proseguire l'estensione dei poteri di sorveglianza». Un memo del 2011 sostiene che i cittadini americani possono essere controllati se viene fornita una giustificazione in termini di «intelligence straniera».

L'Nsa non ha voluto rivelare il numero di individui statunitensi analizzati a questo modo, e i documenti non lo specificano, scrive il *Times*. Tuttavia il senatore Ron Wyden ha lasciato intendere nelle sue domande al direttore dell'Nsa, Keith Alexander, durante una recente audizione in Senato che l'agenzia raccoglie i dati

di localizzazione telefonica di milioni di cittadini americani. Non a caso la proposta di riforma di Wyden, che secondo *Tech Crunch* «potrebbe passare davvero», prevede la fine di questo tipo di prassi.

Come vengono immagazzinati i metadati? E per quanto? Come scrive James Ball sul *Guardian*, gli utenti bersaglio sono «milioni» e i loro dati sono memorizzati dall'Nsa per un lasso di tempo il cui limite superiore è un anno. E questo «a prescindere che si tratti di persone di interesse per l'agenzia»; l'*intelligence* registra tutto, lo trattiene per (fino a) un anno e se in quel lasso di tempo le informazioni dovessero tornare utili, le è possibile reperirle e analizzarle. Del resto, sono già in suo possesso. Tra i documenti forniti al quotidiano londinese da Edward Snowden, infatti, c'è una guida introduttiva all'argomento, a uso dell'intelligence, chiamata in codice «Marina». «Tutti i metadati provenienti da computer raccolti dai sistemi dell'Nsa», si legge, finiscono nel suo database. Per quelli telefonici c'è un «sistema separato». Grazie a Marina è possibile tenere traccia delle navigazioni di un utente, leggere resoconti delle sue attività ed esportare i dati di interesse in «diversi formati», grafici compresi.

In sostanza, si conferma che «tutti i dati "visionati" dall'Nsa sono immagazzinati». Il magazzino contiene, secondo le stime della stessa agenzia di *intelligence*, l'1,6% del traffico Internet del pianeta. Numero che, escludendo audio e video in streaming e limitandosi alle sole comunicazioni interpersonali, lievita non di poco secondo Ball.

Marina conterrebbe i dati di milioni di individui, dunque, americani e non. E l'Nsa, a precisa domanda

sulla *ratio* di una sorveglianza che coinvolge una stragrande maggioranza di innocenti destinati a rimanere tale, ha risposto con il solito comunicato che nega e non dice perché dovremmo credere a quella negazione.

CAPITOLO V: OTTOBRE

L'Nsa registra le liste di contatto di milioni di utenti

La National Security Agency ha un programma di raccolta delle liste dei contatti per servizi mail e *chat* di centinaia di milioni di utenti nel mondo, Stati Uniti compresi. L'ordine di grandezza è di centinaia di migliaia al giorno, scrive il *Washington Post*: secondo una presentazione Power Point ottenuta grazie a Edward Snowden, in sole 24 ore l'Nsa ha ottenuto oltre 440 mila liste di contatti da Yahoo, 105 mila da Hotmail, quasi 83 mila da Facebook, 33 mila da Gmail e 22 mila da altri *provider*. All'anno fanno circa 250 milioni, ciascuna con all'interno nomi, indirizzi, numeri di telefono, informazioni commerciali e sui legami familiari. E, in alcuni casi, anche un'anteprima dei contenuti dei messaggi inviati via mail:

> Presi tutti insieme, questi dati consentirebbero all'Nsa, se le fosse permesso, di comporre mappe dettagliate della vita di una persona, così come raccontata dai suoi contatti in ambito personale, professionale, politico e religioso.

Un ritratto che «potrebbe essere anche fuorviante», prosegue il *Post*, «creando false "associazioni" con ex coniugi o persone con cui il detentore dell'*account* non

ha avuto contatti per molti anni». Per poter esaminare i collegamenti tra contatti di una lista, l'Nsa deve mostrare uno specifico interesse in termini di intelligence straniera. Ma, nota il *Post*, basta figurare tra i contatti di un bersaglio ritenuto «associato a una potenza straniera o a un territorio straniero» per finire nel mirino dell'*intelligence*.

Il processo di raccolta avviene tramite accordi segreti con compagnie straniere di telecomunicazione e agenzie di *intelligence* alleate; i dati sono registrati direttamente dall'Nsa attraverso 18 punti di raccolta del traffico Internet al di fuori del territorio statunitense (chiamati Sigads, Signal Intelligence Activity Designators). L'Nsa, infatti, non è autorizzata a farlo all'interno del Paese, per cittadini Usa. Ciononostante, gli americani coinvolti sarebbero milioni, se non decine di milioni, come confermato dalle fonti di intelligence interpellate dal quotidiano.

Come nota Kurt Opsahl dell'Eff, basta che l'azienda che gestisce la lista dei contatti possieda un *data center* al di fuori degli Stati Uniti per consentire all'Nsa di accedervi. Si tratta, scrive *Business Insider*, di uno stratagemma per violare la legge e sottrarsi al controllo, già scarso o nullo, del Congresso e della Corte Fisa. Per il *Post* la risposta standard dell'Nsa è sostenere che per gli utenti statunitensi i dati sono stati ottenuti «incidentalmente». Per il modo in cui i dati vengono raccolti poi, nota ancora il *Post*, *l'intelligence* non è costretta a notificare l'avvenuta intercettazione delle liste di contatti alle aziende bersaglio. Che, al solito, negano tutte. Yahoo si è spinta fino a dichiarare che da gennaio 2014 le mail inviate tramite il suo servizio

saranno finalmente cifrate. Ma i dati raccolti restano talmente tanti, *spam* compreso, che l'Nsa ha dovuto dotarsi di programmi in grado di eliminare i contenuti inutili o indesiderati.[52]

I tentativi di violare l'anonimato *online*

Avevamo già visto l'interesse dell'Nsa per le comunicazione protette e i sistemi di crittografia,[53] tra i quali Tor rappresenta forse la principale minaccia, dal punto di vista dell'*intelligence* statunitense. A inizio mese il *Guardian* dettaglia ulteriormente gli attacchi proprio verso The Onion Router:

> La National Security Agency ha tentato ripetutamente di sviluppare attacchi contro gli utenti di Tor, un popolare strumento usato per la protezione dell'anonimato *online*, nonostante il *software* sia finanziato principalmente dallo stesso governo americano.

L'*intelligence* non è riuscita tuttavia a comprometterne la sicurezza: ciò che ha potuto fare è stato sviluppare una tecnica per identificare alcuni utenti del pacchetto Tor Browser Bundle e quindi controllarne i computer attraverso un attacco al browser Firefox in uso al suo interno. Come scrive Bruce Schneier, l'esperto di sicurezza informatica messo al lavoro dal quotidiano britannico sui nuovi documenti di Edward Snowden, si tratta della cosiddetta Cne (Computer Network Exploitation), compiuta dal Systems Intelligence Directorate (Sid) dell'agenzia.

In cosa consiste? In sostanza, spiega Schneier, l'Nsa compone una «impronta» *digitale* dell'utente tramite i suoi programmi di raccolta dati in collaborazione con i giganti delle telecomunicazioni, allacciandosi alla *backbone* di Internet (Stormbrew, Blarney e altri); analizza il materiale così ottenuto grazie al database di XKeyscore; infine setaccia in automatico, grazie a

programmi come Turbolence, Turmoil e Tumult, la mole di dati cercando di individuare connessioni a Tor. Una volta individuato un utente, l'Nsa ne infetta il computer riuscendo a ottenerne il «pieno controllo». Compresa, si legge, tutta l'attività *online*, e perfino registrando ogni tasto sia premuto sulla tastiera.

La tecnica va sotto il nome di Egotistical Giraffe, come si legge nella presentazione che la dettaglia. In alcuni casi, il processo di identificazione dell'utente, come sottolineano *Cnet* e svariati osservatori, inizia comprando inserti pubblicitari nel network di Google Adsense. Servono per piazzare *cookie* che traccino le navigazioni del bersaglio. Un sistema difficile da combattere, si legge sempre su *Cnet*, perché basato sul funzionamento stesso della rete.

Un problema per Tor, certo, ma limitato. Prima di tutto, perché per compiere con successo questo tipo di attacchi, sostiene Schneier, serve essere nella posizione privilegiata in termini di accesso e monitoraggio del traffico Internet di cui può disporre solamente un'agenzia come l'Nsa. E poi perché perfino l'Nsa fatica a vincere le barriere innalzate da Tor a difesa dell'utente. Non a caso la presentazione top secret in cui ne parla si chiama *Tor stinks* («Tor fa schifo, puzza»). Al suo interno, poi, si legge l'ammissione dell'intelligence: «non saremo mai in grado di de-anonimizzare tutti gli utenti di Tor sempre». Lo stratagemma adoperato dall'Nsa consente di avere successo solo per una «frazione molto piccola» dell'utenza, e ha fallito nel caso di una richiesta di identificare un utente in particolare.

Un altro documento pubblicato dal *Guardian* evidenzia come Tor sia sicuro al punto di

essere considerato il «re» degli strumenti di anonimato, senza pretendenti al trono in vista.[54]

Restano tuttavia i motivi di preoccupazione. Come scrive il *Washington Post*:

> [I nuovi documenti] suggeriscono che l'Nsa non può gettare lo sguardo direttamente all'interno della rete anonima Tor, ma che ha ripetutamente svelato utenti aggirandone le protezioni. I documenti illustrano anche il potere dell'Nsa di penetrare almeno parzialmente in quello che è stato a lungo considerato l'angolo più sicuro di Internet.

È sempre il *Post*, del resto, a scrivere che gli utenti individuati tramite Egotistical Giraffe sono stati ventiquattro in un singolo week-end, otre a uno dei leader della propaganda di Al Qaeda nella penisola araba. La strategia di infettare i computer dei bersagli individuati è servito all'Nsa per prendere controllo di Freedom Hosting e colpire alcuni utenti Tor che si erano celati dietro ai suoi servizi per fruire di materiale pedo-pornografico.

Il *Post* pubblica anche un documento del 2006 che certifica che gli sforzi dell'Nsa per sconfiggere le protezioni di Tor, e identificare masse di suoi utenti, si protraggono da sette anni.[55]

Una prima risposta di Tor è stata rimarcare che il ricorso a un *browser exploit* dimostra che «non ci sono indicazioni» che l'Nsa possa «violare il protocollo» del *software*, e sottolineare che il procedimento funziona solamente quando non diventi di massa: «anche se l'Nsa vuole sorvegliare tutti e in ogni luogo, deve essere molto più selettiva su quali utenti di Tor spiare».

Il Datagate e l'Italia

Dopo quanto rivelato in estate e i dubbi lasciati dalle istituzioni (in particolare Copasir e governo),[56] l'Italia è di nuovo chiamata in causa sul Datagate. *Der Spiegel* pubblica una documentazione sulla base dei dati prodotti dal programma dell'Nsa Boundless Informant.[57] Stando alla documentazione, tra il 10 e il 28 dicembre 2012, la National Security Agency ha registrato circa 46 milioni di metadati (numero di chiamante e chiamato, durata e localizzazione della chiamata) di conversazioni telefoniche in Italia. *Der Spiegel* ha rivelato i dati sull'Italia per operare un confronto con la quantità di metadati raccolti in Germania (361 milioni); la perfetta congruenza tra il numero evidenziato dal settimanale per la Francia e quello contenuto nelle rivelazioni di *Le Monde*, riaccende lo scandalo in Europa e provoca uno scontro diplomatico tra il governo francese e Barack Obama.

La quantità di metadati telefonici registrati in Italia è inferiore a Germania, Francia e Spagna (poco più di 60 milioni),[58] ma non tale da giustificare il silenzio e le contraddizioni del governo sulla vicenda. Tanto più che negli stessi giorni anche i quotidiani italiani tornano a occuparsi del Datagate e delle implicazioni per il paese. Sul *Corriere della Sera* Fiorenza Sarzanini, infatti, scrive il 22 ottobre:

> I controlli su telefonate e comunicazioni telematiche riguardano anche l'Italia. Chiamate, email, sms: dietro il paravento della sicurezza nazionale gli Stati Uniti hanno acquisito milioni di dati che riguardano i nostri concittadini.

A confermarlo, l'esperienza diretta di una delegazione di membri del Copasir, recatasi «circa tre settimane fa» negli States per giorni di «incontri con i direttori delle agenzie di intelligence e i presidenti delle commissioni del Congresso».

Su *Repubblica*, ne parla Claudio Fava di Sel, tra i partecipanti:

> Dai nostri qualificatissimi interlocutori abbiamo avuto la conferma che telefonate, sms, email tra Italia e Stati Uniti, in entrata e in uscita, sono oggetto di un programma di sorveglianza elettronica del governo Usa regolato esclusivamente dalle leggi federali, che, per quanto i nostri interlocutori ci hanno ribadito, sono la sola bussola che governa questo tipo di attività di spionaggio.

Fava precisa ancora che «non ci sono stati forniti dati sulla dimensione del traffico sorvegliato, ma indicazioni sul metodo che viene utilizzato». L'autore del pezzo, Carlo Bonini, scrive che si tratta di una raccolta di dati basata su criteri di *profiling* su soggetti ritenuti «"sensibili" ai fini della sicurezza nazionale». In sostanza, una formulazione vaga:

> Un meccanismo a strascico per una rete di prevenzione nelle cui maglie possono facilmente restare impigliate le comunicazioni della diplomazia (ambasciate e consolati), quelle militari, piuttosto che quelle delle nostre aziende che operano all'estero o quelle di semplici cittadini.

Informazioni che stridono con quanto dichiara il sottosegretario Marco Minniti dopo la riunione del Copasir del 23 ottobre.[59] L'Agi riporta le dichiarazioni del sottosegretario:

> Relativamente alla questione Datagate il Sottosegretario Minniti ha riconfermato la non conoscenza dell'esistenza del programma Prism da parte del Governo e della nostra *intelligence*; inoltre ha ribadito che, con ragionevole certezza, è stata garantita la privacy delle comunicazioni tra cittadini italiani all'interno del territorio nazionale, oltre che delle comunicazioni originate dalle sedi diplomatiche all'estero.

Ancora Fiorenza Sarzanini, sempre sul *Corriere*, scrive il 24 ottobre di una possibile trattativa tra Stati Uniti e Italia: «il 25 luglio scorso l'Italia ha avuto la conferma che i dati relativi alle nostre telefonate, sms e email vengono acquisiti dagli Stati Uniti». Ciò conferma la versione di Claudio Fava. L'aspetto stupefacente della vicenda è che, secondo la ricostruzione di Sarzanini, è proprio Minniti e proprio al Copasir a «fornire un clamoroso riscontro rispetto a quanto è emerso anche in Francia» circa la raccolta dei metadati delle comunicazioni. Dice il sottosegretario:

> Abbiamo avuto la conferma che queste informazioni vengono acquisite attraverso il traffico che entra e esce dagli Stati Uniti, ma ci è stato assicurato che mai alcuna comunicazione è stata intercettata.

