WIKIPEDIA

Divulgazioni sulla sorveglianza di massa del 2013

Da Wikipedia, l'enciclopedia libera.

> **Questa voce o sezione sull'argomento storia è ritenuta da controllare**.
> **Motivo**: *traduzione troppo letterale di una pagina di en.wiki che pecca di recentismo e disorganizzazione meglio ridistribuire i contenuti fra PRISM, Tempora, NSA e Snowden*

Con **divulgazioni sulla sorveglianza di massa del 2013** si fa riferimento ad una serie di inchieste giornalistiche pubblicate dal mese di giugno del 2013 e volte a rivelare dettagli sulle operazioni di sorveglianza e compromissione di massa, messe in atto dall'Agenzia per la Sicurezza Nazionale statunitense (NSA) in complicità con servizi di intelligence di altri paesi, sia nei confronti di cittadini e istituzioni statunitensi che stranieri.

Tali inchieste sono iniziate alla fine del 2012, quando Edward Snowden ha iniziato a mettere a disposizione di alcuni giornalisti numerosi documenti top secret collezionati durante la sua attività per l'NSA. I primi documenti riservati sono stati pubblicati il 6 giugno 2013 dai quotidiani *The Washington Post* e *The Guardian*, attirando una notevole attenzione da parte del pubblico e del resto dei media[1].

Le prime attività di sorveglianza di massa negli Stati Uniti sono iniziate negli anni 1940, per poi essere notevolmente estese nel corso degli anni 1970, assumendo portata globale grazie al programma ECHELON[2]. Nel 2013, grazie alle rivelazioni di Snowden, sono stati svelati nuovi programmi di sorveglianza di massa, quali PRISM, XKeyscore e Tempora[3]. Tali programmi di spionaggio sono attuati in collaborazione con varie agenzie straniere, in particolare quelle dei paesi dell'accordo UKUSA, un'alleanza tra Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti volta a raccogliere informazioni attraverso attività di SIGINT, e vedono come obiettivi privati cittadini e istituzioni di vari paesi, inclusi alleati occidentali degli Stati Uniti e membri della NATO[4]. Come confermato dal direttore dell'NSA Keith B. Alexander il 26 settembre 2013, ad esempio, l'NSA raccoglie e custodisce sistematicamente informazioni sui tabulati telefonici di tutti i cittadini statunitensi[5]; nonostante il presidente Obama e lo stesso Alexander durante i mesi precedenti avessero più volte negato l'esistenza di un qualsiasi tipo di spionaggio domestico[6]. L'enorme quantità di dati raccolti sono conservati in impianti di stoccaggio di grandi dimensioni, come lo Utah Data Center, una struttura di oltre un milione di metri quadri dal costo stimato di 1,5 miliardi di dollari[7].

Come risultato di tali divulgazioni, diversi movimenti, tra cui Restore the Fourth, sono nati per protestare contro le attività di sorveglianza; l'Electronic Frontier Foundation si è unita ad una coalizione di vari gruppi per avviare azioni legali contro l'NSA; mentre l'amministrazione statunitense si è vista costretta a gestire tensioni diplomatiche con paesi alleati e non[8]. Snowden, con il sostegno di varie associazioni per la tutela dei diritti umani, quali Amnesty International, Human Rights Watch, Transparency International e Index on Censorship[9][10][11][12], il 14 giugno 2013 è stato incriminato in accordo con l'Espionage Act del 1917 con l'accusa di furto di proprietà governativa. In seguito gli è stato concesso un temporaneo asilo politico in Russia, il che ha contribuito a deteriorare le relazioni diplomatiche tra il governo russo e statunitense[13][14].

Indice

Cenni storici

Prime attività di intercettazione statunitense

Durante la seconda guerra mondiale, il Regno Unito e gli Stati Uniti attuarono una serie di accordi per la condivisione delle intercettazioni delle comunicazioni dei nemici[15]. Nel marzo 1946, per mantenere in vita tali accordi anche a guerra conclusa, fu siglato un nuovo patto segreto, il British-US Communication Intelligence Agreement, noto come BRUSA[16]. Nel 1945 fu messo in piedi l'ormai defunto Project SHAMROCK, creato per intercettare tutte le comunicazioni telegrafiche da e verso gli Stati Uniti[17][18]. Più tardi le maggiori compagnie telefoniche statunitensi, tra le quali Western Union e ITT World Communications, aiutarono il governo degli Stati Uniti in un primo tentativo di accedere alle reti di comunicazione globale[19].

Mentre alcune agenzie si dedicavano alle comunicazioni internazionali, l'FBI, sotto la guida di John Edgar Hoover, portava avanti una vasta attività di intercettazione nei confronti di molti personaggi pubblici, tra cui Albert Einstein[20], Frank Sinatra[21], Eleanor Roosevelt[22], Marilyn Monroe[23], John Lennon[24] e Martin Luther King Jr.[25], indicato in un memo dell'FBI come «il più pericoloso e potente leader negro negli USA»[26]. Molte di tale attività vennero esposte al pubblico già durante lo scandalo Watergate[27].

