UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea (Magistrale) in Informatica

UNIVERSIDAD POLITÉCNICA DE VALENCIA

Escuela Técnica Superior de Ingeniería Informática

Grado en Ingeniería Informática

Big Data: Metadatos y su uso para la vigilancia global

Big Data: Metadati e il suo uso per la sorveglianza

Autor: José Alberto Arguisuelas León

Relatore: Prof. J. Carlos Casamayor

Correlatore: Prof. Filomena Ferrucci

Anno Accademico 2016/2017

Ringraziamenti

Ai miei genitori, per appoggiarmi in ogni momento durante questi quattro anni senza mai dubitare di me. Senza la loro forza, i loro consigli e l'infinita pazienza che hanno dimostrato, sarebbe stato impossibile arrivare qui dove mi trovo oggi.

Ai miei compagni e amici dell'Università Diego, Héctor, Jorge y José Alberto. Se siamo riusciti ad arrivare alla fine del nostro percorso, è per essere stati insieme dall'inizio.

Soprattutto, a Valencia, per avermi fatto crescere tanto personalmente. Per dimostrarmi che ci si può sentire come in casa nonostante ci si trovi a chilometri di distanza dalla propria. Per avere tutto il fascino che si è disposti a conoscere.

A Tamara, Laura, Maria, Edu, Guille, Jorge y Fer, per aver formato una famiglia facendo dell'Erasmus un'esperienza indimenticabile e facendo del mio ultimo anno di Università, il migliore di tutti.

A Marta, per essere il più grande e migliore appoggio che una persona possa avere. Non sarei ciò che sono senza di te. Finché varrà la pena, magari possa durare per sempre.

A Olga, Erika e Nicoletta, per aiutarmi (molto) a tradurre la mia tesi. Senza amiche come voi non avrei potuto consegnare questo lavoro tradotto nella lingua più bella del mondo.

Sintesi

La mia tesi consiste, prima di tutto, nella descrizione del mondo del Big Data, definendolo, facendo un breve riassunto della sua cronologia e analizzando alcuni dei problemi sorti in questo campo.
Successivamente, mi sono concentrato sulla descrizione dei metadati, definendoli e mostrando l'importanza che hanno assunto oggigiorno. Inoltre sviluppo alcune delle sue applicazioni. Il tema centrale del mio lavoro, quindi, tratta della relazione che intercorre tra il Big Data e i metadati, dell'uso che ne fanno i governi, specialmente quello Americano, raccogliendo dati di massa al fine di creare una rete di sorveglianza globale della popolazione. Nel Capitolo 5 mostro numerose rivelazioni riguardanti queste reti di sorveglianza pubblicate attraverso vari mezzi di comunicazione.

Indice dei contenuti

Indice delle figure

CAPITOLO 1
INTRODUZIONE

Attualmente, nel mondo dell'informatica, il termine Big Data sta assumendo sempre più importanza. Questo si deve al fatto che le imprese e gli organismi si sono resi conto del valore che ha l'informazione. Però, oggigiorno, che si hanno capacità superiori a quelle di un tempo per raccogliere dati, la difficoltà risiede in come li processiamo.

La soluzione a questo problema è stato il Big Data. Grazie a questa maniera di esaminare la grande quantità di dati di cui disponiamo, abbiamo il modo di poter trattarli e processarli.

Nonostante molte imprese affermino di aver adottato una metodologia che lavora con Big Data, la verità è che siamo ancora lontani dal poter processare, in modo efficiente, tutte le informazioni di cui disponiamo. Possiamo dire che, in questo momento, siamo solo in grado di raccogliere molte informazioni senza sapere come processarle correttamente.

Uno degli aspetti dell'informatica e della telecomunicazione, sono i metadati. Essi si definiscono come i dati dei dati. In altre parole, possiamo dire che i metadati sono i dati che descrivono un archivio, nel caso in cui ci trovassimo in ambito informatico, o i dati di una comunicazione, se ci riferissimo a una telefonata, e-mail, ecc.