Dove si intende che non sono stati intercettati i contenuti. A meno che il bersaglio diventi «sensibile», spiega Sarzanini (e abbiamo scoperto quanto è semplice e aleatorio diventarlo). Insomma, l'Italia come la Francia. Al punto che non è consentito «escludere che il controllo sia avvenuto nei confronti di personalità e autorità, paventando anche il rischio di uno spionaggio politico», scrive ancora Sarzanini. Come avvenuto in

Germania, per Angela Merkel.[60]

La (non) posizione delle autorità italiane si complica a fine mese, a partire dalle indiscrezioni del *Wall Street Journal*, e proseguendo con le affermazioni del direttore dell'Nsa Keith Alexander. A raccogliere i milioni di metadati in Spagna, Francia e Italia non sarebbe stata *l'intelligence* Usa, ma quella dei rispettivi paesi, trasmettendo in seguito i dati ottenuti all'Nsa, Sarebbero stati loro a trasmettere in seguito i dati ottenuti all'Nsa, sulla base di precisi accordi.

Per Alexander, come riportato dal *Washington Post*, chi ha diffuso i documenti prelevati da Edward Snowden non ne ha compreso il contenuto: «quelle non sono informazioni che abbiamo raccolto noi sui cittadini europei», ha detto all'House Intelligence Committee. «Rappresentano informazioni che noi e i nostri alleati della Nato abbiamo registrato in difesa dei nostri Paesi e a supporto delle nostre operazioni militari».

Le Monde ed *El Mundo* confermano. Secondo il primo, lo scambio di informazioni tra Francia e Usa avverrebbe sulla base di un accordo di cooperazione chiamato «Via della seta» e stabilito tra la direzione del Dgse (l'omologo dell'Nsa per la Francia) e Stati Uniti «tra le fine del 2011 e l'inizio del 2012». «Improbabile», aggiunge Le *Monde*, che il governo francese non ne fosse a conoscenza, dato che «sovrintende il finanziamento delle infrastrutture di intercettazione e di stoccaggio del Dgse». Il secondo, invece, si affida a un articolo scritto direttamente dall'ex firma del *Guardian*, Glenn Greenwald, in cui si legge che la sorveglianza di massa statunitense compiuta in Spagna «è più il frutto della cooperazione dei due paesi che di un abuso di potere» da

parte degli Usa. E i servizi spagnoli non solo ne erano a conoscenza: hanno, scrive Greenwald, perfino facilitato le operazioni dell'Nsa. La fonte è un documento fornito da Snowden allo stesso Greenwald.

Può l'Italia fare eccezione? *Le Monde* cita l'Italia tra i paesi dotati della stessa relazione «amicale» con gli Stati Uniti. Lo stesso termine adoperato da *El Mundo*, che include il nostro tra i paesi «affidabili e amici», ma anche «in grado di poter raccogliere dati contro gli interessi americani». Per questo, l'Italia sarebbe considerata tra i partner «di seconda fascia»,[61] subito seguente ai Five Eyes (Gran Bretagna, Nuova Zelanda, Australia e Canada, oltre agli Stati Uniti) di prima. Ma in cosa consisteva questo rapporto di «amicizia»? Lo spiega *Le Monde*:[62]

> [Nell'aver] di fatto consentito ai tecnici della Nsa l'accesso ai cavi sottomarini, le autentiche dorsali da cui passano tutte le comunicazioni nel mondo, posati sulle rispettive piattaforme continentale.

Ossia, quanto rivelato dall'*Espresso* già ad agosto. Non solo. *Der Spiegel*, nei giorni precedenti, rivela che un centro d'ascolto dell'Nsa è presente anche a Roma. *Panorama*, invece, anticipa sul proprio sito un'esclusiva del numero in edicola il 31 ottobre:[63]

> Anche nell'ambasciata statunitense a Roma c'è chi si è occupato di spiare: e presumibilmente ha spiato (e forse spia ancora) politici italiani. È quanto rivela il settimanale Panorama in un articolo pubblicato sul numero in edicola da domani, giovedì 31 ottobre. Secondo quanto risulta a Panorama, all'interno dell'annesso dell'ambasciata americana di Roma, in via Sallustiana 49, esiste una cellula dello Special Collection Service: un nucleo misto di

> supertecnici della National Security Agency (Nsa) e di agenti del servizio clandestino della Cia. *Panorama* rivela che esiste un documento classificato *«top secret»* e datato agosto 2010, proveniente dall'archivio trafugato dalla talpa statunitense Edward Snowden: il documento attesta la presenza dell'unità di élite a Roma, come in altre 79 sedi, di cui 19 in Europa. Dentro una stanza senza finestre e insonorizzata, gli agenti dell'Nsa analizzano il traffico di voci e di dati, intercettano i cellulari delle autorità, seguono i flussi finanziari, provano a decifrare i documenti criptati. I clandestini della Cia invece agganciano e mettono a libro paga i gestori dei sistemi di comunicazione, gli amministratori dei database più delicati, i banchieri che possono dare accesso ai conti correnti e gli ingegneri che gestiscono i siti internet più riservati.

Il governo italiano non ne sapeva nulla? E i servizi italiani nemmeno? E se anche fosse, l'ignoranza sarebbe meno grave? Come si vedrà,[64] l'unica risposta plausibile a queste domande passa per l'ambivalenza volontaria dei protagonisti.

L'Nsa intercetta le comunicazioni tra i *data center* di Google e Yahoo

L'«accesso diretto» ai server di Google e Yahoo tramite il programma Prism è solo uno dei modi attraverso cui la National Security Agency ottiene i dati in possesso dei due colossi web. Come scrive il *Washington Post*, infatti, l'intelligence statunitense li intercetta anche mentre fluiscono tra i loro *data center*. Secondo un documento *top secret* fornito da Edward Snowden al quotidiano datato 9 gennaio 2013, nei 30 giorni precedenti sono stati così raccolti 181.280.466 tra metadati (mittente, ricevente e data delle mail) e contenuti in forma di «testo, audio e video».

Per il *Post*, Muscular[65] (questo il nome del programma messo in atto dall'Nsa insieme alla controparte britannica, il Gchq) consente di copiare «interi flussi di dati» mentre attraversano i cavi in fibra ottica che collegano i *data center* di Yahoo e Google.[66] Allacciandosi a snodi al di fuori degli Stati Uniti, l'Nsa può evitare (almeno formalmente, sappiamo che molto spesso ciò non è avvenuto) le norme che impongono l'ottenimento di una autorizzazione dalla corte Fisc secondo la sezione 702 del Fisa per la sorveglianza cittadini americani. In altre parole, Muscular sarebbe illegale se condotto all'interno degli Usa, scrive il *Post*.

«Intercettare le *cloud* di Google e Yahoo», si legge ancora, «consente all'Nsa di ottenere comunicazioni in tempo reale e dare "uno sguardo retrospettivo sull'attività del bersaglio"». Per quanto riguarda Yahoo,

si tratterebbe di «circa 15 gigabyte al giorno» di dati. Il traffico sarebbe trattenuto per 3-5 giorni in un *buffer* prima di lasciare spazio a nuovi dati.

Le aziende negano di essere state a conoscenza dell'intrusione *dell'intelligence*, anche se sospettavano che quella adottata dall'Nsa avrebbe potuto essere una delle modalità attraverso cui ottenere i loro dati. Non a caso lo stesso *Washington Post* aveva scritto solo il 9 settembre scorso che Google era al lavoro per cifrare proprio i canali di comunicazione tra i suoi data center (Yahoo non ha al momento annunciato di voler fare altrettanto). Eppure nei documenti visionati dal *Post* c'è un passaggio in cui gli analisti dell'Nsa si vantano di essere riusciti a sconfiggerne le protezioni, aggiungendoci uno smile che gli ingegneri di Google non hanno affatto gradito.

CAPITOLO VI: NOVEMBRE

Google e Yahoo: quello che l'Nsa non può smentire

L'Nsa ha tentato ripetutamente di smentire il *Washington Post*, seguendo una linea riassumibile in *no, non ci infiltriamo nei database di Google e Yahoo* (non è quella l'accusa), *e in ogni caso l'articolo con le ultime rivelazioni è semplicemente errato nella descrizione di ciò che facciamo*. Come nota *Ars Technica*, è un cambio di strategia: invece di rispondere condannando la pubblicazione perché dannosa per la sicurezza nazionale e dunque irresponsabile, l'agenzia sostiene (lo aveva fatto altre volte, a dire il vero) che i contenuti sono errati. È comprensibile, viste le reazioni indignate delle aziende coinvolte.[67] Ma c'è una domanda a cui l'Nsa deve rispondere, e proviene dalle nuove *slide* dell'agenzia pubblicate dal *Washington Post*: se non si allaccia ai cavi privati di Google e Yahoo su cui transitano le comunicazioni tra i loro *data center*, come fa l'Nsa a conoscere e riprodurre nelle sue presentazioni il linguaggio e i formati adottati esclusivamente nelle reti interne di Google e Yahoo, proprio per le comunicazioni tra i loro *data center*?

Come spiega il *Post* illustrando il materiale pubblicato, una *slide* mostra una comunicazione tra un *data center* e l'altro, in particolare la conferma o

l'autenticazione che i due stanno «parlando in maniera sicura tra loro». Soprattutto, si tratterebbe di un tipo di traffico non riscontrabile al di fuori della rete interna di Google, e che adotterebbe formati utilizzati solo tra macchine di Google. Anche per Yahoo, una *slide* mostra che l'Nsa è a conoscenza dei formati proprietari dell'azienda che «non viaggiano sulla rete pubblica», al punto di separarne le porzioni di dati scambiati considerate utili da quelle indesiderate. A sostenerlo sono gli esperti interpellati dal *Post* che, secondo la testata, hanno una «conoscenza dettagliata» del funzionamento delle reti interne alle due aziende.[68]

L'intrusione nelle «autostrade private» delle due aziende, come spiegato da *Ars Technica*, è particolarmente utile per l'Nsa: iIntercettare quelle pubbliche consente di ottenere grosse quantità di dati che però sono in buona parte cifrati, e tramite Prism le richieste devono essere almeno formalmente motivate, e quindi limitate. Allacciandosi direttamente ai cavi privati che gestiscono le comunicazioni tra data center di Google e Yahoo, e facendolo al di fuori degli Stati Uniti, invece, l'agenzia può avere accesso a interi archivi di mail, documenti, ricerche e quant'altro, in chiaro (solo recentemente Google ha parlato di cifrare le sue comunicazioni tra *data center*) e senza intoppi legislativi.

Scrive *Ars Technica*:

> Ottenendo l'accesso ai *network* interni ai perimetri di sicurezza di Google e Yahoo, l'Nsa è stata in grado di violare efficacemente la cifratura Ssl utilizzata per proteggere le connessioni web tra utenti e fornitori di servizi *cloud*, dando ai sistemi di filtraggio della rete e *data mining* dell'agenzia un accesso senza restrizioni ai contenuti

> che transitano sulla rete. Il risultato è che l'Nsa ha avuto accesso a milioni di messaggi e transazioni web al giorno senza dover ricorrere a una autorizzazione Fisa per costringere Google e Yahoo a fornire i dati attraverso Prism. E ha ottenuto accesso integrale a milioni di indirizzi email di Yahoo – inclusi gli allegati […].

Il traffico registrato a questo modo è talmente tanto che l'Nsa ha bisogno di un sistema per distinguere informazioni utilizzabili in termini di *intelligence* da mere comunicazioni tra i data center. Muscular non sarebbe che questo, un «sistema distribuito di distribuzione dei dati», ossia l'equivalente di XKeyscore per «raccogliere, filtrare e processare» dati ottenuti all'interno dei network di comunicazione tra *data center*.

In sostanza, c'è un movente, un sistema che lo rende realizzabile, delle prove che testimoniano sia stato messo in atto: l'Nsa è in grado di smentire tutto questo?

Le contraddizioni sul ruolo dell'Italia

Sul Datagate le autorità italiane hanno avuto due volti: uno pubblico, rassicurante nel minimizzare o nel negare le rivelazioni dei giornali; l'altro privato, inaccessibile al pubblico, in cui al contrario e nel frattempo sono confermate tutte o quasi le accuse emerse dai documenti di Edward Snowden. Ulteriori elementi sul ruolo dell'Italia nello scandalo, infatti, vengono da un articolo sul *Corriere della Sera* firmato da Fiorenza Sarzanini, dove sono pubblicati estratti di un «rapporto riservato del Copasir», stilato da una delegazione che comprende il presidente Giacomo Stucchi e i suoi membri Vito Crimi, Rosa Calipari e Claudio Fava al termine della visita alle alte sfere dell'Nsa «a fine settembre».[69]

Dalla lettura degli estratti si ricavano una notizia inedita e quattro contraddizioni. La notizia è che «sono 300 le utenze europee che risultano essere state intercettate». Dovrebbe trattarsi di intercettazioni vere e proprie, dunque sui contenuti delle comunicazioni (non solo sui metadati che producono). Le contraddizioni del Copasir e del governo invece mostrano chiaramente la doppiezza di cui detto. Per dimostrarlo più chiaramente, le intervallo con le dichiarazioni rese dal presidente del Consiglio, Enrico Letta, dal sottosegretario cui è delegata l'autorità in materia, Marco Minniti, e dai massimi vertici del Copasir stesso. Dal giudizio di incoerenza sono sottratti i Cinque Stelle e Sel, che dall'inizio dello scandalo denunciano l'atteggiamento troppo morbido, per così dire, delle

nostre istituzioni sulla vicenda, e il fatto che le audizioni di chiarimento del Copasir non abbiano per l'appunto chiarito nulla.

1. *I servizi italiani «non risulta abbiano mai partecipato alla raccolta dei dati mentre hanno condiviso le informazioni».*
   Marco Minniti al Copasir, 23 ottobre: «mi sento di escludere che i servizi sapessero» [della raccolta dati Usa su comunicazioni italiane, *ndr*].
   Enrico Letta, 20 novembre, durante l'informativa urgente al Parlamento: «escludo che vi sia uno scambio massivo di dati su cittadini italiani».
   Rosa Calipari, 20 novembre: «l'*intelligence* italiana [...] non ha cooperato con altri paesi per raccogliere dati in modo indiscriminato e dal nostro paese non sono state date "burocraticamente" informazioni agli Stati Uniti o altri partner»;
2. *L'Italia è coinvolta? Sì: «il direttore esecutivo [dell'Nsa,* ndr*] Frances Fleisch ha spiegato che l'attività "ai fini di antiterrorismo non consente di poter escludere dalla raccolta i dati relativi ai cittadini di un singolo paese", così confermando come anche l'Italia sia inclusa nell'elenco dei "bersagli"»*
   Giacomo Stucchi, 22 ottobre: «nella sede dell'Nsa ci hanno detto che raccoglievano informazioni sui dati di traffico, ma nessuno in Italia, cioè i Governi Prodi, Berlusconi, Monti e per pochi mesi Letta e quindi nemmeno i servizi, è stato messo al

corrente di quello che stavano facendo».
Enrico Letta, 20 novembre: «fin dal luglio di quest'anno le autorità statunitensi ci hanno assicurato che gli organismi informativi di quel paese non hanno rivolto in via sistematica i propri strumenti di ricerca contro il nostro paese»;

3. *Confermata la raccolta massiva di metadati anche in Italia: «[...] il Copasir nella sua relazione sottolinea come la raccolta "avviene 'a strascico' quindi senza eccezioni e in maniera massiccia prendendo dati grezzi con la possibilità che siano conservati per cinque anni"»; non solo: «"non è stato chiarito in che modo siano utilizzati i metadati in partenza o in arrivo dal nostro Paese che transitano sui provider o sulle compagnie telefoniche statunitensi che potrebbero aver accettato di consegnare i dati alle Agenzie di* intelligence*"». E questo, scrive Sarzanini, «dimostra la mancanza di un "filtro preventivo che l'Italia vorrebbe adesso fosse introdotto"».*
Stucchi, 22 ottobre: «è stato escluso che intercettazioni a strascico fatte col programma Prism potessero aver riguardato in modo indiscriminato cittadini italiani, perché ci è stato detto che ci sono filtri e accorgimenti per evitare che questo avvenga quando ci sono paesi coi quali ci sono vincoli di amicizia».[70]
Comunicazione del Copasir, 23 ottobre (Ansa): «il sottosegretario Marco Minniti "ha ribadito che, con ragionevole certezza, è stata garantita la privacy delle comunicazioni tra cittadini

italiani all'interno del territorio nazionale [...]"»; Giacomo Stucchi, 13 novembre, sull'audizione di Enrico Letta al Copasir: «Letta ha sottolineato che non c'è stata alcuna violazione della privacy né dei cittadini né dei membri del governo».