L'NSA nacque segretamente nel 1952, per volontà del presidente Harry Truman[28].

Sorveglianza di massa a livello globale: il programma ECHELON

(EN)

«Imagine a global spying network that can eavesdrop on every single phone call, fax or e-mail, anywhere on the planet. It sounds like science fiction, but it's true. Two of the chief protagonists - Britain and America - officially deny its existence. But the BBC has confirmation from the Australian Government that such a network really does exist.»

(IT)

«Immaginate una rete di spionaggio globale in grado di intercettare ogni singola telefonata, fax o e-mail, ovunque sul pianeta. Sembra fantascienza, ma è vero. Due dei protagonisti - Gran Bretagna e USA - negano ufficialmente la sua esistenza. Ma la BBC ha ricevuto conferma da parte del governo australiano che una rete del genere esiste davvero.»

(Articolo della BBC del 3 novembre 1999[29])

Nel 1988, un articolo intitolato *Somebody's listening*[30], scritto da Duncan Campbell sul *New Statesman*, riportò per la prima volta l'esistenza del programma ECHELON[31]. Avviato da Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti, insieme noti come AUSCANNZUKUS, e basato sull'accordo UKUSA, era nato con lo scopo di monitorare le comunicazioni

militari e diplomatiche dell'Unione Sovietica durante la guerra fredda[32]. Anche se la sua esistenza era già nota, l'UKUSA agreement divenne ufficialmente pubblico solo nel 2010.

Con il passare degli anni, divenne una rete di intercettazione globale. Negli anni 1990, il sistema ECHELON era in grado di intercettare comunicazioni satellitari, telefonate tradizionali, traffico internet e trasmissioni a microonde. Il suo funzionamento venne descritto nel 1996 nel libro *Secret Power*, di Nicky Hager. Nonostante l'esistenza di ECHELON continuò ad essere ufficialmente negata da vari esponenti del governo statunitense, fu invece confermata da un'indagine del Parlamento europeo del 2001[2], la quale lo definì un «sistema globale di intercettazione di comunicazioni private e commerciali»[32][33].

Effetti dell'11 settembre e fughe di notizie precedenti Snowden

Dopo gli attentati dell'11 settembre 2001, la portata delle attività di intercettazione negli Stati Uniti aumentò esponenzialmente. Allo scopo di evitare il ripetersi di tali eventi, fu siglato il Patriot Act, cui seguirono altri provvedimenti della stessa natura. Tra questi anche il Protect America Act, che rimuove la necessità di un mandato per l'esecuzione di intercettazione nei confronti di obiettivi stranieri[34], e il FISA Amendments Act.

Tra il 2005 e il 2012, *Wired* svelò l'esistenza del sistema di raccolta dati STELLARWIND, voluto dal presidente Bush poco tempo dopo gli attacchi dell'11 settembre[35]. Il programma, il quale prevede l'analisi di metadati raccolti monitorando il traffico internet, oltre che da altri tipi di telecomunicazione, venne continuato dall'amministrazione Obama. Nel marzo del 2012, in particolare, la rivista pubblicò un articolo che faceva riferimento alla costruzione negli Stati Uniti di un centro di sorveglianza di massa di vaste proporzioni[36], il quale divenne presto oggetto di un'interrogazione parlamentare. In tale interrogazione, il direttore dell'NSA Keith B. Alexander negò la veridicità di quanto dichiarato da *Wired*, negando anche l'esistenza di un qualsiasi tipo di programma di sorveglianza di massa sui cittadini statunitensi[37].

Le rivelazioni sulla sorveglianza di massa del 2013

Tra fine 2012 e i primi mesi del 2013, Edward Snowden consegnò tra i 15 e i 20 mila documenti top secret ai giornalisti del *The Guardian* Glenn Greenwald e Laura Poitras[38]. Dal 6 giugno 2013, il quotidiano inglese iniziò a pubblicare parte di tali documenti, portando alla luce come l'NSA abbia messo in piedi una complessa rete di spionaggio, basata su programmi come PRISM, XKeyscore e Tempora, in grado di intercettare il traffico internet e telefonico di utenti di ogni parte del mondo. A tal fine l'NSA ha usufruito oltre al supporto di altre istituzioni statunitensi, quali l'FBI o il Dipartimento di Giustizia, anche di importanti società private, tra le quali Verizon, Telstra, Google e Facebook.

Fondamentale è stata anche la collaborazione dei servizi di intelligence straniera, per accedere ai principali punti di snodo delle telecomunicazioni sparsi per il mondo. Oltre ai servizi degli altri paesi, soprannominati i "cinque occhi", che hanno siglato l'accordo UKUSA, ossia il Defence Signals Directorate australiano, il Communications Security Establishment canadese, il Government Communications Security Bureau neozelandese e il Government Communications Headquarters britannico, l'NSA ha cooperato con agenzie di varia nazionalità, tra cui il Bundesnachrichtendienst tedesco, l'Unit 8200 israeliano e il National Defence Radio Establishment svedese, il quale ha dato accesso ai cavi sotto al mar baltico[39].

