BEHIND DATAGATE

Chiara Marchetti e Matteo Longeri
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Milano, Italia
chiara.marchetti1@studenti.unimi.it,
matteo.longeri@studenti.unimi.it

15 aprile 2015

Indice

Abstract

Nel 2013 le rivelazioni di Edward Snowden hanno dato il via al grande dibattito sulla liceità delle intercettazioni di massa perpetrate in segreto dai più grandi governi mondiali.
Il Datagate ha mostrato al mondo intero come chi detiene il potere riesca a sfruttare a proprio favore leggi e tecnologie per il controllo della popolazione, avanzando come giustificazione alla violazione della privacy dei singoli individui la lotta al terrorismo e a tutte le attività criminali che minano il bene della collettività.
Anche le compagnie del settore IT, coinvolte volontariamente o meno in operazioni di fornitura al governo di dati personali della propria clientela, hanno pagato le conseguenze dello scandalo. Per compensare al danno d'immagine subìto, le aziende hanno proposto al mondo la propria versione dei fatti, chiedendo ai governi coinvolti maggior trasparenza e impegnandosi sin da subito a mettere la privacy degli utenti al primo posto.
Per contrastare l'invadenza delle agenzie di sicurezza governative, gli aspetti tecnologici legati alla riservatezza e alla protezione dei dati scambiati dagli utenti hanno acquisito maggior importanza, spingendo aziende e sviluppatori indipendenti a proporre soluzioni sempre più avanzate in questa direzione.
A distanza di quasi 2 anni dallo scoppio dello scandalo Datagate sembra che il mondo abbia messo in secondo piano quanto accaduto, riservando il dibattito a pochi esperti e diretti interessati. Alla luce di ciò viene da chiedersi se la collettività abbia sacrificato volontariamente la propria privacy in favore di un bene superiore, oppure se si sia semplicemente rassegnata alla sorveglianza di massa sentendosi impotente e rendendo quindi vana la rinuncia alla libertà che Snowden ha fatto.

1 Introduzione

"Il vero valore di una persona non si misura dalle cose in cui sostiene di credere, ma da che cosa è disposto a fare per proteggerle."

(Edward Snowden)

Una delle caratteristiche che differenziano l'uomo dagli altri animali è la propensione al controllo, la tensione a primeggiare, il voler a tutti i costi avere il potere decisionale. Questo ha portato allo scontro diretto con il potere della natura, che l'uomo pensa di poter controllare, alle continue guerre e lotte per la ragione e alle diverse cause in cui la decisione di uno si ripercuote su molti.
Tutto questo porta con sé una parvenza di libertà, dando a chi la prova la sensazione di essere padrone della propria vita.
Invece, come sempre più spesso accade, la nostra libertà ha un qualcosa di finito, il che è una contraddizione all'obiettivo per cui era stato pensato Internet.
Oggigiorno, la vita online non è più separabile da quella offline, il virtuale è estensione del reale, ed entrambi gli aspetti si fondono l'uno con l'altro influenzandosi a vicenda.
"La tua libertà finisce dove inizia quella dell'altro" non è la regola su cui si fonda Internet, essendo che in rete tutti gli utenti hanno la possibilità di trovare e fare quel che vogliono, coperti da anonimato o meno. L'anonimato è il nascondere la propria identità così da potersi esprimere totalmente, senza aver paura di ripercussioni contro il proprio orientamento (sessuale, politico, religioso).

Nel 1890 due giuristi americani pubblicarono l'articolo di legge denominato *"The right to privacy"*, considerato uno dei saggi più influenti nella storia legale americana. Tale documento è considerato la prima pubblicazione, in tutti gli Stati Uniti, in cui è evocato il concetto di diritto alla privacy, inizialmente definito *"right to be left alone"* (ovvero il *"diritto di essere lasciato stare"*) [173] anche se molti studiosi hanno avuto da dire la propria opinione riguardo al "vero e pieno" significato della parola privacy, il che non li metteva né sullo stesso piano di pensiero né tantomeno d'accordo [159].
"Essere lasciato stare" sembra un ossimoro in quest'era digitale, eppure i cittadini di Internet chiedono a gran voce che *"la dimensione più privata della vita di una persona, che essa ha diritto di salvaguardare"* [57] venga loro riconosciuta anche online.
Come l'inventore del *World Wide Web* Tim Berners-Lee ha detto nel 2011 a Roma, durante l'evento *Happy Birthday Web*: *"dobbiamo iniziare a parlare di diritto all'accesso al web e di diritto a non essere spiati. Internet deve restare*

aperto e neutrale. Questo strumento di comunicazione dev'essere impiegato senza timori e con la consapevolezza che esso è utile per crescere, dal punto di vista sia culturale che economico. I governi devono usare il web perché aumenta l'efficienza e l'accessibilità ai dati, non come personale sistema di sorveglianza e dispositivo di repressione".

Nel corso della Storia, l'umanità ha assistito a svariate invasioni della privacy da parte dei propri governi: nel XVI secolo i coloni americani subivano continue perquisizioni delle proprie abitazioni da parte delle autorità britanniche che, munite di mandati *ad personam*, si sentivano legittimate ad eseguire il controllo non solo sulla persona in questione ma indiscriminatamente anche sull'intera popolazione; mentre nei primi decenni degli anni '90 l'antenata della FBI intercettava le comunicazioni in transito su cavi telefonici e telegrafici, sorvegliava il servizio postale e assoldava informatori per tenere sotto controllo chi contestava le politiche del governo in carica [70].
Nei primi anni '50 l'America viveva una paura folle per il comunismo, così che il senatore McCarthy con la sua "caccia alle streghe" riuscì ad accusare molti funzionari del governo e molte persone di varia estrazione sociale di essere spie sovietiche o simpatizzanti comunisti, rendendoli oggetto d'indagini e accuse riguardanti le loro opinioni e la loro adesione a vari movimenti. Verso la metà degli anni Settanta, la FBI aveva schedato come potenziali sovversivi mezzo milione di cittadini americani e spiava con regolarità alcune categorie di persone sulla sola base delle loro convinzioni politiche [70].
L'obiettivo della sorveglianza e dell'ostentazione del potere di controllare i cittadini era ed è quello di "stroncare il dissenso e imporre l'obbedienza" [70], idea ben descritta da Orwell nel suo romanzo distopico del 1948, *"1984"*, in cui governava un sistema tecnologico chiamato *"Grande Fratello"* in grado di monitorare le azioni e le parole di tutti i cittadini, e ancor meglio rappresentata dall'esperimento del *Panopticon* di Bentham del 1791, una struttura architettonica (un carcere) progettata con una torre centrale da cui i sorveglianti erano in grado di monitorare ogni stanza in qualunque momento, mentre gli occupanti non erano in grado di vederli non potendo quindi sapere se erano osservati o meno. La soluzione innovativa di Bentham fu quella di creare *"l'apparente onnipresenza dell'ispettore nella mente delle persone"* [70].
Quest'idea porta gli individui a comportarsi in maniera diversa, ad adeguarsi a determinati comportamenti o regole che non avrebbero scelto se fossero stati davvero "liberi"; il sapere di agire "secondo le regole" porta anche alla conseguente convinzione di non essere mai personalmente obiettivi del monitoraggio e della sorveglianza, ritenendola addirittura un bene, anche nelle sue forme più esagerate e al limite, se non oltre, della legalità.

Guardando ai giorni nostri, troviamo tantissimi casi di intrusione nella privacy da parte dei governi di tutto il mondo, che si giustificano con scuse come il monitorare le attività dei dissidenti nel Nord Africa, il mettere a tacere i dissensi in rete in Cina, il combattere (teoricamente) il terrorismo in America e nel mondo e molti altri motivi ancora. Tuttavia, nelle ultime decine di anni, non si è soltanto verificata sorveglianza a oltranza dei nostri metadati da parte della NSA e degli altri membri dei Five Eyes, ma ci sono stati anche episodi di portata mondiale in cui si è verificata una fuoriuscita di informazioni, stavolta dalle agenzie di sicurezza nazionale verso l'esterno. Questi sono i famosi *leaks*, ovvero "fughe di notizie", che in almeno due occasioni hanno "svelato" al mondo un qualcosa che sarebbe dovuto rimanere *top secret*.

Il primo leak è avvenuto nel 1971, ricordato da tutti come lo scandalo dei *Pentagon Papers*, in cui più di un centinaio di documenti top secret del Pentagono, in relazione ai rapporti e alle strategie che il governo statunitense aveva con il Vietnam nel corso del ventennio precedente, vennero venduti a una testata giornalistica americana da Daniel Ellsberg, uno dei *"Geniacci del Pentagono"* che in 10 anni fotocopiò 7000 pagine. Il compito commissionato dal Segretario della Difesa a lui e ad altri era quello di creare uno storico di tutti i documenti riguardanti la guerra in Vietnam da consegnare al presidente Johnson (lo stesso che dichiarò che *"the price of freedom is eternal vigilance"*); ma come la Storia ricorda il vero destinatario dei documenti fu il mondo intero. L'allora presidente Nixon mandò un'ingiunzione per proibire la pubblicazione dei documenti, che venne respinta a favore del IV Emendamento, e avviò un'indagine sullo stesso Ellsberg e sul Partito Democratico.
Nel 2006 Ellsberg ha ottenuto il *Right Livelihood Award* per la pace.

Una trentina d'anni dopo si verificò un'ulteriore fuga di notizie, di proporzioni maggiori rispetto alla precedente perché supportata da Internet, scatenata da *WikiLeaks*: *"a not-for-profit media organisation, that includes accredited journalists, software programmers, network engineers, mathematicians and others. Our goal is to bring important news and information to the public. We provide an innovative, secure and anonymous way for sources to leak information to our journalists (our electronic drop box). One of our most important activities is to publish original source material alongside our news stories so readers and historians alike can see evidence of the truth"* [174].
Il sito è stato fondato nel 2007 tra gli altri dall'attivista informatico Julian Assange, che ne è anche il caporedattore, con l'obiettivo di una maggior trasparenza da parte dei governi quale garanzia di giustizia, di etica e di una più forte democrazia.
Nel 2008 il sito web è stato chiuso per decisione di un tribunale californiano dietro le pressioni della banca svizzera, ritenutasi diffamata da alcuni docu-

menti pubblicati, ma il mese successivo lo stesso giudice ne ha autorizzato la riapertura citando il I Emendamento [176].
Dopo aver subìto l'estradizione da parte della Svezia, Assange è dal 2012 rifugiato nell'ambasciata dell'Ecuador a Londra.
Sia WikiLeaks che il suo cofondatore sono stati candidati per il Nobel per la Pace e sono stati appoggiati dal responsabile del primo leak, Daniel Ellsberg.
È stato detto che WikiLeaks si preoccupa di mantenere anonime le sue fonti; purtroppo questo non è riuscito nel caso di Bradley Manning (ora conosciuta come Chelsea Manning), un giovane militare statunitense analista d'intelligence che nel maggio 2010 è stato accusato da un hacker di aver fornito materiale top secret a WikiLeaks, nell'ordine delle decine di migliaia. Pochi giorni dopo è stato arrestato e imprigionato in Kuwait, per poi essere spostato in isolamento, prima Virginia e poi in Kansas, dove sconta dal 2013 la sua pena di 35 anni.
È interessante notare la brutalità con cui sta avvenendo la prigionia del giovane, che ha spinto tanti attivisti a schierarsi e a rilasciare dichiarazioni: in un articolo del 2010 Glenn Greenwald dice che *"Manning vive in condizioni che in alcuni stati definirebbero addirittura tortura"* [71], mentre David House, un ricercatore e informatico che fa visita al detenuto due volte al mese, l'ha definito addirittura in stato catatonico a causa dell'isolamento, delle condizioni di vita e della continua sorveglianza alla sua persona.
Manning è stato candidato per tre volte al Premio Nobel per la Pace.

Ai giorni nostri ci troviamo ad avere a che fare con le conseguenze di una nuova fuga di notizie, *"la più rilevante di tutte"* afferma Ellsberg [47], che ha coinvolto non solo l'Agenzia americana NSA e gli USA, ma tutto il mondo.
Il nostro progetto si prefigge di fare un po' di chiarezza sullo scandalo *Datagate* analizzando vari aspetti. Nel capitolo 2 verranno descritte le varie figure coinvolte, persone e istituzioni, oltre alle normative e ai programmi ideati dalla NSA. Col capitolo 3 analizzeremo le più importanti aziende dell'IT statunitense colpite dalle accuse di Snowden, cercando di comprenderne eventuali responsabilità nelle intercettazioni e la risposta delle stesse, in termini di dichiarazioni e tecnologie implementate. Il capitolo 4 vuole essere un approfondimento delle conseguenze che il Datagate ha avuto dal punto di vista sociale, con l'obiettivo di valutare le reazioni dei governi e la percezione delle popolazioni su quanto accaduto. In particolare analizzeremo i risultati di un questionario somministrato a 190 persone con diversa formazione professionale. Nel capitolo 5 verrà fatto un excursus sulle principali tecnologie utilizzabili dagli utenti per proteggere la propria privacy, descrivendone caratteristiche, problematiche e l'eventuale ruolo che hanno avuto nello scandalo. Infine capitolo 6 verranno trattate le conclusioni ed espresse le nostre opinioni su quanto sollevato da Edward Snowden.

2 Il background dello scandalo

L'intento di questo primo capitolo è quello di presentare a 360 gradi i principali personaggi che si sono messi in gioco, le organizzazioni coinvolte nello scandalo, i principali programmi di sorveglianza attuati dalla NSA e dal GCHQ, oltre a proporre un excursus sugli aspetti legali (alle volte forzati nella loro interpretazione) che hanno permesso alle agenzie di spionaggio di portare avanti indisturbati i propri progetti di sorveglianza di massa.

2.1 Edward Snowden

L'identità di Edward Joseph Snowden è stata pressoché sconosciuta al mondo fino al 2013, anno in cui la bomba Datagate è esplosa, facendolo conoscere a tutti come *whistleblower*, un termine non avente un preciso corrispettivo in italiano, come specificato in un interessante articolo dell'Accademia della Crusca [167] secondo la quale l'appellativo più simile, in accordo all'*art. 51 bis della legge "anticorruzione" 190/2012*, potrebbe essere *"denunciante"* o *"segnalante"*.
Ripercorrendo i suoi anni precedenti alla fatidica data si può inquadrare meglio il soggetto, capendo la motivazione che lo ha spinto a compiere una delle più grandi ed importanti divulgazioni di documenti top secret dell'ultimo secolo.

Dopo l'attacco alle Torri Gemelle il patriottismo nei giovani americani crebbe esponenzialmente. Nel 2004, il ventenne Snowden si arruolò nell'esercito statunitense con l'obiettivo di andare in Iraq per liberare la sua popolazione dal giogo dell'oppressione. Purtroppo dopo poco tempo si rese conto che *"la priorità dei suoi superiori era uccidere il maggior numero possibile di arabi, non liberare la gente"* [70]; così tornò a casa, e trovò lavoro in un'agenzia federale (struttura gestita ed utilizzata in segreto dalla NSA, la *National Security Agency*).
Nel corso degli anni, specializzandosi e spiccando per le sue doti, Snowden arrivò alla sede della CIA in Svizzera, dove rimase fino al 2010, lavorando sotto copertura con credenziali diplomatiche. Come lui stesso ha affermato, era considerato *"il tecnico di punta e il massimo esperto di cyber-sicurezza in Svizzera*", per questo veniva mandato in tutto il mondo per risolvere problemi vari.
"Nel 2008 iniziai a capire che il ruolo del mio governo nel mondo non era quello in cui ci avevano insegnato a credere" [70], Snowden iniziò così a riconsiderare il proprio modo di vedere le cose, notando come la trasparenza venisse gradualmente meno man mano che si saliva la scala gerarchica dell'Agenzia.
L'elezione del presidente Obama congelò per qualche tempo il progetto di

Snowden di appropriarsi e divulgare pubblicamente alcuni documenti segreti della CIA; ma presto egli capì che *"non solo Obama stava portando avanti la stessa linea di Bush, ma che in molti casi aveva addirittura peggiorato le cose"* [70]. Tornò così alla NSA, alle dipendenze della Dell Corporation, ricoprendo un ruolo che metteva a disposizione credenziali per l'accesso a segreti di sorveglianza molto più avanzate di quelle già in suo possesso.
Fu trasferito in Giappone, dove divenne *"il tipo di esperto di sicurezza telematica del quale la NSA è costantemente alla ricerca"* [70]. Nel 2011 la Dell Corporation lo inserì in un ufficio della CIA nel Maryland, dove Snowden assistette in prima persona all'accumulo di dati da parte della NSA in collaborazione con l'industria privata delle tecnologie, accumulo atto all'eliminazione di qualsiasi forma di riservatezza a livello mondiale.
Fu questo il fatto che fece crescere ai massimi livelli in Snowden la sensazione di dover fare qualcosa per far aprire gli occhi all'opinione pubblica.
Nel 2012 venne spostato alle Hawaii e assunto dalla Booz Allen Hamilton; questo gli permise di ottenere le credenziali mancanti per poter entrare in possesso degli ultimi documenti top secret che, da lì a poco, avrebbe reso pubblici a tutto il mondo.
Nel maggio 2013 Snowden chiese due settimane di ferie, durante le quali raggiunse un hotel ad Hong Kong, dove rimase fino al giugno dello stesso anno.
Ora Edward Snowden è da qualche parte in Russia, la quale gli ha rinnovato nel 2014 il permesso di soggiorno per ulteriori 3 anni.

2.2 Glenn Greenwald

La bomba Datagate, la rivelazione del programma di sorveglianza globale in atto da parte della NSA americana, è stata armata da Ed Snowden, ma è stata sganciata nella Rete da Greenwald.

Avvocato, giornalista e autore, che mette a disposizione del pubblico le sue conoscenze in materia di legge come collaboratore occasionale della testata The Guardian, senza aver paura delle ripercussioni del suo governo.
"Compito dei media è riportare i fatti, smentire le falsità che i potenti inevitabilmente disseminano per tutelarsi" è il suo motto, anche se nella maggior parte dei casi, sempre più spesso, il governo fa di tutto per distrarre il pubblico dalla notizia vera e propria, screditando in ogni modo il giornalista autore della stessa.
La rubrica gestita da Greenwald assieme ad altri giornalisti, che si occupava delle rivelazioni di Snowden sul programma di sorveglianza globale messo in atto dalla NSA (`http://www.theguardian.com/us-news/the-nsa-files`), ha portato il The Guardian, così come il Washington Post e il libro *"No Place to Hide"* scritto dallo stesso Greenwald, a vincere il premio Pulitzer

nel 2014 [49] [105].
A seguito dello scandalo Greenwald ha anche fondato, assieme a Laura Poitras e Jeremy Scahill, il sito *"The Intercept"* (`https://firstlook.org/theintercept/`), una pubblicazione online della First Look Media che aveva inizialmente l'obiettivo di pubblicare i documenti trafugati da Edward Snowden e che oggi si propone di aiutare i giornalisti di tutto il mondo a rivelare scandali che minano la trasparenza, quando le testate giornalistiche convenzionali non vogliono assumersi la responsabilità di pubblicazioni pericolose.

Greenwald attualmente risiede a Rio de Janeiro, città natale del suo compagno David Miranda, in quanto gli è stata negata la cittadinanza americana e perché lui stesso ha paura di ripercussioni da parte della NSA nel caso dovesse tornare negli USA.

2.3 NSA e GCHQ

La NSA e il GCHQ sono le agenzie governative di sicurezza rispettivamente di Stati Uniti e Regno Unito. Entrambe fanno parte dell'alleanza dei Five Eyes creata dopo la Seconda Guerra Mondiale, che comprende anche Canada, Australia e Nuova Zelanda, raggruppando così i 5 paesi anglofoni.

2.3.1 National Security Agency

La National Security Agency (NSA) è una divisione militare del Pentagono che, insieme alla CIA e alla FBI, si occupa della sicurezza nazionale. In particolare è l'ente incaricato della sicurezza in ambito interno-nazionale con la funzione di monitorare tutto il territorio statunitense per tutelarne l'integrità da attacchi di qualunque tipo, nonché proteggere i dati e i messaggi che giornalmente transitano attraverso gli uffici governativi.

Fondata negli Stati Uniti da un ordine esecutivo presidenziale nel 1947, insieme alla CIA, questa prima versione della NSA non era responsabile della direzione delle unità di comunicazione e di spionaggio elettronico, aveva poco potere e mancava di un meccanismo di coordinamento centralizzato.
Nel 1951 venne proposta un'indagine sulle attività dell'intelligence relativa alle comunicazioni considerate inefficaci; questo portò ad una rivalutazione degli oneri dell'Agenzia, cosicché nell'anno seguente il suo ruolo venne esteso oltre quello delle forze armate.
Nello stesso anno la NSA venne autorizzata dal presidente Truman con un ordine esecutivo classificato e venne istituita formalmente nel novembre del 1953. Il quartier generale si trova a Fort George G. Meade nel Maryland, a

16 km da Washington.
Oggi la NSA è considerata la maggiore agenzia del suo genere al mondo.

Mission, Vision, Values
La missione della NSA è molto chiara e ben definita nella Home Page del sito ufficiale:
"The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances."
"We will protect national security interests by adhering to the highest standards of behavior" introduce una serie di valori e di comportamenti che l'Agenzia adotta per garantire la massima protezione possibile, sottolineando la lealtà alla Nazione e alla Missione [115].
Dopo l'attentato dell'11 settembre 2001, il presidente Bush dette alla NSA maggior spazio d'azione; la sorveglianza non sarebbe più stata limitata ai soli obiettivi stranieri, ma da quel momento in poi l'Agenzia avrebbe iniziato il monitoraggio di tutti i dati di comunicazione che attraversano il territorio degli Stati Uniti, senza un mandato e non garantendo più la privacy.

Dal 2005 all'aprile 2014 la NSA è stata diretta dal generale a 4 stelle Keith B. Alexander che ne ha accresciuto a dismisura la mole e l'influenza; un ex funzionario amministrativo che aveva lavorato a stretto contatto con il generale ha riferito al The Guardian che la strategia di Alexander era quella di *"raccogliere tutto il raccoglibile, e tenerselo stretto il più a lungo possibile"* [70]. Dal momento della sua elezione, il generale si è dimostrato insofferente alle limitazioni imposte dall'intelligence militare americana per quanto riguarda la guerra in Iraq, così ha sfruttato la sua posizione per monitorare la popolazione irachena indiscriminatamente. Da qui, Alexander ha pensato di estendere agli americani lo stesso trattamento di sorveglianza a tappeto.
Il *Foreign Policy* ha definito la sua lotta per costruire la macchina spionistica definitiva *"ai confini della legalità"*, il suo pensiero riassunto in *"la legge non è affar nostro, pensiamo piuttosto a trovare il modo di fare quello che dobbiamo fare"* [70].
Ora il nuovo direttore dell'Agenzia di Sicurezza americana è l'ex vice di Alexander, Michael Rogers.

2.3.2 Government Communications HeadQuarters

Il GCHQ è l'agenzia governativa britannica che si occupa della sicurezza, nonché dello spionaggio e controspionaggio, nell'ambito delle comunicazioni,

attività tecnicamente nota come SIGINT (*SIGnal INTelligence*).

Le sue origini risalgono al 1919, quando alcuni settori dell'intelligence si fusero insieme formando la *Government Code and Cypher School* (GC&CS); fu nel 1942 che l'Agenzia prese ufficialmente il nome attuale.
Durante la Seconda Guerra Mondiale partecipò attivamente alla lotta contro il nazismo gestendo, tra gli altri, il Progetto Enigma.
Nel 2009, il GCHQ spiò i politici stranieri nel summit del G-20 di Londra, con controllo delle chiamate, delle email e monitorando i loro computer, in alcuni casi anche dopo che il summit era terminato [104].
Da giugno 2010, l'Agenzia ha accesso a *PRISM* (vedi paragrafo 2.5), il programma di sorveglianza di Internet attuato dalla collega NSA che, non solo per questo, ritiene il GCHQ il suo alleato più fedele all'interno del gruppo dei Five Eyes.

Sul sito ufficiale del GCHQ, nella sezione *"Who we are"*, si nota questa frase: *"as these adversaries work in secret, so too must GCHQ. We cannot reveal publicly everything that we do, but we remain fully accountable"* [76]. Come la collega NSA, spesso l'Agenzia britannica interpreta, raggira o abusa di alcuni fondamentali documenti o trattati, per raggiungere la massima sicurezza del proprio Paese.

2.4 Terzi coinvolti ed elementi aggiuntivi

Esistono trattati e leggi che regolamentano le metodologie di azione e i limiti di privacy e legalità entro i quali la sorveglianza esercitata dalle agenzie governative dovrebbe rientrare. Di seguito verranno descritti i principali decreti che, nel caso Datagate, sono stati toccati sul vivo.

- **I Emendamento (USA)**: nel 1791 agli articoli della Costituzione americana venne aggiunto il cosiddetto *"Bill of Rights"*, un documento composto da 10 emendamenti sui diritti fondamentali che sarebbero stati riconosciuti nel nuovo stato che stava nascendo. Il I Emendamento sancisce la libertà di parola e la libertà di stampa, così specificate nel testo originale: *«Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances»*.

- **II Emendamento (USA)**: *«A well regulated militia being necessary to the security of a free state, the right of the people to keep and bear arms shall not be infringed»* è il testo del II emendamento adottato

a partire dalla fine del 1791. Questo permetteva agli statunitensi di difendersi dai soprusi dei governi britannico e spagnolo che durante gli anni delle colonizzazioni agivano al di sopra della legge, legittimando le milizie cittadine al possesso di armi.
Una questione che da sempre interessa e accende gli animi è se questo diritto sia esteso o meno anche ai comuni cittadini. In molti stati americani è legale il possesso di un'arma, a patto che questa sia visibile se portata con sé e che non abbia il colpo in canna, mentre è vietato ai minori (escluso il caso di battuta di caccia con supervisione di un adulto).
Con una sentenza della Corte Suprema degli Stati Uniti del 2008 il diritto di possedere armi è stato riconosciuto come inviolabile, al pari di quello al voto e alla libertà d'espressione [181].

- **IV Emendamento (USA)**: già nel XVI secolo era sentita la lotta all'invasione della privacy da parte del governo, infatti i coloni americani erano vittime delle continue perquisizioni, personali e abitative, da parte delle autorità britanniche. Il IV emendamento nel Bill of Rights ha tradotto in legge questa volontà: *«the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized»*.
  Importante ricordare che, nel luglio 2013, il repubblicano Amash propose un emendamento con il quale voleva fermare la *"sorveglianza generalizzata degli americani, limitare la raccolta dei dati da parte del governo, difendendo così il IV Emendamento e la privacy di ogni cittadino statunitense"* [28].

- **Espionage Act**: questo decreto era stato promulgato durante la Prima Guerra Mondiale per permettere al presidente Wilson, e di conseguenza allo Stato, di perseguire tutti coloro che si opponevano alle politiche attuate, punendoli con sanzioni sproporzionate: 20 anni di reclusione o addirittura con la pena di morte.
  L'amministrazione Obama è una delle più accanite attuatrici di questa legge, tanto che il numero dei perseguiti è *"più alto di tutte le precedenti amministrazioni statunitensi messe insieme"* [70]. Un articolo significativo del The Guardian, descrive così lo scopo degli Espionage Acts: *"The purpose of an Espionage Act prosecution, however, is not to punish a person for spying for the enemy, selling secrets for personal gain, or trying to undermine our way of life. It is*

to ruin the whistleblower personally, professionally and financially. It is meant to send a message to anybody else considering speaking truth to power: challenge us and we will destroy you"[88].

- **USA Patriot Act**: acronimo di *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.* È una legge antiterrorismo federale promulgata poco dopo gli attentati dell'11 settembre e firmata dal presidente Bush nell'ottobre dello stesso anno. Inizialmente considerata una legge d'emergenza, nel 2011 il presidente Obama ha proposto, e ottenuto, una proroga di altri 4 anni. Il Patriot Act aumenta enormemente il potere delle agenzie di intelligence degli Stati Uniti per quanto riguarda tutto ciò che consente alle stesse di esercitare e garantire una sorveglianza sul territorio, volta a prevenire un ulteriore disastro.
  Nello specifico la *Section 215 "Access to records and other items under the foreign intelligence surveillance act"*, ridefinisce i requisiti necessari che il governo deve avere per poter consultare documentazione privata: non servono più *"ragionevoli elementi di colpevolezza"* ma *"basta considerare la documentazione materiale di rilievo"*.
  Tuttavia F. James Sensenbrenner Jr, il deputato repubblicano tra i principali autori del Patriot Act, nel luglio 2013 spiegò che la sua legge *"non ha mai avuto l'obiettivo di creare un programma che consenta al governo di domandare i dati telefonici di ogni americano"* [70] [5].

- **Intelligence Services Act (UK)** [170]: questa legge del 1994 (conosciuta anche come ISA) è divisa in 10 sezioni, ognuna delle quali, con l'autorità ministeriale, consente agli organi coinvolti in attività di spionaggio di condurre tutti i tipi di operazioni necessarie. Nello specifico la sezione 3 indica quel che è permesso al GCHQ: *«in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's government in the United Kingdom; or in the interests of the economic wellbeing of the UK; or in the support of the prevention or detection of serious crime»*.

- **Terrorism Act (UK)**: legge antiterrorismo attiva nel Regno Unito dal 2000 la cui finalità è interrogare il soggetto in stato di fermo per appurarne eventuali legami con il terrorismo. Solitamente il tempo di fermo massimo è di 9 ore, durante il quale vengono fatti gli accertamenti opportuni; passato questo primo step di controllo un ordine del tribunale può protrarre il fermo, autorizzare l'arresto o la liberazione del soggetto.

- **FISA**: acronimo di *Foreign Intelligence Surveillance Act*. È una legge federale del 1978 promulgata allo scopo di regolare la sorveglianza statunitense delle attività fisiche ed elettroniche operate dalle intelligence straniere sul suolo americano. Nel 2008 l'emendamento fu espanso con un'aggiunta che mirava ad istituzionalizzare il problema dell'illegalità della sorveglianza, anziché abolirlo.
  Questa legge si fonda sulla sostanziale differenza con cui vengono trattati i diversi cittadini del mondo: per gli *US person*, ovvero i cittadini americani o legalmente presenti in un dato momento sul suolo americano, è necessario per la NSA ottenere un'autorizzazione di sorveglianza dal FISC, mentre per tutte le altre persone, ovunque si trovino, non è richiesto nessun tipo di mandato, anzi questa sorveglianza viene addirittura definita "legittima".
  È sufficiente che all'altro capo di una comunicazione ci sia un cittadino straniero perché possa avvenire l'intercettazione, in questo caso la NSA parla di "acquisizione incidentale, come se spiare cittadini del proprio paese fosse uno spiacevole effetto collaterale" [70].
  Questa legge nella sezione 702 contiene le normative che regolamentano il funzionamento del programma *PRISM* (vedi paragrafo 2.5).

- **FISC**: acronimo di *Foreign Intelligence Surveillance Court*, anche chiamato *Tribunale FISA*. Questo tribunale è stato creato alla fine degli anni '70 per valutare, approvare o negare le richieste di controllo poste dalle varie agenzie di sicurezza americane (NSA e FBI in primo luogo). È composto da 11 giudici federali che raramente rendono pubbliche le loro sentenze, decise in riunioni rigorosamente svolte a porte chiuse e coperte dal massimo segreto di Stato.
  Questo tribunale è considerato dai più come un'istituzione di facciata in quanto, dopo le rivelazioni di Snowden, è venuto alla luce che dal 1978 al 2012 nessuna richiesta è stata respinta, una cinquantina sono state modificate (e poi accettate) mentre per le richieste di sorveglianza *ad personam* l'ammontare dei rifiuti è pari a zero [70].

C'è da sottolineare come, nel sistema legislativo americano, sia presente una normativa che è esattamente l'opposto di quanto viene permesso dalle leggi sopra descritte.
Il **FOIA** (*Freedom of Information Act*) è la legge sulla libertà di informazione emanata dal governo degli Stati Uniti nel 1966 che impone alle amministrazioni pubbliche una serie di regole che dovrebbero garantire la trasparenza nei confronti del cittadino, permettendo così a chiunque di sapere come opera il governo federale, comprendendo l'accesso, totale o parziale, a documenti classificati.

Questa legge tutela inoltre il diritto di cronaca e la libertà di stampa dei giornalisti.
L'ultimo aggiornamento (*E-FOIA*), apportato allo scopo di mantenere la legge al passo coi tempi, risale al 1996 e comprende un'estensione per normare l'accesso ai documenti elettronici.