4. *Confermata l'intercettazione dei cavi che trasportano le comunicazioni (anche italiane?): «durante gli incontri a Washington i parlamentari hanno avuto la conferma che "gli snodi, situati all'estero, dei cavi sottomarini non sono esenti dall'attività di raccolta dei dati" e infatti si chiede un approfondimento con i Servizi britannici che utilizzano "il programma di sorveglianza Tempora"».*
   Giacomo Stucchi, 30 ottobre: «sui cavi collegati alla Sicilia non risulta alcuna intercettazione massiva».

I piani del Gchq per spiare «ogni cellulare, ovunque, sempre»

Gli ingegneri dell'azienda di telecomunicazione Belgacom erano convinti di accedere a Linkedin, o al sito tecnologico Slashdot.org. Invece stavano accedendo a una replica di quei siti allestita dall'*intelligence* britannica, con una sgradevole aggiunta: un *malware* capace di trasformare i loro computer, scrive *Der Spiegel*, in «strumenti» nelle mani degli agenti.

Dello spionaggio su Belgacom (Operation Socialist), tra i cui principali clienti figurano Consiglio, Commissione e Parlamento europeo, il settimanale tedesco aveva già detto il 20 settembre. Ora sappiamo che la stessa tecnica, chiamata Quantum Insert, è stata impiegata dall'unità di *hacking* di sua maestà, MyNoc (My Network Operations Centre), per infiltrare i *network* interni della sussidiaria dell'azienda belga, Bics, e tenere sotto controllo gli ingegneri di altri due Global Roaming Exchange *provider*, Comfone e Mach. Queste aziende, un paio di dozzine in tutto il mondo, in sostanza costituiscono gli snodi principali per il traffico mobile quando l'utente si trova all'estero.

Tramite Quantum Insert, scrive in un altro articolo sempre *Der Spiegel*, sia il Gchq che la National Security Agency statunitense avrebbero violato le reti informatiche dell'Opec (Organizzazione dei Paesi esportatori di petrolio), fondata nel 1960 e tra i cui membri figurano Iran, Iraq, Arabia Saudita, Ecuador e Venezuela. Secondo un documento riservato del Gchq, datato 2010, l'operazione sarebbe stata condotta con

successo su nove impiegati della sede viennese dell'organizzazione, ottenendo i privilegi d'accesso dell'amministratore di sistema e a questo modo «molti documenti d'interesse». Lo spionaggio Nsa non avrebbe risparmiato i piani segreti di Rihad per nascondere il più a lungo possibile un incremento di produzione del greggio.

Secondo Bruce Schneier, Quantum Insert ha giocato un ruolo decisivo anche nei tentativi dell'Nsa andati a buon fine di violare l'anonimato di alcuni utenti di una vecchia versione di Tor, sfruttando una vulnerabilità del browser Firefox.[71]

Scrive Schneier:

> Come parte del sistema Turmoil, l'Nsa piazza server segreti, chiamati in codice «Quantum», in posti chiave della dorsale di Internet. La collocazione assicura che possano reagire più velocemente degli altri siti. Sfruttando quella differenza di velocità, questi server possono impersonificare una pagina *web* visitata dal bersaglio prima che il sito vero e proprio possa rispondere, deviando così il browser del bersaglio su un server FoxAcid. [...] FoxAcid è un sistema dell'Nsa costruito per fungere da connessione tra i potenziali bersagli e gli attacchi sviluppati dall'Nsa, dando all'agenzia l'opportunità di sferrare gli attacchi predisposti contro i loro sistemi.

In altri termini, traduce *Der Spiegel*:

> Quando un bersaglio cerca di collegarsi a un determinato sito [in questo caso, Linkedin, ndr], si attivano quei server. Invece del sito desiderato, ne forniscono una copia esatta, che tuttavia ha installato di nascosto il codice per lo spionaggio degli hacker del governo nei computer bersaglio.

La realizzabilità di Quantum Insert dipenderebbe

strettamente dall'accesso privilegiato di Nsa e Gchq all'infrastruttura di Internet. Nel caso di Linkedin, un documento del 2012 sostiene che il tasso di successo dei tentativi dell'*intelligence* sarebbe «superiore al 50 percento». Qual è l'obiettivo di questo tipo di attacchi? Secondo *Der Spiegel*, che cita un documento del Gchq del 2011, l'*intelligence* britannica mira a «trasformare potenzialmente qualunque telefono cellulare sul pianeta in uno strumento di sorveglianza che può essere attivato in ogni momento». L'idea è enunciata più chiaramente poco oltre: «*any mobile device, anywhere, anytime!*» («ogni cellulare, ovunque, sempre!»).

Lo spionaggio globale dei partner dell'Nsa

Delle spie di Sua Maestà e del rapporto di collaborazione con la National Security Agency si è ripetutamente detto, ma è *Der Spiegel* ad aggiungere un altro tassello al mosaico del controllo di massa: il Gchq ha gestito per tre anni un sistema di monitoraggio automatico delle prenotazioni in almeno 350 alberghi sparsi in tutto il mondo così da individuare e analizzare quelle di «diplomatici e ufficiali governativi». Il programma *top secret* si chiama in codice «Royal Concierge» e ha come scopo conoscere in anticipo i movimenti di soggetti di interesse per l'*intelligence*, così da metterli sotto controllo nelle stanze d'albergo, intercettando il telefono dell'hotel e infiltrandosi nella rete informatica, oltre a impiegare altre tecniche *ad hoc* per i personaggi più influenti, compreso l'invio di spie in carne e ossa per origliarne le conversazioni al bar.

Un primo prototipo del sistema, basato sull'invio automatico al Gchq di notifiche corrispondenti alle email di conferma inviate da domini governativi, è stato testato nel 2010. «I documenti», scrive *Der Spiegel*, «non dicono quanto spesso il programma sia stato usato, ma indicano che se ne è continuato lo sviluppo». Il Gchq non ha voluto confermare né smentire quanto scritto dal settimanale tedesco.

Tra i paesi che collaborano con l'Nsa c'è anche l'Australia. Le rivelazioni più recenti, basate su documenti pubblicati dal *Guardian* e da *Abc*, parlano del tentativo di spionaggio del presidente dell'Indonesia, Susilo Bambang Yudhoyono, e dell'intercettazione dei

telefoni cellulari della moglie, di ministri e confidenti. Yudhoyono, nota il *Guardian*, si aggiunge alla lista di leader spiati dai Five Eyes (Stati Uniti, Gran Bretagna, Canada, Australia e Nuova Zelanda), che annovera già quelli di Germania, Brasile e Messico e che sarebbero in tutto 35 nei circa 200 mila documenti che secondo il capo dell'Nsa costituirebbero il vero totale del materiale prelevato da Snowden. Ma il Defense Signals Directorate (Dsd) australiano collabora in molti altri modi con l'Nsa: aiutandola nella raccolta di centinaia di milioni di liste di contatti mail (fino a 300 mila al giorno), prendendo parte a un'operazione di spionaggio nei confronti dell'Indonesia durante una conferenza climatica a Bali nel 2007, contribuendo al programma XKeyscore, mettendo a disposizione degli agenti Usa quattro strutture dedicate allo spionaggio e cooperando nell'opera di raccolta dei dati prodotti dal traffico asiatico attraverso l'allacciamento ai cavi che trasportano la connessione nella regione. L'*intelligence* statunitense ha anche utilizzato le ambasciate australiane in Asia per registrare informazioni su soggetti attenzionati nel continente.

Ancora una volta si ripropone una domanda topica del Datagate: possibile che lo scopo sia unicamente quello dichiarato del contrasto del terrorismo?

L'Nsa ha infettato 50 mila reti informatiche

La tecnica usata dal Gchq per violare i computer di Belgacom è stata usata anche dall'Nsa. Lo sostiene il quotidiano olandese *Nrc Handelsblad*, secondo cui la National Security Agency «ha infettato oltre 50 mila reti informatiche nel mondo con software malevoli [*malware*, *ndr*] progettati per rubare dati sensibili».[72] La tecnica sarebbe messa in atto dalla divisione dell'Nsa chiamata «Tailored Acces Operations» (Tao).[73] La rivelazione sarebbe contenuta nei documenti di Edward Snowden visionati dal quotidiano, in particolare una presentazione risalente al 2012.[74] Le operazioni, condotte con la tecnica Cne (Computer Network Exploitation, secondo la terminologia dell'Nsa) sarebbero state portate a termine, tra gli altri paesi, in Brasile e Venezuela, consentendo intrusioni «attive per anni senza che siano scoperte». Sulla mappa contenuta nella presentazione pubblicata da *Nrc*, tuttavia, si vedono infiltrazioni anche in reti cinesi, russe e in Medio Oriente. Ancora, i *malware* dell'Nsa possono essere «controllati in remoto» e attivati o spenti semplicemente premendo un bottone. Si tratterebbe insomma di «cellule dormienti» adoperate dall'*intelligence* fin dal 1998.

Per l'Nsa, tuttavia, non basta. Come scrivono James Risen e Laura Poitras sul *New York Times*, ancora nel 2012 l'agenzia premeva per ottenere più poteri e condurre una sorveglianza più estesa e capillare. Lo rivela un *paper* risalente a febbraio 2012, intitolato *Sigint strategy 2012-2016*, che dettaglia la strategia del

quadriennio seguente per la Signals Intelligence (Sigint, appunto), ossia l'intercettazione di comunicazioni elettroniche. Si tratta di «perseguire aggressivamente le autorità legislative» e mettere in piedi un sistema più adatto all'«era dell'informazione». Troppo complessa la tecnologia impiegata dai bersagli, dice l'*intelligence*: se si vogliono acquisire dati «da chiunque, in ogni luogo e sempre» (*anytime, anyone, anywhere*) bisogna sconfig gere tutte le pratiche di *cybersecurity* avversarie, compresi gli standard crittografici commerciali (come ripetutamente detto), anche agendo a livello industriale e con «Humint», ovvero spie in carne e ossa. Ciononostante l'Nsa definisce quella attuale «l'età dell'oro del Sigint», mostrando, come rileva su Twitter Christopher Soghoian dell'Aclu, una nettissima ipocrisia: in pubblico l'*intelligence* lamenta il rischio di rimanere all'oscuro rispetto alle comunicazioni dei bersagli presenti e futuri; in privato, pur lamentando una mancanza di poteri (ingiustificabile rispetto al materiale emerso finora), ammette di non aver mai potuto accedere a tanti dati come ora. Il *paper* svelato da Snowden in sostanza «sottolinea l'obiettivo di lungo termine dell'agenzia di essere virtualmente in grado di registrare tutto quanto sia disponibile nel mondo digitale. Per raggiungere quell'obiettivo», scrivono Risen e Poitras, «il *paper* suggerisce che l'Nsa stia pianificando di ottenere un maggiore accesso, e in vari modi, all'infrastruttura globale delle reti di telecomunicazioni».[75] L'obiettivo esplicito è «incrementare sensibilmente la padronanza della rete globale». A riguardo il *New York Times* cita gli svariati riferimenti (contenuti in altri documenti forniti da

Snowden) al programma Treasure Map, definito nella presentazione dell'Nsa «una mappa interattiva e quasi in tempo reale della rete Internet globale». Combinando dati sul traffico e informazioni commerciali e di *intelligence*, Treasure Map consente di analizzare tra i 30 e i 50 milioni di indirizzi Ip al giorno, oltre a dati di geolocalizzazione e sulle connessioni in Wi-Fi. A questo modo, si vanta l'*intelligence*, il programma può mappare «ogni *device*, in ogni luogo e per sempre», analogamente a quanto visto per il Gchq.[76]

Il documento dell'Onu contro la sorveglianza di massa

Mentre si scopre che l'Nsa ha monitorato le visite a siti pornografici di sei agitatori politici per screditarli, e che i sospetti sull'intercettazione del traffico tra *data center* si addensano anche su Microsoft (dopo Yahoo e Google), Le Nazioni Unite compiono un primo atto concreto per denunciare le conseguenze nefaste della sorveglianza di massa sulla privacy e la libertà dei cittadini.[77]

Il comitato per i diritti umani dell'Onu ha approvato all'unanimità una risoluzione promossa da Germania e Brasile, intitolata *The right to privacy in the digital age*: nel testo l'assemblea si dice «molto preoccupata per l'impatto negativo» del monitoraggio in stile Nsa (non menzionata esplicitamente) «sull'uso e il godimento dei diritti umani». La lotta al terrorismo non può e non deve avvenire in contrasto con il diritto internazionale («in particolare» sui diritti umani) e «gli stessi diritti che le persone hanno *offline* devono essere protetti anche *online*». Tutti gli stati devono:

1. Rispettare e proteggere il diritto alla privacy nel contesto delle comunicazioni digitali;
2. «Mettere in atto misure per porre fine alle violazioni di quei diritti» e «prevenirle», assicurandosi le leggi nazionali rispettino il diritto internazionale;
3. «Rivedere procedure, pratiche e leggi» sulla sorveglianza delle comunicazioni, la loro intercettazione e la raccolta di massa di dati personali;

4. Promuovere trasparenza e responsabilità degli Stati che compiono sorveglianza di massa adottando meccanismi di controllo del loro operato «indipendenti» ed «efficaci».

Si chiede inoltre anche all'Alto Commissario Onu per i diritti umani di «presentare un rapporto sulla protezione e la promozione» della privacy nel contesto della sorveglianza di massa, con consegna fissata al prossimo anno. Il testo, ricorda *Rt*, dopo essere stato votato e approvato a dicembre dall'Assemblea Generale, pur non essendo legalmente vincolante, «avrà un certo peso politico». Pur se la proposta iniziale di Brasile e Germania utilizzava un linguaggio più esplicito, la risoluzione approvata ha incontrato i favori di Access ed Electronic Frontier Foundation.[78]

CAPITOLO VII: DICEMBRE

Di chi sono i segreti di Edward Snowden?

