DATAGATE IN TRE CAPITOLI

Il caso NSA suscitato dalle rivelazioni di Edward Sneuwden sulla gigantesca raccolta di dati telefonici e Internet da parte dell'Agenzia per la Sicurezza americana è molto importante e merita qualche chiarimento.

Alessandro Ovi

La coincidenza con il primo incontro tra i presidenti americano e cinese, che ha toccato in profondità le attività di spionaggio elettronico, ha suscitato un polverone di commenti sul mondo digitale, che hanno mescolato aspetti completamente diversi: la protezione della privacy, lo spionaggio industriale, la guerra digitale.

Privacy

Il caso NSA riguarda il tema delicato, a lungo discusso dall'"11 settembre" in poi, della necessità di mediare tra la protezione dal terrorismo e quella della privacy.

Almeno nei primi anni dopo l'attentato alle Torri Gemelle, l'opinione pubblica americana è stata nella sua maggioranza pronta a rinunciare almeno in parte alla privacy per permettere al governo la raccolta di dati utili a prevenire azioni terroristiche. Di questo argomento si parla abbondantemente in queste pagine e si è già parlato on-line, nei servizi riportati nelle pagine seguenti. Si affrontano il tema del crescente dibattito americano sulla legittimità dell'allargamento del ruolo della NSA, il comportamento dei grandi operatori Internet, il crescente confronto tra Europa e Stati Uniti. È importante evitare la confusione tra la raccolta di dati di telefonate e comunicazioni Internet, di cui il sistema NSA si riferisce, e il problema della pubblicazione delle registrazioni delle intercettazioni telefoniche, così sensibili nell'ambiente italiano.

Spionaggio

Il dialogo tra Obama e Xi ha toccato il tema completamente diverso dello spionaggio industriale via Internet, di cui gli Stati Uniti accusano pesantemente la Cina e di cui abbiamo parlato ampiamente nel fascicolo precedente.

Il Rapporto Madiant fatto divulgare dagli organi di stampa americani ha tentato di fornire le prove di una massiccia e continua attività di spionaggio via Internet effettuata da centro di Shangai.

Tuttavia, già negli interventi della nostra rivista si faceva notare un dubbio che emerge dal Rapporto Mandiant, osservando come fosse strano che questi "furti" siano avvenuti senza nessuna attenzione a nascondere la provenienza dell'attacco informatico.

Il Rapporto si domandava addirittura come fosse possibile che gli operatori che hanno compiuto queste intrusioni, apparissero così poco "professionali". Inoltre anche aziende in Canada, Regno Unito, Sud Africa e Israele sarebbero state prese di mira.

Il fatto però che gli aggressori non si siano preoccupati di utilizzare metodi noti per nascondere il loro indirizzo IP, fa dubitare cha alle loro spalle possa esserci realmente l'esercito cinese, la cui competenza informatica viene valutata di buon livello.

Il Rapporto Madiant è certamente interessante, ma ancora più interessante è che non tutti i commenti dei lettori siano stati come al solito negativi nei confronti dei cinesi. Ancora più interessante è stato leggere un paio di settimane fa, su una fonte autorevole come "Businessweek Technology Insider", una secca smentita della provenienza cinese di queste attività di *cyber crime*, con il sospetto che all'origine vi siano operatori dell'Est Europa. "Businessweek Technology Insider" riprende l'opinione dei più grandi operatori Internet del mondo (Microsoft, Apple, Facebook, Twitter...) che alla Conferenza di Barcellona hanno condiviso le loro esperienze di vittime di attacchi informatici e hanno convenuto che la minaccia viene da molti paesi e quasi sempre per motivi commerciali e non politici.

Guerra digitale

La presenza tra gli oggetti di spionaggio industriale dei sistemi di controllo di grandi infrastrutture di energia, trasporti e telecomunicazioni, ha allargato il discorso a un terzo tema, quello della guerra elettronica, a cui tutti i grandi paesi al mondo si stanno preparando, e non solo per la difesa da attacchi via Internet, ma anche per l'attacco di ritorsione.

Gli Stati Uniti, per esempio, hanno recentemente istituto, con una missione allargata USCYBERCOM, una unità delle Forze Armate che risponde al Comando Strategico dell'Esercito. L'allargamento della missione consiste proprio nel preparare non solo le misure di difesa di tutte le strutture strategiche del paese, ma anche la capacità di rispondere tempestivamente ed efficacemente a eventuali ritorsioni. ■

Alessandro Ovi è direttore della edizione italiana di MIT Technology Review.