Possiamo relazionare entrambi i concetti concentrandoci sulla raccolta di suddetti metadati; per essere più specifici, sulla raccolta dei metadati

nell'ambito delle telecomunicazioni della popolazione da parte del governo. Questa raccolta ha un obbiettivo, la creazione di una rete di sorveglianza mondiale. Questo sarà il tema centrale del mio lavoro, prendendo come punto di partenza il documentario "Citizienfour". Questo documentario parla del caso Snowden, la storia di come Edward Snowden, tecnico informatico della CIA e della NSA, filtrò i documenti che mostrano come il governo statunitense sorvegliava i suoi cittadini alla stampa. A partire da questo evento, si rivelarono altri casi simili dove i governi realizzavano tali atti violando leggi sulla privacy. Il 2013 fu l'anno in cui Snowden si fece conoscere svelando uno dei più grandi segreti del paese nordamericano. Ciò nonostante, negli anni successivi i media di tutto il mondo continuarono a pubblicare notizie relazionate con le reti di sorveglianza mondiale che molti governi, alleati tra loro, crearono segretamente.

In seguito, parlerò della situazione attuale nell'ambito delle leggi esistenti sulla protezione dei dati e sulla privacy negli USA e a livello internazionale.

Dato che ogni governo impone le proprie leggi nel suo territorio e che non esiste uno standard internazionale, mi sono focalizzato sull'analisi delle leggi statunitensi. Il motivo di tale scelta è dovuto sia alla grande concentrazione di imprese di telecomunicazione presenti in questo Paese, sia al fatto che attualmente gli USA si trovano al centro del mirino per le recenti rivelazioni relazionate con la sorveglianza dei cittadini.

Collegandomi al precedente punto, analizzerò alcune notizie pubblicate relazionate con l'attuale presidente americano, Donald Trump, e la privacy dei cittadini all'interno di Internet.

CAPITOLO 2
BIG DATA

2.1 Definizione di Big Data

La definizione di Big Data allude a un insieme di dati che, per volume e varietà, non possono essere processati come di consueto, superando la capacità dei sistemi informatici comuni.

Analizzare questa enorme quantità di dati caricandola in una base di dati relazionale, porterebbe via troppo tempo a causa delle difficoltà di archiviazione, ricerca, condivisione, analisi e visualizzazione. [1]

Il Big Data è il segno del potere che ha l'informazione. Così possiamo distinguere le sue utilità principali:

- Democrazia: I dati analizzati si utilizzano sempre di più nei processi elettorali. Le campagne presidenziali di Barack Obama e Donald Trump usarono tutte le informazioni di cui disponevano per guidare la campagna nella giusta direzione.
- Impresariale: Molte compagnie raccolgono i dati degli usuari per adattare la pubblicità mostratagli. Si raccolgono milioni di dati al giorno per ottenere informazioni precise sulle preferenze dei consumatori.

- Sport: Nel mondo dello sport, l'informazione è un'arma potentissima. Immagazzinare dati, statistiche e partite è di una grande utilità per gli allenamenti degli sportivi professionali.
- Investigazione: L'investigazione basata sull'analisi di una grande quantità di dati può avere due obbiettivi. Il primo, nel campo della medicina e della salute, dove l'investigazione di nuove cure contro le malattie o nell'ambito della chirurgia è molto importante. Il secondo è quello della difesa e della sicurezza contro i cyber attacchi.

2.2 Evoluzione Big Data

Negli anni 60, lo scientifico Derek Prince, osservò l'incredibile sforzo che l'essere umano avrebbe dovuto realizzare nell'ambito dell'investigazione scientifica. I documentari riassunti, che furono creati durante la fine del 1800 con lo scopo di gestire le conoscenze, crebbero a un ritmo troppo elevato per essere controllati.

Oltre il settore scientifico, anche il settore finanziario era interessato all'informazione. Per questo, nel 1960, la maggior parte delle organizzazioni iniziarono a progettare, sviluppare e implementare sistemi informatici per gestire tale quantità di informazioni e automatizzare i sistemi di inventario. [2]

Nel 1970, Edgar F. Codd, grazie ad un articolo, fece conoscere al mondo il concetto di Database Relazionale. In questo articolo, spiegava il modo in cui era possibile accedere alle informazioni immagazzinate in grandi Database, senza sapere come erano strutturate né dove si trovassero. Fino a quel momento, c'era stato bisogno di conoscenze informatiche molto avanzate oltre che di specialisti per recuperare le informazioni, ovvero era necessario un'importante investimento. [3]

Verso la metà degli anni 70, i PC (Personal Computer) erano molto popolari nelle imprese. Questo cambiò i processi di negoziazione e di

contabilità. In questo periodo, nacquero imprese come Oracle, la quale presentò e commercializzò il linguaggio SQL (Structure Query Language).