«Di chi sono i segreti affidati da Edward Snowden a Glenn Greenwald e Laura Poitras?», si chiede Mark Ames su *Pando*. È una questione delicata e importante, a maggior ragione se i due giornalisti sono gli unici ad avere accesso all'archivio integrale dei documenti sottratti da Snowden. E, qui sta il punto chiave, entrambi Greenwald e Poitras sono entrati nella squadra del nascente progetto editoriale Pierre Omidyar, fondatore e presidente di eBay. Per Ames una svolta sostanziale rispetto a casi celebri e recenti di *whistleblowing*, da Daniel Ellsberg (Pentagon Papers) a Chelsea Manning (Cablegate). Perché, scrive, «il *whistleblowing* ha tradizionalmente servito l'interesse pubblico. In questo caso, sta per servire gli interessi di un miliardario che sta lanciando una impresa editoriale che punta al profitto». Mentre Ellsberg e Manning, accusa Ames, hanno affidato il materiale da loro sottratto a organizzazioni senza scopo di lucro (Wikileaks) o a svariate testate e a membri del Congresso contemporaneamente, Snowden si è rivolto a giornalisti che, dopo aver cercato di convincere l'opinione pubblica mondiale della rilevanza dei documenti posseduto dal *whistleblower*, non hanno esitato a monetizzare il loro accesso privilegiat,

«vendendo quei segreti a un miliardario». Greenwald e Poitras avrebbero «privatizzato» i segreti di Snowden, usando materiale di interesse pubblico per il loro tornaconto privato (la carriera). Film e libro in arrivo su Snowden confermerebbero. Se poi si considera il dibattito, per nulla sopito, sul ruolo di Omidyar al tempo del blocco bancario da parte di Pay Pal (di proprietà di eBay) ai danni di Wikileaks,[79] si capisce come la questione sia sostanziale.[80]

Nella replica, Greenwald nota innanzitutto che l'argomentazione di Ames è la stessa adoperata dai vertici dell'Nsa e addirittura da chi vorrebbe vederlo dietro le sbarre per la pubblicazione del materiale di Snowden. Poi passa alla difesa nel merito: dove starebbe l'eccezionalità nel modo in cui ha gestito la diffusione dei documenti dello scandalo Nsa? Anche Bart Gellman, del *Washington Post*, è pagato dal quotidiano per gli articoli pubblicati a partire dalle migliaia di documenti prelevati da Swnoden in suo possesso. Anche Gellman ha un libro sull'argomento in uscita. E anche lui lavora per un «miliardario», il creatore di Amazon, e proprietario del *Post*, Jeff Bezos:

> Significa che Gellman ha «privatizzato» i documenti dell'Nsa, ne sta «traendo profitto», e che ha venduto segreti sugli Stati Uniti al *Washington Post*?

Che dire, continua Greenwald, di Bob Woodward, del *New York Times* o di Jim Risen? Tutti «colpevoli di aver venduto segreti statunitensi?». Il metodo adottato, ammette, è lo stesso adoperato da Wikileaks con il Cablegate e non solo: sono state sfruttate le competenze, le tutele e l'impatto delle principali testate al mondo

(*Guardian*, *Washington Post*, *New York Times*, *Der Spiegel*), stringendo accordi specifici per documenti riguardanti singoli paesi con i giornali di quegli stessi paesi (come *Le Monde*, *El Mundo* e *Nrc*). Le alternative sono tutte peggiori: pubblicare tutto il materiale in un singolo file *online* accessibile a chiunque, per esempio, avrebbe violato la volontà dello stesso Snowden, il quale sapeva benissimo che avrebbe scatenato l'accusa di pubblicare tutto indiscriminatamente (accusa poi usata comunque), mettere a repentaglio vite umane (come si è letto per le pubblicazioni di Wikileaks, senza conferma alcuna). L'impatto sarebbe stato minore rispetto a uscite dilazionate nel tempo e ragionate, dando il tempo all'opinione pubblica di metabolizzarle. Dare i documenti ad altre pubblicazioni, così da velocizzare il processo e sottrarsi all'accusa di comportarsi da monopolisti, significherebbe invece diventare una «fonte» di quel materiale, perdendo così una parte importante della propria tutela legale, quella derivante dal ruolo di giornalista.

Quanto all'accusa di «monopolizzare» o «privatizzare» il materiale, per Greenwald è «senza dubbio l'accusa più stupida» sentita dallo scoppio dello scandalo. *New York Times*, *Guardian*, *Pro Publica*, *Washington Post* hanno migliaia di documenti: che razza di monopolio sarebbe? E un «monopolista» interessato a sfruttare la sua posizione per un soggetto unico (Omidyar) perché starebbe continuando a pubblicare con svariate testate?

La replica non soddisfa *Pando*. Per Paul Carr, *investigations editor* del sito, nonostante «4915 parole di tentata risposta [...] Greenwald ancora rifiuta di fare

una semplice dichiarazione che confermi che applicherà a Omidyar gli stessi *standard*» applicati agli altri. In altre parole, la questione «vale la pena di essere posta», come scrive David Weinberger, proprio perché la critica iniziale di Ames era che «di Omidyar non ci si può fidare». Weinberger non è d'accordo con Ames, ma sostiene che sia meritevole di riflessione il fatto che l'accusa di monopolizzare il materiale *si possa porre*. Solo nell'ecosistema dell'informazione attuale Greenwald può scegliere tra le tante opzioni e modalità di pubblicazione che lui stesso ha evidenziato nella difesa, scrive il ricercatore del Berkman Center di Harvard; altrimenti la *possibilità* stessa dell'accusa di Ames non si porrebbe. Ora che invece c'è un mezzo che consente la pubblicazione diretta e immediata del materiale, selezionarne una parte e gestirne l'uscita può sembrare (anche se per Weinberger è una percezione errata) un'operazione commerciale invece che giornalistica.

Bisognerà attendere che il progetto di Omidyar diventi realtà per comprendere se ci saranno davvero dei risvolti fattuali nelle prossime pubblicazioni dei segreti di Snowden.

L'audizione del direttore del *Guardian* in Commissione Affari Interni

Alan Rusbridger, direttore del *Guardian*, il 3 dicembre compare davanti alla Commissione Affari Interni della Camera dei Comuni britannica per rispondere alle domande dei parlamentari sulle rivelazioni di Edward Snowden,[81] pubblicate sul quotidiano londinese, che chiamano in causa Nsa e Gchq.[82]

Riassumendo i punti principali dell'audizione:

1. Finora è stato pubblicato solo l'1% delle informazioni contenute nei documenti prelevati da Snowden. Il *Guardian*, in particolare, ne ha pubblicati 26 sui circa 58 mila di cui dispone (in totale potrebbero essere 200 mila). Non dobbiamo attenderne molti altri dal suo quotidiano, sostiene Rusbridger;
2. Non tutti i file sono sotto il controllo del *Guardian*: Snowden li ha dati ai giornalisti Glenn Greenwald e Laura Poitras (a loro due in versione integrale) e al *Washington Post*. Il *Guardian* ha poi condiviso quelli in suo possesso con il *New York Times*. I file sotto il controllo del *Guardian*, dice Rusbridger, sono «sicuri». Sostiene poi di non sapere con certezza chi sia in possesso di quali documenti: «forse solo Snowden lo sa». Ma, da quando Greenwald ha lasciato il quotidiano per approdare alla nuova avventura editoriale di Pierre Omidyar, nessun giornalista del *Guardian* è più in contatto con il *whistleblower*;

3. All'interno dei documenti trasmessi al *Times* c'erano nomi e cognomi di agenti dell'*intelligence*, ammette Rusbridger, ma sono stati redatti sia dal *Guardian* che dallo stesso *Times*;[83]
4. Il *Guardian* si è sempre consultato con il Da-Notice, il sistema che suggerisce cosa evitare di pubblicare per questioni di interesse nazionale, prima di ogni pubblicazione. Non solo: Rusbridger dice di avere intrattenuto «oltre 100 contatti» con agenti britannici e statunitensi negli scorsi sei mesi;
5. Il problema è che oltre a Snowden, 850 mila persone hanno avuto accesso a quei documenti, dice Rusbridger. Troppe, ed è questo il motivo per cui poi le autorità ne perdono il controllo (come nel caso di Chelsea Manning). In sostanza, ad aver perso il controllo dei documenti è stata l'Nsa, non il *Guardian*;
6. Il *Guardian*, conferma Rusbridger, ha pagato David Miranda, compagno di Greenwald, per trasportare file riservati,[84] ma gli agenti non sono stati in grado di violare la cifratura che li proteggeva;
7. Tra le domande dei membri della Commissione, spesso fuori fuoco, poco informate o ridondanti, ne spiccano due, «ami il tuo paese?» e «avresti informato i nazisti della decifratura del Codice Enigma?». Sembra, suggerisce Christoph Scheuerman su Twitter, che i parlamentari si siano preparati facendo ricerche su Google all'ultimo minuto. Le espressioni sperdute durante i tre tentativi di Rusbridger di parlare di

Tor paiono confermare l'impressione. Insomma, la politica sembra ancora una volta inadeguata ad affrontare le sfide della contemporaneità;

8. Rusbridger fa due osservazioni che rivelano tutta l'inadeguatezza della Commissione nell'affrontare l'argomento: la prima riguarda la sensazione di stare svolgendo un dibattito analogico in un'era digitale, secondo leggi in altre parole create per regolare un ambiente completamente diverso e oggi inappropriate; la seconda riguarda l'idea che se la politica criminalizza i giornali che pubblicano fughe di notizie, i prossimi Snowden faranno da soli, pubblicando direttamente tutto in rete senza limitazioni (è il cosiddetto *document dump*). E quello sì che rischia di mettere a repentaglio l'incolumità delle persone coinvolte.

È evidente, dice il direttore, che punire chi pubblica non potrà nascondere il fatto che i giornali hanno colmato le lacune istituzionali nel controllo dei poteri dell'*intelligence*. Se quel controllo avesse funzionato, probabilmente niente di tutto questo sarebbe successo.

L'Nsa sa dove sei e con chi parli

Il Gchq non è l'unica *intelligence* ad aver attuato strategie per spiare «ogni cellulare, ovunque, sempre».[85] Il *Washington Post*, basandosi su documenti forniti da Edward Snowden, rivela che la National Security Agency sta attualmente registrando cinque miliardi di dati sulla geolocalizzazione di telefoni cellulari in tutto il mondo. L'agenzia, scrive il quotidiano, è così in grado di «tracciare i movimenti degli individui – e mappare le loro relazioni – in modi che precedentemente erano impensabili». I dispositivi coinvolti sarebbero centinaia di milioni e, nella maggior parte dei casi, appartenenti a cittadini (anche statunitensi, pur se «incidentalmente») innocenti, su cui non pendono ipotesi di reato.

La raccolta massiva di informazioni, che l'Nsa ribadisce essere «legale», non significa che l'*intelligence* ritenga rilevanti per la sicurezza nazionale i movimenti della maggior parte della cittadinanza, spiega il *Post*:

> [i dati di localizzazione, *ndr*] sono registrati in massa perché i suoi più potenti strumenti di analisi, conosciuti collettivamente come Co-Traveler, consentono di cercare sodali sconosciuti di bersagli di *intelligence* noti tracciando le persone i cui movimenti si intrecciano.

In particolare, l'Nsa è in grado di «mappare data, ora e luogo» delle chiamate, ma anche «velocità e traiettoria» degli spostamenti dei chiamanti, così da stimare correlazioni tra un sospetto e i soggetti con cui intrattiene rapporti.

Gli schemi degli spostamenti sarebbero analizzati tramite «sofisticate tecniche matematiche» in grado di

considerare relazioni tra centinaia di milioni di dispositivi. L'*intelligence* controlla dunque a distanza comuni cittadini intenti in incontri d'affari, visite a strutture ospedaliere, in stanze d'albergo come nelle proprie abitazioni. I dati raccolti ammonterebbero a 27 terabyte, cioè mille miliardi di byte, o «più del doppio del testo contenuto nella collezione cartacea della Library of Congress». Una quantità di informazioni tale da esaurire perfino le capacità di immagazzinamento dell'Nsa, come si legge in un *briefing* della stessa agenzia dell'ottobre 2012.

Per l'*intelligence* statunitense la raccolta dei metadati non è soggetta ai vincoli del Quarto Emendamento, che protegge i cittadini da perquisizioni e controlli indebiti. Di conseguenza, la raccolta dei dati di localizzazione, contrariamente ai contenuti veri e propri delle conversazioni, non sarebbe soggetta ad autorizzazione giudiziaria. Il principio, basato su una sentenza della Corte Suprema risalente al 1979, è tutt'altro che pacifico, scrive sempre il *Post* sul blog *The Switch*. Prima di tutto perché il caso su cui si fonda coinvolge un individuo specifico, e già sospetto, mentre qui al contrario si parla di una raccolta massiva[86] e anche (principalmente) su perfetti innocenti. E poi perché le capacità di sorveglianza odierne nel 1979 non erano nemmeno immaginabili.

Il *Washington Post* nota ancora che, come già per l'uso di sistemi di cifratura e anonimizzazione della connessione, anche prendere precauzioni per non essere intercettati (per esempio, usare un telefono solo per brevi chiamate e poi cambiarlo) segnala l'utente come meritevole di un «particolare scrutinio».

Amara la conclusione del quotidiano:

> Le capacità di tracciamento dei dati di localizzazione da parte dell'Nsa sono sconvolgenti, e indicano che l'agenzia è in grado di rendere efficacemente futile la gran parte degli sforzi di mettere in sicurezza le proprie comunicazioni.

I colossi del *web* chiedono di riformare la sorveglianza governativa

Aol, Facebook, Linkedin, Google, Microsoft, Twitter, Yahoo e Apple, per la prima volta, lanciano una campagna congiunta per chiedere a Barack Obama e al Congresso di riformare in profondità le prassi di sorveglianza digitale evidenziate dallo scandalo Nsa. Del resto il Datagate sta compromettendo immagine, credibilità e dunque affari.

Le richieste delle aziende si trovano sul sito Reform Government Surveillance e in una lettera pubblicata in una pagina a pagamento su diversi quotidiani, tra cui il *New York Times*. «È tempo che i governi del mondo affrontino le pratiche e le leggi che regolano la sorveglianza governativa degli individui e l'accesso alle loro informazioni», scrivono i firmatari, perché «crediamo fortemente che le pratiche e le leggi attuali debbano essere riformate», e subito. Quanto al come, sono enunciati cinque principi che il governo dovrebbe attuare:

1. *No alla sorveglianza di massa*. Le autorità statali dovrebbero poter registrare dati solo su individui specifici per «motivi di legge». Servono inoltre nuovi limiti alla possibilità del governo di costringere i provider a consegnargli i dati dei suoi utenti, bilanciando il suo bisogno di dati con il diritto alla privacy dei singoli e con «l'impatto sulla fiducia in Internet» (il fattore più rilevante per il business dei firmatari);
2. *Controllo legale più forte e indipendente dell'operato dei sorveglianti*. Il riferimento è a

quello messo in atto, scarsamente e malamente, dalla corte Fisa;

3. *Trasparenza sulle richieste governative di accesso ai dati degli utenti*. Una richiesta che diverse aziende, Google in testa, vanno ripetendo da tempo per poter dettagliare quante volte, per fini di sicurezza nazionale, i governi chiedano di ottenere informazioni sugli iscritti ai loro servizi. Dovrebbero essere i governi stessi a fornire quei dati, si legge;
4. *Rispettare la libera circolazione dell'informazione*. È la spina dorsale dell'economia globalizzata del Ventunesimo secolo, scrivono i firmatari, che chiedono al governo anche di non costringere i provider a localizzare le loro infrastrutture nei Paesi dove vogliono operare;
5. *Evitare conflitti tra governi*. Serve un quadro normativo internazionale trasparente per gestire le richieste di dati provenienti da giurisdizioni diverse senza intoppi e litigi tra autorità diverse.