Troppi controlli da parte della NSA?

Le comunicazioni elettroniche possono venire monitorate in modi che non sono sempre anticipati dalle leggi sulla privacy.

Alessandro Ovi

Qualche anno fa incontrai a Pechino, con un gruppo di investitori californiani, Jack Ma, il "fondatore cinese visionario" di Alibaba (lui che era solo un insegnante di inglese), già allora uno degli operatori di Internet più potenti al mondo.

Ricordo il momento di imbarazzo tra i miei colleghi americani, quando, rispondendo a una mia domanda, ammise molto tranquillamente che, quando il governo gli chiedeva di fornire tutti i dati di telefonate ed e-mail negli archivi dell'azienda, lui ordinava di consegnarli. Era per la sicurezza nazionale. E ubbidiva.

Oggi leggiamo dello scandalo sollevato dal fatto che la NSA (National Security Agency) americana ha chiesto la stessa cosa a operatori telefonici e Internet americani, a cominciare dal più grande, Verizon. E questi operatori hanno fatto come Alibaba, dando pieno accesso ai dati.

Appare del tutto comprensibile l'imbarazzo che si dice aleggiasse sull'incontro californiano tra Obama e il presidente cinese Xi.

La differenza delle situazioni, sottolineata da NSA (ma a mio parere irrilevante), è che il loro operato non serve a leggere e-mail o ad ascoltare telefonate di qualcuno in particolare, ma solo a operare una raccolta di dati, che parrebbe assolutamente legale. Gli Stati Uniti hanno leggi che proteggono il contenuto delle telefonate, ma offrono pochissima protezione nei confronti dei tanti dati che sono collegati all'uso di un apparato cellulare, dal rilevamento della posizione personale alle transazioni commerciali.

Il *Data Mining* è una tecnologia informatica oggi in fortissimo sviluppo, che serve a trovare blocchi di informazioni specifiche di un certo oggetto in vari settori, (dai profili di consumo al marketing di settore, dalla pubblicità mirata alle analisi di preferenze politiche, fino alle campagne elettorali *one to one*, dalla valutazione di "atmosfere terroristiche" alla identificazione dei soggetti portatori di minaccia potenziale).

Molti pensano, e probabilmente hanno ragione, che il *Data Mining* si sia in realtà sviluppato proprio per soddisfare esigenze di sicurezza nazionale. A dare all'inizio un elevato contenuto tecnologico a questo tipo di ricerche è stato l'accordo tra gli addetti della NSA e la società di Palo Alto, Palantir Technologies, il primo di una serie di altri, da cui è partita la corsa a trovare la chiave di accesso al tesoro dei grandi numeri di dati (*Big Data*).

Si è trattato di una vera rivoluzione del software verso elaborazioni rapidissime di enormi quantità d'informazioni, che ha permesso alla NSA di mettere sotto controllo i "patrimoni digitali" di americani e stranieri, ivi incluso il controllo della posizione e dei movimenti di milioni e milioni di persone nel mondo, incrociando i dati dei GPS degli smartphones con quelli delle celle dei telefoni mobili.

La NSA ha ricevuto miliardi di dollari dal governo nell'ultimo decennio e ha costruito giganteschi centri di calcolo come quello nello Utah, dotato degli elaboratori più veloci per decodificare le informazioni protette.

Secondo il "Guardian", che per primo ha fornito la descrizione del sistema di raccolta dati della NSA, nel marzo 2013 erano qui accumulati 93 miliardi di informazioni provenienti da tutto il mondo, di cui il 14 per cento dall'Iran.

La tecnica è molto apprezzata, e fino a oggi le critiche sono state deboli. Il problema è che una volta che i dati provenienti da varie fonti vengono concentrate in un unico contenitore o in nuvole protette, è l'uso che se ne può fare a rappresentare implicitamente una seria minaccia alla privacy.

Quello che entra in gioco è la definizione della *mission* nell'ambito di cui l'ente che raccoglie i dati deve limitarsi a lavorare.