2.5 Datagate

Con questo termine si indica la serie di rivelazioni, iniziate nel giugno 2013, dell'ex tecnico della NSA e della CIA Edward Snowden, relative al programma di controllo di massa di USA e Regno Unito.
Sono stati resi pubblici migliaia di documenti di cui la maggioranza sono siglati *FVEY* (Five Eyes), ovvero accessibili solo ai quattro partner più stretti della NSA nel campo della sorveglianza, *COMINT* cioè concernenti i servizi di intelligence specializzati in telecomunicazioni o *NOFORN* (No Foreigns), cioè documenti riservati a solo pochi americani e non accessibili a soggetti stranieri.
Tra i tanti programmi di sorveglianza in atto, i più discussi in quanto a coinvolgimento globale ed in base al numero di dati raccolti (si parla di peta byte) sono:

- **VERIZON**: programma che obbliga, tramite un'ordinanza segreta del Tribunale FISA, la principale compagnia telefonica americana Verizon a cedere alla NSA i tabulati telefonici di tutti i suoi abbonati, indipendentemente dal loro essere sospettati o meno di un illecito; il dettaglio d'interesse è infatti che almeno uno dei due interlocutori sia un cittadino americano.
  Obama ha dichiarato pubblicamente, con interviste singole o con annunci ufficiali, che la NSA non ascolta il contenuto delle chiamate dei cittadini *"they cannot and they have not, by law and by rule"*, anche se il senatore repubblicano Saxby Chambliss, uno dei membri della commissione per l'intelligence del Senato, ha affermato: *"everyone's been aware of it for years, every member of the Senate"*.
  Con questo programma all'Agenzia interessa reperire non i contenuti delle singole chiamate ma i metadati, tramite i quali è possibile comunque risalire a molte caratteristiche ed inclinazioni dei soggetti "ascoltati", grazie ad un incrocio con gli archivi di altre agenzie governative.
  Oltre alle telefonate ci sarebbero di mezzo anche le mail, le navigazioni online e le transazioni con carte di credito.

- **PRISM** [118]: è diventato il più famoso e il più tentacolare programma di sorveglianza elettronica di massima sicurezza creato e gestito dalla NSA.
  Sin dal 2007 l'Agenzia è in grado infatti di ottenere qualunque informazione direttamente dai server delle società telematiche, usate in tutto il mondo come principale strumento di comunicazione. Questo è il frutto di *"una moltitudine di negoziati segreti intercorsi tra la NSA e i colossi tecnologici, nel corso dei quali l'Agenzia ha esercitato pressioni per garantirsi un accesso senza restrizioni ai loro sistemi informatici [...] a cui alla fine le aziende hanno finito per cooperare, almeno in una certa misura"* [70] (vedi capitolo 3).
  Il programma sfrutta le caratteristiche di routing della rete, ovvero il fatto che i pacchetti IP non seguono necessariamente il percorso più breve ma quello più economico, così che la maggior parte di essi per forza di cose passa per gli Stati Uniti o per ISP statunitensi, consegnandosi direttamente a *PRISM*. Per cui i dati ottenibili comprendono: email, chat, chat vocali e videochat, video, foto, conversazioni VoIP, trasferimento di file, notifiche di accesso e dettagli relativi a siti di reti sociali [83].
  "PRISM apre la possibilità che le comunicazioni fatte interamente in suolo statunitense siano tracciate senza ordinanza giudiziaria" [28].
  Dal 2010 *PRISM* è accessibile anche al GCHQ Britannico, mentre dal 2012 il programma è condiviso con la FBI e la CIA, che possono richiedere qualsiasi informazione dall'archivio ai sensi dell'ordinanza FISA del 2008.

- **BOUNDLESS INFORMANT**: la NSA aveva concepito questo programma per quantificare e mappare con precisione le attività di sorveglianza quotidiane, effettuate paese per paese da computer e reti telefoniche; queste informazioni sono state catalogate in sofisticate statistiche (nel solo mese di febbraio 2013 una sola unità della NSA aveva raccolto dati su oltre 3 miliardi di telecomunicazioni nel solo territorio statunitense, mentre a marzo 2013 il programma aveva accumulato 97 miliardi di dati su scala globale).
  Da notare come il più alto funzionario per la Sicurezza Nazionale dell'amministrazione Obama, aveva spudoratamente mentito al Congresso nel marzo 2013: a domanda diretta sulla raccolta di qualsiasi tipo di dato sui cittadini americani la risposta era stata un sonoro *"no signore"* [118].

- **BLARNEY**: questo programma di sorveglianza raccoglie i metadati dai colli di bottiglia che vengono a formarsi lungo la dorsale (*backbone*)

di Internet; per dirla come la NSA *"leverage unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches and/or routers throughout the world"*.
Verso la fine del 2010, un aggiornamento del programma in collaborazione con la FBI, ha permesso di fornire all'Agenzia anche contenuti (come chat e filmati caricati dagli utenti stessi) prelevati direttamente da Facebook, dati che prima erano incompleti e inaffidabili. Come viene esplicitato anche da una slide della NSA che presenta questo programma, i social network vengono spiati perché sono *"una preziosissima fonte di informazione sugli obbiettivi"* [117] [58].

- **XKEYSCORE** [116]: è il software che, dal 2007, la NSA utilizza per raccogliere, organizzare e interrogare i dati raccolti con gli altri programmi di sorveglianza e che consente agli analisti di compiere ricerche, senza alcuna autorizzazione, all'interno dei vasti database contenenti email, chat online e lo storico delle navigazioni di milioni di individui [28].
  Secondo il settimanale tedesco Der Spiegel *XKEYSCORE* rende possibile una *sorveglianza digitale quasi totale*, infatti bastano un indirizzo IP o mail per catturare quasi tutte le attività che un utente svolge online (anche di cittadini statunitensi); è inclusa nel programma anche la registrazione dell'attività sui social media che permette, in tempo reale, di leggere i contenuti delle chat e dei messaggi privati su Facebook. Sono inoltre registrabili: il testo dei messaggi di posta elettronica, la cronologia dei siti visitati e le attività di navigazione [28] [70].
  Dai documenti resi noti da E. Snowden, è chiaro come un'importante funzionalità di *XKEYSCORE* permetta agli analisti di viaggiare a ritroso nel tempo per recuperare vecchie sessioni, in quanto il software memorizza per 3-5 giorni l'integralità dei contenuti [70].
  Per contro, la NSA ha replicato sostenendo che: *"l'attività dell'Agenzia riguarda solamente bersagli stranieri legittimi ed ha contribuito a catturare trecento terroristi; inoltre XKEYSCORE rientra nei programmi legalmente predisposti e che gli analisti dell'Agenzia non possono accedere liberamente ai dati raccolti"* [28].

- **MUSCULAR**: questo programma del GCHQ, in collaborazione con la NSA che in questo caso ha avuto un ruolo secondario, permette di copiare e analizzare interi flussi di dati durante l'attraversamento dei cavi in fibra ottica che collegano i data center di Yahoo e Google. In seguito questi vengono trasmessi ai database delle due agenzie governative, per essere utilizzati dagli altri programmi di sorveglianza,

come ad esempio *XKEYSCORE*.
Allacciandosi a snodi al di fuori degli Stati Uniti, la NSA può evitare le norme che impongono il reperimento dei dati esclusivamente attraverso un'autorizzazione FISA [28].
Grazie alle rivelazioni di Snowden, l'esistenza del programma è stata resa pubblica nell'ottobre 2013 [175].

3 Le aziende coinvolte

Le rivelazioni fatte da Edward Snowden nel 2013 non hanno coinvolto unicamente la National Security Agency e i cittadini, ma hanno avuto un forte impatto su molte realtà aziendali specialmente quelle operanti nel settore delle telecomunicazioni e in quello dell'*Information Technology*.
Molti colossi informatici hanno subìto grossi danni d'immagine ed economici a causa della loro partecipazione al programma di sorveglianza *PRISM*. L'accusa generale è stata quella di aver inserito delle *backdoor* nei propri sistemi, per permettere alla NSA di attingere informazioni sulla clientela senza la necessità di formalizzare prima una richiesta specifica.
Stando ai documenti pubblicati dalle principali testate giornalistiche statunitensi e mondiali le diverse società IT hanno iniziato a collaborare con l'intelligence in un periodo compreso tra il 2007 e il 2012. Anche quelle più restie ad una politica di questo tipo (come Twitter e Yahoo) si sono trovate costrette a dover cedere parte dei dati per evitare di pagare le dirette conseguenze del loro rifiuto (anche se come vedremo Twitter sta ancora combattendo la sua battaglia).
In risposta alle accuse, le aziende IT hanno inizialmente negato il proprio coinvolgimento, scontrandosi con le dichiarazioni rilasciate dal consigliere generale della NSA Rajesh De. Secondo lui le compagnie erano perfettamente a conoscenza del programma del governo e dovevano sottostare obbligatoriamente [2].
Nel 2014 Al Jazeera avrebbe rivelato degli scambi di mail tra Keith Alexander (ex vertice della NSA) e i CEO delle più grosse compagnie dell'IT statunitensi, avvenuti nel corso del 2012, volti all'organizzazione di incontri per discutere di diverse problematiche relative alla sicurezza [32].
In aggiunta alle azioni individuali compiute dalle compagnie in seguito all'esplosione dello scandalo (come dichiarazioni, smentite ed integrazioni più rigide di soluzioni a tutela della privacy), i principali colossi della Silicon Valley (Aol., Apple, Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, Twitter e Yahoo) hanno deciso di formare una coalizione dal nome *Reform Government Surveillance* [62].
Quest'alleanza è nata per stilare i punti di una riforma da sottoporre al Senato statunitense, volta ad inibire la sorveglianza di massa degli utenti.
I cinque principi fondanti su cui è stata edificata, facendo appello al I Emendamento americano relativo alla libertà di parola [14] [11], sono:

1. **Limitazione** dell'autorità del governo impedendo di raccogliere in massa le informazioni degli utenti;

2. **Controllo** delle attività di sorveglianza da parte dei giudici e loro responsabilizzazione;

3. **Trasparenza** sulle richieste del governo in modo tale da poterle rivelare ai propri clienti (in termini di numero e contenuti;

4. **Rispetto** del libero flusso di informazione senza inibire l'accesso ai dati archiviati al di fuori del territorio americano;

5. **Evitare** conflitti giurisdizionali tra i governi coinvolti in eventuali intercettazioni, favorendo la cooperazione per risolvere questo tipo di problematiche.

A febbraio del 2014 i colossi dell'IT statunitense sono riusciti ad ottenere dal Dipartimento di Giustizia americano la possibilità di pubblicare semestralmente dati non dettagliati relativi alle intercettazioni. Le aziende hanno commentato questo risultato ribadendo che è necessaria più trasparenza se si vuole ottenere la fiducia dei cittadini [4].
Di seguito verranno prese in analisi alcune delle aziende del settore IT coinvolte dallo scandalo Datagate, allo scopo di esaminarne responsabilità, dichiarazioni e azioni intraprese per cercare di salvaguardare gli utenti e per limitare i danni subiti.
A fine capitolo verrà anche analizzato il caso Verizon che, seppur esule dal progetto *PRISM*, ha visto il coinvolgimento della società statunitense di telecomunicazioni nelle intercettazioni delle chiamate dei suoi clienti e nella raccolta dei metadati relativi a questi.

3.1 Google

La Google Inc. è nata nel 1998 grazie al genio di Larry Page e Sergey Brin i quali, grazie all'algoritmo di ricerca per il web da loro stessi sviluppato, sono riusciti in breve tempo a trasformare il proprio motore di ricerca in un punto centrale per la maggior parte delle ricerche che milioni di utenti ogni giorno effettuano attraverso la rete.
Negli anni l'azienda ha saputo innovarsi continuamente introducendo prodotti e servizi di varia natura, alcuni dei quali sono sopravvissuti e si sono evoluti, mentre altri sono spariti senza troppe spiegazioni a riguardo.
Fondamentale per l'azienda è il ruolo rivestito dagli utenti, essendone la principale fonte d'energia. Per questa ragione la società si è trovata più volte al centro di questioni, sollevate prima dello scoppio dello scandalo Datagate, in relazione all'argomento privacy.

Per esempio, nel 2010 l'avvocato spagnolo Mario Costeja Gonzales è stato coinvolto in una vicenda per la quale egli stesso ha fatto appello all'Agenzia per la Protezione dei Dati spagnola, allo scopo di ottenere la rimozione dei riferimenti a vicende legali ormai risolte riguardanti la sua persona [114].
González è riuscito a ottenere quanto richiesto e la sua vicenda ha portato

successivamente ad una formulazione legale da parte della Comunità Europea di quello che viene definito il *Diritto all'Oblio*.
A seguito della *sentenza della Corte di Giustizia dell'Unione Europea (C-131/12, 13 maggio 2014)*, Google ha implementato una pagina web (`https://support.google.com/legal/contact/lr_eudpa?product=websearch`) con una form attraverso la quale è possibile richiedere la rimozione di determinati risultati dalla pagina di ricerca, fornendo ovviamente una valida motivazione e un documento per comprovare la propria identità.
Google sottolinea chiaramente che: *"a fronte di una tale richiesta, effettueremo un bilanciamento tra il diritto alla privacy della persona e il diritto di rendere accessibili le informazioni e l'interesse pubblico a trovarle"*, ad indicare che la richiesta portata avanti dall'utente deve essere analizzata e ritenuta accettabile secondo i criteri dell'azienda.

Google è stato colpito in pieno dalla bufera scatenatasi in seguito alle rivelazioni di Edward Snowden nell'estate 2013.
Già a febbraio 2010 l'azienda e l'Agenzia di Sicurezza americana avevano avviato una cooperazione in seguito agli attacchi informatici subiti da Google in Cina, che avevano portato alla violazione di alcuni account *Gmail* di attivisti per i diritti umani [190]. All'epoca questa cooperazione aveva suscitato preoccupazioni, tanto che l'*EPIC (Electronic Privacy Information Center)*, preoccupata per le possibili ripercussioni sulla privacy degli utenti, aveva richiesto mediante una lettera [123] di poter accedere ad alcune informazioni riguardanti la collaborazione.
Con lo scoppio dello scandalo Datagate nel 2013, Google si è vista immediatamente attaccata (al pari degli altri colossi dell'IT) a causa della precedente collaborazione col governo, ma questa volta per la presunta partecipazione al progetto *PRISM*. Come per gli altri concorrenti del settore, l'accusa è stata quella di aver fornito alla NSA delle *backdoor* di accesso ai propri sistemi per agevolare l'acquisizione dei dati relativi ai propri utenti.
Alle accuse "Big G" ha risposto di prendere con serietà ed attenzione l'argomento privacy, e di aver fornito informazioni al governo solo ed esclusivamente in risposta ad accuse fondate verso soggetti specifici e comunque sempre nella legalità.
Per quanto riguarda la presenza di *backdoor* nei propri sistemi l'azienda ne ha invece sempre negato l'esistenza [72].
Le intercettazioni attuate dalla NSA sembrerebbero non essere state effettuate unicamente mediante programmi di cooperazione come *PRISM*. Attraverso il progetto *MUSCULAR*, la NSA e il GCHQ inglese avrebbero sottratto informazioni sul traffico degli utenti di Google e Yahoo ponendosi a cavallo delle fibre ottiche che connettono i vari data center delle due compagnie. Attraverso questa tecnica sembrerebbero essere state sottratte milioni di informazioni ogni giorno, lasciando le due società all'oscuro di tutto [192].

In seguito alla diffusione della notizia, Google e Yahoo hanno risposto di non aver mai rilevato questa intrusione da parte delle due agenzie, definendo questa azione, nel caso dovesse essere confermata, completamente oltraggiosa sia nei propri confronti sia nel rispetto degli utenti finali [151]. Il CEO di Google Eric Schmidt ha commentato l'argomento durante un evento a Hong Kong [26], definendolo nuovamente un oltraggio e sottolineando come un'operazione di questo tipo non sia legale seppur compiuta da un'agenzia governativa.
Un'altra importante risorsa sfruttata dalla NSA per collezionare le informazioni personali degli utenti di Google sono i cookie, utilizzati per tracciarne i comportamenti [191]. Non risulterebbe però chiaro come la NSA sia entrata in possesso dei cookie, se attraverso richieste formali, portate avanti mediante il Tribunale FISA, o mediante il progetto *PRISM*.

Allo stesso modo degli altri colossi IT colpiti dalle rivelazioni sull'operato della NSA, la prima reazione di Google è stata quella di negare la sua partecipazione ai programmi di intercettazione dell'Agenzia, definendosi sorpresa dalle notizie pubblicate [143].
Big G, volendo mantenere un atteggiamento il più possibile trasparente per ottenere la fiducia dei propri utenti, ha subito chiesto al governo statunitense di poter pubblicare le informazioni relative alle richieste ricevute [144], così come fatto anche dalle altre aziende coinvolte nello scandalo.
Ad agosto 2013 Obama ha incontrato il vice presidente di Google Vint Cerf, assieme al CEO di Apple e al capo della AT&T, per discutere delle questioni sulla sorveglianza governativa e sulla privacy digitale degli utenti [55].
In seguito al permesso ottenuto dal Dipartimento di Giustizia americano, di poter pubblicare rapporti semestrali non dettagliati sulle richieste ricevute dalle agenzie governative, Google ha dichiarato che nel periodo compreso tra gennaio e giugno 2013 ha fornito i metadati di un numero di utenti inferiore a *999* e i contenuti delle comunicazioni di un numero compreso tra *9000* e *9999* clienti. Il direttore legale di Google Richard Salgado ha comunque precisato che è necessaria una trasparenza sempre maggiore per permettere alle persone di comprendere il funzionamento delle leggi sulla sorveglianza, potendo di conseguenza decidere se queste servano o meno [4].
Sul piano tecnologico, una delle risposte di Google allo scandalo è stata lo sviluppo di un plugin open source per la crittografia *End-to-End* relativa al servizio *Gmail*. La compagnia di Mountain View sta lavorando all'introduzione di un sistema crittografico basato su *OpenPGP* allo scopo di permettere agli utenti di cifrare le mail inviate attraverso il proprio servizio [50]. Secondo alcuni esperti i limiti della funzionalità sono legati a due elementi:

- Il fatto che le chiavi degli utenti vengono memorizzate unicamente in locale (vincolando l'utilizzo del servizio alla macchina) e devono essere importate su un ulteriore PC per fare uso del servizio;

- Nel caso i messaggi fossero crittati Google avrebbe un problema relativo all'inserimento di pubblicità mirata basata sul contenuto semantico delle e-mail. Per questo ci sono dubbi sul fatto che Big G ne incentiverà l'utilizzo di massa.

Va detto comunque che la crittografia di *Gmail* è ancora in fase di sviluppo per cui Google ha tutto il tempo di trovare soluzioni a queste problematiche evidenziate.

Nell'autunno 2014 Google ha ricevuto critiche sul versante privacy anche da Apple e Assange.
Il CEO della "Mela" Tim Cook ha attaccato implicitamente Big G e Facebook, nella lettera indirizzata ai propri clienti apparsa nella nuova sezione del sito di Apple dedicata alla privacy [13], sottolineando come queste aziende di servizi considerino i propri utenti non come clienti ma come prodotti.
All'accusa Google ha risposto attraverso Eric Shmidt sostenendo che: *"siamo da sempre i leader nella sicurezza e nella cifratura. I nostri sistemi sono molto più sicuri e criptati di quelli di chiunque altro, inclusa Apple. Apple sta colmando la distanza, è una buona cosa"* e affermando come probabilmente Tim Cook non sia informato sulle pratiche di Google relative alla gestione della privacy dei propri utenti [101].
Assange invece, in un'intervista rilasciata a Wired [38], ha affermato che *"Google è la versione privata della Nsa. Il business model di Google è la raccolta della vita privata delle persone: raccogliere queste informazioni, archiviarle, indicizzarle e costruire modelli di comporamento basati su questi dati. E tutto questo viene venduto a fini pubblicitari. Di fatto, è il medesimo modello che le agenzie di sorveglianza come la NSA e il GCHQ hanno messo in atto: raccogliere tutto, archiviare tutto, indicizzare tutto e sfruttare tutto"*.

All'indirizzo `https://www.google.it/intl/it/policies/` è possibile accedere alla sezione italiana di Privacy e Termini di Google. La pagina è organizzata in 5 sezioni principali:

- **Introduzione**, che fornisce collegamenti rapidi ai principali elementi chiave riguardanti il tema della privacy e l'accesso agli strumenti che Google offre per tutelarla;

- **Norme sulla privacy**, è la sezione in cui l'azienda spiega che tipi di dati raccoglie, le finalità per cui li utilizza, le possibilità che l'utente ha per gestire la propria privacy, ecc. All'inizio della pagina è presente il link per poter scaricare l'intera normativa in formato PDF, oltre a poter accedere all'archivio comprendente tutte le versioni precedenti delle normative;

- **Termini di servizio**, permette di comprendere i termini che l'utente necessariamente deve accettare per poter utilizzare prodotti e servizi di Google. Sono compresi riferimenti alla gestione del copyright dei prodotti dell'azienda, le garanzie che questa offre e le sue responsabilità in termini legali, ecc. Anche per questa sezione è possibile accedere alle versioni antecedenti;

- **Tecnologie e principi**, in questa sezione il gigante di Mountain View spiega come vengono utilizzate le proprie tecnologie (ad esempio cookie, geo-tagging, riconoscimento di pattern, Google Wallet, ecc.), oltre a fornire una descrizione del funzionamento della pubblicità e dei principi cardine relativi alla privacy;

- **Domande frequenti (FAQ)**, comprende le principali domande poste all'azienda relativamente alla privacy, con le conseguenti risposte.

Un'interessante analisi sull'evoluzione della normativa sulla privacy di Google dalla sua nascita al 2012 è quella svolta da David Crowe e Wasim A Al-Hamdani [35].
L'obiettivo dei due è stato capire come le norme si siano evolute nel tempo, determinando una demarcazione tra quello che loro definiscono il *"Vecchio Internet"* e *"l'Economia dell'Informazione di Domani"*. Secondo Crowe e Al-Hamdani, l'arrivo di questa nuova economia ha alterato il concetto di chi è il *"cliente"* e cosa (o chi) è il *"prodotto"*, cambiando inoltre il significato del termine *"free"*.
Un elenco degli strumenti che Google mette a disposizione dei propri clienti per tutelare privacy e sicurezza degli account è disponibile all'indirizzo (italiano) `http://www.google.it/goodtoknow/online-safety/security-tools/`. L'azienda ha organizzato la pagina in 3 sezioni:

- **Sicurezza e privacy**, spiega come gestire la verifica in due passaggi, come utilizzare la modalità in incognito di *Chrome*, ecc.;

- **Visualizza e controlla le tue informazioni**, indica come poter visualizzare e modificare le proprie informazioni, come accedere alle attività del proprio account, come gestire la cronologia, ecc.;

- **Gestisci le informazioni visibili a inserzionisti e siti web**, offre indicazioni per la gestione delle preferenze degli annunci e per disattivare *Google Analytics* (servizio che genera statistiche sui visitatori dei siti web).

I **Rapporti sulla Trasparenza** di Google si trovano invece in una pagina dedicata (`http://www.google.com/transparencyreport/`) descritta dalla compagnia come *"dati che chiariscono l'influenza di leggi e norme sugli utenti di Internet e sul flusso di informazioni online."* e sono stati organizzati in 7

aree tematiche, per agevolare la ricerca degli utenti.
Particolarmente interessante per lo scandalo del Datagate è la seconda delle 7 aree, quella denominata **Richiesta di informazioni sui nostri utenti**. Google ha realizzato una sezione esaustiva, comprendente tutti i dati che l'azienda è autorizzata a pubblicare (permettendone anche il download in formato *CSV*), i procedimenti legali che impongono la fornitura dei dati alle agenzie governative e una FAQ che cerca di rispondere alle principali questioni sollevate dagli utenti a seguito delle rivelazioni di Snowden.
In coda alla pagina sulla trasparenza, la società riporta le notizie più recenti connesse al tema della privacy nell'ottica delle intercettazioni governative, in più segnala i collegamenti ai rapporti sulla trasparenza delle principali compagnie IT coinvolte nello scandalo.

3.2 Yahoo

Fondata nel 1994 da D. Filo e J. Yang quasi per gioco, *Yahoo* è una società fornitrice di servizi Internet la cui funzione principale è quella di motore di ricerca, anche se presente pure in altri campi, come il settore della comunicazione e della diffusione dei media.
Nel 2008 Microsoft ha fatto delle offerte pubbliche di acquisto, ma la società ha ripetutamente rifiutato, portando il co-fondatore Yang alle dimissioni a causa delle critiche ricevute dagli azionisti per il mancato affare. Da quel momento le azioni di Yahoo hanno costantemente perso valore in borsa. Dal 2008 inoltre Yahoo non è più aggiornato e si limita a proporre i risultati di Bing, il motore di ricerca di Microsoft antagonista di Google [186].

Tra le molteplici risorse che ha la NSA per accedere ai metadati dei cittadini, ci sono anche le minacce; nel 2008 infatti l'Agenzia di Sicurezza americana ha minacciato Yahoo con multe da 250mila dollari al giorno nel caso in cui la società si fosse rifiutata di fornire i dati dei propri utenti, evitando così di entrare a far parte del programma *PRISM*.
Il motivo invocato dal governo per la richiesta dei dati fu che in gioco c'era la sicurezza nazionale, *"i terroristi internazionali (omissis) in particolare, usano Yahoo per comunicare su Internet per cui qualunque altro ritardo nella consegna dei dati da parte di Yahoo potrebbe causare grandi danni agli Stati Uniti"* aveva scritto l'allora direttore dell'intelligence nazionale Mike McConnell; tuttavia la compagnia riteneva che si trattasse di pretese incostituzionali [165] e sperava che, con la sua battaglia, avrebbe portato ad un dibattito sulla privacy e la trasparenza del governo.
Nonostante la tenace opposizione, nello stesso anno Yahoo venne obbligata dal Tribunale FISA [17] ad entrare a far parte di *PRISM*, cedendo quindi alle pressioni governative che includevano *"certain types of communications while those communications are in transmission"*, rendendo chiaro che il

sorvegliare persone al di fuori degli Stati Uniti avrebbe inevitabilmente causato *"incidental collection"* delle comunicazioni degli americani [165].
La sconfitta della società di Filo (che fu la seconda ad aderire al programma di sorveglianza della NSA dopo Microsoft) ebbe una sorta di effetto domino sulle altre che si convinsero a collaborare con la National Security Agency [41].

Nelle rivelazioni di Snowden, all'interno del dossier riguardante *PRISM* [118], si può facilmente notare che nei piani della NSA rientrava l'intercettazione e il reperimento di informazioni di utenti direttamente dalle comunicazioni tra i datacenter di Yahoo e Google. Questo è possibile grazie al programma *MUSCULAR* (vedi paragrafo 3.1), simile a *PRISM*, ma con la differenza che non necessita di mandato FISA per essere operativo [59].
Il direttore della NSA, il generale Keith Alexander, in un'intervista del Washington Post che direttamente chiedeva se l'Agenzia avesse effettivamente accesso ai datacenter di Yahoo rispose *"that's never happened. This is not the NSA breaking into any databases. It would be illegal for us to do that. And so I don't know what the report is, but I can tell you factually we do not have access to Google servers, Yahoo servers"* [60].

Yahoo è stato vittima anche di un altro programma, meno conosciuto rispetto a *PRISM*, attuato tra il 2008 e il 2012 dal GCHQ, il quale permetteva di catturare immagini degli utenti durante l'utilizzo del sito grazie alla loro stessa webcam. Questo programma, chiamato *Optic Nerve*, ogni 5 minuti scattava un'immagine che andava a salvarsi nei database dell'Agenzia inglese, indipendentemente dal fatto che il soggetto catturato fosse o meno di suo interesse. Le informazioni così ottenute venivano processate dai sistemi forniti dalla NSA, che ne teneva comunque una copia anche sui propri server, in modo tale da poterle usare poi come opzioni e tool aggiuntivi nelle ricerche effettuate col programma *XKEYSCORE* (vedi paragrafo 2.5). Un'arma a doppio taglio in quanto usando quest'ultimo programma era possibile incrociare i dati per identificare chiaramente posizione, nome e quanto di più utile sul soggetto fotografato [3].

Nel novembre 2013 Marissa Meyer, l'amministratrice delegata di Yahoo, ha annunciato che da gennaio 2014 la società avrebbe reso più sicuro il servizio e-mail introducendo il protocollo *HTTPS* con cifratura a *2048 bit*, aumentando così di molto la sicurezza degli utilizzatori di questo [147]. Inoltre, entro la primavera di quello stesso anno, l'azienda avrebbe integrato un sistema di crittografia per lo scambio di dati tra i propri data center, allo scopo di combattere *MUSCULAR*, e per tutte le connessioni degli utenti durante l'utilizzo dei diversi servizi offerti.
Nella sezione del proprio sito dedicata alla sicurezza Yahoo dichiara che *"si prende cura seriamente della tua sicurezza e adotta tutte le misure ragionevoli*

per proteggere i tuoi dati. Nessuna trasmissione di dati su Internet o tecnologia per la conservazione dei dati può essere sicura al 100%", ma come ben precisa in seguito *"può solamente adottare misure volte ad aiutarti a ridurre i rischi di accessi non autorizzati"*; anche l'utente quindi deve fare la sua parte [188].
Come le altre aziende anche Yahoo ha dedicato una sezione del proprio sito alla pubblicazione dei rapporti di trasparenza relativi alle richieste governative sui dati dei propri utenti, consultabili al link `https://transparency.yahoo.com`.

3.3 Facebook

È un *social network site* nato nel 2004 in un pensionato universitario di Harvard dalla mente geniale di Mark Zuckerberg e di un paio di suoi compagni. Inizialmente questo sito era stato pensato per i soli studenti universitari del campus, con l'obiettivo di fare conoscenza con altri ragazzi; in seguito fu aperto anche ad altre università, nel 2005 anche ai liceali e poi a tutti coloro che dichiaravano di avere più di 13 anni.
Secondo Alexa, un'azienda americana che si occupa di statistiche sul traffico Internet, nel 2013 Facebook, nome che prende spunto da alcuni dossier con foto e descrizione degli studenti che le università statunitensi forniscono alle matricole per poter conoscere nuovi amici, è diventato il sito più visitato al mondo, superando anche Google [177].
Gli utenti possono accedere al sito previa registrazione gratuita, il primo di alcuni step nel quale vengono richiesti esplicitamente dei dati personali.
È risaputo comunque che questi vengono utilizzati da Facebook per scopi commerciali, essendo i dati "venduti" a terzi per inserzioni pubblicitarie sulle pagine di profilo degli utenti, come infatti scrive l'Huffington Post *"Facebook in tutta la sua esistenza ha usato informazioni sugli utenti a loro insaputa, per guadagnarci, vendendo pubblicità mirata in base ai loro interessi"*. Zuckerberg lascia da pensare anche con un'altra affermazione fatta nel 2010, in cui dichiarava che *"la gente, ormai, non ha problemi, non solo a condividere più informazioni e di generi diversi, ma a farlo in modo più aperto e con un maggior numero di persone"*, quando lui stesso per evitare di avere vicini di casa troppo invadenti comprò le quattro ville vicino alla sua.
Nel 2012 Facebook contava più di 1 miliardo di utenti attivi, tant'è che due anni dopo, in occasione del decennale della nascita del sito, un membro del consiglio di amministrazione della società ha detto: *"la Chiesa Cattolica ci ha messo duemila anni per raggiungere un miliardo e 200 milioni di fedeli, noi abbiamo centrato lo stesso obiettivo in dieci anni"* [127].

Anche Facebook è stato coinvolto nello scandalo Datagate nell'ambito di *TURBINE*, *PRISM* e *BLARNEY* (vedi paragrafo 2.5). Nel Regno Unito, per il GCHQ il 2010 è stato un anno all'insegna dello sfruttamento delle debolezze del social network, così da poter accedere ad un numero sempre crescente di metadati; mentre negli USA la NSA metteva in atto il programma *TURBINE* (dopo averlo testato su una dozzina di "computer cavie") il quale, con una tecnica *One-Man-On-the-Side* chiamata *Quantumhand*, permetteva all'Agenzia di "travestirsi" da server di Facebook in modo tale da trasmettere ingannevoli pacchetti di dati al momento del login dell'utente, facendo credere al computer che a mandarglieli fosse effettivamente il social network. A questo punto la NSA era in grado di infiltrarsi nei computer, su scala massiccia, infettandoli con programmi di sorveglianza e reperendo i dati direttamente dal disco rigido (interessante ed esplicativo il video, creato dalla stessa NSA e pubblicato da The Intercept, che descrive come avviene questo tipo di attacco) [53].
Greenwald in un articolo su The Intercept afferma che dal 2010 al 2014 sarebbero stati infettati tra gli *85000* e i *100000* computer [53].
Dopo le rivelazioni di Snowden, Mark Zuckerberg ha chiamato direttamente il presidente Obama esprimendo la sua delusione e frustrazione: *"non ci siamo proprio [...] quando i nostri ingegneri lavorano instancabilmente per migliorare la sicurezza degli utenti, pensano di doverci proteggere contro i criminali, non contro il governo degli Stati Uniti. Il nostro governo dovrebbe essere il difensore di Internet, non una minaccia. Dovete essere molto più trasparenti su quel che fate, altrimenti il pubblico temerà il peggio"* [127]. Per alcuni giornalisti il plurale utilizzato nella conversazione era riconducibile a tutti i dipendenti dell'azienda, minata nella sua immagine, mentre per altri era stato utilizzato in merito ai colossi della Silicon Valley coinvolti nello scandalo, i cui interessi internazionali erano stati messi in pericolo.
Ovviamente l'ideatore di Facebook non poteva far altro se non pubblicare sulla sua pagina FB ogni dettaglio della chiamata [193] [66], facendo così in modo che moltissimi utenti leggessero il suo messaggio, prendendo in considerazione un aggiornamento della gestione della privacy sul social network.
Oltre all'ideatore di Facebook, anche Jay Nancarrow un portavoce dell'azienda ha detto la sua, in questo caso tramite una email diretta a The Intercept dicendo che la compagnia *"have no evidence of this alleged activity"* e aggiungendo che nel corso del 2013 la compagnia aveva implementato un sistema di cifratura *HTTPS* per gli utenti, rendendo la navigazione meno vulnerabile agli attachi malware [53].