Nel 1985, Barry Devlin e Paul Murphy definirono un'architettura per i rapporti e le analisi di mercato IBM, che terminò convertendosi nella base di immagazzinamento di dati. In questa architettura, tale immagazzinamento è omogeneo e i dati complessi e esatti. [4]

Nel 1989, Howard Dresner ampliò il termine "Business Inteligence (BI)" o Intelligenza Impresariale. Lo definì come "i concetti e i metodi che migliorano il prendere decisioni di mercato attraverso l'uso dei sistemi di appoggio basati su dati reali". Questo concetto sarà molto importante nel mondo impresariale, dato che afferma l'importanza dell'informazione e dei dati nell'ambito del mercato. [5]

Nel 1992, Crystal Reports creò il primo rapporto di un Database semplice con Windows. Questo permetteva alle imprese creare un resoconto con poca programmazione partendo da diverse origini di dati. In questo modo, in questi anni, si produsse un miglioramento tecnologico incredibile, e i dati dell'Intelligenza Impresariale cominciarono a accumularsi sotto forma di documenti Excel.

Così, nel 1997, per la prima volta venne utilizzato il termine Big Data, in un articolo di investigazione della NASA: si confermava il sorprendente ritmo dell'aumento dei dati e il problema presentato dai sistemi informatici dell'epoca. [6]

Verso la fine degli anni 90, molte imprese pensavano che il sistema di estrazione di dati e di informazioni non funzionava. Gli impiegati erano incapaci di trovare una risposta e di accedere ai dati di cui avevano bisogno: dipendevano eccessivamente dai dipartimenti informatici responsabili dell'Intelligenza Impresariale. [7]

In questo modo, nel 2006, come soluzione alla necessità di nuovi sistemi per gestire la quantità di dati presenti nella rete, nacque Hadoop. Scaricabile gratuitamente, questo programma permetteva di processare in parallelo enormi quantità di dati. [8]

Durante il 2007 e il 2008, vari articoli confermavano il fantastico miglioramento che stava avvenendo: i rapporti dell'IDC (international Data Corporation) del 2006 prevedevano che tutte queste informazioni si duplicassero a intervalli di 18 mesi durante 4 anni. Consultando i rapporti del 2010 e del 2012, ci si rese conto del fatto che i dati digitali creati ogni anno, superarono i pronostici iniziali. Il termine "Big Data" cominciò quindi a utilizzarsi sempre più spesso nei circoli tecnologici. [9]

Nel 2009 e nel 2010, l'intelligenza impresariale divenne una delle principali priorità per i direttori delle tecnologie dell'informazione. Le imprese iniziarono a implementare nuove tecnologie per analizzare e ottimizzare grandi quantità di dati e iniziarono a fidarsi sempre di più dell'uso dei dati come attivo di mercato per ottenere vantaggi rispetto alla competenza. [10], [11]

Questa evoluzione nel mondo della tecnologia digitale è descritta nell'articolo della rivista Science Magazine, intitolato "the World's Technological Capacity to Store". Lì si afferma che nel 1986, il 99,2% dell'immagazzinamento dei dati era analogico, ma nel 2007, il 94% di questo era digitale. Questo dimostrò il cambio radicale della maniera di immagazzinare i dati in soli 20 anni. [12]

Possiamo quindi confermare che anno dopo anno l'aumento che si produce nel terreno del Big Data è sempre maggiore. Come possiamo vedere nella figura 1, la linea lilla rappresenta l'aumento del Big Data nel mondo. Se osserviamo attentamente, esistono due punti di inflessione che risaltano.