Per il *New York Times* si tratta del «più ampio e più forte» tentativo di sollecitare un cambiamento da parte dei giganti di Internet, facendo affidamento sull'influenza sempre crescente che i miliardi di dollari prodotti a Silicon Valley hanno sulla politica e su Washington.

Su Twitter, Ryan Paul fa notare l'assenza dei colossi delle telecomunicazioni all'iniziativa. At&T lo dice espressamente: la legge non richiede che gli azionisti sappiano che cosa la compagnia fa con i dati degli utenti; nemmeno qualora (come avvenuto) cerchino di

sapere se sono stati venduti e trasmessi all'Nsa insieme per esempio ai 5 miliardi di dati sulla localizzazione dei telefoni cellulari, circostanza di cui ha scritto recentemente il *Washington Post*.[87] Due settimane più tardi, tuttavia, anche il colosso delle telecomunicazioni, un giorno dopo il rivale Verizon, annuncia la pubblicazione di un Transparency Report per dettagliare le richieste governative ricevute per consegnare dati dei suoi clienti.

Aziende come Google, Yahoo e Microsoft avevano già affermato di essere al lavoro su nuove misure per proteggere la sicurezza dei dati dei loro utenti: per esempio, cifrare tutto il traffico tra i loro *data center*, dopo che si è scoperto che era intercettato dall'Nsa,[88] e implementare più sofisticate tecniche di crittografia.

I realissimi rischi della sorveglianza sui mondi virtuali

Grazie al lavoro di *Guardian*, *New York Times* e *Pro Publica* sul materiale fornito da Edward Snowden, sappiamo che la National Security Agency statunitense e la britannica Gchq hanno infiltrato e monitorato i mondi virtuali di *World of Warcraft*, *Second life* e perfino le conversazioni degli iscritti a XBox Live a caccia di terroristi. Dal documento integrale (82 pagine) a uso interno dell'*intelligence*,[89] datato 2008, traspare il misto di inadeguatezza, superficialità e delirio di controllo che ha informato la decisione di trattare i videogiocatori come potenziali criminali.

Il *paper*, intitolato E*xploiting terrorist use of games & virtual environments* (Gve), è una ricognizione dei mondi virtuali durata un anno, basata sullo studio della letteratura, di articoli di giornale, manuali, ma anche su «esplorazioni *in-game*», frequentazione di seminari dedicati e interviste realizzate appositamente sull'argomento. Alla lettura, risulta più simile a un manifesto di banalità e allarmismo che a un insieme di linee guida teoriche e operative per garantire la sicurezza nazionale. Si sottolinea ripetutamente che bersagli dell'*intelligence* potrebbero essere correlati a eventi *online*, che l'obiettivo è identificare «profili, personaggi e gilde [gruppi di utenti di *WoW*, *ndr*] relazionati a gruppi estremisti islamici, alla proliferazione nucleare e al traffico d'armi», senza che vi siano prove di quelle relazioni. Si parla, senza che vi siano riscontri, di tecniche che «potrebbero» essere

utilizzate, di «scenari fittizi», di «ipotesi» che non devono realizzarsi. Sconcerta soprattutto la visione di fondo del *gaming*, e più in generale di ogni attività umana, da parte dell'Nsa.

Se l'idea che i terroristi potrebbero usare i canali di comunicazione interni ai mondi virtuali per organizzare realissimi attentati è plausibile (e del resto consente di raccogliere infiniti altri metadati utili, da interfacciare con quelli ottenuti da mail e telefonate), ciò non giustifica trattare ogni videogiocatore come un sospetto. Né considerare il *gaming* in sé come un'attività umana da sorvegliare, sempre e comunque. Eppure è proprio così che l'Nsa la dipinge. *Warcraft* diventa «una piattaforma per potenziali bersagli di Sigint», ossia di comunicazioni via Internet rilevanti per l'*intelligence*. E i Gve, i giochi e mondi virtuali appunto, «sono una opportunità», come si legge nel documento, non di svago o crescita, ma di controllo, propaganda e repressione.

«Possiamo usare i Gve per Cne (Computer Network Exploitation)», scrive l'Nsa: ossia per infiltrare reti informatiche, come fatto in oltre 50 mila casi nel mondo.[90] O usarli per «analisi di *social network*» (analisi che anche in questo caso sappiamo non essere limitata ai videogiochi),[91] identificare un bersaglio da far seguire da «Humint» (agenti in carne e ossa), «manipolarne le attività», geolocalizzarlo, conoscerlo, studiarne ogni comunicazione. Del resto, «entro il 2010» i terroristi potrebbero fare un «uso diffuso» dei Gve, usando versioni *ad hoc* di popolari videogiochi per allenare le proprie truppe;[92] sfruttando il carattere «ideologico» di alcune gilde su *WoW*; lanciando

messaggi di fondo coerenti con la Jihad all'interno di simulatori di guerra che potrebbero venire usati dai giovani, per esempio nei territori palestinesi.

I videogiochi, continua l'Nsa, sono «piattaforme ideali di influenza perché incorporano immaginario, narrativa, uno spirito cameratesco e azione». I giochi di ruolo massivi *online* (Mmorpg) come *WoW*, poi, sono «luoghi ideali per condurre comunicazioni sicure tra terroristi»: perché frequentati da milioni di giocatori, perché i produttori non tengono *log* di quello che si dicono gli utenti, non controllano il traffico e il traffico stesso mischia dati del gioco e comunicazioni dei giocatori. Di nuovo, l'ansia dell'Nsa è evitare il *going dark*, cioè che qualcosa avvenga a sua insaputa, per canali comunicativi che non riesce a controllare. Non solo: «i giochi online possono servire da strumenti di reclutamento» per i terroristi, fornendo inoltre il luogo ideale per sviluppare abilità di comando, di interazione tra gruppi per obiettivi specifici, per imparare a comunicare e sviluppare tattiche per realizzarli. Peccato lo stesso esercito Usa, si legge, sfrutti gli stessi meccanismi per gli stessi scopi. A maggior ragione se, come si legge poco dopo, i Gve forniscono ai terroristi la possibilità di «raccogliere e distribuire finanziamenti», quale sarebbe la soluzione del problema: vietare i giochi? No, risponde l'Nsa: serve una strategia dotata di tre differenti operazioni, ma condotta secondo una visione «olistica»:

1. Contro-propaganda all'interno del gioco (facendo partecipare gli agenti, così da «facilitare la viralità dei messaggi» contro-propagandistici nel gioco grazie alle relazioni sviluppate, che aiutano

anche a meglio identificare le fonti della propaganda);
2. Raccolta di elementi di *intelligence* all'interno del gioco (per esempio, dedurre una mappa dei soggetti coinvolti nelle transazioni finanziarie di un terrorista a partire da quelle di beni e in moneta virtuale di un gioco; «di particolare interesse sarebbero i commenti a giochi con messaggi di natura politica»);
3. Sviluppo di nuovi giochi (collaborando con gruppi di studenti, ricercatori e software house).

«Queste tre aree sono perseguite al meglio insieme e in modo olistico, con gli operatori al lavoro in un area che appoggiano gli operatori nelle altre due», si legge. E gli operatori sono impiegati talmente tanto che sono servite addirittura strategie per evitare che gli agenti si pestassero i piedi l'un l'altro (*deconflict*). Le vette del grottesco si raggiungono quando gli estensori del documento vedono il pericolo dell'utilizzo di giochi come *Madden Nfl*, *Sim city* e *Gran turismo* per l'addestramento di terroristi, quando si immaginano le *mod* di *Battlefield 2* come scorciatoie per il proselitismo, quando si menzionano *Nintendogs* e la console *Wii* come esempio dei pericoli futuri che l'industria del *gaming* potrebbe portare all'*intelligence*.

Domina un allarmismo generale:[93]

> I mondi virtuali forniranno le maggiori opportunità per appoggiare operazioni terroristiche, in particolar modo nell'area della comunicazione, del coordinamento, del reclutamento e dei finanziamenti. Man mano che i mondi virtuali si espandono, cresceranno parallelamente le opportunità dei terroristi di sfruttarli.

E se i terroristi mettessero in piedi una rete sofisticata su *Second life* (oggi sostanzialmente defunto)? E se i terroristi sfruttassero il *gold mining* (giocare a Mmorpg per trasformare risultati virtuali in moneta sonante, e realissima) dei giocatori *online* per finanziare le proprie attività? Sono queste alcune delle domande che sembrano far perdere il sonno agli agenti, la cui unica risposta è sorvegliare tutto, sempre, anche in assenza di prove e verifiche.

Se le preoccupazioni non sono del tutto infondate, è inaccettabile criminalizzare un'attività umana (il gioco) e un intero settore produttivo e creativo nel nome di possibilità senza alcun riscontro fattuale. Come dice il filosofo Peter Ludlow a *Russia Today*, l'Nsa ha finito per «sorvegliare ogni singola parte della nostra vita»: le relazioni sociali, emotive, i gusti, le abitudini sessuali, perfino spingendosi fino a sfruttare le visite a siti pornografici per distruggere la reputazione di «radicalizzatori» e a fingersi un orco in *World of Warcraft* per cercare di capire i nostri eventuali propositi bellici contro gli Stati Uniti e Washington. In questo modo il controllo del virtuale fornisce un accesso senza precedenti alle nostre realissime esistenze, nei loro aspetti più privati e radicati in profondità nella nostra psiche. Se mi fingo un terrorista su *Warcraft*, perché è nella mia libera disposizione di essere umano scegliere di impersonificare un terrorista all'interno di un mondo virtuale, rischio di essere attenzionato o considerato un sospetto al di fuori di Azeroth, qui e ora? Il fatto che si possa anche solo porre il dubbio testimonia che la *fine del dualismo digitale* nell'era della sorveglianza di massa ha

prodotto un mostro di controllo da cui è vitale liberarsi al più presto.

Le sentenze di Leon e Pauley

La prima vittoria di Edward Snowden è stata quando le sue rivelazioni hanno portato il presidente Barack Obama ad ammettere che la sorveglianza Nsa andava riformata. Ora che i cambiamenti sembrano imminenti,[94] giunge una seconda vittoria: il giudice federale Richard Leon ha infatti stabilito che la raccolta in massa dei metadati delle conversazioni telefoniche dei cittadini statunitensi è molto probabilmente in violazione del Quarto Emendamento della Costituzione americana, che vieta perquisizioni e sequestri ingiustificati.

Il giudice Leon usa parole durissime in quella che, a tutti gli effetti, è la prima certificazione che la National Security Agency ha operato violando la legge. Nelle 68 pagine della sentenza (pubblicate con tanto di legenda dal *Guardian*) il giudice parla di un programma di sorveglianza dal raggio d'azione «quasi orwelliano», e di una invasione «indiscriminata» e «arbitraria» della privacy «virtualmente di ogni singolo cittadino» per analizzarne le comunicazioni «senza previa autorizzazione giudiziaria». Leon ricorda anche che la base legale fornita dall'Nsa a supporto delle operazioni, un verdetto della Corte Suprema del 1979, è inadeguata a descrivere la situazione attuale: all'epoca niente di ciò che l'*intelligence* fa oggi era anche solo immaginabile. Non solo: in accordo con quanto ha scritto per esempio *Pro Publica*, il giudice argomenta che le autorità statunitensi non hanno portato alcuna prova che una sorveglianza tanto invasiva abbia prodotto

risultati concreti nella lotta al terrorismo. «Il governo non cita un solo caso in cui le analisi dell'Nsa sulla base della raccolta massiva di metadati abbia realmente sventato un attacco terroristico imminente», si legge nell'ingiunzione che ordina lo stop alla registrazione dei dati sulle chiamate dei due attori, l'avvocato conservatore Larry Klayman e Charles Strange, oltre alla distruzione dei metadati ottenuti, pur sospendendola per concedere alle autorità di fare ricorso. Secondo il *New York Times*, potrebbero volerci sei mesi.

Il giudice usa una metafora di sicuro effetto per opporsi all'idea che l'Nsa non raccolga i metadati delle utenze Verizon:

> Per fare un'analogia, se il programma dell'Nsa funziona nel modo suggerito dal governo, allora omettere Verizon Wireless, At&T e Sprint [le compagnie i cui utenti, secondo il *Wall Street Journal*,[95] sono bersaglio della sorveglianza Nsa, *ndr*] dalla raccolta sarebbe come omettere John, Paul e George da un'analisi storica dei Beatles. Ma un database che contenesse solo Ringo non avrebbe alcun senso, e non posso credere che il governo crei, gestisca e difenda così ardentemente un sistema simile.

Edward Snowden, in un comunicato diramato tramite Glenn Greenwald, ricorda di essere stato spinto a diffondere il materiale *top secret* dell'Nsa proprio a partire dalla convinzione che i programmi di sorveglianza fossero in violazione della legge, in particolare della Costituzione. Questo primo verdetto sottratto alla segretezza vigente nel normale, e sostanzialmente inutile, processo di controllo legislativo delle attività dell'*intelligence* non è altro che l'inizio, dice

Snowden, di una lunga serie di rivincite del pubblico e della legalità sull'opacità e gli abusi dell'Nsa. Su Twitter, lo stesso Greenwald parla di un verdetto «straordinario».

Nonostante, come scrive il *New York Times*, si tratti di una «enorme vittoria simbolica» per gli oppositori della sorveglianza di massa, la Casa Bianca non cambia idea su Snowden: niente amnistia, come brevemente ipotizzato, e soprattutto nessun ringraziamento per quello che appare sempre più chiaramente con il trascorrere dei mesi un servizio, e non una minaccia alla nazione.

Si annunciano tempi bui per i sostenitori dell'Nsa, in particolare per chi ha sempre strenuamente sostenuto che tutte le operazioni sono avvenute e avvengono nell'alveo della legalità?[96] La risposta sembra rimandata, stando alla sentenza di un secondo giudice federale, William Pauley, che arriva a dieci giorni di distanza da quello di Leon.

Secondo Pauley, è «legale» la raccolta di massa dei metadati telefonici delle chiamate da e per gli Stati Uniti, oltre che all'interno del paese. Il programma di sorveglianza, scrive il giudice, rappresenta la risposta del governo alle nuove modalità terroristiche di Al Qaeda che, si legge, «ha usato la tecnologia contro di noi». La risposta, scrive tra le righe, è tecnologica: un programma che «funziona solo perché registra tutto» e che consente agli agenti di compilare un «ricco profilo» di un bersaglio, mantenendo, secondo il giudice, l'anonimato di tutti i soggetti intercettati ma non finiti al vaglio dell'*intelligence*. E del resto, le informazioni realmente sfruttate per le analisi dell'Nsa non sarebbero

che una frazione infinitesimale della massa sterminata di dati raccolta: «nel 2012, meno di 300 identificatori» in tutto. Tuttavia, come ha recentemente sostenuto Glenn Greenwald di fronte al Parlamento Europeo, i metadati possono dire paradossalmente più dei contenuti delle telefonate. Di certo non garantiscono l'anonimato dei soggetti intercettati, come scrivono i ricercatori dello Stanford Security Lab in uno studio appena pubblicato: nel 91% dei casi studiati tramite l'applicazione Android *Meta phone*, e grazie all'interpolazione dei metadati ottenuti con dati disponibili pubblicamente in rete, è stato possibile dare un nome ai numeri registrati; ciò rende vana la previsione di non registrare l'identità di chiamante e chiamato prevista dalla legge Usa e che nella sentenza è prevista come argomento a favore della liceità del programma di intercettazione.