Facebook è effettivamente il più grande database di persone mai costruito perché contiene più dati personali, sia intenzionalmente inseriti dal singolo che condivisi dai suoi amici, di ogni altra risorsa.
Nell'aprile 2014 il The Guardian annuncia che *"Facebook is to roll out a*

privacy checkup service to make sure users know when they are publicly sharing data", una delle manovre volte a migliorare le impostazioni di privacy, per la quale il social network mette in gioco due team differenti che si prenderanno cura dei dati personali degli utenti e delle impostazioni con le quali essi dovranno interagire, per gestire la condivisione dei file multimediali e dei post sulla propria bacheca. Il privacy product manager di Facebook ha dichiarato che *"some people have felt Facebook privacy has changed too much in the past, or we haven't communicated as well as we could have. Now we're thinking about privacy not just as a set of controls or settings, but as a set of experiences that help people feel comfortable"* [63]; per questo sono stati pensati sempre nel 2014 alcuni "aiuti fondamentali" per gli utenti meno esperti. Nel novembre dello stesso anno, viene aggiunta al sito la sezione *Privacy Basics* all'indirizzo `https://www.facebook.com/about/basics`, un tutorial interattivo che guida le persone attraverso il percorso per modificare le proprie impostazioni di privacy, rendendoli consapevoli di ciò a cui vanno incontro nel momento in cui accettano i termini d'utilizzo. Una portavoce del social network, consapevole che effettivamente nessun utente li legge, essendo troppo lunghi e complicati da capire, ha dichiarato che *"our hope is that it won't take long for people to read through this and really get it"*, dando voce alla speranza che l'interesse pratico, non solo teorico, per la propria privacy porti gli utenti a diventare "più responsabili" e la compagnia ad essere "meno complicata" nelle sue guide. Perciò la nuova normativa per la privacy (`https://www.facebook.com/about/privacy`) è più *user-friendly*, più corta e più colorata, risultando di stimolo per l'utente all'approfondimento di questo difficile e ostico tema.
Questa presa di coscienza è fondamentale in quanto *"Facebook becomes an increasingly mobile service, adding location and movement as new sets of data being collected by the company"* [148], per cui la mole di dati condivisi è in crescita esponenziale.
Sempre nel 2014 Mark Zuckerberg ha aperto le porte del suo social network anche agli utenti di *Tor* (vedi paragrafo 5.3), che possono accedere alla piattaforma attraverso un dominio ad hoc, il quale consente di non perdere le protezioni crittografiche [187].

Facebook ha da sempre dovuto affrontare accuse riguardanti la sua gestione dei dati e la privacy fornita agli utenti, ma la *class action* mossa dall'Europa nel febbraio 2015 vedrà il colosso di Menlo Park impegnato per parecchio tempo.
L'attivista austriaco Maximilian Schrems ha infatti indetto una causa, nell'agosto 2014, contro la partecipazione di Facebook al programma *PRISM* e ancor di più contro la politica sulla privacy adottata dal social network quando, nel 2012, aveva proposto un cambiamento alla gestione della privacy.
I promotori della class action sostengono che, chiedendo agli utenti di votare sulla pagina apposita `https://www.facebook.com/fbsitegovernance` per

approvare i cambiamenti proposti in materia di privacy, Facebook abbia volutamente introdotto il quorum del 30% degli iscritti, matematicamente impossibile da raggiungere (per le elezioni presidenziali dello stesso anno aveva votato meno della metà di quella percentuale).
Da quest'accusa la società potrebbe difendersi mettendo le mani avanti, sostenendo che i propri utenti non sono effettivamente coinvolti nella problematica privacy avendo risposto alla richiesta del 2012 solo l'1% degli iscritti al social network.
Nel sito di Schrems (`https://www.fbclaim.com/ui/page/updates`) in sei giorni si sono registrate *25 mila* persone, successivamente altre *50 mila* han dato la disponibilità per partecipare ad eventuali class action future.
Ora non rimane che aspettare l'udienza del 9 aprile 2015 a Vienna [48] che dovrà stabilire se le obiezioni presentate da Facebook sulla ricevibilità sono pertinenti e quindi rigettare la class action avanzata, oppure se avviare un procedimenti giudiziario e ordinare la restituzione di 12,5 milioni di euro (500 euro ad utente). Un verdetto di questo tipo avrebbe una duplice valenza: oltre a rappresentare un danno all'immagine e alle quotazioni di Facebook, rappresenterebbe anche un precedente che potrebbe coinvolgere altri colossi delle comunicazioni [113].

Un'altra accusa è stata mossa dalla commissione belga per la privacy dopo un'indagine a carico del *Centre of Interdisciplinary Law and ICT* dell'università di Leuven in Belgio [171] [92], i cui risultati mostrano come l'aggiornamento delle policy sulla privacy di gennaio 2015 non solo abbia allargato le policy che già Facebook attuava nel 2013 ma che, come allora, stia ancora violando le leggi europee sulla protezione degli utenti di servizi.
Il rapporto evidenzia anche come non ci sia la possibilità di fermare Facebook dal collezionare informazioni sulla localizzazione degli utenti tramite smartphone se non brutalmente da lato sistema operativo, scegliendo personalmente se condividere quest'informazione o meno. Questa collezione "tacita" attuata dalla società di Zuckerberg lede in pieno *l'articolo 5(3)* dell'*e-Privacy Directive* europea, il quale richiede il libero e informato consenso dell'utente prima di accedere e archiviare informazioni relative e provenienti da un device [64].
Anche Tim Cook, CEO di Apple, ha lanciato un'accusa alle aziende del web (vedi paragrafo 3.5) che *"trasformano i clienti in prodotti essendo gratuito il servizio di cui fanno uso, vendendone i dati personali a terzi per inserzioni pubblicitarie ritagliate addosso a ciascuno di essi"*; Mark Zuckerberg, sentendo la sua azienda direttamente presa in causa, ha risposto in un'intervista rilasciata a Time che queste sono *"accuse ridicole al modello di business basato sulla pubblicità"*, aggiungendo poi una controaccusa *"pensate forse che siccome i prodotti di Apple si pagano sono più in linea con l'interesse del cliente?"* [101].

Interessante notare come fino all'ultimo Mark Zuckerberg abbia continuato a negare la partecipazione della sua azienda al programma *PRISM*; definendolo nel giugno 2013 addirittura "outrageous", perfino dopo che il presidente Obama in persona aveva confermato l'esistenza e l'organizzazione del programma di sorveglianza, comprese le aziende coinvolte.
"We have never received a blanket request or court order from any government agency asking for information or metadata in bulk, and if we did, we would fight it aggressively" [143], un'altra dichiarazione pesante per il fondatore del social network più famoso al mondo, soprattutto alla luce delle rivelazioni che lo stesso Zuckerberg ha fatto un paio di mesi dopo; l'azienda infatti aveva ricevuto tra le *9000* e le *10000* richieste di dati personali da varie entità governative statunitensi nella seconda metà del 2012, riguardanti gli account di un numero tra *18000* e *19000* dei propri utenti. L'azienda ha aggiunto di aver diffuso l'informazione dopo il raggiungimento di un accordo sulla divulgazione con le autorità nazionali statunitensi della sicurezza [91], pubblicando i rapporti ufficiali sulle richieste di informazioni degli utenti ricevute al link `https://www.facebook.com/about/government_requests`.
Conferma schiacciante sono comunque stati i documenti divulgati da Snowden, nei quali si vede chiaramente come Facebook sia entrata a far parte del programma *PRISM* nel 2009.

3.3.1 WhatsApp

L'applicazione fu creata nel 2009 da Jan Koum, un ingegnere ebreo ucraino con una cultura libertaria, e consente di mandare sms, aprire una conversazione permanente e allegare ai messaggi dei contenuti multimediali a piacere. Ha il vantaggio tecnologico di essere compatibile con qualsiasi sistema operativo mobile e quindi con praticamente tutti gli smartphone in commercio, oltre che ad avere un costo irrisorio (99 centesimi all'anno).
Dopo aver raggiunto *450 milioni* di utenti in solo 5 anni, la microimpresa ha attirato l'attenzione di Mark Zuckerberg che nel febbraio 2014 l'ha acquistata per la somma da capogiro di *19 miliardi* di dollari, dichiarando che *"un servizio che raggiunge simili dimensioni ha un valore incredibile"* [127]. Le due aziende sono molto differenti, a partire dal concetto di base: se Facebook, come Twitter, è un social network che mira a rendere pubblici i propri status, messaggi e quant'altro, WhatsApp torna all'idea della conversazione uno-a-uno, rendendo il tutto più privato e personale.
L'ideatore di WhatsApp, dopo l'acquisizione della sua impresa da parte di Facebook, cercando di rassicurare i suoi utenti per quanto riguarda la gestione della loro privacy aveva dichiarato che *"se associarsi a Facebook avesse significato cambiare i nostri valori, non lo avremmo fatto"* [125]. Koum infatti fin da subito ha dedicato grande attenzione alla tutela della privacy dei propri utenti: dopo aver trasmesso il messaggio al destinatario,

WhatsApp lo cancella dalla memoria dei suoi "server". Questo rende molto più difficile il reperimento dei messaggi da parte della NSA, o di un qualsiasi malintenzionato [127].
Lo scandalo sulla privacy, che ha coinvolto le più grosse aziende americane nel 2014, ha portato WhatsApp ad applicare ai messaggi la crittografia *End-to-End*, in modo che siano decrittabili solo da chi li riceve; questa funzione non reversibile si attiva automaticamente solo per i messaggi scambiati tra utenti che usano il sistema operativo Android, ed è applicabile per le singole chat e non per le conversazioni di gruppo, mentre per i file multimediali e gli altri sistemi operativi è previsto un upgrade a breve.
Responsabile della gestione di questa importante operazione è la piattaforma *Open Whisper Systems*, suggerita anche da Snowden stesso, che conserva tutti i messaggi creati su WhatsApp, grazie alla quale le autorità governative non possono chiedere all'applicazione di messaggistica istantanea di fornire i dati dei propri utenti [187], in quanto essa non ne è effettivamente a conoscenza.
Tuttavia, grazie all'aggiornamento della policy sulla privacy fatto da Facebook nel gennaio 2015, la stessa azienda dichiara che *"riceviamo informazioni su di te dalle aziende di proprietà di Facebook o gestite da Facebook, in conformità con le relative condizioni e normative"* [128], frase che lascia un po' di amaro in bocca e fa intendere tutt'altro rispetto a quel che ha sempre sostenuto il creatore di WhatsApp.

3.4 Twitter

Creato nel 2006 da Jack Dorsey, Twitter è un servizio gratutito di social networking e microblogging in buona parte basato su software open source, estremamente popolare (anche come avversario di Facebook) e che fornisce agli utenti una pagina personale sulla quale pubblicare messaggi di testo di lunghezza massima di 140 caratteri.
Il nome "Twitter" deriva dal verbo inglese *"to tweet"* che significa *"cinguettare"* [185], lanciare perciò dei messaggi brevi, anche ravvicinati tra loro, dando la possibilità di essere aggiornati sempre sui cambi di stato; per questo il servizio ruota intorno al principio dei *follower*.

Come si può notare dalle slide riguardanti *PRISM* [118], Twitter non è mai entrata a far parte del programma di sorveglianza. Questo non vuol dire che la NSA non abbia mai puntato l'attenzione sulla società di microblogging, ma significa che Twitter è stata l'unico colosso *hi-tech* ad opporsi con tutte le sue forze al governo. Come infatti sottolinea The Verge nel suo articolo *"Twitter's refusal to join PRISM highlighted the fact that the company has a history of being uncooperative, and often antagonistic, when the government asks for user data"* [86]. Tuttavia, sotto richiesta esplicita del FISA (vedi

paragrafo 2.4), anche Twitter deve fornire i dati richiesti, molto diverso comunque dal creare un sistema apposito di immediato e diretto passaggio di metadati alle agenzie di sicurezza come invece hanno fatto altre aziende.
La società è da sempre paladina della massima trasparenza con i propri utenti, per questo, ritenendo le azioni del governo e dell'Agenzia di Sicurezza lesive del I Emendamento (vedi paragrafo 2.4), ha preso nel mirino il Dipartimento della Difesa americano, che con le sue regole impedisce di dare un'informazione più completa sui programmi di sorveglianza del governo, sporgendo denuncia alla Corte Federale della California e lasciando così di stucco tutti gli altri colossi che han ceduto alle richieste governative. La NSA, e gli agenti della FBI, hanno imposto infatti delle restrizioni su ciò che Twitter può rivelare a proposito delle richieste avanzate teoricamente nell'ambito di dati attinenti la sicurezza nazionale [133].
Come ha affermato Ben Lee, vicedirettore della società, *"crediamo di avere il diritto in base al I Emendamento di rispondere pienamente alle preoccupazioni dei nostri utenti, informandoli sullo scopo dei programmi di sorveglianza del governo. Dovremmo essere liberi di farlo in maniera piena invece che in maniera incompleta e inesatta"* [133].
Dal 2012 Twitter, per garantire la massima trasparenza, pubblica dei *Transparency Report* (`https://transparency.twitter.com`) per permettere ai propri utenti di monitorare le richieste del governo e la percentuale in cui esse interessano le varie nazioni del mondo, sottolineando come *"our ability to speak has been restricted by laws that prohibit and even criminalize a service provider like us from disclosing the exact number of national security letters ("NSLs") and Foreign Intelligence Surveillance Act ("FISA") court orders received - even if that number is zero"* [97].
Nel 2013 Twitter aveva inoltre annunciato che la protezione della sicurezza dei dati degli utenti era stata aumentata, grazie ad un team interno di ingegneri esperti in sicurezza che vi aveva lavorato per mesi aggiungendo un livello di protezione alla cifratura *HTTPS*, incoraggiando altri siti a fare altrettanto [89].
La "società dei cinguettii" sta quindi combattendo su ogni fronte per garantire la privacy dei propri dati, la trasparenza ai propri utenti e impedire che la NSA faccia breccia nei propri database, ma c'è che si chiede per quanto ancora potrà resistere [86].

3.5 Apple

Fondata nel 1976 da Steve Jobs, Steve Wozniak e Ronald Wayne a Cupertino, la Apple Computer Inc. è una delle principali società statunitensi operanti nel settore IT.
Il mercato principale di cui l'azienda si occupa è la produzione di dispositivi hardware sia in ambito desktop che mobile, al quale vanno ad aggiungersi lo

sviluppo di soluzioni software proprietari e la gestione di diverse tipologie di servizi.
Coprendo un mercato così ampio ed eterogeneo in termini di tipologie di prodotti, più volte il colosso di Cupertino si è trovato coinvolto in questioni riguardanti la privacy, sia per accuse ricevute che per dichiarazioni rilasciate in propria difesa.
In seguito alle rivelazioni di Snowden, Apple si è ritrovata tra le aziende che dovevano fornire le proprie giustificazioni.

Sulla base delle slide realizzate dalla NSA e pubblicate dal The Guardian emerge che Apple sia entrata a far parte della lunga lista di aziende che hanno collaborato al progetto *PRISM*, allo scopo di fornire all'Agenzia delle *backdoor* per un accesso rapido ai dati raccolti con i diversi servizi [72].
Questo ruolo di Apple come azienda collaboratrice dell'Agenzia di Sicurezza americana è stato avvalorato in seguito alle pubblicazioni di Jacob Appelbaum al trentesimo *Chaos Communication Congress* di Amburgo. Stando a quanto riportato dal ricercatore, la NSA avrebbe sviluppato nel 2008 il malware *Dropout Jeep* per *iPhone*, in grado di rispondere a richieste da remoto dell'Agenzia inviandole dati degli utenti di varia natura (contatti, messaggi, mail...) oltre a permettere l'attivazione di sensori come fotocamera, microfono ecc.
Secondo una tesi apparsa su Wired [108], l'unico modo per la NSA di infettare i dispositivi con un simile strumento è che Apple abbia collaborato con questa o che ci siano state infiltrazioni di agenti dell'Agenzia all'interno dell'azienda. In caso contrario la questione rappresenterebbe un grosso problema in termini di sicurezza relativa ai dispositivi *iOS*.
Apple ha risposto alle accuse dichiarando di esserne totalmente all'oscuro e di non aver mai collaborato con la NSA. L'azienda di Cupertino ha sottolineato come la privacy dei propri utenti sia una questione prioritaria nello sviluppo dei prodotti e come sia suo obiettivo risolvere le eventuali falle di sicurezza [142].
Un ulteriore elemento sottolineato da Apple in sua difesa è relativo all'impossibilità di un'installazione remota del tool, essendo necessario l'accesso fisico al dispositivo. Questo, e il fatto che le slide della NSA parlino esclusivamente di *iOS 5* come sistema operativo coinvolto, sembrerebbe garantire la tutela dei dati relativi alla maggior parte della clientela.
Nel 2014 con il rilascio di *iOS 8* per *iPhone* e *iPad* e di *Mac OSX 10.10* in ambito desktop, Apple ha sancito il suo impegno, integrando un sistema di cifratura dei dispositivi all'inserimento di un codice di sicurezza o dell'impronta digitale dell'utente mediante *Touch ID*. L'idea dell'azienda è stata quella di creare dei sistemi operativi per i suoi prodotti che cifrino completamente i contenuti quando vengono bloccati, decrittandoli quando l'utente necessita di utilizzarli dopo aver inserito la propria password/impronta.
In aggiunta a questa misura di protezione, Apple non sarebbe in possesso

di una chiave *"passepartout"* per accedere ai contenuti cifrati dei dispositivi privati dei propri utenti. Questo le permetterebbe di giustificarsi di fronte ad eventuali richieste da parte delle autorità, offrendo una tutela sia per gli utenti che per sé stessa.
Bisogna sottolineare però che questo protocollo di sicurezza agisce unicamente a livello dei dispositivi fisici. Per quanto riguarda i dati conservati su *iCloud Drive* (il servizio di cloud storage della Mela), questi risultano comunque accessibili dall'azienda e possono di conseguenza essere forniti al governo in presenza di valide motivazioni.
Se da un lato la soluzione descritta ha dimostrato una rimarcatura dell'impegno della società nella difesa dei propri clienti, dall'altro le sono state mosse accuse come quelle del direttore della FBI James Comey che in un'intervista ha dichiarato che questa politica rischia di *"trasformare gli USA in uno stato non più governato dalla legge"* [74].
In seguito all'adozione da parte di Apple di questa strategia per ottenere consenso da parte degli utenti e deresponsabilizzarsi dall'impossibilità di violare i dispositivi protetti da password o impronta, Comey ha cercato di far leva sull'argomento "attentati o crimini" allo scopo di portare le persone a boicottare queste misure di sicurezza.
Secondo il direttore della FBI, l'impossibilità di accedere ai dati conservati nei dispositivi Apple può trasformarsi in un grave problema qualora quei dispositivi appartengano a criminali, terroristi o alle vittime stesse di un reato, in quanto delle prove potrebbero risiedere negli stessi device e l'impossibilità di decrittarli potrebbe compromettere le indagini [166].
Sembrerebbe comunque che il sistema di sicurezza realizzato da Apple per tutelare i dati degli utenti che risiedono sui device personali non sia immune da falle che permetterebbero agli investigatori di accedere alle informazioni personali.
In un articolo apparso su Wired US [68] viene sottolineato come l'esperto forense Jonathan Zdziarski abbia trovato un modo per decrittare i dati personali cifrati con *iOS 8*: quando il dispositivo mobile viene connesso ad un computer viene richiesta l'autorizzazione per poterne effettuare il backup mediante *iTunes* o scaricare foto e video in *iPhoto*. Questa autorizzazione crea una chiave di sicurezza che permetterebbe al computer di accedere al dispositivo senza richiedere l'inserimento della password per le operazione di sincronizzazione.
Se gli agenti avessero accesso ad una macchina autorizzata potrebbero quindi estrarre la chiave avvalendosi di appositi software forensici avendo la possibilità così di decifrare i contenuti protetti sui dispositivi bypassando il sistema di sicurezza.
L'unico modo per potersi tutelare da questo tipo di exploit sarebbe quello di effettuare la cifratura del disco di ogni computer autorizzato a collegarsi ad un dato *iPhone* o *iPad*. In questo modo risulterebbe impossibile estrarre la chiave di sicurezza utilizzata per la sincronizzazione automatica.

In aggiunta alla risposta tecnologica di Apple sul piano della sicurezza, l'azienda di Cupertino ha rilasciato diverse dichiarazioni attraverso il suo CEO Tim Cook, allo scopo di sottolineare l'importanza della privacy degli utenti e gli sforzi che vengono compiuti per preservarla.
A settembre 2014 è apparsa sul sito ufficiale di Apple una sezione interamente dedicata alla privacy `https://www.apple.com/it/privacy/`, che evidenzia gli sforzi compiuti sul piano tecnologico e che cerca di mettere in risalto quelle che sono state le richieste di informazioni riservate sugli utenti da parte delle autorità governative, per l'anno 2013 e 2014, riportando anche quante di queste siano state davvero esaudite in presenza di valide motivazioni.
Analizzando la lettera di Tim Cook in prima pagina emerge lo sforzo di Apple per sottolineare come il suo modello di business, rispetto gli altri colossi del settore, non si basi sulla profilazione della clientela, quanto sulla qualità dei prodotti.
Seppur non siano presenti riferimenti espliciti, è chiara l'accusa volta ad aziende come Facebook e Google. Cook riporta infatti un'idea che è venuta a formarsi negli ultimi anni in relazione ai servizi gratuiti offerti dalle più grandi compagnie del web: *"quando un servizio online è gratuito, non sei più il cliente: sei il prodotto"*, che indica come le informazioni personali possano essere monetizzate dalle aziende IT. Va sottolineato come ciò non sia una massima generale applicabile ad ogni contesto, in quanto in determinati casi si ottiene un guadagno sui dati degli utenti anche per servizi a pagamento e viceversa servizi gratuiti potrebbero non considerare i propri utenti come prodotti.
Per quanto riguarda il rapporto con le autorità, Apple sottolinea che nel *93%* dei casi le richieste di accesso ai dispositivi vengono effettuate dal cliente (ad esempio in seguito ad un furto) e solo il restante *7%* sono effettivamente mirate ad accedere direttamente alle informazioni personali degli account.
Sempre in riferimento ai dati ufficiali pubblicati dall'azienda, viene riportato che meno dello *0,00385%* della clientela è stato soggetto di divulgazioni di informazioni personali in seguito a richieste da parte delle autorità.
Sono inoltre disponibili documenti rappresentativi dell'impegno intrapreso per difendere i diritti dei clienti, oltre a quelli sulla lotta nei confronti dei mandati extraterritoriali che obbligherebbero le aziende a fornire dati risiedenti in server esteri.
Il 13 febbraio 2015 si è tenuto presso l'Università di Stanford il *Vertice sulla Sicurezza Informatica e la Tutela dei Clienti* indetto dalla Casa Bianca.
Durante l'evento ha preso parola Tim Cook riguardo l'importanza della privacy e dell'impegno di Apple per tutelarla [150].
Il CEO della Mela ha fatto leva sulle gravi conseguenze che la rinuncia al diritto alla privacy comporterebbe, sottolineando come troppe persone nel mondo non sono libere di professare la propria religione, esprimere un'opinione o mantenere l'orientamento sessuale che preferiscono. Secondo

lui in contesti di questo tipo la tutela della privacy rappresenta la linea di demarcazione tra la vita e la morte, ed è per questo che risulta necessario proteggerla.

Nonostante le recenti dichiarazioni in seguito allo scandalo Datagate, negli anni Apple è stata più volte accusata di violazioni nei confronti della privacy dei propri clienti.
Nel 2011 ad esempio, i ricercatori Pete Warden e Alasdair Allan fecero emergere alla conferenza *Where 2.0* di San Francisco la questione relativa alla presenza di log della posizione degli *iPhone* all'interno dei dispositivi stessi. Con le prime release di *iOS 4* infatti, ad intervalli regolari il telefono memorizzava in un file la sua posizione in termini di latitudine, longitudine e relativo timestamp [9].
Risultava sufficiente esportare questo file dal device e aprirlo con un apposito programma per visualizzare l'evolvere della posizione dell'*iPhone* nel tempo all'interno di una mappa.
In risposta alla questione Apple si limitò a commentare che i dati raccolti risultavano essere anonimi, in ogni caso con un update successivo rimosse il file o comunque lo rese inaccessibile.
Un'altra questione sulla gestione dei dati personali si è aperta in seguito al rilascio di *Siri*, l'assistente vocale di Apple apparso per la prima volta nel 2011 con l'uscita dell'*iPhone 4S*. L'avvocato dell'ACLU Nicole Ozer ha cercato di fare chiarezza sulla lunghezza del periodo durante il quale le frasi pronunciate dagli utenti risiedono sui server di Apple, non essendo questo specificato nei termini della privacy relativi al servizio *Siri*.
Come riportato da Wired US [107] la società ha ufficialmente dichiarato che i clip audio delle richieste vengono conservati per un periodo di due anni. Sebbene questi risultino essere completamente anonimi ed utilizzati al solo scopo di migliorare l'algoritmo di *Siri*, Ozer ha evidenziato quanto sia importante che gli utenti prestino attenzione a ciò che pronunciano, dato che i clip potrebbero rivelare informazioni personali sensibili.
Con la nuova pagina dedicata alla privacy, Apple ha voluto evidenziare come *Siri* associ, mediante apprendimento, un ID casuale al dispositivo utilizzato dall'utente. Seppur scollegato dall'*Apple ID*, e di conseguenza anonimo, risulta sufficiente disattivare e riattivare *Siri* per eliminare dal server dell'azienda ogni clip precedente in quanto la nuova attivazione genera in automatico un nuovo ID casuale.
Un terzo servizio di Apple accusato di violare la privacy degli utenti, o quantomeno di non renderli sufficientemente consapevoli del proprio funzionamento, è *iCloud*, il servizio di cloud computing offerto dalla Mela che con il rilascio di *iOS 8* e *Mac OSX Yosemite* si è evoluto in *iCloud Drive*.
La funzionalità specifica che ha preoccupato maggiormente gli esperti è quella di salvataggio automatico che il servizio offre di default per tutti i principali software della suite di Apple. Quando viene creato un nuovo

documento di testo in *Pages*, una nota in *TextEdit*, ecc. il file viene memorizzato immediatamente sulla "nuvola" prima ancora che l'utente decida esplicitamente di salvarlo in locale o lasciarlo in quella posizione.
Se da un lato questo permette in caso di problemi di non perdere il lavoro svolto, dall'altro, come denuncia l'esperto di sicurezza Jeffrey Paul, i nuovi file creati ed il loro contenuto vengono esposti in rete senza un consenso specifico dell'utente [164], comportando conseguenze negative in termini di sicurezza.
Paul e il crittografo Matthew D. Green evidenziano come, in aggiunta a questo problema relativo ai nuovi file, aggiornando all'ultima versione del sistema operativo anche i vecchi file archiviati vengono spostati in una posizione sincronizzata con l'account *iCloud*.
Apple non dovrebbe rimuovere questa funzionalità, ma permettere agli utenti di decidere a priori cosa fare dei propri file, evitando una prima memorizzazione in cloud nell'attesa di una decisione.

Oltre alle dichiarazioni ufficiali in merito alla gestione dei dati degli utenti e alla pubblicazione dei vari report, nella sezione privacy del proprio sito Apple descrive le principali caratteristiche di sicurezza relative alle diverse applicazioni presenti di default sui propri dispositivi.
Tra queste risultano interessanti i principali servizi di comunicazione: *iMessage* e *FaceTime*.
Apple sottolinea come nel caso dei messaggi questi siano protetti mediante crittografia *End-to-End* tra i dispositivi in comunicazione, oltre ad essere cifrati in locale tramite la password o l'impronta dell'utente. L'azienda dichiara di non memorizzare ne messaggi ne conversazioni sui propri server, che non risulterebbero comunque decifrabili essendo completamente crittati.
La trasmissione dei messaggi attraverso *iMessage* fa uso del protocollo *TLS* per lo scambio e dell'*APNS (Apple Push Notification Service)* per le notifiche.
Per poter inviare un messaggio questo viene firmato con la chiave privata del mittente e viene quindi crittato con la chiave pubblica del ricevente, il quale decritterà il messaggio con la propria chiave privata e verificherà l'autenticità di questo mediante la chiave pubblica del mittente. Maggiori dettagli sul funzionamento del protocollo sono disponibili in [33].
Una ricerca condotta dalla Quarkslab Innovative Security nel 2013 [124] accusa Apple di mentire sulla sicurezza di *iMessage*, non essendo la sua crittografia efficiente come da lei dichiarata.
Secondo i ricercatori *@pod2g* e *gg*, essendo l'infrastruttura di gestione delle chiavi controllata da Apple, l'azienda stessa potrebbe cambiare le chiavi in qualsiasi momento falsificando i certificati e permettendo la lettura dei contenuti. Questo sistema potrebbe essere sfruttato dalla NSA per decrittare i messaggi scambiati dagli utenti.
In risposta alle accuse Apple ha dichiarato che così come è progettato ora il sistema sarebbe impossibile sfruttare l'exploit. Di conseguenza sarebbe

necessario reingegnerizzare l'intero protocollo, azione che l'azienda non sembra essere interessata ad attuare.
Per quanto riguarda le applicazioni *iOS* di terze parti, Apple ha cercato di definire negli anni delle linee guida che gli sviluppatori devono seguire nel rispetto e nella tutela dei dati personali degli utenti. In particolar modo queste direttive risultano essere molto restrittive nel caso di applicativi dedicati ai bambini di età inferiore ai *13 anni* [42].
È molto importante nello sviluppo di questo genere di software prestare attenzione all'inserimento di banner pubblicitari oltre a garantire il controllo parentale per l'utilizzo.

3.6 Microsoft

La Microsoft Corporation è stata fondata nel 1975 da Bill Gates e Paul Allen ad Albuquerque, Messico, ma alla fine degli anni '80 la sede è stata spostata a Redmond nello stato di Washington.
Fin dalla sua nascita, l'azienda ha operato nel campo dello sviluppo software e negli ultimi anni ha affiancato a questa attività l'implementazione di servizi e piattaforme per il settore consumer e per quello del business.

Nel 1999, quattordici anni prima delle rivelazioni di Edward Snowden, il The Guardian pubblicò un articolo [82] nel quale faceva riferimento all'inserimento di una *"chiave"* (chiamata *NSA Key*) della NSA in tutti i sistemi operativi di Microsoft da *Windows '95* in poi.
Con una chiara citazione del "Big Brother" di Orwell veniva spiegato come la NSA fosse in grado di accedere ad e-mail e documenti privati degli utenti attraverso una *backdoor*, scoperta da alcuni esperti di sicurezza.
Microsoft da parte sua negò la presenza di questa *backdoor*. Secondo gli esperti, questo elemento poteva essere stato inserito su richiesta dell'Agenzia senza che i manager dell'azienda fossero informati a riguardo.
Questo fatto venne in seguito confinato al mondo delle teorie del complotto, ma le rivelazioni del 2013, e nello specifico quelle sul programma *PRISM*, hanno mostrato al mondo come il colosso di Redmond abbia collaborato con l'Agenzia di Sicurezza americana fin dal 2007.
Nel periodo in cui esplose lo scandalo Datagate lo slogan di Microsoft era *"your privacy is our priority"* [72]. Nonostante questo però, l'azienda fu la prima a fornire alla NSA delle *backdoor* per permettere di accedere ai dati relativi ai propri utenti.
Tra i documenti forniti da Edward Snowden, diversi riguardavano nello specifico la collaborazione di Microsoft con la NSA, mettendo in risalto gli aspetti tecnologici coinvolti nel programma di spionaggio.
Il The Guardian ha pubblicato a luglio del 2013 quelli che sono i punti chiave estratti dalla documentazione [73]:

- Microsoft avrebbe collaborato con la NSA per violare la crittografia delle web chat di *Outlook.com*;
- La NSA avrebbe avuto accesso alle e-mail in una fase prioritaria rispetto alla cifratura di queste;
- Microsoft avrebbe collaborato con la FBI per dare alla NSA l'accesso al servizio *SkyDrive* (oggi *OneDrive*);
- Microsoft avrebbe collaborato col reparto DIU (Data Intercept Unit) della FBI per investigare i possibili pericoli della caratteristica di *Outlook.com* che permette agli utenti di creare degli alias per le e-mail;
- Dopo l'acquisizione di Skype da parte di Microsoft, sono triplicate le intercettazione di videochiamata da parte dell'Agenzia di Sicurezza;
- Il materiale raccolto attraverso il programma *PRISM* sarebbe stato condiviso con CIA e FBI in quello che la NSA ha definito uno "sport di squadra".

Alle accuse ricevute, Microsoft ha risposto al The Guardian argomentando il suo discorso in quattro punti:

- In primo luogo l'azienda dice di aver fornito dati sugli utenti al governo "solo" nel caso di processi legali;
- Il secondo elemento riguarda il fatto che la società analizza ogni richiesta di informazioni, rifiutando quelle non ritenute valide;
- Il terzo punto esposto è relativo alla fornitura di un numero ristretto e specifico di account alle autorità, in caso di valide motivazioni esplicitate;
- Infine Microsoft fa leva sul fatto di essere impossibilitata a volte nel fornire informazioni relative alle richieste delle autorità per questioni legali, e per questa ragione l'azienda starebbe combattendo per poter utilizzare maggior trasparenza nei confronti degli utenti.