Il primo nel 1998, quando l'aumento inizia a sperimentare una salita più evidente rispetto agli anni anteriori. Questo si deve in parte alla creazione di Google, l'attuale motore di ricerca più grande del mondo oltre che all'aumento degli usuari di Internet.

Il secondo punto corrisponde all'anno 2006, dove si osserva un aumento della pendente nella linea di aumento di tutti i paesi e del mondo in generale. Questo impulso nell'aumento del Big Data è dovuto all'auge delle reti sociali. Ogni usuario in una rete sociale, nel momento in cui caricano una foto, un

video o un semplice testo, sta creando dati che vengono immagazzinati nei server. [13]

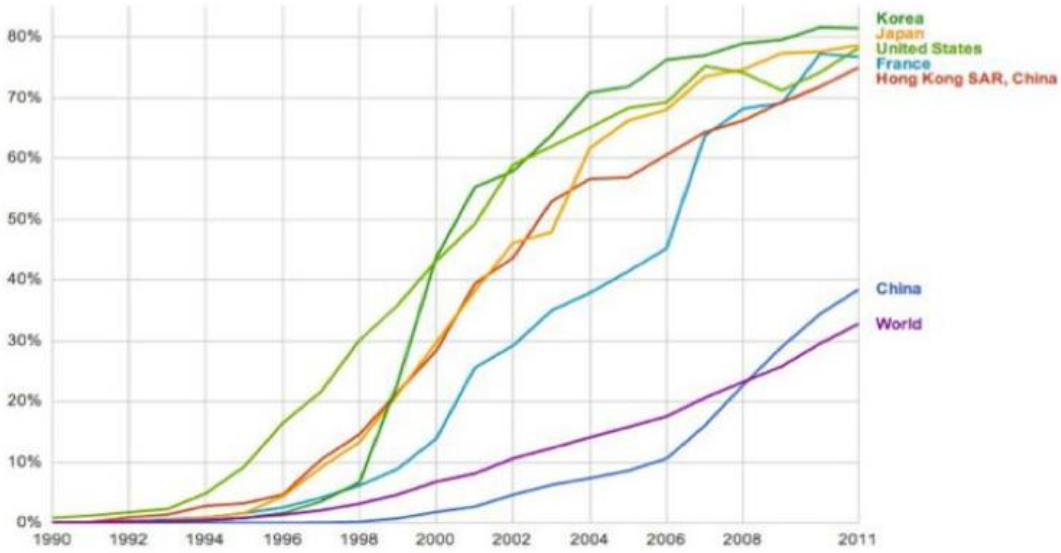

Figura 1: Aumento del Big Data negli ultimi 20 anni

2.3 I problemi del Big Data

Un aspetto che non era stato affrontato fino ad ora è la serie di problemi che apporta questa esplosione di dati. Come abbiamo osservato, tutte le previsioni fatte sulla quantità di dati che dovremmo accumulare nel tempo non corrispondono alla realtà, avendo superato di gran lunga le aspettative.

I problemi che devono risolvere le imprese decise a manipolare una tale quantità di dati e introdursi nel mondo del Big Data sono:

2.3.1 Volume

Conservare una grande quantità di dati in un hard disk è un compito complicato. Per potersi fare un'idea della quantità di dati che si dovrebbero immagazzinare, potremmo concentrarci sulla rete sociale Twitter. Questa compagnia deve salvare circa 340 milioni di tweets al giorno, l'equivalente a 1 TB di memoria. Immagazzinare 1 TB di memoria al giorno può risultare un

problema logistico importante. Una soluzione possibile per questo problema sono i File System Distribuiti.
Un File System distribuito è un sistema di archivio per PC che serve per condividere documenti e periferiche di immagazzinamento persistente. Questi file System possiedono le seguenti proprietà:

- Immagazzinamento di informazioni permanente.
- Identificano gli archivi in uno spazio strutturato.
- Permettono l'accesso contemporaneo di vari processi.
- Trasparenza nell'identificazione. Questo permette di avere uno spazio di nomi unico e indipendente del client.
- Trasparenza nella posizione. Permette la mobilità del file da una posizione a un'altra.
- Scalabilità, permettendo spazi di nomi strutturati e replicazione per evitare colli di bottiglia
- Robustezza ai guasti, per evitare che i problemi dei client influenzino il servizio.
- Disponibilità e tolleranza ai guasti. La replicazione è un metodo che lo permette.
- Consistenza, cercando di mantenere la semantica dei sistemi centralizzati.
- Sicurezza, fornendo autenticazione remota attraverso credenziali invece di liste d'accesso.