In un servizio sulla edizione americana di MIT Technology Review, Tom Simonite e Rachael Metz puntano il dito proprio sull'allargamento della *mission* della NSA che, uscendo dall'ambito del controllo dei soli cittadini stranieri, ha dato l'impressione agli Stati Uniti di trovarsi all'improvviso nelle mani del famigerato Grande Fratello. È stata la sorveglianza telefonica a supportare l'idea che la NSA abbia allargato troppo gli orizzonti della sua *mission*, derivante dal Patriot Act del 2001.

Per tranquillizzare l'opinione pubblica, il Presidente Obama è arrivato al punto di dire che "nessuno ascolta le vostre telefonate". Ma quello che è successo va al di là del problema dell'ascolto. Significa che prima la *mission* della NSA era interpretata come la possibilità di chiedere caso per caso l'accesso a dati specifici esistenti, dopo un controllo del FISC (Foreign Intelligence Surveillance Court). Oggi invece in una nuova interpretazione segreta del Patriot Act, come ha chiaramente dichiarato James Clipper, Direttore della National Intelligence, si considera legale l'accesso completo a tutti i dati esistenti e futuri, indipendentemente da un loro interesse specifico.

Gli esperti di democrazia e sicurezza pensano che il bilanciamento tra le due interpretazioni stia scivolando verso la seconda a sfavore della prima.

Sulle telefonate, quindi, tutti d'accordo. Diverso è l'atteggiamento nei confronti di PRISM (il sistema di raccolta dei dati preseti su Internet) che è probabilmente non lecito in altre parti del mondo, come l'Unione Europea, ma è certamente considerato accettabile negli Stati Uniti.

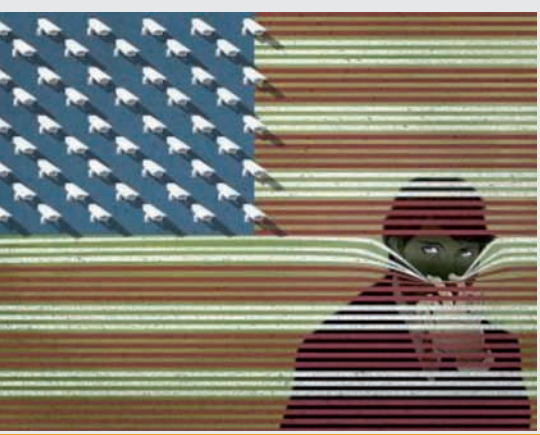
Dice un lettore di MIT Technology Review: «Sono sorpreso che la gente non comprenda che la tecnologia dell'informazione è destinata a produrre una continua perdita di privacy. Non stiamo parlando di persone che vengono sorvegliate nella loro casa. Stiamo parlando di persone che lasciano informazioni in un posto pubblico. Se volete che nessuno le legga, e-mail, tweet o blog che siano, non usate questi canali. Non ci può essere alcuna aspettativa di privacy in una comunicazione che transita e può essere raccolta in ogni computer di Internet. Se la comunicazione lascia la vostra casa non dovete aspettarvi che sia privata, a meno che

un giudice la dichiari tale e consideri che vi sia un danno per voi se qualcuno la diffonde. Contro il terrorismo e i suoi tremendi rischi bisogna fare tutto ciò che serve. Ma pensare che la vostra comunicazione sia più sicura in una rete privata (motore di ricerca o social network che sia) che non nella rete della NSA è naif e senza senso. È troppo tardi per diventare paranoici per la perdita della privacy, dopo che avete accettato più volte di perderla in cambio di servizi gratuiti».

Ma un altro lettore risponde: «La Costituzione degli Stati Uniti fa specifico divieto al governo federale di effettuare questo tipo di monitoraggio su cittadini innocenti. È assolutamente necessario ripristinare la regola della legge. Il nostro governo ha smarrito la retta via e ogni senso dei limiti del proprio potere».

Un terzo lettore considera un diverso aspetto del problema: «L'amministrazione non è estranea a usare il potere dell'informazione per motivi politici e questo è uno sviluppo molto pericoloso».