Le pubblicazioni dei documenti che hanno portato allo scoppio dello scandalo Datagate hanno dimostrato chiaramente come il ruolo delle compagnie IT sia stato fondamentale per la NSA nelle operazioni di recupero delle informazioni sensibili degli utenti [103].
Microsoft in sua difesa ha dichiarato di essere rimasta turbata dalle rivelazioni, dicendo che se si fossero rivelate vere avrebbero determinato una *"significativa violazione della fiducia"* nei governi statunitense ed inglese. Inoltre la società ha rimarcato come siano necessarie riforme a tutela della privacy dei clienti.
Quanto emerso dai documenti della NSA e quanto affermato dall'azienda

risulta essere fortemente in contrasto. Nel primo caso Microsoft appare come complice mentre nel secondo sembra anch'essa una vittima schierata a fianco degli utenti.
Le accuse verso l'azienda di Redmond non sono arrivate unicamente attraverso gli articoli apparsi sulle principali testate americane, ma anche da ex dipendenti dell'azienda come Caspar Bowden, consigliere di Microsoft sulla privacy dal 2002 al 2011, che ha dichiarato di aver perso la sua fiducia verso l'azienda in seguito alle rivelazioni di Snowden, ritenendo gravi le accuse di coinvolgimento di quest'ultima nel programma *PRISM*. L'esperto ha affermato di utilizzare unicamente software open source e di non aver utilizzato il telefono cellulare negli ultimi anni allo scopo di evitare possibili intercettazioni.
Secondo Bowden è difficile, dopo quanto emerso, fidarsi di figure con posizioni influenti nella vita governativa. L'accesso alle informazioni di chiunque potrebbe comportare che le decisioni prese a livello istituzionale, siano dettate unicamente da interessi personali allo scopo di favorire le proprie carriere [10].

In seguito alle accuse ricevute, per tutelarsi Microsoft ha rilasciato diverse dichiarazioni allo scopo di chiarire la propria posizione.
L'azienda non ha negato di aver ricevuto richieste da parte del governo riguardanti informazioni personali relative ad alcuni clienti. Ciò che ha contestato, come del resto hanno fatto anche gli altri concorrenti del settore, è l'aver fornito alla NSA strumenti tecnologici atti ad accedere direttamente alle informazioni senza la necessità di una richiesta formale.
Più volte Microsoft ha ribadito la sua volontà di pubblicare informazioni dettagliate riguardanti le richieste ricevute allo scopo di rendere più trasparente la propria posizione, scrivendo anche al procuratore generale degli Stati Uniti, Eric Holder, richiedendo di poter rilasciare dati precisi alla clientela circa gli elementi emersi nello scandalo [145].
A seguito dell'autorizzazione del Dipartimento di Giustizia di poter pubblicare ogni sei mesi dei rapporti non dettagliati relativi alle richieste di intercettazione, è emerso che Microsoft nel periodo compreso tra gennaio e giugno 2013 ha ricevuto meno di *1000* ordinanze dal Tribunale FISA, relative ad un numero di account (o identificatori individuali) compreso tra *15000* e *15999*.
L'attuale CEO di Microsoft, Satya Nadella, parlando alla conferenza *Le Web* di Parigi nel dicembre 2014 ha sottolineato che gli utenti (sia business che consumer) utilizzano la tecnologia solo se si fidano di questa. Per questo motivo i governi, compreso quello statunitense, dovrebbero lavorare per poter ripristinare questa fiducia calata in seguito alle rivelazioni di Edward Snowden [43].
Una proposta su come il governo dovrebbe intervenire in quest'ottica, è arrivata a giugno 2014 dal consigliere generale di Microsoft e vice presidente

esecutivo Brad Smith, che suggerisce [158] di:

- **Riconoscere** che i mandati di perquisizione americani terminano ai confini dello stato;
- **Terminare** la raccolta di informazioni di massa;
- **Riformare** il Tribunale FISA, in un'ottica di maggior trasparenza;
- Impegnarsi a **non violare** più i data center e le reti delle compagnie.;
- Continuare ad **incrementare** la trasparenza, permettendo alle compagnie di fornire informazioni più dettagliate sulle richieste del governo.

Microsoft ha creato una sezione sul suo sito web ufficiale (`http://www.microsoft.com/en-us/twc/privacy/default.aspx`) con l'obiettivo di fornire chiarificazioni ai principali quesiti riguardanti la privacy, organizzandola in tre collegamenti alla principali macro aree di interesse:

- **Our Commitment**, permette di accedere alle informazioni generali sull'impegno di Microsoft nella tutela della privacy;
- **Cloud Privacy**, che permette di accedere a tutte le informazioni legate ai servizi di cloud computing offerti. Da segnalare che dal 17 febbraio 2015 Microsoft è la prima azienda ad aderire allo standard Iso/Iec 27018, che specifica le linee guida da seguire per tutelare le informazioni d'identificazione personale. Maggiori informazioni a riguardi si trovano in [8];
- **For Consumers**, che dovrebbe fornire informazioni utili ai consumatori, anche se al 30 marzo 2015 il link non risulta essere raggiungibile.

In aggiunta a queste 3 sezioni, l'azienda riporta collegamenti ad informazioni aggiuntive sulla gestione della privacy da parte sua e a report relativi al trattamento dei dati attraverso i vari servizi erogati.
Ulteriori informazioni dettagliate sulle politiche della società per quanto riguarda gli aspetti specifici che afferiscono alla dimensione della privacy, divisi per prodotti e servizi, sono accessibili all'indirizzo `http://www.microsoft.com/privacystatement/en-us/core/default.aspx`.
In queste pagine sono totalmente assenti riferimenti relativi alla raccolta di informazioni personali da parte del governo.
I rapporti ufficiali sull'argomento sono invece rilasciati da Microsoft all'indirizzo web `http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/` dove è possibile accedere ai report sia in formato *PDF* che *XLS*, attraverso una struttura organizzata per anni e stati.
In aggiunta l'azienda mette a disposizione degli utenti una FAQ dedicata ed

una sezione riservata unicamente alle richieste pervenute dalla US National Security attraverso ordinanze del Tribunale FISA.
Inoltre è possibile trovare dichiarazioni sull'impegno di Microsoft a favore di una maggior trasparenza sul suo blog ufficiale. In una nota di Brad Smith di agosto 2013 [157] viene riportato l'impegno della società, già citato in precedenza, di lottare a fianco degli altri colossi dell'IT per ottenere maggior trasparenza da parte delle istituzioni governative, con l'obiettivo di poter pubblicare tutti i dettagli relativi alle istanze del Tribunale FISA. Smith nel suo post riporta un riferimento esplicito alla costituzione americana e al diritto per l'azienda di poter comunicare liberamente e in maniera trasparente con i propri clienti.
Ad aprile 2014 Microsoft ha modificato i propri termini di servizio relativi alla possibilità della compagnia di investigare, con ogni mezzo a propria disposizione, nel caso di attività illecite interne.
Questa azione è la conseguenza di un fatto avvenuto a marzo dello stesso anno, quando l'architetto software dell'azienda Alex Kibkalo venne arrestato per aver passato ad un blogger informazioni riservate della società relative a *Windows 8*. La notizia fece scalpore perché l'azienda di Redmond rivelò di aver scoperto il leak analizzando le mail scambiate tra il tecnico e il blogger. Seppur in linea con i regolamenti aziendali, in seguito all'accaduto Brad Smith ha espresso la necessità di modificare i termini di utilizzo, limitando il potere di Microsoft in casi di questo tipo, lasciando alle autorità il controllo delle indagini.
Secondo Smith, sebbene questo possa essere un limite per la società, dopo le rivelazioni di Edward Snowden è emersa chiaramente la necessità di rispettare la privacy degli utenti e i loro dati personali [149].

3.6.1 Skype

Skype è una soluzione software di telecomunicazione rilasciata nel 2003 dalla Skype Technologies. Negli anni è diventata leader nel settore *VoIP (Voice over IP)* in particolar modo per il suo utilizzo come sistema di videochiamata. Nel 2009 l'applicazione è stata acquisita al *65%* dalla eBay Inc. priva di codice sorgente, per poi essere rivenduta dopo pochi mesi senza motivi apparenti.
Nel 2011 la Microsoft Corporation ha acquisito l'intera società alla cifra record di *8.5 miliardi* di dollari, entrando in possesso anche del codice sorgente al contrario del precedente acquirente. La Skype Technologies è diventata così a tutti gli effetti una divisione del colosso di Redmond [12].

Già prima dello scoppio dello scandalo Datagate sono state realizzate diverse pubblicazioni sulle possibili falle di sistemi *VoIP*, tra cui Skype, in grado di compromettere la privacy degli utenti.

In [96] un gruppo di esperti ha portato avanti una ricerca allo scopo di localizzare un individuo attraverso il suo indirizzo *IP* e determinarne il traffico di file sharing. L'esperimento condotto è stato organizzato in 3 fasi:

- *Recupero* dell'ID Skype del soggetto così da ottenere il suo indirizzo IP (anche nel caso in cui si trovi dietro NAT) attraverso una serie di chiamate ripetute;
- *Dimostrazione* di come sfruttare ciclicamente questo sistema per determinare gli spostamenti dell'utente;
- *Analisi* del traffico BitTorrent generato dal soggetto, effettuando un handshake del protocollo verso il suo IP, dopo averlo contattato.

Altre ricerche condotte sull'analisi del traffico Skype si trovano in [169], dove viene analizzato dai ricercatori il traffico a livello di pacchetti per determinare i flussi generati dall'architettura dell'applicativo, e in [40], dove si dimostra il funzionamento di un algoritmo che permette di identificare il traffico crittato di Skype, utilizzando un estimatore dell'entropia del payload.

Alcuni dei documenti rivelati al mondo riportano informazioni relative a *Project Chess*, il progetto della NSA il cui scopo è l'intercettazione delle comunicazioni effettuate attraverso Skype.
L'avvio di questo progetto risale al febbraio 2011, prima dell'acquisizione dell'azienda da parte di Microsoft.
Skype Technologies ha negato che l'acquisizione da parte di Microsoft sia stata dettata dalla necessità di agevolare l'accesso alle conversazioni da parte del governo, facendo leva sul fatto che *"niente sarebbe più contrario alla filosofia di Skype"* [146].
Nonostante le smentite della casa di Redmond, Snowden con le sue rivelazioni ha sollevato diversi elementi che farebbero propendere per un'acquisizione conclusa appositamente per aiutare il governo nelle sue intercettazioni.
In seguito all'accorpamento di Skype come divisione di Microsoft, la sua struttura è stata completamente snaturata, passando da un architettura distribuita e costellata di super-nodi ad una totalmente centralizzata e protetta da un sistema di crittografia proprietario [153].
La spiegazione dell'azienda di Redmond a questo cambio di architettura è stata motivata dalla crescita del numero di utenti e dall'impossibilità di continuare a gestirli in maniera distribuita. Questa operazione è stata però vista sotto una cattiva luce da parte degli attivisti per i diritti umani, che si affidavano all'applicativo come canale protetto dalle intercettazioni dei regimi oppressivi [87].
Un'ulteriore accusa è stata formulata sulla base del brevetto *"Legal Intercept"* depositato da Microsoft allo scopo di rendere possibile l'intercettazione del protocollo VoIP allo stesso modo della rete telefonica tradizionale.

Inoltre la NSA avrebbe sfruttato il proprio progetto *RAMPART-A* per poter intercettare le conversazioni VoIP effettuate attraverso Skype in aggiunta alle intercettazioni dei canali tradizionali quali telefonate, SMS, fax, e-mail, ecc. [51]. Attraverso *RAMPART-A*, l'Agenzia di Sicurezza americana ha potuto accedere ai nodi nevralgici delle connessioni in fibra ottica dei principali paesi mondiali, potendo filtrare i pacchetti di passaggio allo scopo di intercettare informazioni degli utenti.

In risposta a questi scandali sono iniziate ad emergere alcune soluzioni software il cui obiettivo è offrire un'alternativa a Skype per le comunicazioni degli utenti in rete.
Con un annuncio ufficiale su Twitter, a gennaio 2015 Kim Dotcom (creatore di Megaupload, Megavideo e più di recente di MEGA) ha presentato la prima release in beta pubblica di MegaChat. Si tratta di un servizio di chat con crittografia *End-to-End* il cui scopo è garantire la privacy degli utenti impegnati in conversazioni attraverso la rete Internet, promettendo di essere a prova di NSA [65]. L'ubicazione dei server del servizio è la Nuova Zelanda e il suo creatore ha promesso che nel tempo verranno affiancati alla chat dei servizi di videochiamata e trasferimento veloce di file facendo sempre grande attenzione alla privacy.

Informazioni ufficiali sulla gestione della privacy da parte di Skype sono consultabili all'indirizzo `http://goodies.skype.com/en/security/`. La pagina è organizzata in due sezioni principali:

- La prima offre indicazioni all'utente relativamente a ciò che questi può fare per tutelare la propria privacy durante l'utilizzo del servizio;
- La seconda elenca gli impegni dell'azienda nel garantire la privacy dei propri utenti, concentrandosi principalmente sulla crittografia applicata alle comunicazioni.

Non sono disponibili sul sito ufficiale del servizio rapporti di trasparenza relativi alle intercettazioni portate avanti dai governi. Essendo però diventata a tutti gli effetti una divisione di Microsoft, questi possono essere ritrovati direttamente sul sito del nuovo proprietario.

3.7 Verizon

Fino al 6 giugno 2013 la Verizon Communications era una delle maggiori compagnie telefoniche americane, un'azienda di spicco tra le tante per i servizi di banda larga e di telecomunicazioni; da quella data in poi Verizon è legata alla prima notizia pubblicata riguardante lo scandalo Datagate.
Greenwald, in un articolo sul The Guardian [69], rivela come un'ordinanza

segreta del Tribunale FISA di aprile 2013, resa disponibile per intero qui [163] obbligava Verizon a cedere alla NSA i tabulati telefonici di tutti i suoi clienti americani giornalmente e su base continuativa (per almeno 3 mesi), senza distinzioni tra telefonate in transito all'interno degli Stati Uniti o tra gli Stati Uniti e l'estero.
Il governo aveva solo bisogno di dimostrare che le informazioni richieste erano parte di *"authorized investigation"*, senza che gli utenti prescelti fossero necessariamente collegati al terrorismo o ad attività criminali.
Questa dichiarazione, supportata dai documenti diffusi da Snowden, collima in pieno con quanto Verizon stessa aveva dichiarato nel 2006 [110] [112], sottolineando sì che la NSA aveva tentato di siglare un accordo per essere rifornita di tutti i metadati dei propri clienti, ma precisando come la compagnia si fosse rifiutata completamente. Nel 2013 si venne a scoprire invece come le intercettazioni fossero attive già da sette anni.
Il punto cruciale è che è grazie ad una legge, nello specifico la sezione 215 del Patriot Act (vedi paragrafo 2.4), che la NSA può collezionare milioni di dati al giorno riguardanti le telefonate degli americani. Quest'idea avuta dal presidente Bush, la cui amministrazione era risaputo avesse interessi per i metadati dei propri cittadini, è stata migliorata e portata avanti ai massimi livelli dall'attuale amministrazione Obama.
Un decisivo cambio di direzione, per Obama, che nel periodo in cui era senatore decantava come avrebbe dato la caccia ai terroristi *"without undermining our commitment to the rule of law, or our basic rights and liberties"* [121], sottolineando come nessuno avrebbe dovuto essere al di sopra della legge.
Il giorno successivo alla pubblicazione dell'articolo di Greenwald [69], un portavoce della Casa Bianca ha preso subito parola per difendere l'operato della NSA dichiarando come l'operato dell'Agenzia di Sicurezza sia *"uno strumento irrinunciabile per proteggere la nazione dalle minacce terroristiche"* [137]. Sempre negli immediati giorni seguenti alle rivelazioni sulle intercettazioni, la deputata democratica presidente del Comitato per l'Intelligence del Senato americano Dianne Feinstein, rincarava la tesi del *"lo facciamo per difendervi"* sottolineando come le pratiche di accumulo di metadati provenienti da Verizon *"is called protecting America, people want the homeland kept safe"* [138], e come questa possibilità consentiva alla FBI, nel momento stesso in cui fosse nato un sospetto di terrorismo verso qualcuno, di fare delle verifiche e così prevenire il pericolo. La presidente, nota per la sua propensione spassionata verso le azioni della NSA, ha tirato in campo le solite argomentazioni post 11 settembre, sulla lotta al terrorismo e sul fatto che i terroristi sono sempre alle porte pronti ad attaccare, per le quali i cittadini sono spaventati e succubi.
Significativa è la dichiarazione del senatore democratico Jeff Merkley fatta a dicembre 2013, 6 mesi dopo lo scoppio dello scandalo; lui stesso infatti ammette come il programma di sorveglianza e intercettazione sia addirittura

fuori dalla portata persino del solo pensiero dei cittadini, con queste parole: *"citizens generally assume our government is not spying on them. If they had any inkling of how this system really works, the details of which I cannot discuss, they would be profoundly appalled"* [138].
Molti esponenti importanti, tra cui l'ACLU (american Civili Liberties Union) e il senatore democratico Mark Udall, dichiararono che il governo americano stava addirittura andando oltre, sfruttando fino all'abuso i propri poteri e libertà.
A tutta questa vicenda Verizon ha solo una risposta, ovvero il giustificare le proprie azioni ponendo l'attenzione dei media sulla segretissima ordinanza FISA [163] che gli era stata imposta, tra l'altro garantendo il rispetto della privacy degli utenti.
Sempre il 6 giugno 2013, il vicepresidente esecutivo di Verizon, Randy Milch, inviò a tutti i dipendenti dell'azienda questa nota [110], mentre gli investitori alzarono la voce volendo a tutti i costi che l'azienda dicesse quanti e quali dati dei clienti sarebbero stati destinati alla NSA [56].
Dal canto suo Verizon Communications ha dedicato una sezione del suo sito (`https://www.verizon.com/about/privacy/`) alla *Privacy Policy Summary*, con vari approfondimenti sul tipo di informazioni raccolte, sulle terze parti con cui queste vengono condivise e sui metodi utilizzati, ma sono descrizioni talmente lunghe che sorge spontaneo chiedersi se veramente i clienti dedichino tempo a leggerle.
I rapporti ufficiali sulle richieste di intercettazione ricevute dal governo sono invece disponibili all'indirizzo `http://transparency.verizon.com`

Nel 2014 proprio dall'amministrazione Obama era arrivata una proposta di legge *"volta a porre fine allo spionaggio indiscriminato delle telefonate degli americani e che quindi avrebbe limitato la capacità di raccolta di dati da parte della NSA. Le società telefoniche, tra le quali Verizon non sarebbero più state tenute a consegnare i dati delle telefonate all'Agenzia per la Sicurezza Nazionale a meno di un ordine speciale da parte FISC. Sarebbe inoltre stata incrementata la privacy e sarebbe stato maggiormente circoscritto il concetto di «target di sorveglianza»"* [95]. Peccato che la proposta sia stata respinta per soli 2 voti.
Tuttavia a marzo 2015 la NSA ha ottenuto una proroga fino al 1 giugno dello stesso anno per l'accumulo di massa dei metadati relativi al traffico telefonico della rete mobile [135].

Dal 2013 ad oggi Verizon, con altre compagnie telefoniche mondiali, è stata coinvolta nell'ulteriore scandalo delle SIM card hackerate in modo tale da ottenere le chiavi di decrittazione usate per proteggere le proprie attività mobile, dalle chiamate ai messaggi alla navigazione. L'articolo di Gallagher del 2014, pubblicato su The Intercept descrive minuziosamente questa *OPERATION AURORAGOLD* [52] che continua tutt'oggi.

3.8 Le aziende in sintesi

Analizzate nello specifico le principali aziende interessate dallo scandalo Datagate, verrà riportata di seguito una tabella riassuntiva (Tabella 1) che vuole mettere in evidenza i punti salienti rappresentativi del loro coinvolgimento.

Azienda	**Operazioni NSA**	**Accuse ricevute**	**Azioni difensive**	**Tecnologie implementate**
Google	• Cooperazione post attacchi a Gmail in Cina • PRISM • MUSCULAR	• Tim Cook: cliente = prodotto • Assange: speculazione sui dati	• Coalizione R.G.S. • Rapporti sulla trasparenza • Negazione PRISM	• Crittografia End-to-End per Gmail
Yahoo	• Multe se mancata cooperazione • PRISM • MUSCULAR • Optic Nerve		• Coalizione R.G.S.	• Crittografia a 2048 bit • Protocollo HTTPS per e-mail
Facebook	• PRISM • BLARNEY • TURBINE	• Tim Cook: cliente = prodotto • Class action europea: PRISM • Commissione belga: privacy	• Coalizione R.G.S. • Negazione PRISM • Chiamata ad Obama per TURBINE • Nuove regole privacy	• Protocollo HTTPS • Dominio .onion per utenti Tor
Whatsapp		• Acquisizione Facebook: cambio policy privacy		• Crittografia End-to-End versione Android
Twitter	• Richieste collaborazione mai accettate		• Coalizione R.G.S. • Rapporti sulla trasparenza • Fornitura dati solo su richiesta FISA	• Protocollo HTTPS

Apple	• Malware Dropout Jeep • PRISM	• Salvataggio automatico iCloud Drive • Quarkslab Innovative Security: crittografia iMessage • FBI: crittografia locale iOS	• Coalizione R.G.S. • Rapporti sulla trasparenza • Negazione Dropout Jeep • Negazione PRISM • Discorso Tim Cook al vertice della Casa Bianca	• Linee guida gestione privacy app • Crittografia End-to-End iMessage • Crittografia locale iOS
Microsoft	• Backdoor da Windows 95 • PRISM	• Bowden: complicità NSA?	• Coalizione R.G.S. • Rapporti sulla trasparenza • Fornitura dati solo su richiesta FISA • Modifica ToS interno dopo caso Kibkalo	
Skype	• Project Chess • RAMPART-A	• Possibili falle sicurezza (pre PRISM) • Acquisizione Microsoft: architettura da distribuita a centralizzata • Brevetto "Legal Intercept" di Microsoft	• Negazione Project Chess	
Verizon	• Ordinanza FISA cessione giornaliera tabulati telefonici • OPERATION AURORA-GOLD • Proroga intercettazioni fino a giugno 2015		• Rapporti sulla trasparenza • Negazione intercettazioni • Jeff Merkley: ammissione intercettazioni	

Tabella (1): Tabella riassuntiva delle principali aziende coinvolte dallo scandalo Datagate

4 "Effetto Snowden"

Lo scopo di questo capitolo è cercare di analizzare e comprendere quelle che sono state le principali reazioni che l'Europa ha avuto a seguito delle rivelazioni di Edward Snowden nel giugno del 2013.
La scelta del titolo "Effetto Snowden" è stata dettata dall'utilizzo di questa terminologia da parte di vari giornalisti delle principali testate mondiali per fare riferimento alla serie di conseguenze avvenute con reazione a catena, a seguito dell'esplosione dello scandalo.
Nella prima parte del capitolo verrà analizzato come i principali stati europei hanno reagito al Datagate, evidenziando il punto di vista dei rappresentanti dei singoli governi e delle opinioni pubbliche nazionali.
Nella seconda parte del capitolo invece, verranno analizzate le risposte date da un gruppo di 190 intervistati italiani ad alcune domande poste in relazione allo scandalo, cercando di contestualizzare le loro affermazioni sulla base di alcuni elementi personali, restando comunque nell'anonimato.

4.1 La reazione dell'Europa

Le rivelazioni di Snowden hanno stravolto il mondo per com'era conosciuto coinvolgendo e sconvolgendo, oltre alle aziende (vedi capitolo 3), intere nazioni prese nel mirino della sorveglianza americana e britannica.
È importante precisare come la NSA abbia instaurato 3 diversi tipi di rapporti con l'estero:

- Five Eyes, il gruppo ristretto di paesi (Regno Unito, Canada, Australia, Nuova Zelanda) che gli Stati Uniti spiano di rado, solo dopo richiesta o esplicitazione dei partner stessi, e grazie ai quali sorvegliano paesi terzi;
- Stati con cui la NSA collabora per specifici progetti di sorveglianza, oltre a controllarli in modo continuativo;
- Paesi che gli USA sorvegliano regolarmente e con i quali non cooperano quasi mai.

Analizzeremo ora alcuni governi europei compresi nel secondo gruppo (esclusa la Russia che ricade nel terzo), rappresentativi in termini di reazioni e richieste poste al governo statunitense a seguito dello scandalo.
Su Wikipedia US è stata realizzata un'apposita pagina dal titolo *Reactions to global surveillance disclosures* [183], allo scopo di raccogliere le reazioni mondiali degli stati coinvolti dai programmi di sorveglianza del governo americano.

4.1.1 Francia

Il quotidiano francese Le Monde, grazie alle rivelazioni di Snowden, ha reso noto nell'ottobre 2013 che la NSA intercettava in maniera massiccia le comunicazioni telefoniche dei cittadini francesi, specificando come in soli trenta giorni, dal 10 dicembre 2012 all'8 gennaio 2013, avesse spiato *70 milioni* di chiamate.
Tra i vari metodi di intercettazione di cui la NSA dispone, per la Francia è stato utilizzato un apposito segnale che faceva scattare automaticamente la registrazione delle conversazioni, nonché il recupero degli sms in funzione di parole chiave, se queste partivano dal territorio francese, conservando un tabulato storico di tutte le connessioni dei soggetti che stava sorvegliando.
In seguito a questo articolo, i personaggi di spicco del governo francese avevano immediatamente rilasciato dichiarazioni, amareggiati dal comportamento degli USA: il presidente francese Hollande, durante una chiamata diretta a Obama, aveva espresso profondo biasimo e disapprovazione per l'operato della NSA verso il suo Paese, proponendo l'argomento direttamente al vertice UE di Bruxelles. Nel corso del vertice, però, non era stato trovato un accordo tra i leader sulla direttiva per la protezione dei dati.
Il premier francese d'allora, Ayrault, aveva protestato dicendo: *"è incredibile che un Paese amico, un alleato come gli USA, possa spiare così tante comunicazioni private; è una cosa che non ha giustificazioni strategiche o di difesa nazionale"*, esigendo risposte chiare in modo da porre fine a questo tipo di spionaggio, mentre il ministro degli esteri francese Fabius aveva immediatamente convocato a Parigi l'ambasciatore americano, per ottenere spiegazioni in merito alle rivelazioni di Snowden pubblicate sul quotidiano Le Monde [129].

Una nuova notizia, contrastante con l'atteggiamento iniziale tenuto dai vertici francesi, è arrivata dall'Eliseo il 19 marzo 2015: il governo francese si sta apprestando a stilare un proprio *Patriot Act* che garantirà una libertà di sorveglianza antiterroristica illimitata, come mai vista in Europa. L'Eliseo vuole svincolare i propri servizi segreti dal mandato del giudice, obbligando inoltre le società di comunicazione a sottostare a strumenti automatizzati di monitoraggio. Il governo francese ha già parlato con le principali aziende americane di social networking, della possibilità di fornire i messaggi decrittati scambiati dai sospettati di terrorismo; inoltre vorrebbero ricevere in automatico anche i metadati filtrati.
Tutto questo ha del preoccupante: dopo l'attacco alla sede del giornale *Charlie Hebdo* il clima di tensione in Francia è aumentato, a causa della pressione dei governi e dei cittadini stessi, e rischia di produrre effetti simili a quelli dell'attacco alle Torri Gemelle dell'11 settembre 2001 [37].

4.1.2 Germania

Nell'ottobre 2013 uscì, tra le altre notizie rivelate da Snowden, la conferma che il cellulare della Cancelliera tedesca Angela Merkel fosse sotto la sorveglianza della NSA. Il governo tedesco quindi convocò l'ambasciatore americano a Berlino per avere spiegazioni in merito, nonostante avesse già telefonato al presidente Obama in persona, il quale assicurò che *"gli USA non stanno intercettando e non intercetteranno le telefonate della Cancelliera"*; ciò non escludeva però che questo fosse già accaduto in passato.
La stampa tedesca aveva solo una parola per commentare l'accaduto: "affronto" e, facendo riflettere i propri lettori con la frase: *"difficile immaginare come i servizi segreti di Obama trattino i Paesi nemici, quando si osserva come si comportano con i loro alleati più stretti"*, concludeva i propri articoli con un *"Barak Obama non è un Premio Nobel per la Pace ma uno che semina zizzania"* [31].
La Cancelliera dal canto suo portò al summit di Bruxelles dello stesso anno la questione "intercettazioni", proponendo congiuntamente al presidente francese Hollande di definire un "codice etico di spionaggio" per i servizi segreti alla luce di quanto emerso dalle rivelazioni di Snowden, secondo le quali nessun leader mondiale sarebbe stato risparmiato dalle intercettazioni americano-britanniche. Tutti i Paesi erano stati invitati a partecipare, spinti alla cooperazione dalla necessità di fermare il terrorismo; non sorprese l'opposizione del Regno Unito all'accordo. *"Non vogliamo giocare una partita anti-Obama, non c'è questo sentimento. Ma non possiamo rimanere con le mani in mano"* dichiarò un partecipante dopo il vertice europeo [189]. L'accordo, pensato per essere portato a termine nel 2014, verrà concluso entro il 2015 [98].
Nel febbraio 2014 la Merkel voleva addirittura proporre a Hollande l'ipotesi di far nascere un network europeo di comunicazioni, così da *"mantenere un alto livello di protezione dei dati così che le mail e gli altri dati dei cittadini europei non debbano attraversare l'Atlantico"* [131], essendo ancora molto sconvolta dalle intercettazioni del proprio cellulare.
A riguardo era intervenuto anche il presidente del Parlamento Europeo Martin Schulz secondo il quale l'Unione Europea avrebbe addirittura dovuto "sospendere" l'accordo tra UE e Stati Uniti per il monitoraggio delle transazioni finanziarie a fini antiterroristici, precisando di dover: *"discutere con i nostri amici americani di questa situazione che ricorda la guerra fredda"* [31], il tutto alla luce delle presunte intercettazioni illegali di dati bancari di cittadini europei [156].
Sempre nel 2014, venne fatto arrestare in Germania un membro dei servizi segreti tedeschi, dopo aver scoperto che da circa due anni era in combutta con l'America, alla quale forniva informazioni sull'inchiesta riguardante il Datagate aperta nella sua nazione [132]. Questo non ha aiutato il clima già teso tra la Germania e gli altri Paesi stranieri tanto che, secondo Spiegel

online, il governo tedesco abbia scritto a tutte le ambasciate a Berlino intimando loro di fornire i nomi di tutti i loro 007 attivi in Germania in nome della trasparenza, dopo aver cacciato niente poco di meno che il capo della CIA dal proprio territorio [18]. La Germania risultava inoltre già a conoscenza dei nomi di circa *200 agenti* dei servizi segreti di altri paesi, anche se molti infiltrati erano comunque sconosciuti [130].
Per sopperire a questa mancanza di fiducia generale il governo tedesco dal 2014 si è mobilitato, sulla scia della Russia, per l'uso di macchine da scrivere per stilare documenti top secret; in più è stato dato il via per la costruzione di *2000* cellulari blindati, dotati di un sofisticato sistema anti-intercettazione per difendersi dallo spionaggio americano [99].
Ultima decisione nota presa dal governo tedesco è stata quella di interrompere in anticipo di un anno il contratto che lo legava a Verizon, in scadenza nel 2015; la compagnia statunitense era incaricata di gestire il network di comunicazione fra i ministeri tedeschi, quelli statunitensi e le altre amministrazioni, ma dopo gli scandali che l'hanno coinvolta nelle intercettazioni della NSA, la Germania ha deciso di tagliare i ponti e di affidarsi ad una compagnia tedesca [122].
La Cancelliera Merkel sembra molto decisa ad andare fino in fondo alle questioni di trasparenza e di autonomia dell'Europa dall'America; *"nel frattempo"* ha detto *"controlleremo e spieremo tutti, non potendo escludere dalle precauzioni nemmeno gli Stati Amici"* [161].

4.1.3 Italia

La bufera che ha investito Francia, Germania e Spagna nell'ottobre 2013 ha colpito anche il nostro Stato. Stando alla documentazione fornita da Snowden, si scoprì come la NSA avesse raccolto 46 milioni di metadati italiani grazie al programma *BOUNDLESS INFORMANT*, nel solo periodo tra il 10 e il 28 dicembre 2012.
Immediatamente anche il nostro Stato si mobilitò, inviando una delegazione del *COPASIR*, il Comitato Parlamentare per la Sicurezza della Repubblica, in America così da poter avere spiegazioni direttamente dal governo americano circa i programmi di spionaggio verso il nostro Paese [152].
Le conferme non hanno tardato ad arrivare. Come dichiarò il membro del comitato inviato negli USA Claudio Fava di SEL: *"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"*. Sembrerebbe che la NSA l'avesse fatto unicamente per proteggere gli italiani, intercettando soltanto le persone ritenute sensibili ai fini della sicurezza nazionale [23].
Affermazioni decisamente contrastanti con quanto aveva dichiarato invece l'allora sottosegretario alla presidenza del Consiglio con delega all'Intelli-

gence Marco Minniti, il quale proprio negli stessi giorni di ottobre 2013 garantiva di *"escludere che i servizi segreti italiani sapessero dello spionaggio americano attraverso PRISM"*, così come assicurava la privacy dei cittadini italiani [156].
Le rivelazioni dell'allora generale Keith Alexander a riguardo crearono grande scalpore: egli dichiarò infatti che la raccolta di metadati in Europa non fu attuata dalla NSA, bensì dai vari governi europei che solo in seguito avevano trasmesso le informazioni ottenute all'agenzia americana.
Tutta questa vicenda è ben descritta da Fabio Chiusi nel suo *"Grazie Mr Snowden"*, nella sezione appositamente dedicata al rapporto Datagate-Italia [28].
Negli stessi giorni per fortuna (o per sfortuna) era in visita in Italia il Segretario di Stato USA John Kerry, anche se per altri motivi (Libia e Siria). Il presidente del Consiglio Letta, ebbe la possibilità di sollecitare la *"necessità di verificare la veridicità delle indiscrezioni su eventuali violazioni della privacy"*, anche se le testate giornalistiche italiane sottolinearono subito la linea morbida della conversazione e l'atteggiamento cooperativo del Segretario di Stato americano, al contrario di quanto avvenuto nelle telefonate tra Obama e i premier francese e tedesco [30].
Dopo questo colloquio, Letta riferì alla Camera dei Deputati che *"in base all'analisi svolta non risulta compromessa la sicurezza delle comunicazioni dei vertici del governo italiano, né delle nostre ambasciate. E non risulta che la privacy dei cittadini italiani sia stata violata in alcun modo"* [85].
Interessante leggere l'articolo di Domenico Damodeca, una voce fuori dal coro che si discosta dagli altri per il tono sarcastico e per le dichiarazioni forti indirizzate all'allora presidente del consiglio Letta, definito "succube degli USA" [25].
Una richiesta della NSA era effettivamente arrivata in Italia, nello specifico alla società Telecom Italia alla quale nel 1998 venne chiesto di accedere agli snodi siciliani della rete di cavi sottomarini in fibra ottica (connessione effettivamente attuata sembrerebbe dal 1999 al 2001) [22]. Questa notizia tuttavia non aveva mai trovato conferma ufficiale, infatti Il Sole 24 Ore affermò che *"chi sa non è autorizzato a parlare"*, mentre Massimo D'Alema continuava a sostenere che *"nessun governo italiano ha mai autorizzato gli americani a effettuare intercettazioni di cittadini italiani"* [141].