La struttura che hanno normalmente i sistemi distribuiti (database distribuiti) è quella del client-server, e la troviamo in tre moduli:

- Client. È l'interfaccia locale con l'applicazione.
- File service. Mantiene il contenuto dei file, delle directory e gli attributi dei file. Un file si identifica attraverso un identificatore unico di file (UFID).
- Name Service: fornisce trasparenza di localizzazione.

Nella Figura 2 possiamo osservare uno schema che ci mostra uno dei vantaggi dei sistemi di archiviazione distribuiti: la trasparenza nei nomi e nella localizzazione. Quando l'usuario vuole accedere a un archivio, non ha bisogno di conoscere la localizzazione esatta di quest'ultimo. Semplicemente si connette al nameserver, il quale offre un'interfaccia unica dove è possibile trovare tutte le localizzazioni che si trovano nello stesso spazio. [14]

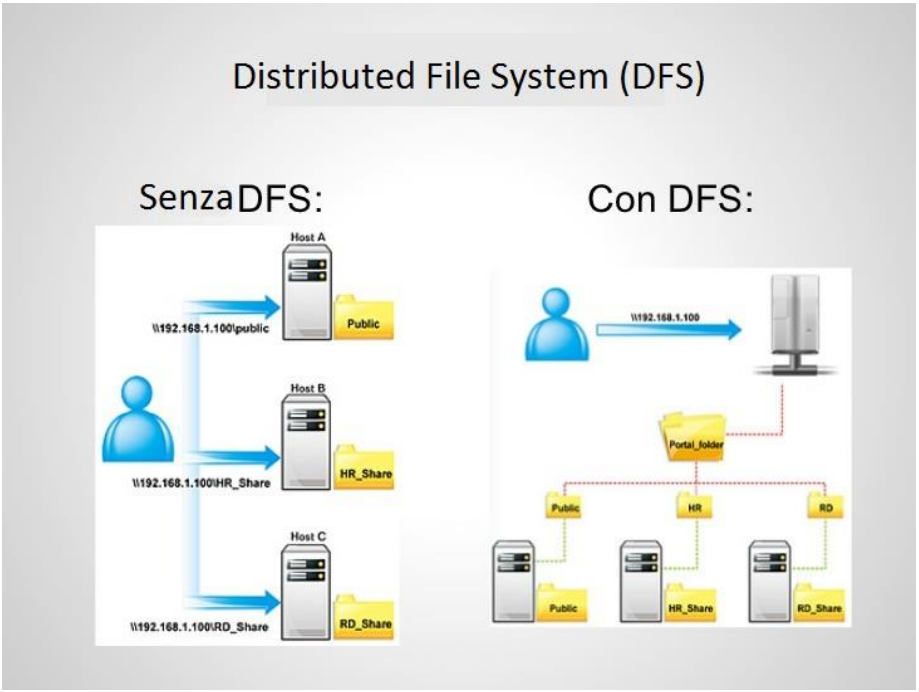

Figura 2: Schema DFS

In questo modo si risolve uno dei problemi che si presenta nel momento in cui si lavora con il Big Data, ossia l'archiviazione di molti dati nello stesso tempo. In questo modo, si possono distribuire le informazioni in diversi terminal, offrendo la visione di un'interfaccia unica.

2.3.2 Velocità

Oltre a dover tener conto della quantità dei dati che si devono immagazzinare, un altro fattore importante di cui è necessario tenere conto è la velocità. Esistono molti servizi che, oltre a dover elaborare una quantità di dati e informazione enormi, devono farlo con una velocità accettabile. Non è

sufficiente una banda larga, bensì è necessario qualche altro meccanismo. Una possibile soluzione a questo problema sono i Sistemi di Distribuzione dei Processi.