Quanto alle capacità di analisi dell'Nsa, Pauley scrive che gli agenti possono risalire «solo» a tre gradi di separazione (*hop*) da un singolo *seed* (il numero bersaglio). Ma i tre balzi sono sufficienti per raggiungere, attraverso un solo numero, altre migliaia se non milioni di numeri.[97] Secondo Pauley, inoltre, non ci sono prove che questo straordinario potere di sorveglianza sia stato utilizzato per scopi diversi dalla prevenzione di attacchi terroristici e dunque dalla difesa della sicurezza nazionale. Ancora, il giudice giustifica il programma di sorveglianza sostenendo fosse necessario per il contrasto di Al Qaeda e del terrorismo, e in particolare per comprenderne le nuove dinamiche. Se solo l'Nsa avesse potuto operare la raccolta indiscriminata che opera

oggi, si legge, l'*intelligence* sarebbe stata in grado di sapere che l'attentatore dell'11 settembre Khalid al-Mihdhar stava contattando una cellula terroristica nello Yemen, da San Diego, e dunque dall'interno degli Stati Uniti; «il governo ha imparato dal suo errore», scrive Pauley, «e si è adattata per confrontare un nuovo nemico». L'aneddoto, come fa notare su Twitter Trevor Timm dell'Eff, è falso: l'Nsa sapeva già da tempo che il terrorista si trovava all'interno dei confini nazionali. Mentre l'affermazione di Pauley secondo cui «non può essere messo seriamente in discussione» che il programma di sorveglianza abbia sventato attacchi terroristici nei casi di Najibullah Zazi, Khalid Oazzani e David Headley si scontra con chi contesta questo legame effettivo, per esempio *ProPublica*. Allo stesso modo, è difficile, dopo quanto emerso i questi mesi, sostenere come fa Pauley che tra i giusti bilanciamenti al potere dell'Nsa ci siano lo scrutinio del Congresso (che in buona parte non sapeva, perché non informato) e della corte Fisa, talmente deficitario da rappresentare uno dei principali punti da riformare[98] perfino secondo il comitato di esperti nominato da Barack Obama.

Per quanto riguarda la già citata sentenza della Corte Superma del 1979 (Smith vs Maryland), usata per sostenere che i cittadini non hanno alcuna legittima aspettativa di privacy sui propri metadati telefonici, il parere di Pauley è opposto a quello di Leon: la ritiene ancora valida e per nulla obsoleta sul piano tecnologico. Allo stesso modo, è difficile, dopo quanto emerso dall'inizio del Datagate, sostenere che tra i giusti bilanciamenti al potere dell'Nsa ci siano lo scrutinio del Congresso (che in buona parte non sapeva, perché non

informato) e della corte Fisa (talmente deficitario da rappresentare uno dei principali punti da riformare perfino secondo il panel di esperti nominato da Barack Obama).

Kevin Gosztola, su Firedoglake, nota l'argomentazione più assurda usata da Pauley per giustificare la sorveglianza telefonica Nsa: se non fosse stato per le rivelazioni (non autorizzate) di Snowden, l'Aclu non avrebbe mai nemmeno saputo dell'esistenza del programma di sorveglianza in esame. E «non è possibile che la condotta illegale di un *contractor* del governo che rivela segreti di stato – inclusi gli strumenti e i metodi di raccolta di *intelligence* – vanifichi gli intenti del Congresso». Il giudice lo dice chiaramente:

> Il Congresso non intendeva che i bersagli degli ordini emanati secondo la sezione 215 [del Patriot Act, cioè la norma che secondo l'Nsa consente la raccolta indiscriminata dei metadati telefonici, *ndr*] ne venissero mai a conoscenza.

Commenta Gosztola:

> Essenzialmente, se un giornalista pubblica materiale non autorizzato o lo fa trapelare in un articolo di giornale e la causa fallirebbe senza quelle informazioni, il giudice sta suggerendo che il caso dovrebbe essere probabilmente chiuso. La segretezza è più importante di ciò che è stato rivelato e lo stesso dicasi della criminalità del *whistleblower*, del fatto che lei o lui abbiano dovuto violare la legge per rilasciare informazioni chiave che erano nell'interesse pubblico.

È sempre più probabile che l'ultima parola spetti alla Corte Suprema; nel frattempo, non si può fare a meno di

notare il contesto in cui è maturata la decisione di Pauley. Resta da valutare non solo la legalità, a questo punto discussa, del programma di sorveglianza dei metadati telefonici, ma anche quella di tutti gli altri: per esempio, è legale spiare istituti di beneficenza e leader europei, tra cui il responsabile delle politiche concorrenziali, nel nome della lotta al terrorismo? Restano da valutare le tutele dei cittadini non statunitensi rispetto all'operato dell'Nsa e dei suoi alleati, una questione che ha portato alcuni a ipotizzare che la Germania debba stabilire per contratto un divieto per le aziende operanti nel suo territorio di fornire informazioni ai servizi Usa. Restano da valutare le proposte del comitato voluto da Obamapredisposte dagli esperti della Casa Bianca. La battaglia legale insomma si preannuncia lunga e non certo limitata al caso in esame.[99]

Tao, l'unità di hacker per la sorveglianza globale

Nuovi documenti riservati della National Security Agency, visionati e raccontati da *Der Spiegel*,[100] dettagliano il funzionamento della sua unità di punta, il Tao (Tailored Access Operations). Si tratta della più sofisticata unità operativa dell'Nsa: può accedere ai bersagli più difficili per produrre gli elementi di *intelligence* più rilevanti («come una squadra di idraulici da chiamare quando il normale accesso a un bersaglio è impedito», si legge). Il Tao, inoltre, è l'unità dell'intelligence che più è cresciuta negli ultimi anni. E, si legge in un *paper* che ne definisce le prospettive, deve continuare a crescere e ottenere «accesso pervasivo e persistente alla rete globale». Il ramo dislocato ad Austin, Texas, per esempio, nel 2015 passerà dai 60 specialisti che impiegava nel 2008 a 270.

Le attività del Tao spaziano dagli attacchi informatici allo spionaggio tradizionale. Soprattutto, l'unità Nsa deve infiltrare, manipolare e sfruttare reti informatiche. Questi compiti sono esplicitamente parte del mandato e fanno pensare che quelli del Tao siano gli hacker (di punta) dell'Nsa. Come vedremo più nel dettaglio in seguito, il Tao ha anche un dipartimento interno deputato allo sviluppo di nuove tecnologie di sorveglianza.[101]

Secondo *Der Spiegel*, i bersagli violati nella seconda metà degli anni 2000 sono stati 258 in 89 paesi; nel solo 2010 il Tao avrebbe condotto 279 operazioni in tutto il mondo. Per riuscirci, gli agenti usano la tecnica di intrusione chiamata Quantum Insert e gestiscono i

server «segreti» su cui si basa il sistema denominato FoxAcid, usato dal Tao, per esempio, per fingersi Linkedin. In questo caso l'inganno funziona nel 50% dei casi; la tattica raggiunge picchi di successo dell'80%, contro l'1% del metodo tradizionale, che consiste nel' inviare *spam* via mail con un link contenente *malware*.[102]

Grazie ai nuovi documenti raccontati da *Der Spiegel*, ora conosciamo meglio i contorni (e il nome) dell'operazione condotta ai danni del presidente messicano Calderon. Si chiamava Whitetamale, serviva a sapere tutto del traffico di droga e di uomini al confine tra Usa e Messico, ed è proseguita per anni, fino a quando lo *Spiegel* ne ha rivelato l'esistenza a ottobre. Gli agenti potevano leggere le mail e gli accessi dai computer degli impiegati della segreteria del presidente, conoscerne tutto il traffico, guardare le immagini del circuito di videosorveglianza in uso. Ancora, sappiamo che il Tao si prende gioco di Microsoft, in particolare sfuttando i *pop-up* per indicare un errore di sistema in Windows come occasione per violare le difese del computer bersaglio (o meglio, leggerne i dati in uscita via Internet, ciò che il Tao chiama «accesso passivo») usando l'ormai noto programma XKeyscore[103] per identificare e distinguere i *crash report* dal flusso del traffico globale. Il metodo ha poca utilità pratica, scrive *Der Spiegel*, ma «agli agenti dell'Nsa sembra piacere perché gli consente di farsi qualche risata alle spese del gigante del software di Seattle».

I documenti confermano inoltre che l'Nsa ha intercettato (secondo il materiale visionato da *Der Spiegel*, il 13 febbraio 2013) le comunicazioni fluite

attraverso il cavo in fibra ottica sottomarino Sea-Me-We-4 che, come raccontato dall'*Espresso*,[104] ha un nodo anche a Palermo e vede tra i proprietari anche Telecom Italia Sparkl. L'unità, per accedere alle informazioni che transitano sui cavi sottomarini, fa ricorso non solo a Quantum Insert, ma anche all'«accesso fisico al bersaglio», ossia alle stazioni di trasmissione. Agli spostamenti degli agenti in carne e ossa del Tao pensa l'Fbi, mettendo a disposizione del Tao gli aerei dell'agenzia.

Il Tao intercetta inoltre le spedizioni di computer acquistati da soggetti, agenzie o aziende bersaglio, li trasferisce nelle sue postazioni di lavoro (*load station*), apre i pacchi e inserisce *malware software* e addirittura componenti *hardware* per garantirsi porte di accesso privilegiate e nascoste all'utente (*backdoor*). Tutti i passaggi successivi, scrive *Der Spiegel*, possono essere condotti in remoto, una volta che il computer è giunto a destinazione.

In un altro articolo *Der Spiegel* svela l'esistenza di un catalogo di 50 prodotti di «una divisione dell'Nsa chiamata Ant». Grazie all'Ant (Advanced o Access Network Technology), l'*intelligence* è riuscita a infiltrarsi nei componenti dei maggiori produttori *hardware* del mondo, da Cisco a Huawei e Dell. I prezzi delle *backdoor* arrivano fino a 250 mila dollari a unità. Non ci sono solo le componenti *hardware*: l'Ant «sviluppa anche *software* per compiti speciali», come infiltrare tramite *malware* i Bios dei computer, ossia il codice lanciato all'avvio del Pc, così da resistere alla formattazione e all'installazione di un nuovo sistema operativo («Persistenza»).[105] Altri programmi hanno

come bersaglio il *firmware* degli *hard disk* costruiti da Western Digital, Seagate, Maxtor e Samsung, i *firewall hardware* intesi a protezione delle reti informatiche di aziende e «router per utilizzo professionale». Per *Der Spiegel* non ci sono prove che le aziende bersaglio ne fossero a conoscenza, e anzi Cisco per esempio si dichiara «molto preoccupata» per le rivelazioni del settimanale tedesco.

Le modifiche alla sorveglianza Nsa proposte a Obama

Il comitato di esperti nominato da Barack Obama[106] lo scorso 27 agosto per suggerire proposte concrete di riforma della sorveglianza e del funzionamento della National Security Agency e, più in generale, del modo in cui gestire e procurarsi materiale di *intelligence*, ha infine prodotto un rapporto di 300 pagine, *Liberty and security in a changing world*, che la Casa Bianca rende pubblico. Le raccomandazioni al presidente formulate dai cinque esperti sono 46, e confermano alcune delle anticipazioni di *New York Times* e *Wall Street Journal* uscite nei giorni precedenti la pubblicazione.

Ecco in sintesi le raccomandazioni:

1. Sulla raccolta dei metadati telefonini, va cambiata la sezione 215 del Patriot Act per fare sì che la corte Fisa possa ordinare a terze parti di consegnare dati su singoli cittadini *solo se* è «ragionevole» ritenere che le informazioni così ottenute siano «rilevanti» per proteggersi da attività terroristica internazionale e *solo se* l'ingiunzione è «ragionevole nel focus, nello scopo e nell'ampiezza»;
2. Lo stesso criterio va applicato per le National Security Letter;
3. Le National Security Letter vanno inoltre assoggettate agli stessi vincoli della sezione 215 del Patriot Act;
4. «Al governo non dovrebbe essere consentito registrare e immagazzinare» in massa le

informazioni personali dei cittadini per rendere possibili analisi future a scopi di *intelligence*. Tutto deve essere «strettamente calibrato sul perseguimento di un importante interesse del governo»;

5. Mettere fine alla raccolta massiva di metadati telefonici e passaggio a un sistema in cui quei metadati sono detenuti da terze parti o da *provider* privati, e in cui il governo li può ottenere solo a seguito di un decisione della corte (sulla base dei nuovi criteri stabiliti dalla raccomandazione 1);
6. Il governo dovrebbe commissionare uno studio approfondito sulla differenza tra metadati e contenuto delle comunicazioni [ha ancora senso? *ndr*];
7. «Informazioni dettagliate» sulle operazioni dell'Nsa devono essere fornite «regolarmente» a Congresso e cittadini, sulla base di una «forte presunzione di trasparenza», così che gli americani possano farsi un'idea da sé della bontà o meno dei programmi di sorveglianza;
8. L'ordine di non rivelare operazioni Nsa deve essere emanato solo dopo che un giudice abbia accertato che rivelarle potrebbe «ragionevolmente» mettere a repentaglio la sicurezza nazionale (può avere efficacia solo per 180 giorni senza ulteriore autorizzazione giudiziaria) e senza che sia mai impossibile metterne in discussione la legalità;
9. Chi riceve ordini di consegnare dati personali deve poter dettagliare numero delle richieste,

numero di richieste cui ha acconsentito, tipologia delle richieste (generica), numero di persone coinvolte per tipologia di richiesta (cambieranno dunque i Transparency Report, come volevano i grandi di Internet, *ndr*);

10. La stessa trasparenza deve essere fornita dal governo, a meno che non riesca a dimostrare che rivelare quei dati «mette a repentaglio la sicurezza nazionale»;
11. I programmi di sorveglianza massivi e invasivi, come quello per la raccolta dei metadati telefonici, si possono nascondere ai cittadini statunitensi solo se è necessario per tutelare l'interesse del governo, e solo se l'efficacia di quel programma è «danneggiata in modo sostanziale nel caso i nemici vengano a conoscenza della sua esistenza». In ogni caso, per programmi di questo tipo vale «la forte presunzione di trasparenza che è centrale per una *governance* democratica»;
12. Qualora un programma di intercettazione mirato a raccogliere dati su un bersaglio straniero captasse informazioni su un cittadino americano con cui sta parlando, quei dati non devono poter essere usati contro di lui in un processo, devono essere cancellati a meno che non abbiano valore per l'*intelligence*, e il contenuto di quelle comunicazioni non può essere analizzato senza autorizzazione giudiziaria;
13. Quanto alla sorveglianza di cittadini non statunitensi, deve avvenire solo sulla base di quanto dice la legge, essere diretta «esclusivamente» alla protezione dell'interesse

nazionale o degli alleati (dunque non per ottenere segreti commerciali o ricavare vantaggi economici). Va poi esplicitato che il governo Usa non spia cittadini stranieri sulla base di convinzioni politiche e religiose, che la trasparenza del monitoraggio deve essere la massima possibile (compatibilmente con la difesa della sicurezza nazionale) e che la supervisione dell'operato Nsa deve essere «attenta»;