4.1.4 Regno Unito

Il GCHQ britannico è conosciuto per essere il partner ufficiale nel programma di spionaggio e intercettazioni della corrispettiva Agenzia di Sicurezza americana.
Senza il minimo pentimento o risentimento, nel 2014 il direttore generale dell'Ufficio per la Sicurezza e l'Antiterrorismo britannico, Charles Farr, ha

affermato come sia *"assolutamente legale spiare gli utenti online britannici"*, conscio del fatto che il GCHQ può infatti liberamente curiosare, senza alcun mandato, sull'utilizzo di Google, YouTube e dei principali social network da parte dei cittadini britannici [61].
Ha fatto specie perciò quando nel febbraio 2015, per la prima volta in 15 anni, l'*Investigatory Powers Tribunal* britannico, che si occupa dei casi riguardanti l'intelligence, si è pronunciato chiaramente contro il GCHQ, definendo "illegale" l'attività di spionaggio attuata a fianco dell'alleata NSA [134].
Il primo ministro Cameron ha tuttavia sottolineato come la linea seguita dall'agenzia segreta britannica non cambierà in quanto *"il giudizio del tribunale non chiede al GCHQ di cambiare le sue operazioni"*.
Il premier inglese è fortemente a favore dei poteri di cui i servizi segreti godono, grazie ai quali a suo parere *"lo spionaggio salva la gente dal terrorismo"* [141].

4.1.5 Russia

La Russia è un'importante nazione da considerare essendo l'attuale residenza della talpa Edward Snowden, il quale, viaggiando nel giugno 2013 verso un non meglio precisato paese del Sud America (Venezuela o Ecuador presumibilmente), venne bloccato dal governo statunitense e britannico proprio nella nazione governata dal presidente Putin. In merito a questo, dal Cremlino arrivò al quotidiano locale Izvestia la dichiarazione che riteneva Snowden un cittadino libero e non meritevole dell'estradizione, al punto da concedergli il permesso di restare, sebbene il governo americano continuasse a insistere per riaverlo nel proprio territorio. La Russia accusò inoltre gli USA di aver spaventato gli altri paesi "intrappolando" un uomo contro il suo volere in una nazione estera [139].
Gli 007 russi del servizio delle guardie federali (*FSO*), discendenti del vecchio *KGB*, dal canto loro, presero nello stesso mese dello scoppio dello scandalo la decisione di tornare alle vecchie macchine da scrivere per la gestione di informazioni riservate, considerando la carta molto più affidabile ed inviolabile rispetto ai sistemi informatici ed elettronici. Come infatti afferma l'ex capo dei servizi segreti russi Nikolai Kovaliov: *"dal punto di vista della sicurezza ogni collegamento elettronico è vulnerabile: da un computer si può prendere qualsiasi informazione perché la protezione non è mai garantita al 100%. Dunque bisogna privilegiare i mezzi più primitivi per comunicare e tra questi ci sono i documenti scritti a mano o con la macchina per scrivere"* [168].

A causa delle informazioni rivelate da Snowden, anche i rapporti con la vicina Svezia si sono incrinati: da un lato, per le intercettazioni attuate dagli svedesi

a discapito dei russi sin dalla Seconda Guerra Mondiale, dall'altro, per la cancellazione da parte della Casa Bianca del summit nel 2013 tra Obama e Putin, in favore di una tappa extra dalla sua alleata nordica. La decisione era stata presa a causa dell'asilo temporaneo concesso a Snowden [94], che aveva molto deluso Obama [140] [29].
In risposta alla scelta statunitense, il governo del Cremlino promise di aumentare la propria sorveglianza nei confronti della Svezia.

4.1.6 Spagna

Tra il 25 e il 28 ottobre 2013 i quotidiani El Mundo ed El Pais pubblicarono articoli, firmati anche da Glenn Greenwald, riguardanti le intercettazioni della NSA in Spagna, che mostravano (grazie ai documenti forniti da Snowden e girati a El Mundo da Greenwald stesso) come fossero state registrate dall'agenzia milioni di chiamate (in termini di metadati e non di contenuti), sms, email e traffico relativo a Internet e ai social network (oltre 60 milioni tra il 10 dicembre 2012 e l'8 gennaio 2013).
Il premier spagnolo Rajoy aveva subito dichiarato: *"se tutto sarà confermato, il tradizionale clima di fiducia che intercorre tra i due Paesi potrebbe rompersi"*, supportato dal suo ministro degli esteri Garcia-Margallo, il quale aggiunse come non si trattava solo di un "comportamento inaccettabile per un Paese amico e alleato", ma che *"la Spagna protegge i diritti alla privacy dei propri cittadini con il codice penale"*.
L'ambasciatore USA, dal canto suo, oltre a non aver smentito le intercettazioni dell'agenzia del suo governo verso la Spagna, ha riferito la risposta americana per la questione posta dal governo iberico: *"ciò che è successo lo fanno anche gli altri"*, senza però entrare nel dettaglio del "cosa" sia avvenuto [126].
Nel luglio 2013 inoltre la Spagna aveva rifiutato la richiesta di asilo presentata da Edward Snowden (una tra le 21 avanzate a diverse nazioni mondiali), in quanto, come sottolineò il primo ministro spagnolo, non legalmente ammissibile non trovandosi in territorio spagnolo.

4.1.7 Svezia

Nel dicembre 2013 la televisione statale svedese Sveriges Television (SVT) dichiarò, con l'ausilio di un video di Glenn Greenwald, come l'Agenzia dei Servizi Segreti svedese *FRA* (Försvarets radioanstalt, o National Defence Radio Establishment) fosse un'importante partner della NSA sin dal 2009, intercettando per suo conto fondamentali informazioni che comprendevano obiettivi russi ad alta priorità, come la leadership del Cremlino e membri della sua politica interna.

A riguardo della notizia un portavoce della FRA dichiarò: *"non possiamo commentare questo tipo di informazione, né i dettagli delle nostre collaborazioni in termini di intelligence"*.
Importante notare come l'80% del traffico elettronico russo passi per la Svezia [162].

4.1.8 Intervista a Mikko Hypponen

Il finlandese Mikko Hypponen, esperto di sicurezza e Chief Research Officer di F-Secure (compagnia finlandese per la sicurezza e la privacy online), è stato intervistato esattamente un anno dopo le rivelazioni di Snowden allo scopo di ottenere un riscontro circa l'impatto che gli eventi accaduti nel 2013 hanno avuto sulle persone e sulle aziende.
In generale secondo Hypponen oggi si può dire di stare meglio, essendo aumentata l'attenzione per la questione privacy e per la gestione dei dati, sia da parte delle aziende che dei cittadini stessi. Tuttavia, alla domanda *"Ma le persone stanno realmente abbandonando i servizi Internet basati negli USA?"* il finlandese constata che effettivamente è difficile lasciare i vecchi servizi per adottarne di nuovi, soprattutto quando l'alternativa al servizio americano non c'è. Bisognerebbe creare servizi analoghi ospitati e gestiti dall'Europa per poter "restare in casa".
Le aziende invece hanno ora la consapevolezza che il governo americano ha il diritto di poter controllare qualsiasi dato si trovi archiviato nei servizi cloud gestiti dagli USA, motivo per cui le compagnie stanno spostandoli su piattaforme ospitate sul suolo europeo.
Hypponen afferma anche che, a suo parere, il governo americano a seguito dello scandalo Datagate si è immediatamente attrezzato per migliorare la protezione della privacy dei propri cittadini, tralasciando quella di tutti gli altri, in quanto *"i politici devono soddisfare chi li vota e noi stranieri non potremo votare contro di loro"*.
Per liberarsi dallo spionaggio in generale Hypponen aveva invitato tutti a scrivere a `http://campaigns.f-secure.com/digitalfreedom/`, una pagina ospitante un documento in crowdsourcing il cui scopo era promuovere la libertà digitale nel mondo (questo si poteva fare fino al 30 giugno 2014).
In ultima battuta, il finlandese lascia un messaggio di speranza, secondo lui rappresentata proprio da Edward Snowden *"un ragazzo che ha sacrificato tutto (non sempre nel modo corretto) per salvarci e noi come cittadini del mondo dovremmo essergli riconoscenti. Quindi spero vengano alla ribalta più Snowden da altre superpotenze"* [36].

4.2 Cosa dicono i nostri intervistati

Dal 5 al 17 marzo 2015 abbiamo condotto un'indagine anonima sulla percezione relativa allo scandalo Datagate e alla figura di Edward Snowden che hanno le persone in Italia.
I dati analizzati sono stati raccolti mediante la somministrazione di un questionario composto da 10 domande:

- *6* chiuse relative al fenomeno;
- *4* chiuse e aperte personali, per inquadrare il background dei soggetti, così da poterne contestualizzare le risposte.

Il questionario è stato realizzato facendo uso di un modulo *Google Drive* e ha coinvolto nella sua compilazione *190* persone con formazione professionale e grado di istruzione differente, sia esperti del settore IT che non, allo scopo di rendere i dati quanto più rappresentativi di un'ampia porzione di popolazione.
Prima della formulazione delle domande abbiamo fornito una breve descrizione, sia sulla figura di Snowden sia sul Datagate, per permettere agli utenti coinvolti di avere una panoramica sintetica della tematica che sarebbe stata affrontata nei quesiti successivi:
"Nel 2013 l'agente della National Security Agency (NSA) degli Stati Uniti d'America, Edward Snowden, è stato protagonista della più grande fuga di notizie relativa a documenti confidenziali riguardanti le intercettazioni che il governo statunitense ha portato avanti per diverso tempo, registrando telefonate degli utenti, e-mail, contenuti dei social network sites, metadati, ecc. sia di cittadini americani che di vari stati esteri.
In seguito a questo è esploso a livello mondiale lo scandalo denominato Datagate che ha costretto Snowden ad allontanarsi dagli USA trovando rifugio in diversi paesi stranieri.
Di seguito verranno poste alcune domande anonime circa la propria percezione riguardante la persona di Snowden e lo scandalo."

La prima domanda (Figura 1) è stata posta allo scopo di ottenere un feedback immediato sulla conoscenza di Edward Snowden per capire quanti, prima della compilazione del questionario, avessero almeno una vaga idea di chi egli fosse.
La maggior parte dei soggetti coinvolti (il *68,9%*) ha dichiarato di conoscere questo personaggio. Dei restanti il *25,8%* ha negato di conoscerlo e soltanto il *5,3%* ha cercato informazioni su di lui prima di procedere allo svolgimento del questionario.
Sembrerebbe quindi che buona parte delle persone abbia almeno idea di chi sia Snowden, seppur con gradi di approfondimento differenti.

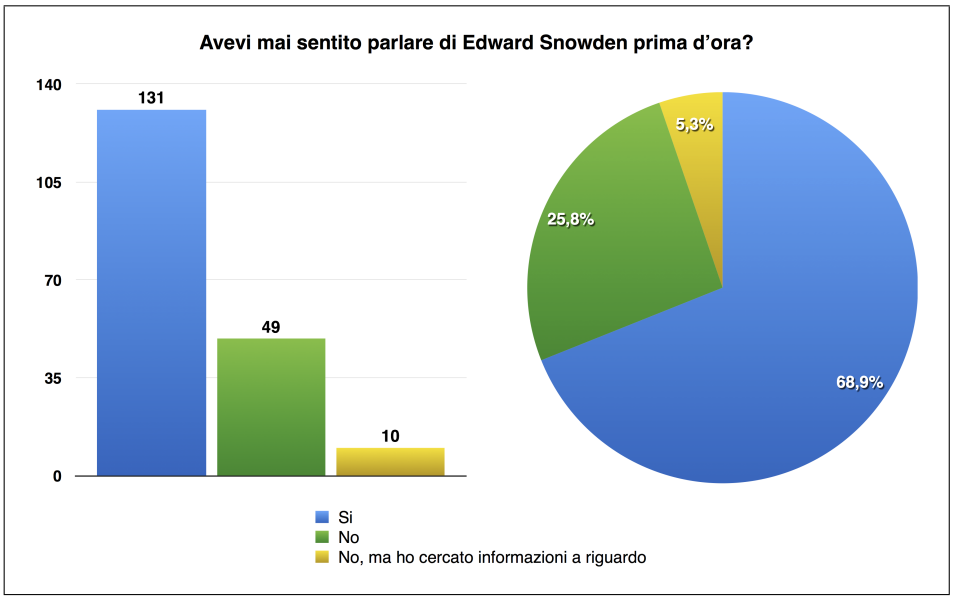

Figura (1): Questionario scandalo Datagate - Domanda 1

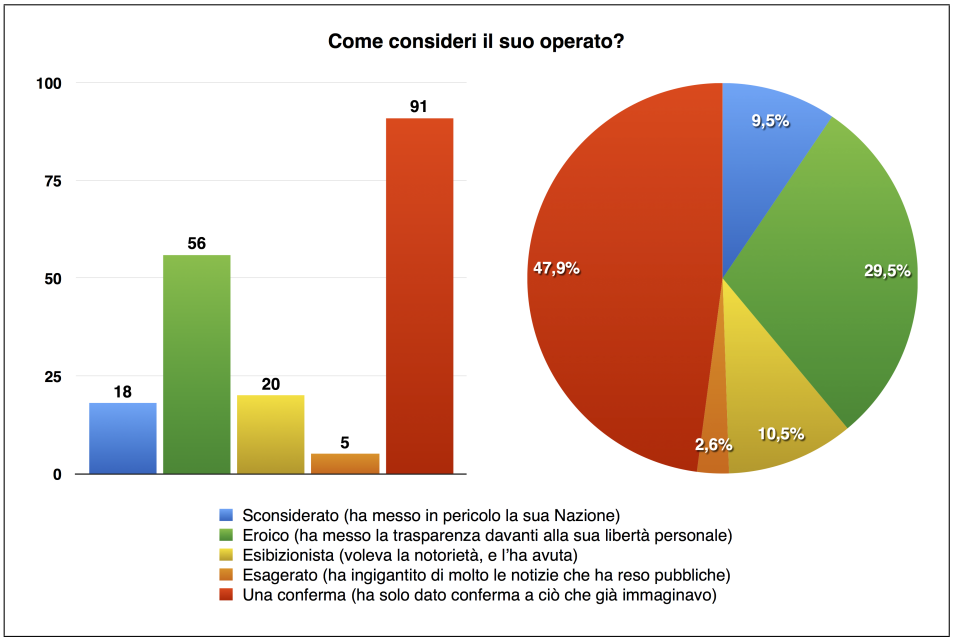

Figura (2): Questionario scandalo Datagate - Domanda 2

La seconda domanda (Figura 2) è stata formulata per cercare di comprendere (sulla base della conoscenza pregressa o su quanto appreso dalla descrizione) come l'atto di Snowden sia risultato agli occhi delle persone.
Quasi la metà dei soggetti (*47,9%*) ha detto che quanto rivelato dall'ex agente della NSA è stato soltanto una conferma dei sospetti che già avevano sulle intercettazioni delle comunicazioni da parte dei governi.
La seconda risposta più selezionata, col *29,5%*, è quella che descrive Snowden come un'eroe, sacrificatosi per il bene collettivo.
Quasi a pari merito, in termini di voti, sono state le affermazioni che indicano la talpa come uno sconsiderato (*9,5%*), per aver messo in pericolo il suo paese con le proprie azioni, e come un esibizionista (*10,5%*), volendo col suo gesto ottenere soltanto la notorietà.
La risposta meno votata, col *2,6%*, è quella che identifica Snowden come un esagerato, che ha reso le informazioni top-secret di dominio pubblico unicamente per ottenere la notorietà.
Nell'insieme delle risposte date appare chiaro come molti siano consapevoli dell'operato dei governi mondiali sulle intercettazioni, ma nonostante ciò non si sono mai registrate significative manifestazioni di protesta nei confronti di questo genere di abusi.

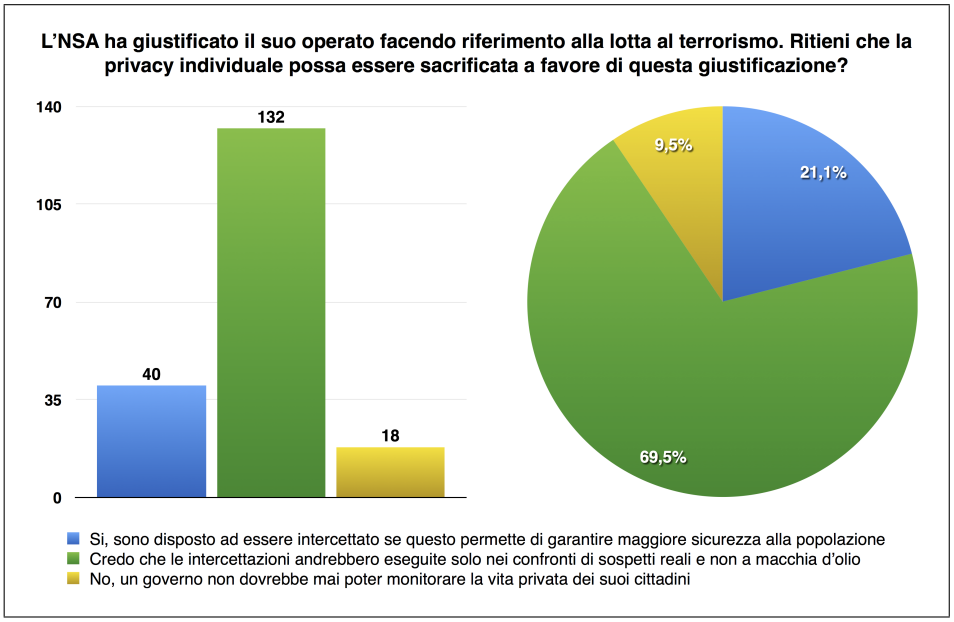

Figura (3): Questionario scandalo Datagate - Domanda 3

Con la terza domanda (Figura 3) volevamo capire se le persone siano disponibili al sacrifico del diritto alla privacy individuale a favore di una giustificazione come quella della lotta al terrorismo, a prescindere dell'utilità concreta di questa privazione personale.

Quello che il *69,5%* degli intervistati ha risposto è che le intercettazioni possono avere una loro utilità solo se mirate al monitoraggio di minacce reali, diventando di conseguenza inutili, se non deleterie, quando effettuate ad ampio spettro.
Il *21,1%* si dichiara disponibile all'intercettazione a patto che questa sia effettivamente garante dell'incolumità e della sicurezza dei cittadini. Soltanto il *9,5%* è convinto che mai alcun governo dovrebbe violare la privacy individuale senza un mandato trasparente, nemmeno nel caso di sospetti reali verso dei soggetti.
Tra le risposte fornite era presumibile che per molti le intercettazioni possono essere un importante strumento atto a garantire la sicurezza, se utilizzate con discrezione e limitatamente ad accuse fondate. Interessante la percentuale non piccola di persone che sono disposte a sacrificare qualsiasi forma di privacy nella convinzione che questo garantirebbe un livello di sicurezza maggiore all'interno della società.

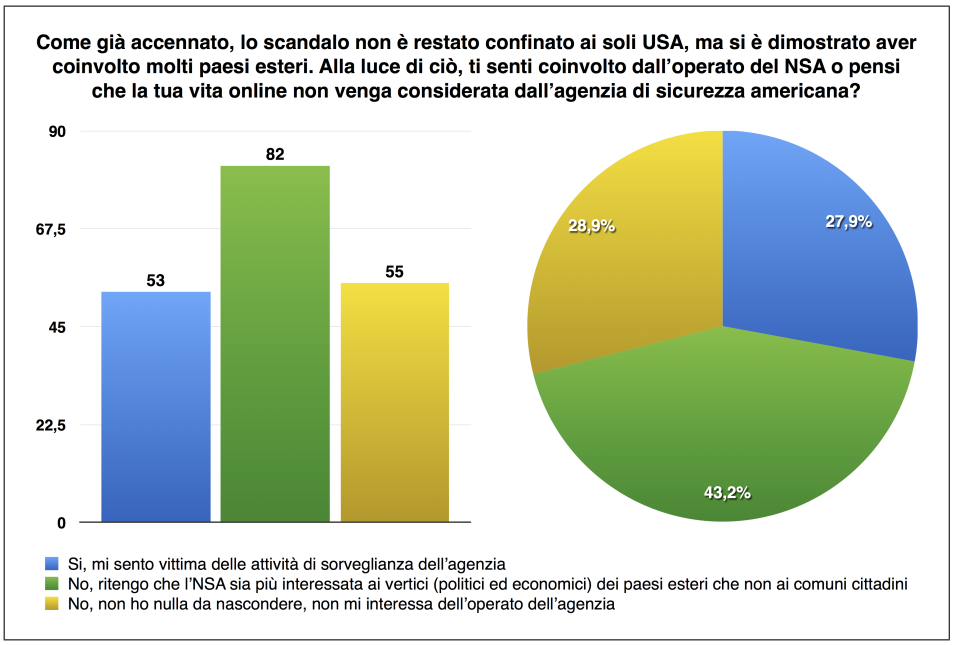

Figura (4): Questionario scandalo Datagate - Domanda 4

Il quarto quesito (Figura 4) sottoposto ai partecipanti riguardava la percezione di un coinvolgimento personale, come "bersagli" delle operazioni d'intercettazione da parte dell'Agenzia di Sicurezza americana.
Tra le tre possibili risposte alla domanda non c'è stata una netta prevalenza di una rispetto ad altre. La maggior parte delle persone (il *43,2%*) ha dichiarato di non sentirsi coinvolta dalle operazioni della NSA, ritenendo che il governo statunitense sia più interessato ad intercettare le comunicazioni

di figure rilevanti nella scena mondiale piuttosto che quelle dei comuni cittadini. Probabilmente questa sensazione è anche frutto dell'informazione che i mezzi di comunicazione hanno fornito: è stata data più importanza alle intercettazioni tra capi di stato che a quelle svolte a danno dei cittadini.
A percepire sulla propria pelle la violazione della privacy, perpetrata dall'Agenzia, è invece il *27,9%* degli intervistati che dichiarano di sentirsi "vittime" della sorveglianza di massa.
Il *28,9%* delle persone coinvolte dall'indagine risulta disinteressata dell'operato del governo, ritenendo di non aver nulla da nascondere. Di conseguenza per questa porzione d'individui la violazione della privacy, attuata attraverso le intercettazioni governative, non è vissuta come un problema né tantomeno come un danno personale.
Tuttavia alcuni comportamenti ritenuti dai più di "uso comune" sono spesso ai limiti della legalità o individuabili come veri e propri reati. Il problema a volte è dovuto alla confusa interpretazione della legge da parte degli organi competenti, non aiutando in questo modo i cittadini ad avere un'idea chiara a riguardo. Inoltre alcune azioni illegali, vengono considerate "corrette" o quasi, perché compiute dalla massa.

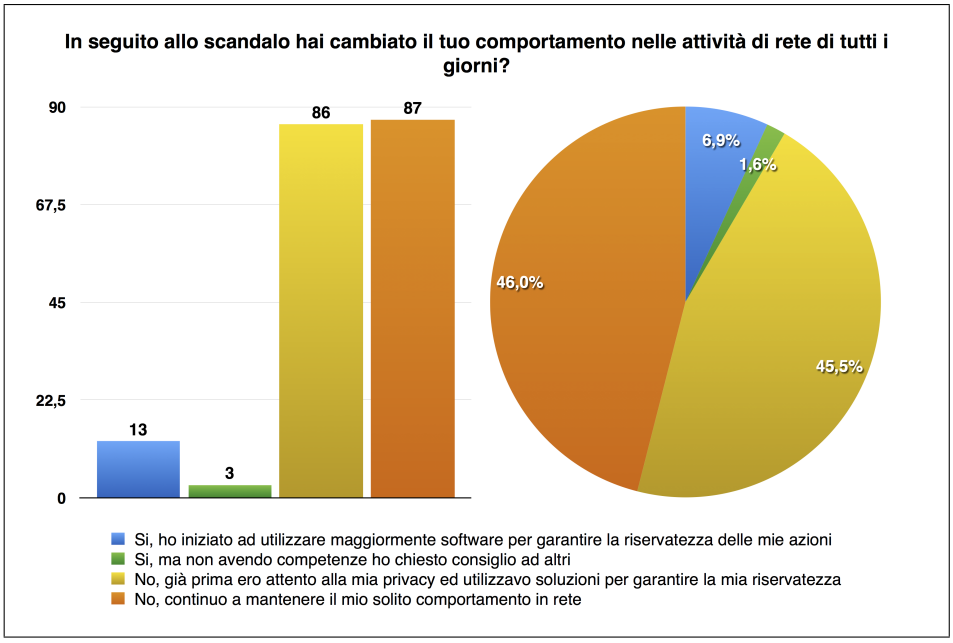

Figura (5): Questionario scandalo Datagate - Domanda 5

Con la quinta domanda (Figura 5) l'intento era quello di comprendere se il polverone sollevato da Snowden abbia in qualche misura comportato delle modifiche alle abitudini quotidiane delle persone, per quanto riguarda le attività in rete e di telecomunicazione.

Dai risultati emerge come la stragrande maggioranza dei soggetti dichiari di non aver apportato modifiche al proprio comportamento. Praticamente a pari merito (con un solo voto di scarto tra le risposte) il *45,5%* ha sottolineato come già prima dello scandalo tutelasse la propria privacy, adottando strumenti e tecniche di difesa volti a proteggerla, mentre il *46%* ha detto di continuare a mantenere il solito comportamento, senza quindi adoperare particolari contromisure nei confronti delle possibili intercettazioni.
In coda troviamo che il *6,9%* ha iniziato ad utilizzare delle soluzioni software di sicurezza con l'obiettivo di migliorare la riservatezza delle proprie azioni quotidiane e solo l'*1,6%*, non avendo competenze informatiche adeguate ma essendo comunque stato stimolato dalle rivelazioni di Snowden, ha chiesto aiuto ad altri per migliorare la propria sicurezza in rete.
È molto interessante il fatto che, tolti quelli che già prima erano attenti alla propria privacy, la maggior parte degli intervistati ha continuato a comportarsi come sempre. Questo evidenzia come quanto rivelato da Snowden potrebbe non aver sortito l'effetto sperato dall'ex-agente della NSA (almeno per il campione di persone da noi esaminato).

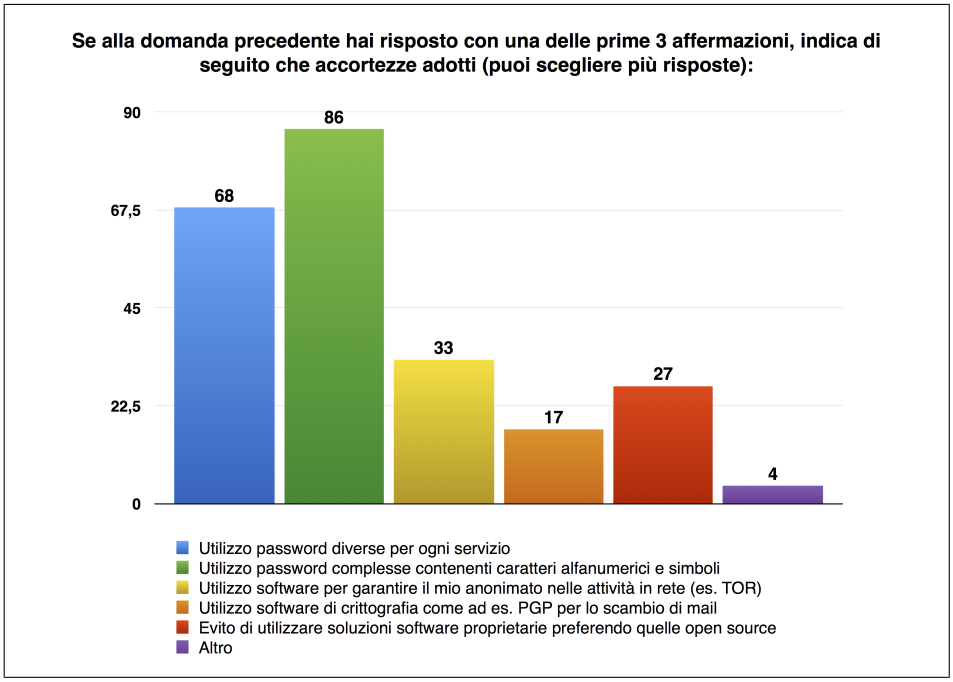

Figura (6): Questionario scandalo Datagate - Domanda 6

La sesta domanda (Figura 6) non era obbligatoria ma dava la possibilità di selezionare più di una risposta ed eventualmente aggiungere degli strumenti all'elenco di quelli già inseriti, ed era rivolta essenzialmente a chi con la risposta precedente aveva dichiarato di utilizzare delle soluzioni in grado di

offrire agli utenti una miglior riservatezza delle comunicazioni e della propria attività in rete.
68 partecipanti hanno dichiarato di utilizzare password diverse per ogni servizio, evitando di commettere il grave errore (che purtroppo molti fanno) di avere una password unica per tutto. *86* partecipanti hanno dichiarato che utilizzano password complesse, composte da caratteri alfanumerici e da simboli, per renderne più complicata l'individuazione da parte di malintenzionati, mentre la risposta indicante l'utilizzo di software per l'anonimato in rete come *Tor* è stata scelta da *33* persone.
Soltanto *17* soggetti hanno affermato di utilizzare la crittografia per lo scambio di messaggi sensibili, utilizzando ad esempio sistemi come *PGP*.
A preferire l'utilizzo di software open source, permettendo di conoscere ogni singola riga che compone il codice, sono *27* partecipanti.
Infine soltanto *4* persone hanno spuntato la risposta *"Altro"* aggiungendo ognuno un qualcosa di differente:

- Una persona utilizza connessioni *SSL* per la posta elettronica;
- Una persona imposta i settaggi relativi alla privacy dei programmi che utilizza;
- Una persona ha dichiarato di non aver nulla da nascondere e che protegge la propria privacy solo per principio;
- Una persona ha selezionato *"Altro"* non specificandolo, probabilmente per non dover rispondere alla domanda senza aver letto che questa non era obbligatoria.

Al termine di questa prima parte relativa allo scandalo Datagate e alle sue conseguenze, abbiamo posto altre quattro domande per poter contestualizzare le riposte fornite, cercando di ottenere un profilo (anonimo) di ciascuno dei soggetti coinvolti nell'indagine.

Dalla domanda sul sesso dei partecipanti (Figura 7) abbiamo ricavato che il *74,7%* di questi sono uomini e il *25,3%* donne. Non sappiamo se questo rapporto di *3* ad *1* possa essere stato determinato da qualche elemento particolare, ma sembra che le persone di sesso maschile risultino maggiormente interessate all'argomento, decidendo di conseguenza di prendere parte al sondaggio.
Sarebbe interessante amplificare la portata del questionario, coinvolgendo un campione molto più ampio per capire se effettivamente gli uomini mostrino più interesse delle donne sul fenomeno delle intercettazioni e della privacy o se questo risultato da noi ottenuto sia stato puramente casuale.