Scopi e obiettivi della sorveglianza di massa

Nati con la giustificazione della lotta al terrorismo e la preservazione della sicurezza nazionale, i vari programmi di sorveglianza sono stati estesi a pieno campo ed impiegati impropriamente ed illecitamente per valutare la politica estera e la stabilità economica di altri paesi, e per raccogliere informazioni riservate di natura commerciale industriale, anche riguardanti soggetti privati; ciò anche allo scopo di avvantaggiare l'amministrazione statunitense durante le trattative durante la preparazione di trattati internazionali o accordi di natura economica con altri paesi[40][41].

Segue un elenco di alcuni obiettivi della rete di sorveglianza dell'NSA svelati tra i mesi di giugno e ottobre 2013[42].

- L'NSA colleziona metadati sulle telefonate effettuate attraverso tutti i gestori statunitensi.
- Una speciale divisione dell'agenzia chiamata "Follow the Money" raccoglie dati sulle transazioni finanziarie di soggetti privati da importanti istituti internazionali come Visa, Mastercard e SWIFT.
- Grazie ad alcuni programmi come Fairview e centri d'ascolto sparsi per il mondo, l'NSA e la CIA sono in grado di accedere ai dati generati dal traffico telefonico e internet anche di altri paesi; i soli paesi "immuni" sono quelli dell'accordo UKUSA, ossia Australia, Canada, Nuova Zelanda e Regno Unito. Il 31 luglio 2013 il *The Guardian* riportò l'esistenza del programma XKeyscore, il quale si avvale di una rete di 500 server segreti i quali registrano «quasi tutto quello che fa un utente medio su internet»[43].
- Attraverso il programma di sorveglianza PRISM l'NSA ha accesso diretto ai server di molte delle principali aziende dell'informatica statunitense, quali Microsoft, Google, Yahoo!, Facebook, Apple, YouTube e Skype. Alcune di tali aziende hanno anche collaborato con l'NSA per craccare i sistemi di criptaggio dei dati utilizzati. L'agenzia monitora quindi le attività degli utenti, compresi scambi di messaggi, foto e video, conservando in particolare le liste di indirizzi utente usate nei servizi e-mail e di messaggistica istantanea. Secondo un articolo del *Washington Post* in un solo giorno del 2012 l'agenzia ha collezionato oltre 400.000 indirizzi mail solo da Yahoo![44].
- Sono stati spiati anche capi di stato o di governo, tra cui Dilma Rousseff (Brasile), Felipe Calderón (Messico) e Angela Merkel (Germania). In particolare, l'agenzia avrebbe intercettato i telefoni personali di 35 leader politici stranieri, tra cui il cellulare privato di Angela Merkel[45]. Tra gli organi di governo stranieri spiati, figurano il Ministero dell'Energia brasiliano e il Ministero per gli affari esteri francese, oltre che vari componenti del governo indiano.
- In collaborazione con la CIA, l'NSA ha piazzato strumenti di intercettazione in circa 80 tra ambasciate e consolati in tutto il mondo[46].
- Sono state spiate anche diverse sedi della NATO, dell'ONU, dell'Unione europea, e loro funzionari di primo livello, tra cui il segretario generale Ban Ki-moon[46][47][48]. Attività di spionaggio sono state condotte anche in occasione di summit internazionali, in cui sono finiti nel mirino degli agenti segreti vari diplomatici e leader politici.
- Tra le attività di spionaggio industriale, sono finite nel mirino dell'NSA anche Google, Petrobras, società leader nella trivellazione nelle profondità marine[49], e SWIFT.
- Nel 2006 l'NSA inserì una backdoor in uno dei principali standard di codifica addirittura del National Institute of Standards and Technology, istituto guida americano responsabile di definire le norme di sicurezza del cyberspazio.

Nomi dei programmi e sistemi utilizzati

Tra i principali programmi di sorveglianza e software svelati dai documenti di Snowden sono presenti:

- PRISM, programma per il monitoraggio del traffico generato da vari fornitori di servizi elettronici e telematici, compresi Apple, Microsoft, Facebook, Google e Skype.
- Boundless Informant, programma per la gestione dei dati raccolti.
- Tempora, programma di sorveglianza elettronica e telematica del British Government Communications Headquarters.
- XKeyscore, programma per l'analisi del traffico internet generato da utenti al di fuori degli Stati Uniti.
- Mail Isolation Control and Tracking, sistema di tracciamento della posta ordinaria, con il collezionamento di tutti gli indirizzi usati.
- Fairview, programma per l'intercettazione delle telecomunicazioni originate al di fuori degli Stati Uniti.
- Dropmire, programma per le intercettazioni all'interno di ambasciate e consolati stranieri.
- Genie, nome in codice di una botnet utilizzata per infiltrarsi in reti protette.
- Bullrun, nome derivante dall'omonima battaglia, è un software per l'analisi del traffico internet criptato.
- Edgehill, nome derivante dall'omonima battaglia, è l'equivalente di Bullrun utilizzato da British Government Communications Headquarters.