14. Il Privacy Act del 1974 deve applicarsi a cittadini Usa e non (a meno di eccezioni dimostrabili);
15. Limiti all'autorità Nsa per continuare a monitorare bersagli conosciuti quando entrano in suolo statunitense;
16. Obama deve creare una nuova procedura che identifichi limiti precisi alla sorveglianza dei leader stranieri;
17. Revisione delle priorità dell'*intelligence*, ma anche di metodi e obiettivi a ogni livello;
18. Il Director of National Intelligence dovrebbe «stabilire un meccanismo di monitoraggio della raccolta e della disseminazione dell'attività dell'*intelligence*», e redigere un rapporto annuale sull'argomento;
19. Prima di tenere sotto controllo leader stranieri, chiedersi se sia necessario per sventare minacce «significative», se si tratti del leader di un paese alleato, se ci sia ragione di sospettare nasconda informazioni rilevanti sulla sicurezza nazionale, se esistano altri modi per rivelare le informazioni di cui si ha bisogno e, ultimo ma non meno

importante, cosa succederebbe qualora si fosse scoperti;

20. Il governo dovrebbe esaminare la «realizzabilità» di *software* che facilitino intercettazioni mirate piuttosto che di massa;
21. Sviluppo di norme e prassi comuni con gli alleati più stretti, così da proteggere con le stesse regole cittadini di paesi diversi;
22. «Il presidente dovrebbe considerare una nomina civile [e non militare, *ndr*] per il prossimo direttore Nsa»;
23. Ristabilire che l'Nsa si occupa di *intelligence* straniera, e di niente altro;
24. Direttore Nsa e comandante del Cyber Command militare dovrebbero diventare due ruoli separati;
25. L'Information Assurance Directorate dell'Nsa dovrebbe diventare un'agenzia a se stante all'interno del Dipartimento di Difesa;
26. Creazione di un figura professionale deputata alla tutela della privacy e dei diritti civili;
27. Creazione di un organo, il Civil Liberties and Privacy Protection Board (Clppb) che supervisioni l'attività dell'Nsa, funga da «recipiente per le denunce dei *whistleblower* che abbiano a che fare con privacy e diritti civili». Creazione, inoltre, di un «Ufficio Valutazione Tecnologica» per promuovere tecnologie rispettose della privacy;
28. Nomina di un Privacy Interest Advocate, difensore della privacy di fronte alla corte Fisa. I giudici della corte, poi, dovrebbero avere a

disposizione «maggiore competenza tecnologica», l'operato di questa dovrebbe essere più trasparente e anche il processo di nomina dei suoi giudici dovrebbe essere rivisto;

29. Il governo statunitense dovrebbe «promuovere pienamente e non indebolire gli sforzi per creare gli standard crittografici»; «non compromettere, indebolire o rendere vulnerabile in alcun modo la crittografia commerciale di largo utilizzo», e anzi «incrementare l'utilizzo della crittografia e sollecitando le aziende statunitensi a fare altrettanto, così da meglio proteggere i dati in transito, statici, nella *cloud* e immagazzinati in altro modo»;
30. Lo sfruttamento di vulnerabilità precedentemente sconosciute in una applicazione o un sistema informatico (Zero-Day) è ammissibile solo per raccolte di *intelligence* «ad alta priorità» e dopo uno scrutinio che coinvolge le diverse agenzie;
31. Promuovere norme e accordi internazionali che prevedano misure specifiche per aumentare la sicurezza *online*;
32. Serve un Assistente Segretario di Stato che sia incaricato di gestire la diplomazia delle questioni tecnologiche internazionali;
33. Promozione di un modello di *governance* della Rete che sia davvero *multistakeholder*, nel senso di considerare non solo la voce dei governi, ma anche quella degli altri portatori di interesse;
34. Ottimizzare il processo per le richieste legali di dati a livello internazionale;

35. Per i programmi di *big data* e *data mining* devono essere prodotte valutazioni di impatto sulla privacy, ma anche sulla loro bontà statistica ed efficacia in relazione ai costi sostenuti per svolgerli;
36. Per i prossimi sviluppi tecnologici, va fatta una «valutazione programma per programma» da parte di esperti (anche del Clpbb) per rispondere a possibili nuove criticità sulla privacy;
37. L'esame delle credenziali del personale che ha accesso a materiale riservato deve essere svolto solo dal governo o da enti no-profit privati;
38. L'esame delle credenziali deve essere continuo, invece che periodico;
39. Differenziazione delle credenziali di accesso al materiale riservato, separando soggetti che possono accedere al materiale «amministrativo»/tecnico e soggetti che hanno accesso a scelte politiche e materiale d'intelligence;
40. La capacità di accesso deve essere valutata tramite un punteggio apposito (Access Score), da aggiornare periodicamente;
41. Solo chi ha realmente bisogno di accedere a determinati documenti riservati deve accedervi, senza che ciò coinvolga la diffusione a soggetti «meramente interessati»;
42. Le reti protette che contengono il materiale governativo riservato devono usare «i migliori *hardware* e *software* di cybersicurezza disponibili». Ogni anno il presidente deve ricevere un rapporto dettagliato che lo certifichi.

Tutte queste reti poi devono essere soggette a controllo continuo e costante per assicurarsi non siano soggette a intrusioni e attività anomale;

43. Immediata implementazione dell'ordine esecutivo con cui il presidente aveva dato le direttive per «migliorare la sicurezza delle reti riservate»;
44. Un comitato deve rivedere annualmente lo stato della sicurezza delle reti che trasportano segreti, consentendo anche il punto di vista di un ulteriore comitato indipendente composto da membri di diverse agenzie;
45. Tutte le agenzie e i dipartimenti del governo statunitense che gestiscono materiale riservato devono «espandere il loro utilizzo di *software*, *hardware* e procedure che limitano l'accesso a dati e documenti ai soggetti specificamente autorizzati ad accedervi»;
46. Per formulare decisioni e giudizi sulla sicurezza del personale e delle reti informatiche, il consiglio è usare l'analisi costi-benefici e approcci di gestione del rischio.

Note

1. «Secondo il paper, intitolato "Do NSA's Bulk Surveillance Programs Stop Terrorists?" e basato su «un'analisi approfondita di 225 individui reclutati da Al Qaeda o gruppi affini o ispirati ad Al Qaeda, e accusati di terrorismo dall'11 settembre», le affermazioni dei vertici USA sui 50 attentati sventati sono «esagerate» e «fuorvianti». In particolare, il controverso programma di intercettazione dei metadati telefonici dei cittadini statunitensi (e non), autorizzato dalla sezione 215 del Patriot Act, «sembra aver avuto un ruolo riconoscibile nel dare il là alla meglio all'1,8%» dei casi esaminati. Quanto agli altri programmi di sorveglianza, per quelli riguardanti cittadini non-USA secondo la sezione 702 del FISA Amendments Act, la percentuale sale appena al 4,4% delle minacce terroristiche analizzate. La sorveglianza NSA regolata da «autorità non identificate» si ferma all'1,3%. In altre parole, «la sorveglianza NSA di qualunque tipo» è stata utile a iniziare il 7,5% dei casi esaminati. I metodi tradizionali, per contro, sono stati usati in tal senso circa sei volte su dieci.»

2. Greenwald diventa già oggetto di un profilo piuttosto ambiguo. Che cosa significa infatti, scrivere in modo «ossessivo» su un argomento, come riporta il *New York Times*?

3. Metadati al centro anche dello scandalo riportato dall'*Associated Press*.

4. Electronic Frontier Foundation.

5. American Civil Liberties Union.

6. Segnalato da Gianni Riotta su Twitter.

7. Il *Guardian* conferma con un altro scoop, firmato da Nick Hopkins: i documenti ottenuti mostrano come il Gchq acceda ai dati di Prism da giugno 2010, «generando 197 rapporti di *intelligence* l'anno scorso».

8. Secondo il *Washington Post*, Prism è anzi la fonte «più prolifica» del «*daily brief*» del presidente Obama, che lo cita 1.477 volte solo nell'ultimo anno. Un rapporto su sette dell'Nsa sarebbe basato sul materiale grezzo ottenuto da Prism, dicono le fonti e il materiale consultato dal quotidiano.

9. *Politico* racconta come diversi membri del Congresso, repubblicani e democratici, sostengano il contrario: per sapere di Prism bisognava far parte della commissione Intelligence o fare specifica richiesta (dopo esserne venuti a conoscenza da un collega informato).

10. Tutte le argomentazioni del governo sono raccolte in questo documento.

11. Il 20 giugno il *New York Times* rivela inoltre l'esistenza di un programma segreto di Skype, Project Chess, «per esplorare le questioni legali e tecniche concernenti il rendere le chiamate via Skype immediatamente disponibili all'agenzia di *intelligence* e alle forze dell'ordine». A conoscenza di Project Chess, cominciato cinque anni fa (prima dunque della cessione a Microsoft), sarebbe «meno di una dozzina di persona all'interno» dell'azienda.

12. Secondo le fonti di *The Week*, l'Nsa avrebbe accesso in tempo reale – in molti casi in modo continuo dal 2006 – ai dati di cinquanta aziende, tra cui agenzie di *rating* creditizio e *Internet service provider*.

13. Al riguardo, su *The Atlantic* James Fallow si domanda perché mai fossero *top secret*.

14. Le affermazioni di Nadler appaiono coerenti con quanto dichiarato da Edward Snowden durante la videointervista al *Guardian* e, non meno importante, con quanto portato alla luce

già nel 2006 dall'ex impiegato di At&T, Mark Klein e in diversi resoconti giornalistici prodotti nel corso degli anni e citati da *Cnet*.

15. Tra le righe dei documenti pubblicati dal *Guardian*, come sottolinea *Ars Technica*, si legge che l'utilizzo di software di anonimizzazione come Tor o di servizi di email e messaggeria istantanea crittati potrebbe aumentare le chance di finire sotto lo sguardo dell'Nsa.

16. Di nuovo, il tutto è perfettamente coerente con i documenti e le ricostruzioni prodotte da Mark Klein, citato in precedenza.

17. Questo scenario si aggiunge a quello descritto dal *New York Times* nei giorni precedenti, relativo ad accordi tra aziende e governo Usa per strutture dedicate a rendere più semplice il trasferimento dei dati.

18. Programma iniziato, per l'appunto, durante la presidenza Bush e dopo gli attentati dell'11 settembre 2001.

19. Alex Stamos compone addirittura una tassonomia analitica di Prism sul proprio *blog*.

20. Per distinguere tra il flusso di dati ricevuto dalle aziende già in formato strutturato e consultabile (quello di Prism) e quello grezzo prelevato dal *backbone* a cui dare senso (Blarney).

21. Sebbene sia possibile, ma non confermato, il fraintendimento sull'espressione «accesso diretto» ai server.

22. Forse per questo Schneier dice ad *Associated Press* che, in conclusione, «non importa realmente come funzioni dal punto di vista tecnico Prism»: comunque stiano davvero le cose (e nessuno sta dicendo la verità in proposito, argomenta l'esperto di sicurezza informatica), dobbiamo assumere che «il governo registri tutto».

23. Mi limito a riportarlo, traducendolo.

24. Su *Gigaom* Mathew Ingram scrive che potrebbe trattarsi di una «rivelazione esplosiva circa l'ampiezza del programma Prism».

25. Nomi in codice per l'ambasciata italiana: «Bruneau» e «Hemlock».

26. L'articolo era disponibile all'indirizzo http://www.guardian.co.uk/world/2013/jun/29/european-private-data-america, prima di essere rimosso.

27. Gli attivisti per la privacy, durante le proteste in occasione dell'Indipendence Day (4 luglio), hanno per l'appunto criticato questa interpretazione.

28. Il programma è lo stesso che ha prodotto la sorveglianza «indiscriminata» di «milioni di telefonate e mail» in Brasile, come sostiene Glenn Greenwald su *O Globo* (con Roberto Kaz e Jose Cansado). Ne scrive anche, in inglese, sul suo blog sul *Guardian*, basandosi ancora una volta su documenti *top secret* forniti da Snowden. Il programma si chiama Fairview, e ha come bersaglio i cittadini di Paesi «amici» degli Stati Uniti. Il giornalista ne spiega così il funzionamento: «Secondo quel programma, l'Nsa stringe accordi con una grossa azienda di telecomunicazioni statunitense, la cui identità è attualmente sconosciuta, e quell'azienda a sua volta si accorda con le telecom di paesi stranieri. Queste collaborazioni consentono alle compagnie statunitensi di accedere ai sistemi di telecomunicazione di quei paesi, e quell'accesso viene quindi sfruttato per dirigere il traffico ai depositi dell'Nsa».

29. Segnalo la testimonianza di un ex ingegnere dell'Nsa su Prism raccolta dal *Sole 24 Ore* (riporto uno stralcio preso dall'*Huffington Post Italia*): «"è spaventoso quello che si può fare", ci dice l'ingegnere, che manterremo anonimo. A suo dire con circa cento milioni di dollari è possibile monitorare l'intera rete di un gestore nazionale di alto livello Tier One – parliamo di At&T, Deutsche Telekom, Vodaphone o Telecom Italia – e poi individuare ed estrapolare qualsiasi tipo di dato tecnico e contenutistico».

30. Per XKeyscore si veda il paragrafo successivo.

31. La Cancelliera tedesca nei giorni precedenti le rivelazioni di *Der Spiegel* aveva chiesto un accordo mondiale sulla protezione dei dati, sul modello di quello di Kyoto sui cambiamenti climatici.

32. Nelle stesse ore l'Nsa è messa alle strette in altre occasioni. La prima alla Black Hat Conference di Las Vegas, dove il direttore Keith Alexander, come racconta *Forbes*, durante il discorso è incalzato dal pubblico a suon di «bugiardo» e «non mi fido» accompagnati dagli applausi dei presenti. La seconda in un'udienza in Senato dedicata specificamente a ottenere i chiarimenti finora mancanti, durante la quale il democratico Al Franken ha annunciato la presentazione di una proposta di legge per rendere davvero trasparente la sorveglianza dell'Nsa (la proposta è successiva alla bocciatura dell'emendamento Amash, discussa al paragrafo successivo). Infine, il direttore della sicurezza nazionale James Clapper ha «declassificato» (nell'«interesse pubblico») i documenti riguardanti la raccolta dei metadati telefonici secondo la sezione 215 del Patriot Act.

33. Un buon riassunto in inglese del pezzo di *O Globo* è sul sito della *Reuters*.

34. Ad agosto Greenwald aggiunge un altro elemento al quadro: i programmi di sorveglianza digitale della National Security Agency hanno avuto come bersaglio gli stessi presidenti di Brasile, Dilma Rousseff, e Messico, Pena Nieto.