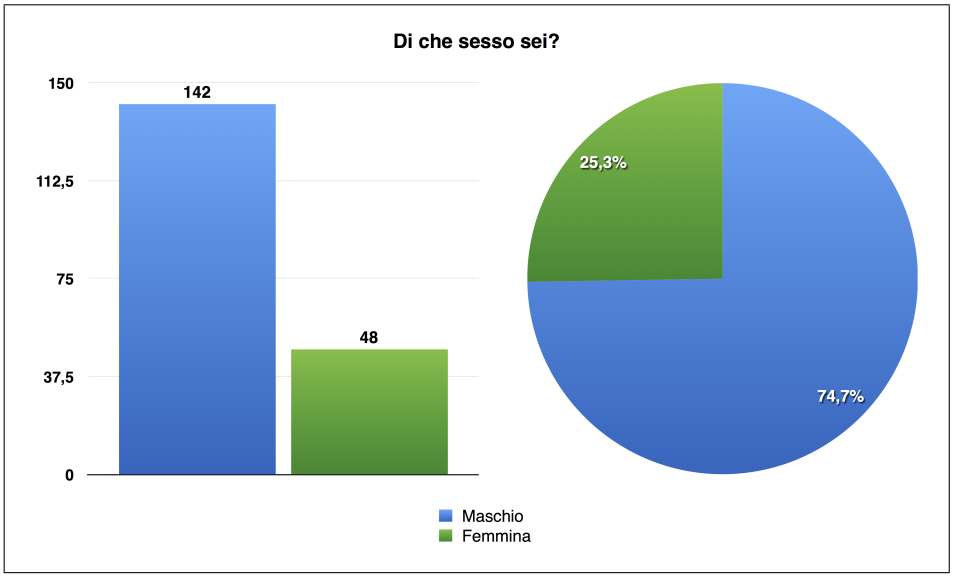

Figura (7): Questionario scandalo Datagate - Domanda 7

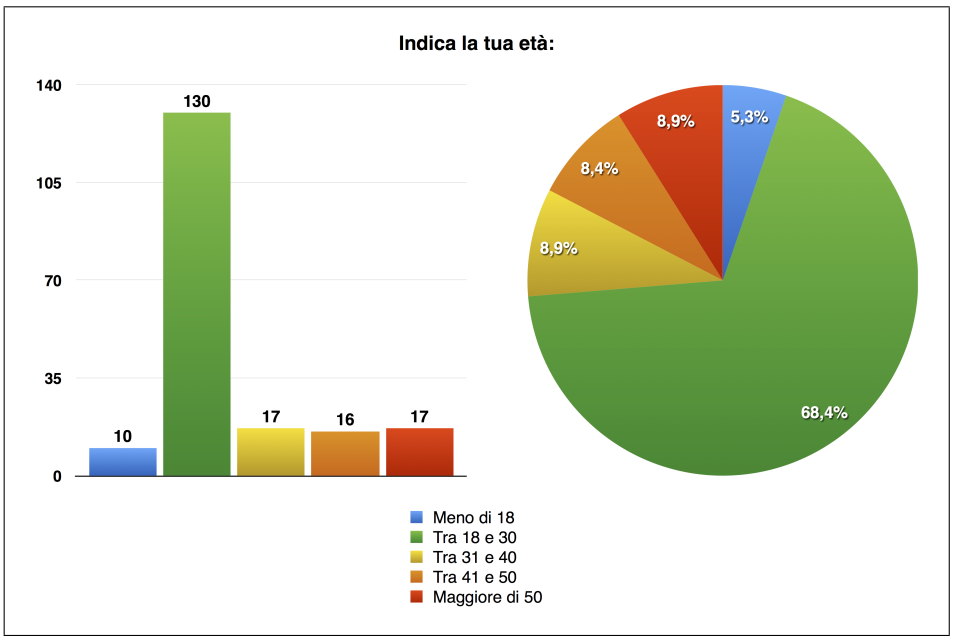

Figura (8): Questionario scandalo Datagate - Domanda 8

Tra le persone che hanno preso parte al sondaggio (Figura 8), il *68,4%* ha dichiarato di avere un'età compresa tra i *18* e i *30 anni*.
Solo il *5,3%* dei soggetti sono risultati essere minorenni, mentre le fasce di età *31-40*, *41-50* e over *50* hanno avuto una distribuzione simile, con delle percentuali rispettivamente pari a *8,9%*, *8,4%* e *8,9%*.
La grossa discrepanza tra la fascia dei giovani e le altre quattro categorie, è legata molto probabilmente a diversi fattori:

- Il primo è la *forma* del questionario. Come detto è stato realizzato attraverso un modulo *Google Drive*, questo ha sicuramente comportato una maggior affinità dei giovani a compilare un sondaggio in formato digitale rispetto a persone con un'età maggiore abituate magari a formati alternativi come il cartaceo;

- Il secondo è il *canale* attraverso il quale il questionario ha avuto una maggior diffusione. Abbiamo fatto uso di Facebook, condividendo e richiedendo ad altri di fare lo stesso, per raggiungere quante più persone possibili. I giovani risultano sicuramente più affini ai social, perciò la scelta di questo canale di diffusione ha sicuramente avuto un ruolo determinante nella distribuzione;

- Un terzo elemento infine potrebbe essere il fatto che, essendo noi stessi nella fascia d'età *18-30*, la maggior parte degli *"amici"* che abbiamo in Facebook sono nostri coetanei.

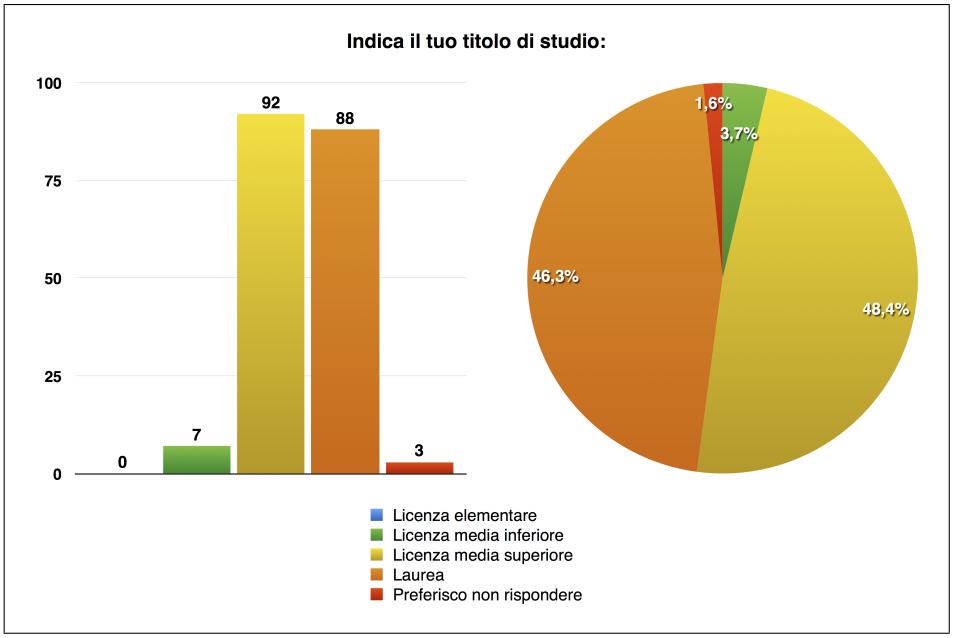

Figura (9): Questionario scandalo Datagate - Domanda 9

Con la nona domanda (Figura 9) volevamo comprendere quale fosse il grado di istruzione delle persone che hanno preso parte al sondaggio, per cercare di contestualizzare le risposte date in relazione a questo.
Come presumibile, la maggior parte degli individui ha selezionato come risposta "licenza media superiore" (*48,4%*) e "laurea" (*46,3%*).
Solo il *3,7%* ha dichiarato di avere la "licenza media inferiore", mentre l'1,6% ha preferito non rispondere alla domanda.
Nessuno dei soggetti ha selezionato "licenza elementare" come proprio grado di istruzione.
Le risposte ottenute a questa domanda sono abbastanza allineate con quanto atteso. Potrebbe esserci un leggero sbilanciamento verso la laurea dettato dal fatto che molti di quelli che hanno preso parte al questionario sono nostri colleghi universitari e professori.

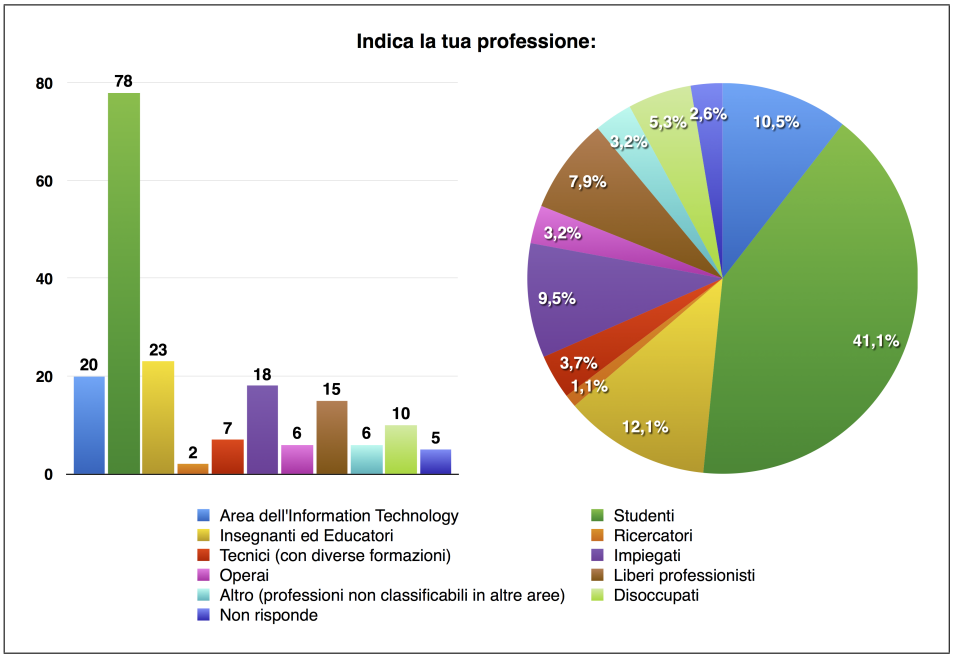

Figura (10): Questionario scandalo Datagate - Domanda 10

L'ultima domanda del sondaggio (Figura 10) richiedeva, attraverso un campo di testo, di indicare la propria professione. Non avendo predefinito le professioni tra cui scegliere, questa domanda ha visto molte risposte differenti; per quanto possibile abbiamo cercato di analizzarle a raggrupparle in macro aree.
Quello che principalmente volevamo capire era quanti dei soggetti avessero un profilo professionale legato al mondo dell'IT rispetto al totale dei partecipanti, per determinare se le risposte relative allo scandalo possano considerarsi rappresentative di un campione eterogeneo in termini di competenze.

Il *10,5%* ha dichiarato di appartenere al mondo dell'*Information Technology* in termini professionali, seppur con mansioni diverse.
Il *41,1%*, quindi quasi la metà dei partecipanti, sono *studenti*. Di questi non c'è stato possibile determinare quanti fossero studenti di informatica e quanti di altre facoltà non essendo stato dichiarato esplicitamente.
Il *12,1%* sono *insegnanti*, *professori* ed *educatori*. Come nel caso degli studenti anche per questa risposta non abbiamo ricevuto una specificazione dell'area di competenza.
I ricercatori coinvolti sono stati solo l'*1,1%* del totale.
Le altre mansioni indicate le abbiamo suddivise in diverse categorie: *tecnici* con differenti formazioni (*3,7%*), *impiegati* (*9,5%*), *operai* (*3,2%*), *liberi professionisti* (*7,9%*) e *altro* (*3,2%*), a rappresentare quelle professioni che non siamo stati in grado di inserire nelle precedenti categorie.
Infine il *5,3%* ha detto di essere *disoccupato* e il *2,6%* ha preferito non rispondere alla domanda. Anche per questi ultimi due gruppi non ci è stato possibile determinare se possiedono comunque delle competenze in ambito informatico o meno.

In coda all'analisi del questionario, vorremmo citare e ringraziare **Tom's Hardware Italia** per averci aiutato a condividere il sondaggio attraverso la propria pagina Facebook quando, in data 9 marzo 2015 in seguito ad una nostra richiesta, ha condiviso il nostro questionario attraverso un post accompagnato dal seguente messaggio:
"Due lettori di Tom's stanno preparando un progetto sul Datagate per l'esame di Cittadinanza Digitale e Tecnocivismo per il corso di laurea in Informatica dell'Università degli Studi di Milano. Gli diamo una mano rispondendo al loro questionario?".

5 Gli strumenti per difendersi

Nell'era dell'informatizzazione in cui viviamo, privarsi delle tecnologie allo scopo di tutelare la propria privacy è un compromesso troppo grande e difficilmente accettabile da chiunque.
Seppur non tutte le persone adottino gli strumenti digitali allo stesso modo, come tipologia e quantità, sarebbe pressoché impossibile un rifiuto totale dei sistemi informatici e delle reti di telecomunicazione.
Lo scopo di questo capitolo è quello di analizzare alcune delle principali soluzioni software disponibili sul mercato che permettono alle persone di comunicare, mantenendo alto il livello di sicurezza dei propri messaggi, delle proprie azioni, ecc.

5.1 Chat OTR e CryptoCat

Parlando di chat *OTR* si fa riferimento ad un protocollo crittografico che permette lo scambio di messaggi cifrati tra due o più interlocutori attraverso la rete Internet.
La prima versione del protocollo venne presentata nel 2004 da Nikita Borisov, Ian Goldberg ed Eric Brewer con un paper dal titolo *"Off-the-Record Communication, or, Why Not To Use PGP"* [24]. Per i ricercatori un grosso limite e pericolo del protocollo *PGP* è la possibilità, nel caso un estraneo venga a conoscenza della chiave privata di un utente, di decrittare tutti i messaggi cifrati con la corrispondente chiave pubblica.
Il funzionamento della chat *OTR* si basa su un segreto che viene condiviso tra gli interlocutori mediante l'utilizzo dello scambio di chiavi *Diffie-Hellman (D-H)* [6]. Questa tecnica permette di scambiare le chiavi utilizzando un canale pubblico.
Utilizzando il protocollo *OTR* solo le parti coinvolte nella conversazione sono a conoscenza del contenuto semantico scambiato, infatti quando la conversazione termina non resta alcun log dei messaggi. Se questo impedisce l'archiviazione delle informazioni, si rivela essere molto efficace nel caso di comunicazioni a "bassa latenza" tra due interlocutori.
Per garantire la sicurezza nel caso le chiavi venissero intercettate, ad ogni ricezione di un messaggio l'interlocutore genera un nuovo esponente *D-H* e tramite coppie di questi esponenti vengono create nuove chiavi *D-H*. In questo modo l'entrare in possesso di una chiave non permette di risalire ai messaggi precedenti, portando la comunicazione ad essere *"Off-the-Record"*.
Negli anni sono state rilasciate nuove versioni del protocollo *OTR*, con l'obiettivo di colmare i problemi di sicurezza che sono emersi nel tempo.
Basandosi sul protocollo *OTR* nel 2011 Nadim Kobeissi ha rilasciato *CryptoCat*, un'applicazione che permette agli utenti di dialogare in maniera crittografata.

Ad oggi l'applicativo è disponibile come plugin per quasi tutti i browser in commercio e come applicazione nativa per ambiente *Mac OSX* e *iOS*.
L'obiettivo di Kobeissi era quello di fornire agli utenti finali un applicativo che fosse semplice da utilizzare per poter effettuare sessioni di chat crittate, potendosi anche integrare con la chat nativa di Facebook per l'invio di messaggi cifrati su quel canale. Senza utilizzare il famoso social network site è comunque possibile interagire con singoli utenti o con gruppi semplicemente scegliendo un nome per la conversazione e un proprio nome utente.
Rispetto all'utilizzo di estensioni per integrare il protocollo *OTR* in software di instant messaging, *CryptoCat* risulta indubbiamente più rapida e di facile utilizzo.
Tuttavia l'applicativo ha alcune limitazioni che gli sono state contestate dalla iSECPartners [39], infatti è possibile per il membro di una chat modificare la chiave *OTR* senza che questo venga notificato agli altri membri. In questo modo con un attacco *Man-in-th-Middle* potrebbe essere modificata la chiave, compromettendo la cifratura dei messaggi che risulterebbero così visibili all'attaccante.
Inoltre la necessità di verificare la fingerprint tra gli utenti all'inizio di ogni conversazione rende teoricamente inutile utilizzare la chat, dato che già esiste un canale sicuro.
La chat *OTR* (e nello specifico *CryptoCat*) è lo strumento principale che il giornalista americano Glenn Greenwald ha utilizzato per dialogare con Edward Snowden e le altre figure coinvolte nella fuga di notizie.
La scelta del protocollo è stata dettata dal fatto che la NSA americana non dovrebbe essere in grado di decifrare il contenuto dei messaggi scambiati attraverso questo sistema. In alcune conversazioni intercettate infatti risultano diversi omissis riportanti la dicitura *"OC: No decrypt available for this OTR encrypted message."* (`http://fr.slideshare.net/FranckLecluse/media-35552-comint-rel-usa-nsa`).

5.2 PGP e GnuPG

PGP, acronimo di *Pretty Good Privacy*, è un meccanismo di protezione di informazioni digitali mediante chiavi asimmetriche, creato da Phil Zimmermann nel 1991.
Il funzionamento di questo sistema di sicurezza parte dall'assunto che ogni utilizzatore possieda una propria chiave privata, che solo lui conosce, e la rispettiva chiave pubblica a disposizione di chiunque voglia comunicare con lui.
Le due chiavi vengono generate mediante appositi algoritmi matematici in maniera tale che ciò che viene cifrato dalla prima sia decifrabile dalla seconda e viceversa.
Grazie a *PGP* è possibile offrire garanzie di *Privacy* e *Autenticazione* [77], in

modo tale che le informazioni non siano decrittabili da soggetti esterni e che il destinatario abbia la possibilità di verificare eventuali alterazioni subite dal messaggio lungo il canale di trasmissione.
Per garantire la *Privacy* del messaggio, il mittente deve cifrarlo con una chiave simmetrica generata casualmente e successivamente cifrare questa con la chiave pubblica del destinatario, il quale potrà così ottenere la chiave simmetrica decifrandola unicamente con la propria chiave privata.
Nel caso dell'autenticazione invece, viene generato un hash dell'intero messaggio mediante un'apposita funzione. Quest'ultimo viene quindi cifrato con la chiave privata del mittente in modo tale che il destinatario, decifrandolo con la chiave pubblica dell'altro, sia in grado di confrontare questo hash con quello che lui calcola sul messaggio finale. Se i due sono uguali il destinatario ha la garanzia che il messaggio non è stato alterato.
Dal 1993 al 1996 lo US Customs Department ha indagato sul lavoro svolto da Zimmermann e dai sui collaboratori, con l'accusa iniziale di violazione del brevetto a tutela dell'algoritmo RSA sul quale PGP si basa e accusando successivamente Zimmermann dell'esportazione di software crittografico senza licenza [54].
In seguito ai problemi legali dovuti ai brevetti e al crescere dell'importanza di *PGP* a livello mondiale, nel 1997 Zimmermann propose all'IETF le specifiche dello standard *OpenPGP*. Lo standard viene continuamente aggiornato e le ultime specifiche ufficiali rilasciate sono contenute nella *RFC 4880* di novembre 2007 [179], a seguito delle quali diverse istituzioni hanno iniziato a lavorare alle proprie soluzioni compatibili con lo standard.
La Free Software Foundation ha rilasciato nel 1999 la prima versione di *Gnu Privacy Guard* (*GnuPG* o *GPG*) con licenza *GPL*. L'obiettivo era quello di offrire un'alternativa alla suite *PGP* originale, rispettando la RFC ufficiale di *OpenPGP* [182].
Esistono diverse suite basate su *GnuPG* compatibili con i diversi sistemi operativi, che permettono agli utenti finali di utilizzare i vari strumenti crittografici in maniera relativamente semplice.
Diversi ricercatori, sottolineano come oggi in *PGP* siano insite problematiche che non lo rendono più sicuro. Matthew Green della Johns Hopkins University afferma sul suo blog che *"it's time for PGP to die"* [67]. Il ricercatore solleva diversi dubbi circa l'affidabilità di *PGP*; tra questi uno dei più importanti è relativo alla complessità delle chiavi.
Non essendo possibile verificarle manualmente per via dell'enorme lunghezza, risulta necessario fidarsi dei server di chiavi che associano ai vari utenti la rispettiva chiave pubblica. Senza controlli sull'affidabilità del server utilizzato per reperirle, all'utente potrebbe essere restituita una chiave pubblica sbagliata rispetto a quella del destinatario che, se utilizzata per cifrare il messaggio, permetterebbe ad un malintenzionato in possesso della rispettiva chiave privata di decifrarlo.
In seguito alle rivelazioni di Snowden, Phil Zimmerman ha dichiarato in

un'intervista al The Guardian che seppur *PGP* permetta di proteggere il contenuto dei messaggi, non può fare nulla per cifrare i metadati relativi ad essi [78]. Per come sono implementati i principali protocolli, relativi allo scambio di e-mail, sarebbe impossibile secretare informazioni quali mittente, destinatario, ecc. senza inficiare il funzionamento del servizio. Nonostante questa limitazione, per il suo creatore *PGP* resta sicuro ed affidabile.

5.3 Tor

Il progetto *Tor* (*The Onion Router*) nasce nel 2002 con l'idea di rendere anonima la navigazione in rete degli utenti.
Il funzionamento dello strumento si basa sul fatto che i pacchetti, invece di viaggiare in chiaro da un nodo A ad un nodo B, attraversano un percorso casuale di nodi nel mezzo, venendo cifrati ad ogni passaggio con una nuova coppia di chiavi generate di volta in volta.
Il cuore vero e proprio dell'intera infrastruttura sono i nodi ripetitori sui quali viene costruito il percorso, permettendo a questi ultimi di garantire l'anonimato della comunicazione e la cifratura dei dati che li attraversano [111].
È possibile riconoscere 3 tipi principali di nodi che compongono l'architettura di *Tor* [184], ovvero:

- *Nodi Client*, che permettono all'utente di connettersi alla rete *Tor*;
- *Nodi Intermediari*, che compongono i percorsi casuali per i pacchetti, occupandosi di cifrarli con chiavi negoziate con i nodi successivi, sempre interni alla rete;
- *Nodi d'Uscita*, che mettono in contatto con la risorsa richiesta. Questa tratta finale risulta essere anch'essa anonima se la risorsa è interna alla rete Tor altrimenti esiste il pericolo che i pacchetti in chiaro possano essere intercettati.

Alcuni studi hanno evidenziato come il comportamento di alcuni nodi sia diverso rispetto ad altri. Col crescere della popolarità della rete alcuni volontari hanno mantenuto maggiormente online, rispetto ad altri, le proprie macchine per svolgere l'attività di nodo. Questi nodi sono stati identificati come *Super Nodi* ed è stato studiato il loro impatto sull'anonimato della rete [100]. Degli attacchi diretti a questi nodi nevralgici potrebbero mettere in serio pericolo l'anonimato della rete *Tor*.
Diversi documenti trafugati da Edward Snowden, fanno riferimento all'interesse della NSA circa il funzionamento di Tor e la ricerca di vulnerabilità per deanonimizzare gli utenti che ne fanno uso, come ha ben descritto Bruce Schneier in questo articolo [154].
Quello che fa inizialmente la NSA è distinguere gli utenti che si nascondono

attraverso la rete *Tor* da quelli che navigano in chiaro attraverso sistemi più tradizionali. La seconda fase prevede di sfruttare dei server denominati *"Quantum"* che, grazie ad accordi con le compagnie di telecomunicazioni, hanno latenza molto più bassa degli altri server della rete. In questo modo possono fare da intermediari nella comunicazione tra il client e la risorsa, collocandosi in un punto di uscita dal percorso anonimo.
Con questo attacco di tipo *Man-in-the-Middle* l'Agenzia è in grado di ridirigere la macchina dell'utente anonimo ad un ulteriore server, chiamato in codice *"FoxAcid"*, il quale si occupa di infettare il client permettendo all'Agenzia di violarne l'identità.
Sembra inoltre che diversi attacchi informatici subiti dalla rete *Tor* siano stati guidati da NSA e GCHQ per scoprire l'identità di quanti più utenti possibile.

5.4 Telegram

Telegram si presenta come un'applicazione open di instant messaging molto simile a *WhatsApp* e ad altre applicazioni concorrenti, ma integrante caratteristiche di crittografia orientate alla riservatezza delle comunicazioni. È nata nell'agosto del 2013 dal lavoro dei due fratelli russi Nikolai e Pavel Durov anche se, una grande crescita in termini di adozione da parte degli utenti (si parla di diversi milioni) si è verificata solo alcuni mesi più tardi, in seguito all'acquisizione da parte di Facebook della killer-application *WhatsApp* (vedi paragrafo 3.3.1) [46].
Il funzionamento dell'applicativo è molto simile a quello delle altre soluzioni di instant messaging per mobile permettendo l'invio di messaggi, la condivisione di foto, video, posizione, ecc.
La caratteristica interessante che ha incuriosito molti utenti, è però la possibilità di avviare conversazioni cifrate con il proprio interlocutore, permettendo l'oscuramento dei messaggi con crittografia *End-to-End* e la possibilità di iniettare nei pacchetti inviati dei timer per l'autodistruzione. Rispetto alle conversazioni normali che restano salvate in cloud, queste rimangono confinate in locale sui dispositivi dei due utenti coinvolti.
Sul sito ufficiale di *Telegram* sono riportati i principali componenti del protocollo crittografico ovvero: la codifica simmetrica *AES* a *256 bit*, la codifica *RSA* a *2048 bit* e lo scambio di chiavi sicuro *Diffie-Hellman*.
Certi della robustezza del sistema, i due creatori hanno indetto diversi concorsi per cercare di violare il proprio algoritmo, il cui premio previsto è attualmente di 300000$ in *Bitcoin* per chi dovesse riuscire ad estrapolare username e password scambiate tra due utenti attraverso una sezione di chat crittata.
In un articolo apparso sul blog Zimperium Mobile Security, l'utente Zak Avraham spiega come sia riuscito a violare dei messaggi cifrati di *Telegram*, agendo non sul canale di comunicazione, ma direttamente sui dispositivi

mobili sui quali è installato il client analizzando il contenuto della memoria del sistema [15].

5.5 Tox

Attualmente in fase di sviluppo, *Tox* si presenta come un software di messaggistica sicura in quanto integra funzioni crittografiche.
Sul sito ufficiale (`https://tox.im`) gli sviluppatori del progetto dichiarano: *"con l'aumentare dei programmi di monitoraggio da parte del governo, Tox è un'applicazione facile da usare che ti permette di connetterti con gli amici e le persone amate senza nessuno che stia a spiarvi"*. Il loro obiettivo è quindi quello di realizzare un'applicazione che permetta di scambiare messaggi ed effettuare chiamate e videochiamate, garantendo la riservatezza di questi senza però rinunciare all'usabilità grazie ad una GUI di semplice utilizzo.
A seguito della creazione del proprio account, agli utenti vengono assegnate una chiave privata e la rispettiva chiave pubblica; quest'ultima deve essere scambiata con i propri amici per poter quindi essere contattati.
Tox nasce con l'idea di libertà sia in termini commerciali (sarà gratuito e privo di pubblicità), sia in termine di codice, essendo sviluppato con approccio open source per permettere a chiunque di conoscerne ogni singolo aspetto ed eventualmente di modificarlo.
Il diretto concorrente di questo nuovo applicativo è *Skype*, la più famosa soluzione *VoIP* del mercato (oggi di proprietà di Microsoft) che è finita al centro delle cronache a seguito delle rivelazioni di Snowden (vedi paragrafo 3.6.1). Uno dei fondatori di *Tox* ha dichiarato che proprio quanto sollevato dall'ex-agente della NSA li ha spinti a lavorare a questo progetto.
Il protocollo di trasmissione dei dati crittografati sul quale *Tox* si basa non fa uso di un server centrale, ma lavora in modalità *P2P* utilizzando nello specifico il sistema *Perfect Forward Secrecy* [178], il quale dovrebbe garantire che la compromissione di un singolo messaggio non permetta di decifrare gli altri. Come riporta Repubblica [136], l'unico limite attuale è che gli indirizzi IP degli utenti che accedono a *Tox* risultano essere in chiaro, problema facilmente arginabile utilizzando l'applicazione attraverso la rete *Tor*.
Attualmente esistono diversi client sviluppati in parallelo, compatibili con l'architettura di *Tox*, scritti in linguaggi diversi e compatibili con un numero variabile di sistemi operativi.

5.6 Prism-Break

Il sito *Prism-Break* (`https://prism-break.org`) nasce con lo scopo di offrire agli utenti della rete una raccolta delle possibili soluzioni software adottabili

in contesti diversi, per contrastare l'operato delle agenzie come la NSA e garantire l'anonimato nelle diverse attività.
Il creatore di questo portale è Peng Zhong, un designer cinese che ha voluto offrire agli utenti uno strumento semplice per cercare l'applicativo o il servizio più indicato per le proprie necessità, con un occhio di riguardo alle alternative open-source rispetto a quelle proprietarie leader del settore.
Il sito è stato organizzato per poter cercare i software organizzandoli per categoria, per piattaforma o per protocollo utilizzato.

5.7 I2P

Nato dalla community di *Freenet*, l'obiettivo di *I2P* (o the *Invisible Internet Project*) è quello di creare uno strato di rete in cui gli utenti possano comunicare protetti da identificatori crittografici come pseudonimi.
Per comunicare si sfruttano dei tunnel crittati che rappresentano i vari percorsi possibili attraverso i router della rete che instradano i pacchetti. I router da attraversare per un dato tunnel sono decisi dal suo creatore, il quale dovrà condividerne l'identificatore per permettere l'invio dei pacchetti attraverso di esso [34].
Il framework *I2P* è stato scritto principalmente in Java e si basa su due principali protocolli di trasporto *P2P*: *NTCP* e *SSU*, per gestire rispettivamente le comunicazioni *TCP* ed *UDP*.
Il suo elemento principale sono i router *I2P* che, implementandone il protocollo, si occupano di mantenere statistiche sui peer, costruire i tunnel e gestire crittatura e decrittatura [80].
È molto importante comprendere che l'obiettivo di *I2P* non è uguale a quello di *Tor*, motivo per cui ad oggi non ha avuto un'analoga diffusione.
Come spiegato nell'articolo [90] qualsiasi macchina che esegue *I2P* diventa un router dell'intera rete, la quale non è stata pensata per navigare verso l'esterno in maniera anonima, come nel caso di *Tor*, ma per permettere ai partecipanti della rete di scambiare comunicazioni tra di loro.
In questo modo viene ad alimentarsi quello che in gergo è definito *Deep-Web*, un web parallelo rispetto a quello cui si è abituati, fruibile solo attraverso la suddetta intranet.
Tuttavia questo strumento non solo è utilizzato come arma di difesa dallo spionaggio ma, come fa notare Stuart Dredge [45], è sfruttato da molti criminali impossibilitati a vendere merce e "servizi" illegali protetti dall'anonimato alla luce del sole.

5.8 Freenet

La piattaforma *Freenet* è una sorta di sistema di archiviazione distribuito, in cui ogni nodo che la compone memorizza parte dell'informazione allo scopo di renderla decentralizzata e più facilmente proteggibile da attacchi esterni. In questo ambiente *P2P* è possibile sia ricercare che condividere contenuti di vario genere, garantendo l'anonimato dei partecipanti [20].
L'eliminazione invece avviene in maniera automatica raggiunto un certo livello di non consultazione.
Ognuno dei nodi possiede una tabella contenente gli indirizzi dei vicini che compongono la rete per poter propagare la ricerca fino a ritrovare il contenuto di interesse.
La possibilità di condividere materiale di ogni tipo in maniera anonima ha portato però con sè diverse problematiche, infatti attraverso l'infrastruttura virtuale di *Freenet* circolano senza autorizzazione molti contenuti protetti da diritti di copyright.
Rispetto ad altre soluzioni di file-sharing, fermare *Freenet* risulterebbe molto più complesso, in quanto i contenuti si trovano replicati su più nodi e gli utenti sono inconsapevoli di quali file si trovino sulla propria macchina. Questo rende difficile identificare un responsabile reale.
In un'intervista al The Guardian del 2000 [106], Ian Clarke, uno dei fondatori di *Freenet*, aveva dichiarato: *"nessuno - incluso me stesso - può spegnere Freenet. Qualsiasi azione legale contro di me sarebbe ridicola quanto avviare un'azione legale contro il produttore di collant da donna che sono state utilizzate in una rapina in banca"* per spiegare come la natura decentralizzata del sistema renda pressoché impossibile fermarlo.
Come nel caso di altre piattaforme di condivisione in anonimato, anche *Freenet* viene utilizzato come strumento del *Deep-Web* per condividere materiale illegale e sensibile, come ad esempio immagini pedopornografiche. Purtroppo la possibilità di nascondere la propria identità porta i criminali a sfruttare queste soluzioni di anonimato a loro vantaggio.
In risposta a questo problema Clarke spiega come sarebbero in grado di creare un filtro per distruggere questa tipologia di contenuti, tuttavia a quel punto ci sarebbero pressioni da parte di detentori di copyright per fare lo stesso con altre tipologie di contenuti portando infine il sistema stesso a morire [16].

5.9 GNUnet

GNUnet è un framework di rete *P2P* sicuro e decentralizzato, il cui obiettivo è garantire la sicurezza e la privacy degli utenti che ne compongono l'infrastruttura. Ogni utente rappresenta un nodo della rete, il quale possiede una coppia di chiavi attraverso cui vengono cifrate le comunicazioni con gli altri nodi. Lo scambio di messaggi non avviene in maniera diretta ma è

fondamentale il ruolo dei vari nodi come intermediari della comunicazione.
Per conoscere la conformazione della rete viene fatto utilizzo di *Distributed Hash Table (DHT)*, tabelle distribuite tra i vari nodi contenenti informazioni relative ai vicini [180].
Per proteggere il sistema da eventuali attacchi *DoS* di tipo *Flooding* viene utilizzato un sistema di crediti, che vengono assegnati positivamente o negativamente in relazione alle risposte alle query. In questo modo le richieste effettuate dai vari nodi vengono processate secondo la loro priorità.
Alcune possibilità di attacco per violare l'anonimato degli utenti della rete *GNUnet* e per effettuare censura su larga scala sono descritte in [93].