I sistemi di distribuzione dei processi si basano su di un sistema operativo distribuito. Questa è l'unione logica di un gruppo di sistemi operativi su un insieme di nodi di calcolo indipendenti, connessi in rete, che si comunicano e fisicamente separati. Ogni nodo contiene in modo individuale un sottoinsieme specifico dei programmi che compongono il sistema operativo distribuito. [16]

Questo modello di sistema operativo richiede:

- Trasparenza, perché il sistema operi senza sapere dove si trovino fisicamente i componenti.
- Comunicazione tra i processi.
- Gestione dei processi, che forniscono le politiche e i meccanismi per l'intercambio efficace e efficiente dei ricordi tra i processi distribuiti.
- Gestione delle risorse come la memoria, gli archivi o i dispositivi che si devono distribuire in tutto il sistema.

Rispondendo a questa serie di requisiti, quello che il modello del sistema operativo distribuito ci offre in cambio è:

- Affidabilità
- Disponibilità
- Rendimento
- Sincronizzazione

2.3.3 Varietà

Accumulare grandi quantità di informazioni di tipo differente presenta un problema, dato che avere molti dati non ordinati non ci permette di realizzare uno studio affidabile. Una delle soluzioni a tale problema, già commentata precedentemente, sono i Database Relazionali.

Un database relazionale è una raccolta di elementi di dati organizzati in un insieme di tabelle descritte formalmente, dalle quali è possibile accedere ai dati o rimontarli in modo diverso senza dover riorganizzare le tabelle del Database. Questo modello relazionale fu inventato da Edgar Frank Codd nel 1970 e ad oggi risulta essere il più usato. [17]

Possiamo vedere uno schema di come si struttura un Database relazione nella Figura 3. In questo esempio, vediamo una tabella di Dipendenti (EMP). Ogni dipendente è formato da tre attributi:

- Un attributo EMP_INFO che è di tipo PERSON
- Un attributo ADDR_INFO che è di tipo ADDRESS
- Un attributo PHONE che è di tipo NUMBER.

I primi due attributi vincolano la tabella EMP ad altre (PERSON, ADDRESS), che sono un altro tipo di dati complessi. In questo modo, si possono salvare diversi tipi di dati in uno stesso Database.

Questo esempio è un modello semplice, visto che un Database relazionale reale può arrivare ad avere moltissime tabelle relazionate tra loro.