35. Come visto nel secondo capitolo.

36. Alle proteste si aggiunge, il 17 luglio, il Center for Democracy e Technology, che si fa portavoce di una vasta coalizione senza precedenti di colossi *web* e attivisti per la privacy e la libertà di espressione per chiedere maggiore trasparenza al governo degli Stati Uniti sui dati acquisiti nei programmi di sorveglianza di massa dell'*intelligence*, e per poter informare il pubblico delle richieste di informazioni sui loro utenti ottenute in relazione a questioni di sicurezza nazionale. La

coalizione, che include tra le altre aziende come Apple, Facebook, Microsoft, Google, Twitter e organizzazioni come Aclu, Eff e Human Rights Watch, dettaglia le richieste in una lettera.

37. Secondo *Tech Crunch*, la chiusura di Silent Mail è particolarmente degna di nota, dato che «il suo co-fondatore e presidente è Phil Zimmerman, l'inventore del programma molto diffuso di crittografia dei servizi mail Pretty Good Privacy».

38. È disponibile sul sito del *Guardian* il video dell'intervista.

39. Discusso è anche un possibile ruolo nell'operazione della Casa Bianca, informata dalle autorità britanniche quando si sono rese conto che il suo nome figurava tra i passeggeri del volo Berlino-Heathrow. Washington ha tuttavia affermato che l'iniziativa è stata presa in maniera autonoma dal governo britannico.

40. Segnalatomi da Francesco Costa su Twitter.

41. Analisi segnalatami da Mario Tedeschini Lalli.

42. Gli attacchi dell'*intelligence* statunitense sono stati 231 nel 2011, scrive sempre il *Washington Post*: i documenti forniti da Snowden dimostrano un'aggressività dell'amministrazione Obama nei confronti di sistemi informatici stranieri ben superiore a quanto finora conosciuto.

43. L'Nsa ha dedicato oltre 25 milioni di dollari del suo budget all'acquisto di *malware* prodotti da privati, il cui mercato si sviluppa principalmente in Europa.

44. In alcuni casi, il *malware* è piazzato in operazioni sul campo, spesso con l'aiuto di agenti della Cia, scrive il *Post*. Ma di norma avviene via software, e direttamente su reti informatiche più che su singoli computer, a opera di una unità apposita della Nsa chiamata Tao, Tailored Access Operations e dei suoi migliori hacker, all'opera nel Roc (Remote Operations Center).

I software utilizzati sarebbero in grado di resistere agli *upgrade* della strumentazione, di copiare dati archiviati, di prelevare informazioni selezionate e accedere a ulteriori canali di comunicazione. Per il Tao vedere qui al settimo capitolo.

45. Delle intercettazioni svolte nelle rappresentanze dell'Unione Europea a Washington, *Der Spiegel* aveva già scritto il 29 giugno.

46. Per Joshua Foust, quella di Greenwald è l'ipotesi meno credibile.

47. Come visto nel primo capitolo.

48. Del funzionamento della crittografia si è occupato il *Guardian*.

49. Della collaborazione tra Nsa e Microsoft per Outlook e Skype, il *Guardian* aveva già scritto il 12 luglio.

50. Il *Guardian* ha pubblicato anche un documento riguardante il progetto Bullrun.

51. Tor è a sua volta stato oggetto di attacchi, come si legge in questo articoli di Carola Frediani per *Wired*, e nel capitolo successivo.

52. Tra questi Scissors, descritto in una serie di *slide* di presentazione pubblicate sempre dal *Washington Post*.

53. Qui al quarto capitolo.

54. Gli attivisti dell'Electronic Frontier Foundation, notano di passaggio (su Twitter) che le spiegazioni sul funzionamento di Tor siano tratte da un loro manuale realizzato in Creative Commons ed etichettato *top secret* per l'occasione dall'Nsa. Violando così, tra l'altro, i termini della licenza.

55. Per meglio spiegare la complessa materia, c'è il Faq del *Washington Post*.

56. Qui al secondo capitolo.

57. Su Boundless Informant si veda qui al primo capitolo.

58. Secondo i numeri di Boundless Informant, i metadati raccolti a livello globale nel mese di riferimento sarebbero 124,8 miliardi, di cui buona parte in Pakistan, Afghanistan e India (rispettivamente 12,7, 22 e 6,3 miliardi).

59. Lo stesso giorno, il Presidente del Consiglio Letta incontra John Kerry, segretario di Stato americano, senza però rilasciare dichiarazioni ufficiali. Kerry stesso ha annullato la conferenza stampa prevista dopo l'incontro, affidandosi all'«ambasciata Usa». Il risultato è un insieme di dichiarazioni generiche che non chiarisce i punti oscuri della vicenda.

60. *L'Espresso* il 24 ottobre scrive che «i documenti di Snowden contengono molte informazioni sul controllo delle comunicazioni italiane, destinate a essere rivelate nelle prossime settimane». Tra le nuove rivelazioni che seguono, per l'appunto, quella sullo spionaggio relativo alla fine del Governo Monti.

61. Francia, Spagna e Germania, secondo il *Guardian* (da documenti *top secret* forniti da Snowden) hanno sviluppato programmi di sorveglianza in collaborazione con il Gchq. L'Italia sarebbe stata esclusa per la reputazione tutt'altro che lusinghiera della nostra *intelligence*: «Nel segnapunti degli alleati europei, sembra che gli italiani siano quelli che ne escono peggio. Il Gchq esprime la sua frustrazione per le frizioni interne alle agenzie italiane e per i limiti legislativi alle loro attività».

62. Riportato dall'Agi.

63. In una seconda anticipazione è menzionata anche l'intercettazione dell'attuale Papa, quando era il cardinale Bergoglio.

64. Qui nel sesto capitolo.

65. In un successivo resoconto, il *Guardian* ha corretto il *Washington Post*: «nel suo articolo, il Post ha suggerito che il progetto di intercettazione fosse chiamato Muscular, ma il *Guardian* ha appreso da altri documenti forniti da Snowden che il termine fa invece riferimento al sistema che consente la prima analisi delle informazioni raccolte dall'Nsa o dal Gchq allacciandosi ai cavi. I dati prodotti da Muscular sono quindi inoltrati ai database dell'Nsa o del Gchq, o a sistemi come lo strumento di ricerca XKeyscore, di cui il *Guardian* ha già detto in precedenza».

66. Sul sito del *Washington Post* è disponibile un'infografica su come viaggiano i dati nostri computer ai *data center* di Google.

67. Lo stesso Eric Schmidt, che solo a metà settembre si rifiutava di esprimere un giudizio sulle operazioni dell'Nsa e definiva la sorveglianza governativa «la natura della nostra società», ora parla di «spionaggio scandaloso» e «potenzialmente illegale».

68. Ancora, il *Post* sostiene che l'intercettazione delle comunicazioni internet al *cloud* di Google e Yahoo avverrebbe in Gran Bretagna e a gestirlo sarebbe principalmente il Gchq britannico. Una collaborazione grazie alla quale l'Nsa potrebbe evitare le (pur poche) restrizioni alla raccolta dei dati previste dalla legge statunitense.

69. Come visto nel quinto capitolo.

70. Invece, come riporta il *Guardian*, lo spionaggio dell'Nsa si spinge fino agli alleati più stretti, i membri del Five Eyes.

71. Si tratta dell'attacco *man-in-the-middle*, una tecnica che L'Nsa e il Gchq hanno impiegato anche per impersonificare Google.

72. Segnalo, a margine dell'articolo, il dibattito che è nato su Twitter e che ha coinvolto Wikileaks e Glenn Greenwald, riassunto sul mio blog *Chiusi nella Rete*. A far nascere il dibattito è la *slide* pubblicata da *Nrc* con supervisione di

Greenwald: la *slide* è stata sottoposta a un pesante intervento editoriale che ha oscurato molte località coinvolte. Il dibattito si allarga al controllo delle fonti, ed è di particolare interesse in uno scenario italiano in cui (come fa ad esempio Gianni Riotta sulla *Stampa*) si cerca ancora di far passare la distinzione tra *old media*, che controllano le fonti con i mezzi del giornalismo classico, e *new media*, che pubblicano indiscriminatamente. Proprio questo dibattito dimostra la fallacia della distinzione.

73. Per maggiori dettagli sul Tao si veda qui nel settimo capitolo.

74. *Nrc* cita anche l'articolo del *Washington Post* (30 agosto 2013) dedicato al *black budget* dell'Nsa, tema qui trattato nel terzo capitolo. Lì il *Post* parlava di 20 mila reti infettate nel 2008, numero che, in cinque anni, si è più che raddoppiato.

75. Per il 2016, l'agenzia contava di migliorare le proprie capacità di violare comunicazioni cifrate anche di singoli individui, integrare i sistemi di intercettazione e raccolta dati a sua disposizione in una «rete nazionale di sensori» in grado di allertarsi «alla velocità di una macchina» e soprattutto di poter condividere in modo ancora più capillare le masse di informazioni raccolte, così da consentirne una analisi più efficace.

76. Secondo l'hacker ed esperto di sicurezza informatica Jacob Appelbaum, si tratta di uno dei programmi più intrusivi nella privacy individuale tra quelli a disposizione dell'Nsa.

77. La stessa Onu (come visto qui, nel terzo capitolo) aveva subito l'hacking dell'Nsa.

78. Che tuttavia hanno lanciato, insieme a Privacy International e molte altre organizzazioni per i diritti umani, anche una petizione per l'applicazione delle linee guida per una sorveglianza responsabile dettagliate nell'iniziativa *Necessary and proportionate*.

79. Si veda questo articolo di Alexa O'Brien.

80. Perfino Wikileaks, che attraverso Sarah Harrison ha accompagnato Snowden in tutti i passaggi seguenti il suo disvelamento al pubblico, esprime i propri dubbi su Twitter.

81. Il 18 dicembre, invece, è Glenn Greenwald a rispondere a un'audizione, stavolta del Committee of Civili Liberties and Home Affair del parlamento europeo. Greenwald risponde in collegamento video dal Brasile.

82. Un resoconto dell'audizione si trova riassunto nel *live blog* dello stesso *Guardian*.

83. Proprio su questa trasmissione dei file si concentra il tentativo di colpevolizzare il *Guardian*, poiché i nomi non sono stati redatti prima del passaggio. Mario Tedeschini Lalli ben riassume la questione, centrale, su Facebook: «le accuse politico/giuridiche sono di aver "comunicato" all'esterno materiali secret e top secret, il che equivarrebbe a una violazione delle leggi anti-terrorismo. La cosa interessante è che questa "comunicazione" non sarebbe avvenuta con la pubblicazione dei servizi del giornale, ma con la trasmissione dell'intero insieme di 58.000 *files* al *New York Times* per sicurezza. E senza (ovviamente) averli prima ripuliti di informazioni che avrebbero potuto essere pericolose per la sicurezza (es.: nomi di agenti). Rusbridger, per rassicurare i parlamentari britannici, ha affermato che ora egli stesso e la direttrice del quotidiano americano Jill Abramson hanno un "controllo congiunto" (*joint control*) sui materiali. Questo sembrerebbe implicare che la Abramson non potrebbe pubblicare niente se non in accordo col collega britannico. Può essere, ma mi sembra poco probabile conoscendo gli usi della stampa americana».

84. Qui al terzo capitolo.

85. Come visto nel sesto capitolo.

86. Il funzionamento del sistema adoperato dall'Nsa è spiegato dal *Washington Post* in un'infografica.

87. Come visto al paragrafo precedente.

88. Qui al quinto capitolo.

89. Lo hanno pubblicato integralmente *Pro Publica* e il *Times*; il *Guardian* si è limitato a due pagine.

90. Come visto qui al sesto capitolo.

91. Qui al quarto capitolo.

92. Hezbollah lo avrebbe fatto con *Special forces 2*, mentre i piloti dell'11 settembre si sarebbero allenati con *Flight simulator* di Microsoft

93. In particolare, invece, è il *mobile gaming* a preoccupare, per l'idea che possa essere implementato nella pianificazione degli attentati.

94. Come anticipato da *New York Times* e *Wall Street Journal*; si veda anche qui al paragrafo successivo.

95. Come visto nel primo capitolo.

96. Pochi giorni prima, del resto, arriva la rivelazione del *Washington Post* che l'*intelligence* «ha la capacità di violare la tecnologia di cifratura di più diffuso utilizzo al mondo» per le comunicazioni via telefono cellulare, riuscendo così a «decifrare la gran parte dei miliardi di chiamate e messaggi» che solcano l'etere ogni giorno.

97. In sostanza, secondo l'Aclu, il soggetto che a giugno ha promosso la causa contro l'Nsa su cui il giudice si è espresso, se un sospetto di terrorismo ha 40 contatti nella sua rubrica, l'Nsa può ottenere il numero di telefono di 2,5 milioni di persone.

98. Si veda al paragrafo successivo.

99. L'Aclu, intanto, ha annunciato su Twitter ricorso.

100. La fonte delle nuove rivelazioni sono «documenti interni all'Nsa» visionati da Der Spiegel. Glenn Greenwald, su Twitter, puntualizza che i documenti non sono forniti da Snowden.

101. Si veda al sesto capitolo per casi già noti di attacchi del Tao e per la tecnica Quantum Insert, usata anche dal Gchq per infettare la rete della Belgacom (come visto ancora nel sesto capitolo.

102. La lista dei bersagli delle Quantum Capabilities, pubblicata per la prima volta da *Der Spiegel* (e riportata in rete da *Cryptome*, che non smette di lamentarsi della scarsità dei documenti pubblicati a fronte di quelli raccontati dai giornalisti negli articoli sul Datagate), contiene i servizi Internet più popolari: da You Tube e Yahoo a Facebook e Twitter.

103. Visto nel secondo capitolo.

104. Qui al secondo capitolo. Per il coinvolgimento dell'Italia nel Datagate, invece, si veda al quinto capitolo.

105. *Der Spiegel* pubblica successivamente un'infografica interattiva con i contenuti del catalogo di prodotti di sorveglianza che la National Security Agency può acquistare dall'Ant. Stando al nuovo materiale, L'Nsa aveva il controllo totale degli iPhone di prima generazione, potendo «scaricare o caricare file» sul telefono da remoto, dirottarne gli sms, scorrere la rubrica dell'utente bersaglio, intercettarne i messaggi vocali, localizzare il telefono in qualunque momento e perfino accenderne la videocamera all'insaputa del possessore. Tutto tramite un *malware* che l'*intelligence* sostiene abbia avuto successo nel 100% dei casi. Una circostanza che ha fatto avanzare un dubbio all'esperto di sicurezza informatica Jacob Appelbaum, durante il suo recente intervento al trentesimo Chaos Communication Congress di Amburgo: Apple ne era a conoscenza? E ha aiutato in segreto l'Nsa a compromettere i suoi device? «Spero Apple chiarisca», ha detto Appelbaum, che tuttavia è pessimista: «non credo davvero che Apple non abbia aiutato l'Nsa». tutti i documenti pubblicati sono reperibili su Leaksource.

106. Qui al terzo capitolo.

Ringraziamenti

Ringrazio il gruppo editoriale L'Espresso - Finegil, il Messaggero Veneto e Valigia Blu per lo stimolo, la collaborazione e per aver accettato la sfida di pubblicare questo e-book.

F. C.

Indice