5.10 MaidSafe

MaidSafe è l'acronimo di *Massive Array of Internet Disk - Secure Access For Everyone*.
Si tratta del progetto di una startup scozzese il cui obiettivo è risolvere i problemi di anonimato e sicurezza degli utenti con la realizzazione di una struttura decentralizzata e crittata. L'idea del progetto è spostare l'infrastruttura della rete Internet sulle macchina degli utenti stessi, piuttosto che avere server centrali all'interno dei quali conservare i dati.
All'interno della rete *MaidSafe* ogni contenuto viene suddiviso in 4 chunk, crittati e distribuiti casualmente attraverso i nodi che la compongono, e spostato continuamente da un nodo ad un altro con l'obiettivo di renderne sconosciuta l'ubicazione esatta in un dato momento [7].
I due principali attori del sistema sono la *Safe-Network* e la *Client-Application*.
Con *Safe-Network* si fa riferimento all'intera struttura di storage distribuita tra i nodi che compongono la rete. La *Client-Application* è invece il sistema con il quale gli utenti possono accedere al sistema per condividere e ricercare informazioni.
Essendo che il sistema non fa uso di server centrali, una volta effettuato l'accesso tramite *PIN*, *parola chiave* e *password*, il controllo sull'utente è demandato ai quattro nodi ad esso più vicini che valutano il grado di partecipazione dell'utente alla rete in termini di spazio messo a disposizione per la conservazione di chunk.
I controllori possono variare nel tempo, infatti se dovesse accedere alla rete un nodo più vicino, questo prenderebbe il posto di uno dei quattro. Il concetto di distanza è determinato attraverso un'operazione di *XOR* tra gli indirizzi dei nodi [120].
Nick Lambert, uno dei creatori di *MaidSafe*, ha paragonato il comportamento dei nodi di questa rete a quello delle formiche. Per lui comprendere il concetto di colonia e le sue potenzialità è fondamentale per capire appieno i vantaggi che *MaidSafe* porta con sé. Il funzionamento dei nodi in sinergia tra di loro permetterebbe di superare notevolmente qualsiasi supercomputer [102].

Per ricompensare la partecipazione degli utenti al sistema, mettendo a disposizione potenza di calcolo e spazio di storage, è stato introdotto il *Safecoin*, una critto-valuta simile a *Bitcoin*, la quale può essere scambiata all'interno di questo ambiente come valuta alternativa a quella reale [160].
Proprio per questo elemento è stato fondamentale inserire il sistema di autocontrollo tra nodi descritto sopra, per permettere l'autoregolamentazione della rete senza la necessità di autorità centrali.
Dal punto di vista della sicurezza gli ideatori ritengono che il sistema sia più stabile e protetto rispetto alla struttura classica di Internet, infatti l'utilizzo di un'architettura distribuita piuttosto che centralizzata permette di resistere maggiormente ad attacchi di tipo *DoS*.
Inoltre il continuo spostamento dei chunk e la distribuzione di questi su nodi diversi dovrebbe rendere più complessa l'attività operata da parte di enti come la NSA essendo tutti i dati crittati con algoritmi robusti. Rispetto ad una struttura come quella di *Tor*, dove il monitoraggio potrebbe avvenire a livello dei nodi di uscita, in *MaidSafe* questo non può accadere non essendoci relazione con l'ambiente esterno ma restando tutto confinato alla sua infrastruttura interna.

5.11 Bitcoin

Parlando di *Bitcoin* si fa riferimento ad un protocollo di critto-valuta creato nel 2009 da Satoshi Nakamoto, pseudonimo che sembra essere legato non ad un singolo soggetto ma ad un gruppo, con lo scopo di permettere lo spostamento di valuta elettronica garantendo la privacy degli utilizzatori.
L'idea di Bitcoin è offrire agli utenti la possibilità di operare mediante molteplici portafogli elettronici utilizzando le chiavi private ad essi associate contenute in dei file. Gli utenti diventano quindi responsabili di questi file e del valore dei portafogli ad essi associati.
Per tenere traccia delle transazioni viene fatto uso di una *"Block-Chain"* che, tenendo conto degli indirizzi di ogni singola operazione, permette di tracciare l'ammontare dei vari portafogli, identificati da numeri casuali per garantire l'anonimato [81].
Per ricevere *Bitcoin* gli utenti generano una coppia di chiavi e condividono quella pubblica con cui poter effettuare la cifratura.
Per inviarli invece deve essere avviata una transazione in broadcast attraverso la quale viene verificato il possesso della valuta e viene indicato l'indirizzo del ricevente, che deve comunicare in modalità broadcast il proprio indirizzo per poter essere raggiunto. L'operazione può essere individuata da un "minatore" che si occupa di trasformare la transazione in un blocco, aggiungendovi il proprio indirizzo per poter ricevere una ricompensa per il lavoro svolto [109]. I blocchi creati vengono collocati lungo la *Block-Chain*.
Un'analisi di possibile attacco nei confronti del protocollo *Bitcoin* con lo

scopo di deanonimizzare gli utenti che si trovano dietro *NAT*, analizzando l'indirizzo *IP* delle transazioni, è stato messo in pratica nel lavoro [19].
Negli ultimi anni i *Bitcoin* hanno iniziato ad assumere un valore concreto, iniziando ad essere accettati come valuta da diverse attività di e-commerce ed in alcuni casi anche da attività commerciali fisiche.
Secondo Marshall Van Alstyne il loro successo ed il riconoscimento del loro valore concreto sono dovuti a 4 fattori fondamentali [172]:

- L'utilizzo di chiavi pubbliche associate alle transazioni tutela il legittimo proprietario delle singole "monete" ed impedisce duplicazioni illecite;
- Non sono previste commissioni al contrario delle forme di pagamento elettronico classiche;
- Impediscono operazioni fraudolente da parte dei soggetti coinvolti richiedendo l'autenticazione mediante chiavi pubbliche;
- Il fatto stesso di essere accettati dalle persone porta i *Bitcoin* ad acquisire un valore tangibile.

Probabilmente i *Bitcoin* non sostituiranno le forme di pagamento cui le persone sono abituate in maniera naturale, ma col tempo diventeranno sempre più una valida alternativa di pagamento per le attività in rete.
In particolare un grosso mercato in cui stanno riscontrando successo è quello del *Deep-Web*, dove commerci più o meno leciti sempre più spesso si servono di *Bitcoin* per i pagamenti, forti dell'anonimato garantito da questa crittovaluta.

5.12 File System Crittografici

Scopo dei file system crittografici è offrire agli utenti la possibilità di utilizzare il sistema garantendo protezione dei dati (file e cartelle) mantenendo un costo in termini computazionali accettabile e agendo per quanto possibile in maniera passiva rispetto all'utente.
CFS (Cryptographic File System), descritto in [21] e [1], ad esempio offre possibilità di storage sicuro ed affidabile basandosi su *UNIX*. Viene fatto uso di una chiave per crittare e decrittare i dati, garantendo comunque la possibilità di effettuare operazioni in background quale ad esempio il backup.
Un'ulteriore esempio di file system crittografico, basato su *CFS*, è *TCFS*. L'idea di questo sistema è garantire la crittografia per l'utente in un contesto distribuito [27], dove il file system client deve "fidarsi" del server remoto nelle operazioni di comunicazione.
eCryptfs invece è un file system crittografico che offre funzionalità simili a quelle di *GnuPG*, integrando il servizio di portachiavi del *kernel Linux* ed

ulteriori funzionalità in maniera trasparente rispetto l'utente [75].
In ambito proprietario, Apple ha implementato di default l'attivazione del sistema *File Vault 2* in *Mac OSX 10.10 (Yosemite)* [79], che permette di cifrare completamente il disco di sistema al termine di ogni sessione, utilizzando il proprio *Apple ID* come chiave di sicurezza. Ad ogni avvio del sistema o ripresa dallo stand by viene richiesta la password utente per decifrare i contenuti del disco.
Un sistema analogo viene utilizzato in ambiente mobile con *iOS* dove la *password* del dispositivo (o il *Touch ID* sui dispositivi più recenti) permette di proteggere completamente i file contenuti nel device.

6 Conclusioni

Al termine di questo lungo elaborato, dovendo trarre le somme di quanto visto e approfondito, possiamo dire di aver vissuto questo lavoro su Snowden e sul Datagate con molta passione, in quanto abbiamo avuto la possibilità di andare a fondo, per quanto possibile, ad una vicenda che sicuramente ha sconvolto il mondo intero, anche se con gradi di coinvolgimento differenti.

Edward Snowden è un ragazzo di soli 31 anni che ha messo tutto da parte: libertà personale, lavoro e reputazione per mettere in risalto i programmi di sorveglianza sviluppati dai governi (nello specifico quello statunitense e quello inglese) all'insaputa della popolazione mondiale, essendo per lui la trasparenza un elemento imprescindibile per il corretto funzionamento della società e valendo la pena per questo di rischiare tutto.
Se una sola persona ha potuto sconvolgere il mondo con le proprie rivelazioni, cosa si potrebbe ottenere se ogni giorno ognuno di noi fosse disposto a sacrificare qualcosa, anche di piccolo, in favore della libertà?
Potrebbero essere discutibili i metodi utilizzati dalla talpa della NSA per mettere a conoscenza il mondo intero di ciò che stavano compiendo le agenzie governative; d'altro canto è difficile immaginare strade alternative che l'ex-agente avrebbe potuto seguire per raggiungere il suo scopo.
La linea di demarcazione tra "cosa è giusto" e "cosa è sbagliato" è sottilissima. Indubbiamente l'operazione di trasparenza attuata da Snowden non ha potuto filtrare i destinatari delle rivelazioni, mettendo così al corrente, al pari dei comuni cittadini, anche coloro che agiscono nel male permettendogli di sfruttare queste informazioni per i propri scopi a danno della società.
Per poter esprimere un giudizio è necessario disporre di tutti gli elementi e le informazioni attinenti all'avvenimento; purtroppo per il caso Datagate, seppur presenti in gran numero, ad oggi mancano ancora molti tasselli, come dimostrano le continue news che i giornali pubblicano ogni giorno a distanza ormai di quasi 2 anni dallo scoppio dello scandalo.
Quel che noi meri "spettatori", nonché vittime della vicenda, possiamo fare è prendere una posizione sulla base delle notizie pubblicate fin qui e determinare se siamo disposti ad accettare l'idea di sacrificare la nostra privacy personale sulla base della massima Macchiavelliana *"il fine giustifica i mezzi"*.
Molti hanno visto quanto rivelato da Snowden come la conferma di un sentimento già presente nell'immaginario collettivo, che ogni giorno è supportato dalle teorie complottistiche amplificate dalla "Rete" e dal cinema Hollywoodiano, ricco di trame basate sulle cospirazioni governative.

Le aziende IT coinvolte nello scandalo hanno subìto un danno d'immagine notevole, motivo per cui hanno dovuto investire nel miglioramento e

nell'implementazione di tecnologie di sicurezza, allo scopo di rinsaldare il rapporto di fiducia con i propri clienti che è andato ad incrinarsi in seguito alle rivelazioni.
Le funzionalità di crittografia integrate nei software sono passate dall'essere caratteristiche riservate ad una elité di "addetti ai lavori", ad una feature rappresentativa della buona qualità di un prodotto di massa.
Il grosso problema sollevato dall'introduzione di funzionalità, il cui scopo è quello di nascondere le comunicazioni o l'operato degli utenti, è il fatto che queste diventano disponibili per tutti, a prescindere dall'uso che ne verrà fatto: non sono gli strumenti ad essere pericolosi, bensì i loro utilizzatori. Ciò non può diventare tuttavia una giustificazione per limitare il progresso.

Il CEO della Apple, Tim Cook, nella sua lettera ai clienti ha utilizzato una frase di Metacritic che esprime l'idea formatasi negli ultimi anni in relazione ai principali servizi offerti dal Web 2.0: *"se non paghi per qualcosa, sei tu il prodotto"*. Ciò significa che i dati personali si sono trasformati nella risorsa principale dei colossi operanti nel settore dell'Information Technology.
Gli utenti si sono evoluti così da consumer a prosumer, divenendo i principali creatori dei contenuti per tutte quelle aziende aventi come loro core-business le relazioni sociali (ad esempio Facebook non avrebbe senso di esistere senza il materiale pubblicato quotidianamente dai propri utenti).
È però importante precisare che anche in contesti in cui i servizi sono offerti a pagamento, gli utenti possono comunque diventare una fonte di guadagno per le aziende. Basti pensare a WhatsApp che ha fatto degli utenti il proprio valore, nonostante si paghi il servizio con un abbonamento annuale (seppur dal costo irrisorio).
Allo stesso tempo la gratuità non per forza è sinonimo di un tornaconto sui dati personali degli utilizzatori; infatti in molti contesti open source vengono offerti gratuitamente software e servizi realizzati dalla cooperazione volontaria di individui, il cui scopo è semplicemente quello di fornire alla comunità un'alternativa alle soluzioni commerciali esistenti.
Viene da chiedersi se le aziende aderenti al progetto *PRISM* della NSA avessero almeno una vaga idea della finalità per la quale l'agenzia raccoglieva i dati degli utenti in maniera massiccia ed "ingorda".
Rispetto al passato le agenzie di sicurezza possono contare su approcci meno invasivi dal punto di vista fisico grazie all'utilizzo delle moderne tecnologie informatiche per intercettare le comunicazioni private dei cittadini. Se un tempo era necessario piazzare cimici, sottrarre documenti cartacei, ecc. oggi è sufficiente perpetrare attacchi attraverso la rete Internet, per raccogliere i dati che ognuno di noi dissemina navigando attraverso le infrastrutture che compongono il web.
Le tracce che ognuno di noi lascia quotidianamente, accedendo ai diversi servizi che offre la rete, sono frammentate a tal punto che esercitare il diritto all'oblio per tutti i contenuti a noi connessi risulterebbe praticamente

impossibile, essendosi assottigliata sempre di più la linea di demarcazione tra la nostra vita nel mondo reale e quella nel mondo virtuale.

Purtroppo l'utente medio è molto pigro nel documentarsi e nel cambiare le proprie abitudini, anche dopo aver dichiarato che qualcosa non va. Come emerso dalle risposte fornite attraverso il nostro questionario (vedi paragrafo 4.2), molte persone hanno dimostrato un certo disinteresse di fronte ai fatti messi in evidenza da Snowden, considerando il proprio operato in rete come qualcosa di "non degno di nota". L'affermazione classica che molti hanno fatto, a seguito dello scoppio dello scandalo, è stata: *"tanto io non ho niente da nascondere!"*, non capendo che il problema delle intercettazioni non riguarda unicamente la responsabilità per fatti compiuti, quanto il potere che un governo può avere conoscendo ogni singolo dettaglio della vita di ciascuno dei propri cittadini, potendo reprimere sul nascere ogni forma di opposizione.
In aggiunta è importante sottolineare che spesso le persone sono convinte di agire nella legalità, senza rendersi conto che alcune azioni "quotidiane" da loro compiute ricadono nella categoria degli illeciti. Nel caso dell'Italia nello specifico, a complicare questa situazione interviene anche il contorto sistema legislativo, che lascia spesso spazio ad interpretazioni contrastanti per alcune tipologie di reato.
Un esempio tra tanti è la percezione che molti hanno della condivisione di materiale multimediale in formato digitale. Se in generale si è d'accordo che la pirateria a scopo di lucro sia un'attività illegale, per quanto riguarda il download effettuato per uso personale la situazione diventa più complessa.
La legge originale che tutela il diritto d'autore in Italia è la numero *633 del 22 aprile 1941* [119], aggiornata negli anni, risultando comunque "vecchia" rispetto alla velocità con cui i nuovi strumenti digitali evolvono di giorno in giorno. Se la SIAE si appella a questa ritenendo qualsiasi tipologia di download non autorizzato di materiale protetto da copyright illegale, la Terza Sezione Penale della Corte di Cassazione, con una sentenza del 2007, ha dichiarato legale lo scaricamento per utilizzo privato, condannando tuttavia la condivisione del materiale stesso a fini di lucro [84].
Nei casi in cui la legge risulta difficilmente interpretabile dagli organi giudiziari senza ombra di dubbio, o addirittura adattabile alle situazioni specifiche, le persone sono portate ad avere una percezione confusa e talvolta errata della legalità delle proprie azioni.
Sembra che la maggior parte delle persone abbia passivamente accettato quanto fatto dalle Agenzie di Sicurezza. Cercando su Twitter hashtag come *#snowden*, *#nsa*, *#datagate* abbiamo trovato pochi profili privati che, a distanza di quasi 2 anni dallo scandalo, pubblicano *tweet* sull'argomento; sono principalmente organizzazioni, giornalisti, blogger ed esperti del settore IT a postare oggi contenuti relativi al Datagate, oltre agli attivisti che si battono per la liberazione di Snowden e degli altri whistleblower che hanno avuto un ruolo chiave nella storia digitale recente.

Una ricerca del CIGI, ovvero il Centre for International Governance Innovation canadese, condotta tra il 7 ottobre e il 12 novembre del 2014, denominata "Global Survey on Internet Security and Trust", ha avuto lo scopo di quantificare l?impatto dello scandalo Datagate sulle persone comuni [44].
I risultati, consultabili all'indirizzo `https://www.cigionline.org/internet-survey`, mostrano come il 60% degli intervistati sia a conoscenza della figura di Edward Snowden, dei quali soltanto il 39% ha effettivamente fatto qualcosa per proteggersi contro le intercettazioni di massa. Il campione analizzato dal CIGI è composto da 23376 persone distribuite in 24 paesi, un numero ristretto paragonato alla totalità della popolazione mondiale.
Una visione contrastante è quella di Bruce Schneier, un crittografo e saggista IT statunitense, che nel suo blog non solo ha dichiarato di essere in disaccordo con le ricerche effettuate dal CIGI, oltre ad accusarli di aver male interpretato i dati raccolti, ma sottolinea come invece le rivelazioni di Snowden abbiano avuto un enorme impatto. Secondo i suoi calcoli, seppur la maggior parte delle persone non si sia opposta in maniera marcata alla sorveglianza di massa, circa 750 milioni di persone hanno evidenziato attraverso il questionario il loro disagio relativo alle intercettazioni subite, dichiarando di essersi in qualche modo impegnate per contrastarle [155].
Tuttavia, alla luce degli articoli analizzati relativi allo scandalo riguardanti l'Europa, e più nello specifico il nostro Paese, sembrerebbe vero quel che la ricerca del CIGI ha sottolineato, cioè che quanto rivelato dall'ex-agente della NSA non abbia sortito l'effetto da lui sperato. In seguito al boom iniziale, l'interesse dell'opinione pubblica verso questi argomenti è sfumato in favore di altri fatti di cronaca, rendendo il Datagate appannaggio di una ristretta cerchia di esperti ed interessati alla questione. Nonostante continuino ad uscire notizie riguardanti lo scandalo, il loro clamore non è mai sufficiente a portarle al centro dell'attenzione della collettività.
Una testimonianza di ciò, che ci ha letteralmente sconvolto, è il fatto che cercando su Twitter l'hashtag *#prism*, i *tweet* relativi al programma di intercettazione realizzato dalla NSA hanno un peso uguale, se non inferiore, a quelli riguardanti l'ultimo album discografico pubblicato dalla cantante pop Katy Perry.

La giustificazione che i governi riportano a favore dei loro programmi di sorveglianza è la lotta al terrorismo: considerando il largo utilizzo che certe organizzazioni criminali fanno della rete per diffondere la propria propaganda, com'è possibile che la NSA e il GCHQ, col potenziale delle tecnologie a loro disposizione che gli permette di intercettare "tutto di tutti", non siano in grado di prevenire fatti gravi come l'attentato al giornale francese Charlie Hebdo, nel pieno centro di Parigi, o l'attacco ai turisti occidentali nel Museo del Bardo di Tunisi?
Che senso ha quindi violare la privacy di miliardi di persone se in questo

modo non si è in grado di fermare quei pochi che davvero minacciano la "Sicurezza Nazionale"?
Che si abbia una posizione favorevole o contraria rispetto all'operato delle agenzie governative, non ci sono dubbi che queste abbiano oggi gli strumenti per poter "controllare il presente".
George Orwell in *1984* scriveva: *"chi controlla il passato controlla il futuro e chi controlla il presente controlla il passato"*. Speriamo non sia questo l'intento dei moderni "Grandi Fratelli".

Riferimenti bibliografici

[1] Mohammad Reza Abbasy, Mahdi Sharifi, and Mohammad Reza Najaf Torkaman. Cryptographic file system: easy and reliable? *International Journal of Information and Electronics Engineering*, 3(6), Novembre 2013.

[2] Spencer Ackerman. US tech giants knew of NSA data collection, agency's top lawyer insists. `http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de`, Marzo 2014. [Online; ultimo accesso 15-marzo-2015].

[3] Spencer Ackerman and James Ball. Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ. `http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo`, Febbraio 2014. [Online; ultimo accesso 12-marzo-2015].

[4] Spencer Ackerman and Dominic Rushe. Microsoft, Facebook, Google and Yahoo release US surveillance requests. `http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests`, Febbraio 2014. [Online; ultimo accesso 13-marzo-2015].

[5] ACLU. Reform the Patriot Act | Section 215. `https://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-section-215`. [Online; ultimo accesso 03-marzo-2015].

[6] Chris Alexander and Ian Goldberg. Improved user authentication in Off-the-Record messaging. In *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, pages 41–47. ACM, 2007.

[7] Martin Anderson. Is MaidSafe 'Internet 2.0' or 'Internet too'? `http://thestack.com/maidsafe-bitcloud-internet-090215`, Febbraio 2015. [Online; ultimo accesso 05-marzo-2015].

[8] Alessandro Andriolo. Privacy sulla "nuvola", Microsoft aderisce allo standard ISO. `http://www.ictbusiness.it/cont/news/privacy-sulla-nuvola-microsoft-aderisce-allo-standard-iso/34024/1.html#.VQL360IV5CP`, Febbraio 2015. [Online; ultimo accesso 13-marzo-2015].

[9] Charles Arthur. iPhone keeps record of everywhere you go. `http://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears`, Aprile 2011. [Online; ultimo accesso 11-marzo-2015].

[10] Charles Arthur. Ex-Microsoft privacy adviser: I don't trust company. `http://www.theguardian.com/world/2013/sep/30/microsoft-privacy-chief-nsa`, Ottobre 2013. [Online; ultimo accesso 12-marzo-2015].

[11] Charles Arthur. Microsoft joins Google in demanding to disclose FISA requests. `http://www.theguardian.com/technology/2013/jun/28/microsoft-google-fisa-united-states-government`, Giugno 2013. [Online; ultimo accesso 13-marzo-2015].

[12] Charles Arthur. Skype: has Microsoft's $8.5bn spending paid off yet - and can it? `http://www.theguardian.com/technology/2013/aug/30/skype-microsoft-acquisition-analysis`, Agosto 2013. [Online; ultimo accesso 14-marzo-2015].

[13] Charles Arthur. Apple's Tim Cook attacks Google and Facebook over privacy flaws. http://www.theguardian.com/technology/2014/sep/18/apple-tim-cook-google-facebook-privacy-surveillance, Settembre 2014. [Online; ultimo accesso 16-marzo-2015].

[14] Charles Arthur and Dominic Rushe. NSA scandal: Microsoft and Twitter join calls to disclose data requests. `http://www.theguardian.com/world/2013/jun/12/microsoft-twitter-rivals-nsa-requests`, Giugno 2013. [Online; ultimo accesso 13-marzo-2015].

[15] Zuk Avraham. How I hacked Telegram's "encryption". http://blog.zimperium.com/telegram-hack/, Febbraio 2015. [Online; ultimo accesso 04-marzo-2015].

[16] Andy Beckett. The dark side of the Internet. http://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet, Novembre 2009. [Online; ultimo accesso 04-marzo-2015].

[17] Ron Bell. Shedding light on the Foreign Intelligence Surveillance Court (FISC): court findings from our 2007-2008 case. http://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence, Settembre 2014. [Online; ultimo accesso 10-marzo-2015].

[18] Noam Benjamin. Merkel caccia il capo della Cia: "Chi ci spia spreca energie". http://www.ilgiornale.it/news/merkel-caccia-capo-cia-chi-ci-spia-spreca-energie-1036535.html, Luglio 2014. [Online; ultimo accesso 30-marzo-2015].

[19] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 15–29. ACM, 2014.

[20] Bartosz Biskupski, Jim Dowling, and Jan Sacha. Properties and mechanisms of self-organizing MANET and P2P systems. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 2(1):1, 2007.

[21] Matt Blaze. A cryptographic file system for UNIX. In *Proceedings of the 1st ACM conference on Computer and communications security*, pages 9–16. ACM, 1993.

[22] Blitz Quotidiano. Datagate: la richiesta Usa a Telecom ('98) per l'accesso ai cavi di Palermo. http://www.blitzquotidiano.it/politica-mondiale/datagate-richiesta-usa-telecom-cavi-palermo-1701705/, Ottobre 2013. [Online; ultimo accesso 20-marzo-2015].

[23] Carlo Bonini. Datagate, ecco come gli USA spiano l'Italia: "Ma lo facciamo solo per proteggervi". http://www.repubblica.it/politica/2013/10/23/news/ecco_come_gli_usa_spiano_l_italia_ma_lo_facciamo_solo_per_proteggervi-69226215/, Ottobre 2013. [Online; ultimo accesso 19-marzo-2015].

[24] Nikita Borisov, Ian Goldberg, and Eric Brewer. Off-the-Record communication, or, why not to use PGP. In *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, pages 77–84. ACM, 2004.

[25] Domenico Camodeca. Kerry in Italia: Letta succube degli USA sul Datagate. http://www.informazioneweb.org/notizie/politica/3143-kerry-in-italia-letta-succube-degli-usa-sul-datagate.html, Ottobre 2013. [Online; ultimo accesso 20-marzo-2015].

[26] Rory Carroll. Google chairman: NSA spying on our data centres 'outrageous'. http://www.theguardian.com/technology/2013/nov/04/eric-schmidt-nsa-spying-data-centres-outrageous, Novembre 2013. [Online; ultimo accesso 15-marzo-2015].

[27] Giuseppe Cattaneo, Luigi Catuogno, Aniello Del Sorbo, and Pino Persiano. The design and implementation of a transparent cryptographic file system for UNIX. In *USENIX Annual Technical Conference, FREENIX Track*, pages 10–3. Citeseer, 2001.

[28] Fabio Chiusi. *Grazie Mr. Snowden*. Messaggero Veneto, 2014.

[29] Barbara Ciolli. Datagate, cosìPutin dà scacco a Obama. http://www.lettera43.it/politica/datagate-cosi-putin-da-scacco-a-obama_43675104228.htm, Agosto 2013. [Online; ultimo accesso 18-marzo-2015].

[30] Corriere della Sera. Italia-USA, Letta riceve John Kerry: «Datagate, fare luce sulle violazioni». http://www.corriere.it/cronache/13_ottobre_23/italia-usa-john-kerry-incontra-letta-tavolo-anche-dossier-datagate-12583b08-3baf-11e3-ac98-5d5614d1875c.shtml, Ottobre 2013. [Online; ultimo accesso 20-marzo-2015].

[31] Corriere della Sera. Merkel sul Datagate: «Spiare non è accettabile». E Letta: «Non possiamo tollerare zone d'ombra». http://www.corriere.it/esteri/13_ottobre_24/nsagate-germania-convoca-ambasciatore-usa-9f13fc34-3c87-11e3-b96f-84c91179c77b.shtml, Ottobre 2013. [Online; ultimo accesso 18-marzo-2015].

[32] Simone Cosimi. NSA, quei meeting segreti con Google & co. Le relazioni con le big company. http://www.repubblica.it/tecnologia/2014/05/06/news/nsa_google_relazioni_pericolose-85389964/, Maggio 2014. [Online; ultimo accesso 15-marzo-2015].

[33] Scott E Coull and Kevin P Dyer. Traffic analysis of encrypted messaging services: Apple iMessage and beyond. *ACM SIGCOMM Computer Communication Review*, 44(5):5–11, 2014.

[34] Ryan Craven, Christopher Abbott, Harikrishnan Bhanu, Juan Deng, and Richard R Brooks. Orwell was an optimist. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, page 57. ACM, 2010.

[35] David Crowe and Wasim A Al-Hamdani. Google privacy: something for nothing? In *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference*, page 27. ACM, 2013.

[36] Data Manager Online. L'effetto Snowden un anno dopo le rivelazioni. http://www.datamanager.it/news/l-effetto-snowden-un-anno-dopo-le-rivelazioni-56992.html, Giugno 2014. [Online; ultimo accesso 20-marzo-2015].

[37] Dario D'Elia. Patriot Act francese: super poteri di spionaggio digitale, senza mandato del giudice. http://www.tomshw.it/news/patriot-act-francese-super-poteri-di-spionaggio-digitale-senza-mandato-del-giudice-64909, Marzo 2015. [Online; ultimo accesso 17-marzo-2015].

[38] Philip Di Salvo. Wired intervista Julian Assange: "Google è la versione privata della NSA". http://www.wired.it/attualita/politica/2014/09/18/julian-assange-google-nsa/, Settembre 2014. [Online; ultimo accesso 16-marzo-2015].

[39] Alban Diquet, David Thiel, and Scott Stender. Open technology fund CryptoCat iOS - Application penetration test. Technical report, iSEC Partners Inc., 2014.

[40] Peter Dorfinger, Georg Panholzer, Brian Trammell, and Teresa Pepe. Entropy-based traffic filtering to support real-time skype detection. In *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*, pages 747–751. ACM, 2010.

[41] Gianluca Dotti. Governo USA, minacce a Yahoo per sostenere il progetto PRISM. http://www.wired.it/attualita/tech/2014/09/12/governo-usa-minacciava-yahoo-prism/, Settembre 2014. [Online; ultimo accesso 10-marzo-2015].

[42] Stuart Dredge. Apple adds new rules on children's apps to iOS developer guidelines. http://www.theguardian.com/technology/2013/aug/15/apps-apple, Agosto 2013. [Online; ultimo accesso 11-marzo-2015].

[43] Stuart Dredge. Microsoft's Satya Nadella: governments must restore trust in technology. http://www.theguardian.com/technology/2013/dec/10/microsoft-satya-nadella-surveillance-ceo-governments-nsa, Dicembre 2013. [Online; ultimo accesso 13-marzo-2015].

[44] Stuart Dredge. Edward Snowden revelations have had limited effect on privacy – Open thread. http://www.theguardian.com/technology/2014/nov/25/edward-snowden-privacy-open-thread, Novembre 2014. [Online; ultimo accesso 09-aprile-2015].

[45] Stuart Dredge. How you could become a victim of cybercrime in 2015. http://www.theguardian.com/technology/2014/dec/24/cybercrime-2015-cybersecurity-ransomware-cyberwar, Dicembre 2014.

[46] Stuart Dredge. Messaging app Telegram added 5m new users the day after WhatsApp outage. http://www.theguardian.com/technology/2014/feb/24/telegram-messaging-app-whatsapp-down-facebook, Febbraio 2014. [Online; ultimo accesso 04-marzo-2015].

[47] Daniel Ellsberg. Stasi Unita d'America. http://temi.repubblica.it/micromega-online/stasi-unita-damerica/?printpage=undefined, Giugno 2013. [Online; ultimo accesso 05-marzo-2015].

[48] FBClaim. Facebook to face 25,000 users in court: first hearing of european privacy class action in april. http://www.europe-v-facebook.org/pa_vbs_en.pdf, Gennaio 2015. [Online; ultimo accesso 12-marzo-2015].

[49] Roberto Festa. Pulitzer 2014, premiati Guardian e Washington Post per lo scoop su Datagate. http://www.ilfattoquotidiano.it/2014/04/15/pulitzer-2014-premiati-guardian-e-washington-post-per-scoop-su-datagate/951916/, Aprile 2014. [Online; ultimo accesso 27-marzo-2015].

[50] Klint Finley. Google renews battle with the NSA by open sourcing email encryption tool. http://www.wired.com/2014/06/end-to-end/, Giugno 2014. [Online; ultimo accesso 16-marzo-2015].

[51] Ryan Gallagher. How secret partners expand NSA's surveillance Dragnet. https://firstlook.org/theintercept/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/, Giugno 2014. [Online; ultimo accesso 14-marzo-2015].

[52] Ryan Gallagher. Operation AURORAGOLD how the NSA hacks cellphone network worldwide. https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/, Dicembre 2014. [Online; ultimo accesso 17-marzo-2015].

[53] Ryan Gallagher and Glenn Greenwald. How the NSA plans to infect 'millions' of computers with malware. https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/, Dicembre 2014. [Online; ultimo accesso 12-marzo-2015].

[54] Simson Garfinkel. Pretty Good Privacy (PGP). In John Wiley and Sons Ltd., editors, *Encyclopedia of Computer Science*, pages 1421–1422. John Wiley and Sons Ltd., 4th edition, 2003.

[55] Juliette Garside. Apple, Google and AT&T meet Obama to discuss NSA surveillance concerns. http://www.theguardian.com/technology/2013/aug/09/nsa-surveillance-apple-google-obama, Agosto 2013. [Online; ultimo accesso 16-marzo-2015].

[56] Juliette Garside. Investors: AT&T and Verizon must say how much customer data goes to NSA. http://www.theguardian.com/business/2013/nov/21/investors-att-verizon-customer-data-nsa, Novembre 2013. [Online; ultimo accesso 16-marzo-2015].

[57] Garzanti Linguistica. Privacy. http://www.garzantilinguistica.it/ricerca/?q=privacy, 2015. [Online; ultimo accesso 04-febbraio-2015].