Le ultime rivelazioni sull'uso esteso della raccolta dati a vari livelli stanno rimettendo tutto in discussione. Siamo al punto che sono in molti a chiedere l'istituzione di un nuovo Church Committee (un Comitato guidato dal senatore democratico Church, che nel 1970 aveva investigato sulla raccolta di informazioni del governo e sulla sorveglianza domestica, portando alla formazione del Foreign Intelligence Surveillance Act e della Foreign Intelligence Surveillance Court). Sta per esplodere negli Stati Uniti un nuovo confronto tra la necessità di controllo e quelle di democrazia e privacy. Sarà bene che sia un confronto basato su una riflessione profonda. ■



Facebook, Google e NSA

Mark Zuckerberg e Larry Page hanno negato di conoscere le operazioni della NSA.

Alessandro Ovi

Un po' a sorpresa, Zuckerberg e Page hanno negato di essere a conoscenza dell'accesso della NSA ai loro dati. Per motivarlo, hanno affermato che quanto fatto con Verizon è troppo esteso.

In un messaggio on-line entrambi hanno dichiarato di non conoscere nulla dell'uso da parte della NSA del programma PRISM per raccogliere dati dai loro utenti.

Pure non dando alcuna spiegazione su quali dati avessero fornito in altro modo all'Agenzia per la Sicurezza Nazionale, hanno tuttavia mostrato preoccupazione per l'allargarsi delle tattiche usate allo scopo di ottenere i dati delle telefonate di Verizon.

La NSA sta dando una nuova interpretazione allargata al Patriot Act per avere più libertà nelle sue attività di sorveglianza. Zuckerberg e Page si dicono preoccupati che ciò possa estendersi anche ai dati dei loro utenti.

Dice Page: «Il livello di segretezza che circonda queste procedure, mina gravemente la libertà della quale noi godiamo». Analogamente Zuckerberg dichiara che, nel caso Facebook fosse soggetto allo stesso tipo di trattamento, lo combatterebbe con forza.

Tuttavia, se anche questa resistenza avesse luogo, né Google né Facebook sarebbero in grado di parlarne, dato che ordini come quello impartito a Verizon dalla Foreign Intelligence Surveillance Court sono accompagnati da clausole molto restrittive di segretezza.

Qualche giorno dopo la stesura di questa nota, il principale legale di Facebook, Ted Ullyot, a seguito dei negoziati con i responsabili della sicurezza nazionale statunitense, ha riconosciuto che il più grande social network del mondo ha ricevuto nella seconda metà del 2012 tra 9mila e 10mila richieste di dati da varie entità governative statunitensi, riguardanti casi relativi a bambini scomparsi o a minacce terroristiche. ■

Privacy o sicurezza?

Si prevedono forti ripercussioni in Europa per la violazione della privacy di cittadini europei.

David Talbot

Le stesse società americane che pare abbiano dato accesso a enormi quantità di dati alla NSA, hanno allo stesso tempo concordato di aderire alle regole europee sulla privacy, molto più severe di quelle americane. Di conseguenza le aziende Internet americane (incluse Google, Microsoft, Yahoo, Facebook e AOL) hanno sottoscritto i principi denominati Safe Harbour, promettendo il rispetto dei principi europei sulla protezione della privacy.

Ora, pare che abbiano fornito fiumi di dati alla NSA (National Security Agency), riguardanti cittadini stranieri, tra i quali moltissimi europei. Si può prevedere, quindi, che i regolatori e gli utenti europei daranno il via a reazioni molto severe. Secondo gli esperti di oltre oceano, è probabile che partano azioni legali molto dure con la richiesta di chi usura delle attività di aziende attive in Europa, come Facebook o Google (di qui probabilmente la reazione pubblica contro la NSA di Zuckerberg e Page).

La domanda ovvia è in che modo questo passaggio di dati abbia luogo. Una possibilità è che venga segretamente realizzato un canale per il trasferimento automatico dei dati. Una seconda possibilità è che le aziende forniscano dati su richiesta specifica della NSA. In entrambi i casi si tratta di qualcosa che non può avvenire a loro insaputa.

I principi del Safe Harbor richiedono la comunicazione alle persone oggetto della pratica, tutte le volte che un'informazione è condivisa, in modo che possano chiedere approfondimenti o fare ricorso. Si debbono anche rivelare i mezzi impiegati perché la diffusione pubblica possa venire limitata al massimo possibile.

Dal punto di vista legale, ci troviamo di fronte a un conflitto tra l'Europa, preoccupata della privacy, e gli Stati Uniti, preoccupati invece più della sicurezza. ■