[58] GCHQ. Exploiting Facebook traffic in the passive environment to obtain specific information. https://www.aclu.org/files/natsec/nsa/20140722/Exploiting%20Facebook%20Traffic%20in%20the%20Passive%20Environment%20to%20Obtain%20Specific%20Information.pdf.

[59] Barton Gellman and Ashkan Soltani. NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html, Ottobre 2013. [Online; ultimo accesso 10-marzo-2015].

[60] Barton Gellman, Ashkan Soltani, and Andrea Peterson. How we know the NSA had access to internal Google and Yahoo cloud data. http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/, Novembre 2013. [Online; ultimo accesso 10-marzo-2015].

[61] Andrea Gentili. Datagate: in UK lo spionaggio virtuale è legale, ma in Italia si prepara la costituzione dei diritti digitali. http://ilreferendum.it/2014/06/20/datagate-in-uk-lo-spionaggio-virtuale-e-legale-ma-in-italia-si-prepara-la-costituzione-dei-diritti-digitali/, Giugno 2014. [Online; ultimo accesso 20-marzo-2015].

[62] Samuel Gibbs. Facebook, Google and Apple lobby for curb to NSA surveillance. http://www.theguardian.com/technology/2014/nov/17/facebook-google-apple-lobby-senate-nsa-surveillance, Novembre 2014. [Online; ultimo accesso 11-marzo-2015].

[63] Samuel Gibbs. Facebook implementing 'privacy checkup' for users sharing publicly. http://www.theguardian.com/technology/2014/apr/09/facebook-privacy-checkup-for-users-sharing-publicly, Aprile 2014. [Online; ultimo accesso 12-marzo-2015].

[64] Samuel Gibbs. Facebook's privacy policy breaches European law, report finds. http://www.theguardian.com/technology/2015/feb/23/facebooks-privacy-policy-breaches-european-law-report-finds, Febbraio 2015. [Online; ultimo accesso 13-marzo-2015].

[65] Samuel Gibbs. Kim Dotcom launches end-to-end encrypted voice chat 'Skype killer'. http://www.theguardian.com/technology/2015/jan/22/kim-dotcom-launches-encrypted-voice-chat-skype-killer, Gennaio 2015. [Online; ultimo accesso 14-marzo-2015].

[66] Dan Gillmor. Mark Zuckerberg called Obama about the NSA. Let's not hang up the phone. http://www.theguardian.com/commentisfree/2014/mar/13/mark-zuckerberg-obama-nsa-facebook-message, Marzo 2014. [Online; ultimo accesso 12-marzo-2015].

[67] Matthew Green. What's the matter with PGP? http://blog.cryptographyengineering.com/2014/08/whats-matter-with-pgp.html, Agosto 2014. [Online; ultimo accesso 03-marzo-2015].

[68] Andy Greenberg. Despite Apple's privacy pledge, cops can still pull data off a locked iPhone. http://www.wired.com/2014/09/apple-iphone-security/, Settembre 2014. [Online; ultimo accesso 10-marzo-2015].

[69] Glenn Greenwald. NSA collecting phone records of millions of Verizon customers daily. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, Giugno 2013. [Online; ultimo accesso 16-marzo-2015].

[70] Glenn Greenwald. *No Place to Hide - Sotto Controllo: Edward Snowden e la sorveglianza di massa*. Rizzoli, 2014.

[71] Glenn Greenwald. The inhumane conditions of Bradley Manning's detention. http://www.salon.com/2010/12/15/manning_3/, Dicembre 2015. [Online; ultimo accesso 06-marzo-2015].

[72] Glenn Greenwald and Ewen MacAskill. NSA Prism program taps in to user data of Apple, Google and others. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, Giugno 2013. [Online; ultimo accesso 10-marzo-2015].

[73] Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe. Microsoft handed the NSA access to encrypted messages. http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data, Luglio 2013. [Online; ultimo accesso 12-marzo-2015].

[74] Ken Gude. The FBI is dead wrong: Apple's encryption is clearly in the public interest. http://www.wired.com/2014/10/fbi-is-wrong-apple-encryption-is-good/, Ottobre 2014. [Online; ultimo accesso 10-marzo-2015].

[75] Michael Austin Halcrow. eCryptfs: an enterprise-class encrypted filesystem for linux. In *Proceedings of the 2005 Linux Symposium*, volume 1, pages 201–218, 2005.

[76] Robert Hannigan. Welcome to GCHQ. http://www.gchq.gov.uk/who_we_are/Pages/welcome-to-GCHQ-from-Robert-Hannigan.aspx. [Online; ultimo accesso 19-febbraio-2015].

[77] Kevin Henry. Getting started with PGP. *Crossroads*, 6(5):8, 2000.

[78] Alex Hern. Email surveillance could reveal journalists' sources, expert claims. http://www.theguardian.com/technology/2013/sep/30/email-surveillance-could-reveal-journalists-sources-expert-claims, Settembre 2013. [Online; ultimo accesso 03-marzo-2015].

[79] Alex Hern. Apple defies FBI and offers encryption by default on new operating system. http://www.theguardian.com/technology/2014/oct/17/apple-defies-fbi-encryption-mac-osx, Ottobre 2014. [Online; ultimo accesso 07-marzo-2015].

[80] Michael Herrmann and Christian Grothoff. Privacy-implications of performance-based peer selection by onion-routers: a real-world case study using I2P. In *Privacy Enhancing Technologies*, pages 155–174. Springer, 2011.

[81] Dominic Hobson. What is bitcoin? *ACM Crossroads*, 20(1):40–44, 2013.

[82] Mark Honigsbaum and Duncan Campbell. Microsoft's 'secret link to Big Brother'. http://www.theguardian.com/technology/1999/sep/05/microsoft.business, Settembre 1999. [Online; ultimo accesso 12-marzo-2015].

[83] Sandro Iannaccone. Come funziona PRISM, il programma che spia web e telefoni. http://daily.wired.it/news/tech/2013/06/10/nsa-prism-obama-462785.html, Giugno 2013. [Online; ultimo accesso 03-marzo-2015].

[84] Il Sole 24 Ore. Scaricare da Internet file protetti non è reato se non ci si guadagna. http://www.ilsole24ore.com/art/SoleOnLine4/Attualita%20ed%20Esteri/Attualita/2007/01/Pirateria-Cassazione.shtml?uuid=ebcaf9a8-a89e-11db-aee1-00000e25108c&, Gennaio 2007. [Online; ultimo accesso 09-aprile-2015].

[85] Internazionale. Cosa ha detto Letta alla camera sul caso Datagate. http://archivio.internazionale.it/news/italia/2013/11/20/cosa-ha-detto-letta-alla-camera-sul-caso-datagate, Novembre 2013. [Online; ultimo accesso 20-marzo-2015].

[86] Adrianne Jeffries. Escape from PRISM: how Twitter defies government data-sharing. http://www.theverge.com/2013/6/13/4426420/twitter-prism-alex-macgillivray-NSA-government, Giugno 2013. [Online; ultimo accesso 11-marzo-2015].

[87] Poul-Henning Kamp, Jim Waldo, Alan Ramos, Weina Scott, William Scott, Doug Lloyd, Katherine O'Leary, Whitfield Diffie, Susan Landau, and Katie Shilton. More encryption is not the solution. *ACM Queue*, 11(7):10, 2013.

[88] John Kiriakou. Obama's abuse of the Espionage Act is modern-day McCarthyism. `http://www.theguardian.com/commentisfree/2013/aug/06/obama-abuse-espionage-act-mccarthyism`, Agosto 2013. [Online; ultimo accesso 03-marzo-2015].

[89] Jemima Kiss. Twitter adds more security to thwart predators – and government agencies. `http://www.theguardian.com/technology/2013/nov/23/twitter-security-google-facebook-data-nsa`, Novembre 2013. [Online; ultimo accesso 11-marzo-2015].

[90] Kate Knibbs. I2P: the super-anonymous network that silk road calls home. `http://gizmodo.com/i2p-the-super-anonymous-network-that-silk-road-calls-h-1680940282`, Gennaio 2015. [Online; ultimo accesso 04-marzo-2015].

[91] David Kravets. Facebook gave 38K users' data to governments in 6 months. `http://www.wired.com/2013/08/facebook-divulged-user-data/`, Agosto 2013. [Online; ultimo accesso 13-marzo-2015].

[92] Ku Leuven. ICRI/CIR and iMinds-SMIT advise Belgian Privacy Commission in Facebook investigation. `http://www.law.kuleuven.be/icri/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation`, Febbraio 2015. [Online; ultimo accesso 13-marzo-2015].

[93] Dennis Kügler. An analysis of gnunet and the implications for anonymous, censorship-resistant networks. In *Privacy Enhancing Technologies*, pages 161–176. Springer, 2003.

[94] La Repubblica. Datagate, Obama annulla incontro con Putin. Presidente Usa parteciperà a G20 in Russia. `http://www.repubblica.it/esteri/2013/08/07/news/datagate_obama_annulla_incontro_con_putin-64428627/`, Agosto 2013. [Online; ultimo accesso 18-marzo-2015].

[95] La Stampa. Datagate, smacco per Obama: il Senato Usa boccia la riforma della NSA. `http://www.lastampa.it/2014/11/19/esteri/datagate-riforma-nsa-bocciata-al-senato-usa-Hz29jHK5wJVXE3yUZk5HEK/pagina.html`, Novembre 2014. [Online; ultimo accesso 16-marzo-2015].

[96] Stevens Le Blond, Chao Zhang, Arnaud Legout, Keith Ross, and Walid Dabbous. I know where you are and what you are sharing: exploiting P2P communications to invade users' privacy. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pages 45–60. ACM, 2011.

[97] Ben Lee. Taking the fight for #transparency to court. `https://blog.twitter.com/2014/taking-the-fight-for-transparency-to-court`, Ottobre 2014. [Online; ultimo accesso 11-marzo-2015].

[98] Lettera 43. Datagate, Francia e Germania vogliono un codice etico dello spionaggio. `http://www.lettera43.it/politica/datagate-francia-e-germania-vogliono-un-codice-etico-dello-spionaggio_43675111959.htm`, Ottobre 2013. [Online; ultimo accesso 19-marzo-2015].

[99] Lettera 43. Datagate, Germania prepara 2 mila cellulari anti spie. `http://www.lettera43.it/cronaca/datagate-germania-prepara-2-mila-cellulari-anti-spie_43675136393.htm`, Luglio 2014. [Online; ultimo accesso 19-marzo-2015].

[100] Chenglong Li, Yibo Xue, Yingfei Dong, and Dongsheng Wang. Super nodes in Tor: existence and security implication. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 217–226. ACM, 2011.

[101] Patrizia Licata. Tutti gli attriti fra Cook (Apple) e Zuckerberg (Facebook). http://www.formiche.net/2014/12/09/apple-cook-zuckerberg-facebook-attriti/, Dicembre 2014. [Online; ultimo accesso 13-marzo-2015].

[102] Natasha Lomas. The server needs to die to save the Internet. http://techcrunch.com/2014/07/23/maidsafe/, Luglio 2014. [Online; ultimo accesso 06-marzo-2015].

[103] Ewen MacAskill and Dominic Rushe. Snowden document reveals key role of companies in NSA data collection. http://www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms, Novembre 2013. [Online; ultimo accesso 12-marzo-2015].

[104] Sanchez Manning. British spies at GCHQ 'spied on foreign politicians at G20 summit meetings in London'. http://www.independent.co.uk/news/uk/home-news/british-spies-at-gchq-spied-on-foreign-politicians-at-g20-summit-meetings-in-london-8661182.html, Giugno 2013. [Online; ultimo accesso 25-marzo-2015].

[105] Marco Vigevani Agenzia Letteraria. No Place to Hide: il libro inchiesta di Glenn Greenwald su Edward Snowden. http://www.marcovigevani.com/no-place-to-hide-il-libro-inchiesta-di-glenn-greenwald-su-edward-snowden/, Maggio 2014. [Online; ultimo accesso 27-marzo-2015].

[106] Jane Martinson. Freenet takes music copyright battle to US. http://www.theguardian.com/technology/2000/aug/01/copyright.efinance, Agosto 2000. [Online; ultimo accesso 04-marzo-2015].

[107] Robert McMillan. Apple finally reveals how long Siri keeps your data. http://www.wired.com/2013/04/siri-two-years/, Aprile 2013. [Online; ultimo accesso 11-marzo-2015].

[108] Riccardo Meggiato. Datagate, il ruolo di Apple negli iPhone violati dall'NSA. http://www.wired.it/attualita/tech/2014/01/02/datagate-ruolo-apple-iphone-violati-da-nsa/, Gennaio 2014. [Online; ultimo accesso 10-marzo-2015].

[109] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of Bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140. ACM, 2013.

[110] Randy Milch. From the desk of Randy Milch. http://publicpolicy.verizon.com/blog/entry/from-the-desk-of-randy-milch, Giugno 2013. [Online; ultimo accesso 16-marzo-2015].

[111] Kelley Misata. The Tor project: an inside view. *XRDS: Crossroads, The ACM Magazine for Students*, 20(1):45–47, 2013.

[112] Arshad Mohammed. Verizon says it did not give customer records to NSA. http://www.washingtonpost.com/wp-dyn/content/article/2006/05/16/AR2006051601749.html, Maggio 2006. [Online; ultimo accesso 16-marzo-2015].

[113] Giuditta Mosca. In 25mila contro Facebook: la più grande class action europea in aula il 9 aprile a Vienna. http://www.wired.it/internet/social-network/2015/02/02/class-action-europa-vs-facebook/, Febbraio 2015. [Online; ultimo accesso 12-marzo-2015].

[114] John Naughton. Google privacy ruling is just the thin end of a censorship wedge. http://www.theguardian.com/technology/2014/may/17/google-privacy-ruling-thin-end-censorship-wedge, Maggio 2014. [Online; ultimo accesso 15-marzo-2015].

[115] NSA. NSA/CSS Mission, Vision, Values. https://www.nsa.gov/about/values/index.shtml. [Online; ultimo accesso 19-febbraio-2015].

[116] NSA. XKEYSCORE. https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf, Febbraio 2008. [Online; ultimo accesso 03-marzo-2015].

[117] NSA. BLARNEY exploits the social network via expanded Facebook collection. https://www.aclu.org/files/natsec/nsa/20140722/BLARNEY%20Exploits%20the%20Social%20Network%20via%20Expanded%20Facebook%20Collection.pdf, Marzo 2011. [Online; ultimo accesso 03-marzo-2015].

[118] NSA. PRISM/US-984XN Overview or the SIGAD used most in NSA reporting overview. https://s3.amazonaws.com/s3.documentcloud.org/documents/813847/prism.pdf, Aprile 2013. [Online; ultimo accesso 03-marzo-2015].

[119] Parlamento Italiano. Legge a protezione del diritto d'autore e di altri diritti connessi al suo esercizio. http://www.altalex.com/index.php?idnot=34610, Febbraio 2015. [Online; ultimo accesso 09-aprile-2015].

[120] Greig Paul and James Irvine. A protocol for storage limitations and upgrades in decentralised networks. In *Proceedings of the 7th International Conference on Security of Information and Networks*, page 69. ACM, 2014.

[121] Rand Paul. NSA's Verizon surveillance: how the White House tramples our constitution. http://www.theguardian.com/commentisfree/2013/jun/07/nsa-verizon-surveillance-constitution, Giugno 2013. [Online; ultimo accesso 16-marzo-2015].

[122] Andrea Persons. German government to drop Verizon over NSA spying fears. http://www.washingtonpost.com/blogs/the-switch/wp/2014/06/26/german-government-to-drop-verizon-over-nsa-spying-fears/, Giugno 2014. [Online; ultimo accesso 19-marzo-2015].

[123] Matthew Phillips. Freedom of information act request and request for expedited processing. http://www.wired.com/images_blogs/threatlevel/2010/02/nsa-google_foia_request.pdf, Febbraio 2010. [Online; ultimo accesso 15-marzo-2015].

[124] @pod2g and gg. iMessage privacy. Technical report, Quarkslab Innovative Security, Ottobre 2013.

[125] Valerio Porcu. WhatsApp: rispettiamo la privacy anche con Facebook. http://www.tomshw.it/cont/news/whatsapp-rispettiamo-la-privacy-anche-con-facebook/54415/1.html, Marzo 2014. [Online; ultimo accesso 13-marzo-2015].

[126] Silvia Ragusa. Datagate, "in Spagna 60 milioni di intercettazioni in un mese". http://www.ilfattoquotidiano.it/2013/10/28/datagate-in-spagna-60-milioni-di-intercettazioni-in-mese/759374/, Ottobre 2013. [Online; ultimo accesso 17-marzo-2015].

[127] Federico Rampini. *Rete Padrona - Amazon, Apple, Google & co. Il volto oscuro della rivoluzione digitale.* Feltrinelli Fuochi, Settembre 2014. [Online; ultimo accesso 12-marzo-2015].

[128] Elena Re Garbagnati. WhatsApp quasi pronta a telefonare, per Facebook bufera privacy in vista. http://www.tomshw.it/cont/news/whatsapp-quasi-pronta-a-telefonare-per-facebook-bufera-privacy-in-vista/62266/1.html, Febbraio 2015. [Online; ultimo accesso 13-marzo-2015].

[129] Repubblica.it. Datagate, polemica Francia-USA. 70 milioni di chiamate intercettate. http://www.repubblica.it/esteri/2013/10/21/news/datagate_registrate_milioni_di_telefonate_francesi_parigi_scioccante_ora_spiegazioni-69059578/, Ottobre 2013. [Online; ultimo accesso 17-marzo-2015].

[130] Repubblica.it. Datagate, Berlino alle ambasciate straniere: "Dateci i nomi degli 007 in Germania". http://www.repubblica.it/esteri/2014/08/08/news/nsa_merkel_ambasciate-93425886/, Agosto 2014. [Online; ultimo accesso 19-marzo-2015].

[131] Repubblica.it. Merkel a Hollande: "Costruire rete web indipendente da USA". http://www.repubblica.it/tecnologia/2014/02/15/news/merkel_a_hollande_costruire_una_rete_web_indipendente_dagli_usa-78679542/, Febbraio 2014. [Online; ultimo accesso 19-marzo-2015].

[132] Repubblica.it. NSA e spie doppiogiochiste, la Germania accusa gli USA: "Tradita la fiducia". http://www.repubblica.it/esteri/2014/07/07/news/nsa_e_spie_doppiogiochiste_la_germania_accusa_gli_usa_tradita_la_fiducia-90899142/, Luglio 2014. [Online; ultimo accesso 19-marzo-2015].

[133] Repubblica.it. Twitter fa causa a governo USA: "Ci impedisce di informare gli utenti sulle richieste dell'NSA". http://www.repubblica.it/tecnologia/2014/10/08/news/twitter_fa_causa_a_governo_usa_ci_impedisce_di_informare_gli_utenti_sulle_richieste_dell_nsa-97618289/, Ottobre 2014. [Online; ultimo accesso 11-marzo-2015].

[134] Repubblica.it. Datagate, il tribunale GB si pronuncia sull'operato dell'intelligence: "Sorveglianza illegale". http://www.repubblica.it/tecnologia/2015/02/07/news/datagate_il_tribunale_gb_si_pronuncia_sull_operato_dell_intellingence_sorveglianza_illegale-106735102/, Febbraio 2015. [Online; ultimo accesso 20-marzo-2015].

[135] John Ribeiro. NSA authorization to collect bulk phone data extended to June 1. http://www.pcworld.com/article/2890952/nsa-authorization-to-collect-bulk-phone-data-extended-to-june-1.html, Marzo 2015. [Online; ultimo accesso 16-marzo-2015].

[136] Rosita Rijtano. TOX, l'alternativa open a Skype e co. Fuori dal controllo dei big del web. http://www.repubblica.it/tecnologia/2014/09/06/news/tox_l_alternativa_open_a_skype_e_co_fuori_dal_controllo_dei_big_del_web-94925360/, Settembre 2014. [Online; ultimo accesso 24-marzo-2015].

[137] Dan Roberts and Spencer Ackerman. Anger swells after NSA phone records court order revelations. http://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records, Giugno 2013. [Online; ultimo accesso 16-marzo-2015].

[138] Dan Roberts and Spencer Ackerman. Senator Feinstein: NSA phone call data collection in place 'since 2006'. http://www.theguardian.com/world/2013/jun/06/court-order-verizon-call-data-dianne-feinstein, Giugno 2013. [Online; ultimo accesso 16-marzo-2015].

[139] RQuotidiano. Datagate, Putin: "E' libero, nessun delitto". Gli Usa: "Espelletelo subito". http://www.ilfattoquotidiano.it/2013/06/25/datagate-putin-e-uomo-libero-non-ha-commesso-nessun-delitto/637199/, Giugno 2013. [Online; ultimo accesso 18-marzo-2015].

[140] RQuotidiano. Datagate, Snowden ottiene l'asilo per un anno in Russia. Usa: 'Delusi'. http://www.ilfattoquotidiano.it/2013/08/01/datagate-snowden-ha-acquisito-status-di-rifugiato-in-russia/673672/, Agosto 2013. [Online; ultimo accesso 18-marzo-2015].

[141] RQuotidiano. Datagate, "Spiato governo spagnolo". Merkel: "Trovare rimedi con Usa". http://www.ilfattoquotidiano.it/2013/10/25/datagate-merkel-francia-e-germania-presto-intesa-comune-con-usa/756171/, Ottobre 2013. [Online; ultimo accesso 20-marzo-2015].

[142] Dominic Rushe. Apple insists it did not work with NSA to create iPhone backdoor program. http://www.theguardian.com/technology/2013/dec/31/apple-nsa-backdoor-iphone-program, Dicembre 2013. [Online; ultimo accesso 10-marzo-2015].

[143] Dominic Rushe. Facebook and Google insist they did not know of PRISM surveillance program. http://www.theguardian.com/world/2013/jun/07/google-facebook-prism-surveillance-program, Giugno 2013. [Online; ultimo accesso 13-marzo-2015].

[144] Dominic Rushe. Google and Facebook ask DoJ for permission to publish FISA requests. http://www.theguardian.com/technology/2013/jun/11/google-doj-permission-publish-fisa-requests, Giugno 2013. [Online; ultimo accesso 16-marzo-2015].

[145] Dominic Rushe. Microsoft pushes Eric Holder to lift block on public information sharing. http://www.theguardian.com/technology/2013/jul/16/microsoft-eric-holder-permission-information-national-security, Luglio 2013. [Online; ultimo accesso 13-marzo-2015].

[146] Dominic Rushe. Skype's secret Project Chess reportedly helped NSA access customers' data. http://www.theguardian.com/technology/2013/jun/20/skype-nsa-access-user-data, Giugno 2013. [Online; ultimo accesso 14-marzo-2015].

[147] Dominic Rushe. Yahoo to add encryption to all services in wake of NSA spying revelations. http://www.theguardian.com/technology/2013/nov/18/yahoo-encryption-nsa-revelations-privacy, Novembre 2013. [Online; ultimo accesso 10-marzo-2015].

[148] Dominic Rushe. Facebook updates privacy policy to clarify how it uses data from 1.3bn users. http://www.theguardian.com/technology/2014/nov/13/facebook-updates-privacy-policy-data, Novembre 2014. [Online; ultimo accesso 12-marzo-2015].

[149] Dominic Rushe. Microsoft announces privacy changes in wake of blogger's email search. http://www.theguardian.com/technology/2014/mar/28/microsoft-privacy-changes-bloggers-email-search, Marzo 2014. [Online; ultimo accesso 13-marzo-2015].

[150] Dominic Rushe. Apple CEO Tim Cook challenges Obama with impassioned stand on privacy. http://www.theguardian.com/technology/2015/feb/13/apple-ceo-tim-cook-challenges-obama-privacy, Febbraio 2015. [Online; ultimo accesso 11-marzo-2015].

[151] Dominic Rushe, Spencer Ackerman, and James Ball. Reports that NSA taps into Google and Yahoo data hubs infuriate tech giants. http://www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links, Ottobre 2013. [Online; ultimo accesso 15-marzo-2015].

[152] Fiorenza Sarzanini. Email, SMS, conversazioni: intercettata anche l'Italia. Il Copasir vuole chiarezza. http://www.corriere.it/esteri/13_ottobre_22/email-sms-conversazioni-intercettata-anche-italia-copasir-vuole-chiarezza-f8fdecec-3ad8-11e3-95f2-9a7a296f615f.shtml, Ottobre 2013. [Online; ultimo accesso 19-marzo-2015].

[153] Marco Schiaffino. Datagate: Skype nel mirino, "violava privacy". Ma le alternative sono poche. http://www.ilfattoquotidiano.it/2013/07/12/datagate-skype-nel-mirino-violava-privacy-ma-alternative-sono-poche/654542/, Luglio 2013. [Online; ultimo accesso 14-marzo-2015].

[154] Bruce Schneier. Attacking Tor: how the NSA targets users' online anonymity. http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity, Ottobre 2013. [Online; ultimo accesso 04-marzo-2015].

[155] Bruce Schneier. Over 700 million people taking steps to avoid NSA surveillance. https://www.schneier.com/blog/archives/2014/12/over_700_millio.html, Dicembre 2014. [Online; ultimo accesso 09-aprile-2015].

[156] Sky TG 24. Germania: forse spiato il cellulare della Merkel. Obama nega. http://tg24.sky.it/tg24/mondo/2013/10/23/datagate_nsagate_kerry_letta_usa_audizione_minniti_copasir.html, Ottobre 2013. [Online; ultimo accesso 19-marzo-2015].

[157] Brad Smith. Standing together for greater transparency. http://blogs.microsoft.com/on-the-issues/2013/08/30/standing-together-for-greater-transparency/, Agosto 2013. [Online; ultimo accesso 13-marzo-2015].

[158] Brad Smith. Unfinished business on government surveillance reform. http://blogs.microsoft.com/on-the-issues/2014/06/04/unfinished-business-on-government-surveillance-reform/, Giugno 2014. [Online; ultimo accesso 13-marzo-2015].

[159] Daniel J Solove. 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego law review*, 44:745, 2007.

[160] Jon Southurst. Decentralized Internet project MaidSafe to raise funds via 'Safecoin' sale. http://www.coindesk.com/decentralized-internet-project-maidsafe-raise-funds-via-safecoin-sale/, Aprile 2014. [Online; ultimo accesso 06-marzo-2015].

[161] Andrea Tarquini. La svolta della Germania dopo il Datagate: controlleremo e spieremo tutti. http://www.repubblica.it/tecnologia/2014/02/16/news/germania_spie_nsa_usa-78788097/, Febbraio 2014. [Online; ultimo accesso 19-marzo-2015].

[162] Gabriella Tesoro. Datagate, "La Svezia spiava la Russia per conto dell'NSA". http://it.ibtimes.com/articles/59952/20131206/fra-svezia-usa-nsa-snowden-guardian-greenwald-spionaggio-controllo-internet-cellulari.htm, Dicembre 2013. [Online; ultimo accesso 18-marzo-2015].

[163] The Guardian. Verizon forced to hand over telephone data – full court ruling. http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order, Giugno 2013. [Online; ultimo accesso 16-marzo-2015].

[164] Craig Timberg. How one man's private files ended up on Apple's iCloud without his consent. http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/30/how-one-mans-private-files-ended-up-on-apples-icloud-without-his-consent/, Ottobre 2014. [Online; ultimo accesso 11-marzo-2015].

[165] Craig Timberg. U.S. threatened massive fine to force Yahoo to release data. http://www.washingtonpost.com/business/technology/us-threatened-massive-fine-to-force-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html, Settembre 2014. [Online; ultimo accesso 10-marzo-2015].

[166] Trevor Timm. Your iPhone is now encrypted. The FBI says it'll help kidnappers. Who do you believe? http://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default, Settembre 2014. [Online; ultimo accesso 10-marzo-2015].

[167] Maria Cristina Torchia. Che cosa indica e come si traduce la parola inglese whistleblower? http://www.accademiadellacrusca.it/it/lingua-italiana/consulenza-linguistica/domande-risposte/cosa-indica-come-si-traduce-parola-inglese-w, Ottobre 2014. [Online; ultimo accesso 24-marzo-2015].

[168] Francesco Tortora. Effetto Datagate, gli 007 russi ritornano alle «vecchie» macchine per scrivere. http://www.corriere.it/esteri/13_luglio_11/datagate-macchine-da-scrivere-spie-russia_bea8a980-ea27-11e2-8099-3729074bd3db.shtml, Luglio 2013. [Online; ultimo accesso 17-marzo-2015].

[169] Brian Trammell, Elisa Boschi, Gregorio Procissi, Christian Callegari, Peter Dorfinger, and Dominik Schatzmann. *Identifying Skype traffic in a large-scale flow data repository*. Springer, 2011.

[170] UK Legislation. Intelligence Services Act 1994. http://www.legislation.gov.uk/ukpga/1994/13/contents, 1994.

[171] Brendan Van Alsenoy and et al. From social media service to advertising network - a critical analysis of Facebook's revised policies and terms. Technical report, Belgian Data Protection Authority, Febbraio 2015. [Online; ultimo accesso 13-marzo-2015].

[172] Marshall Van Alstyne. Why Bitcoin has value. *Communications of the ACM*, 57(5):30–32, 2014.

[173] Samuel D Warren and Louis D Brandeis. The right to privacy. *Harvard law review*, pages 193–220, 1890.

[174] Wikileaks. What is WikilLaks? https://wikileaks.org/About.html, Maggio 2011. [Online; ultimo accesso 06-marzo-2015].

[175] Wikipedia. MUSCULAR (surveillance program). http://en.wikipedia.org/w/index.php?title=MUSCULAR_(surveillance_program)&oldid=629760469, 2014. [Online; ultimo accesso 26-marzo-2015].

[176] Wikipedia. WikiLeaks. https://it.wikipedia.org/w/index.php?title=WikiLeaks, 2014. [Online; ultimo accesso 07-marzo-2015].

[177] Wikipedia. Facebook - Privacy e controversie. https://it.wikipedia.org/wiki/Facebook#Privacy_e_controversie, 2015. [Online; ultimo accesso 12-marzo-2015].

[178] Wikipedia. Forward secrecy. https://en.wikipedia.org/w/index.php?title=Forward_secrecy&oldid=651716297, 2015. [Online; ultimo accesso 24-marzo-2015].

[179] Wikipedia. GNU Privacy Guard. https://en.wikipedia.org/wiki/GNU_Privacy_Guard, 2015. [Online; ultimo accesso 03-marzo-2015].

[180] Wikipedia. GNUnet. https://en.wikipedia.org/w/index.php?title=GNUnet, 2015. [Online; ultimo accesso 05-marzo-2015].

[181] Wikipedia. II emendamento della Costituzione degli Stati Uniti d'America. //it.wikipedia.org/w/index.php?title=II_emendamento_della_Costituzione_degli_Stati_Uniti_d%27America&oldid=71356171, 2015. [Online; ultimo accesso 25-marzo-2015].

[182] Wikipedia. Pretty Good Privacy. https://en.wikipedia.org/wiki/Pretty_Good_Privacy, 2015. [Online; ultimo accesso 03-marzo-2015].

[183] Wikipedia. Reactions to global surveillance disclosures. https://en.wikipedia.org/w/index.php?title=Reactions_to_global_surveillance_disclosures&oldid=646072833, 2015. [Online; ultimo accesso 17-marzo-2015].

[184] Wikipedia. Tor (software). https://it.wikipedia.org/wiki/Tor_(software), 2015. [Online; ultimo accesso 03-marzo-2015].

[185] Wikipedia. Twitter. https://it.wikipedia.org/w/index.php?title=Twitter, 2015. [Online; ultimo accesso 11-marzo-2015].

[186] Wikipedia. Yahoo! https://it.wikipedia.org/w/index.php?title=Yahoo!, 2015. [Online; ultimo accesso 10-marzo-2015].

[187] Yahoo. Whatsapp, messaggi criptati per gli utenti Android. https://it.notizie.yahoo.com/whatsapp-messaggi-criptati-per-gli-utenti-android-115442567.html, Novembre 2014. [Online; ultimo accesso 12-marzo-2015].

[188] Yahoo. Sicurezza in Yahoo! https://info.yahoo.com/privacy/it/yahoo/security/, 2015. [Online; ultimo accesso 10-marzo-2015].

[189] Marco Zatterin. Datagate, Francia e Germania: "Un codice di condotta per gli 007". Letta: "Basta zone d'ombra tra alleati". http://www.lastampa.it/2013/10/25/esteri/leuropa-forte-segnale-a-obama-le-intercettazioni-minano-la-fiducia-x6zCZgS1SO5wQzkS7ffelL/pagina.html, Ottobre 2013. [Online; ultimo accesso 19-marzo-2015].

[190] Kim Zetter. Google asks NSA to help secure its network. http://www.wired.com/2010/02/google-seeks-nsa-help/, Febbraio 2010. [Online; ultimo accesso 15-marzo-2015].

[191] Kim Zetter. Google cookies help NSA identify targets for hacking and spying. http://www.wired.com/2013/12/nsa-spy-cookies/, Dicembre 2013. [Online; ultimo accesso 15-marzo-2015].

[192] Kim Zetter. Report: NSA is intercepting traffic form Yahoo, Google data centers. http://www.wired.com/2013/10/nsa-hacked-yahoo-google-cables/, Ottobre 2013. [Online; ultimo accesso 15-marzo-2015].

[193] Mark Zuckerberg. Post Facebook di Mark Zuckerberg. https://www.facebook.com/zuck/posts/10101301165605491, Marzo 2014. [Online; ultimo accesso 12-marzo-2015].