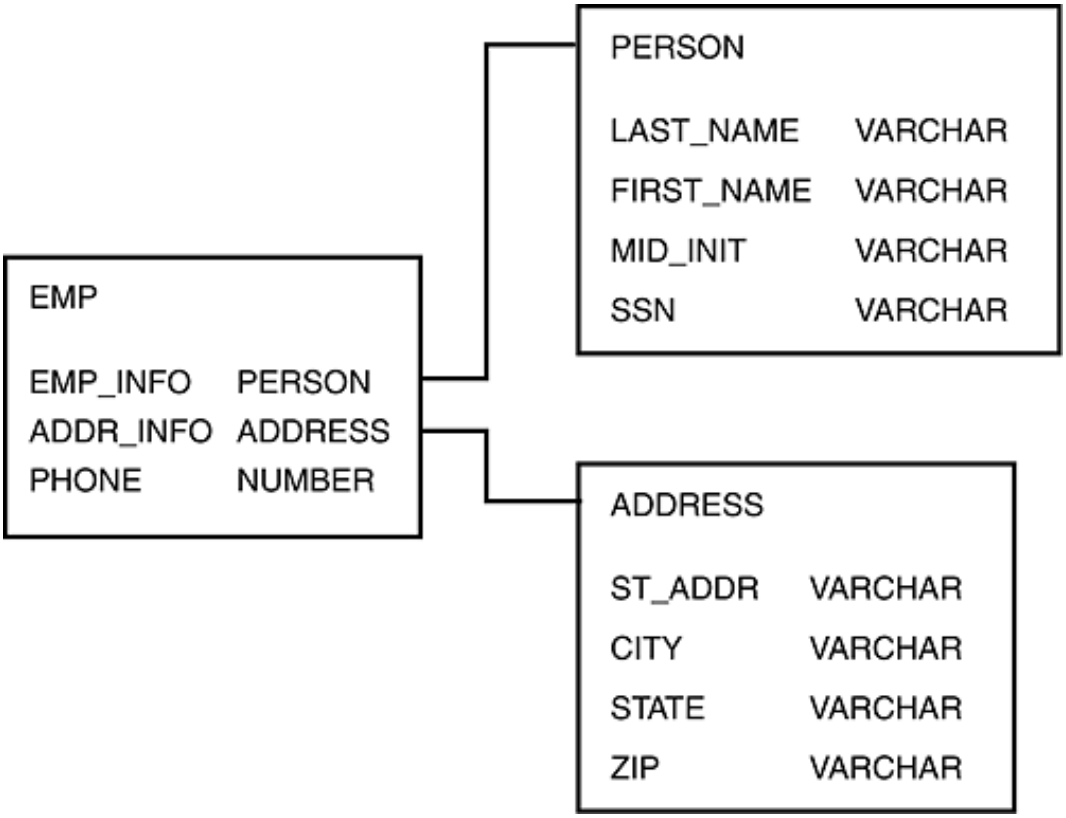

Figura 3: Schema Database Relazionale

Il motivo per cui la maggior parte dei Database segue questo modello relazionale sono i suoi vantaggi:

- Garantisce l'evitare doppioni nel momento del registro.
- Garantisce l'integrità referenziale.
- Favorisce la normalizzazione.

CAPITOLO 3
METADATI

3.1 Definizione e importanza dei metadati

La definizione più semplice della parola metadati sarebbe “dati sui dati”. Ampliando questo concetto, possiamo dire che i metadati sono dati associati a oggetti che aiutano a fornire informazioni su di essi. Possono descrivere il contenuto, la qualità, le condizioni, la storia, la disponibilità e altre caratteristiche dei dati.
Nell’ambito dell’informatica si utilizza anche il termine “metadata”, che si riferisce alle informazioni generate dagli usuari quando utilizzano tecnologie digitali. [19]
Forse può sembrare che questi metadati abbiano poca importanza, meno dei dati e del contenuto in sé, ma il suo studio può rivelare molte informazioni, come modelli, relazioni e comportamenti.

Gli esempi più chiari circa la importanza dei metadati li troviamo nelle chiamate telefoniche e nelle e-mail. Sono due mezzi di comunicazione che si compongono di un trasmettitore, di un messaggio e di un destinatario.

Nel caso delle chiamate telefoniche, esiste un intercambio di messaggi vocali, ovvero il contenuto della chiamata. Questi messaggi non sono l'unica fonte di informazione presente. Da tale chiamata possiamo ottenere altri dati (i metadati) come i tempi di configurazione della telefonata, il trasmettitore, il recettore e la durata. Riassumendo questi dati, si possono stabilire i modelli, le abitudini e la routine di una persona, senza avere la necessità di conoscere il contenuto di una telefonata.

L'e-mail è un altro esempio molto simile. In questo caso, possiamo ottenere metadati come trasmettitori, ricevitori, data e ora di invio. Con questi dati si può stabilire la rete di contatti di una persona, senza dover leggere in nessun momento il testo del messaggio.

Nel 2013, tre impiegati del MIT (Massachussets Institute of Tecnology) realizzarono un progetto chiamato Immersion. Questo progetto realizza uno schema interattivo sulla propria rete di contatti a partire dalle e-mail, solo dando accesso ai campi del destinatario, CC, ora e data (i metadati delle e-mail).

Come è possibile vedere nell'esempio della Figura 4, quanto maggiore è il flusso di messaggi con una persona, maggiore è la grandezza del cerchio che rappresenta un destinatario. Da questo si vanno formando sotto reti di contatti relazionati tra loro.

Questo schema è capace di rivelare molte informazioni riguardanti una persona se si analizza correttamente. Per esempio, se notiamo che qualche cerchio è formato da un'e-mail con un dominio di qualche università, possiamo dedurre che questa persona frequenta l'università, e che la sotto rete formata intorno a questo cerchio sono amici dell'università con cui tale persona ha contatti.

L'obbiettivo di questo esempio è mostrare tutte le informazioni di una persona che i metadati di un'e-mail possono rivelare. [20]

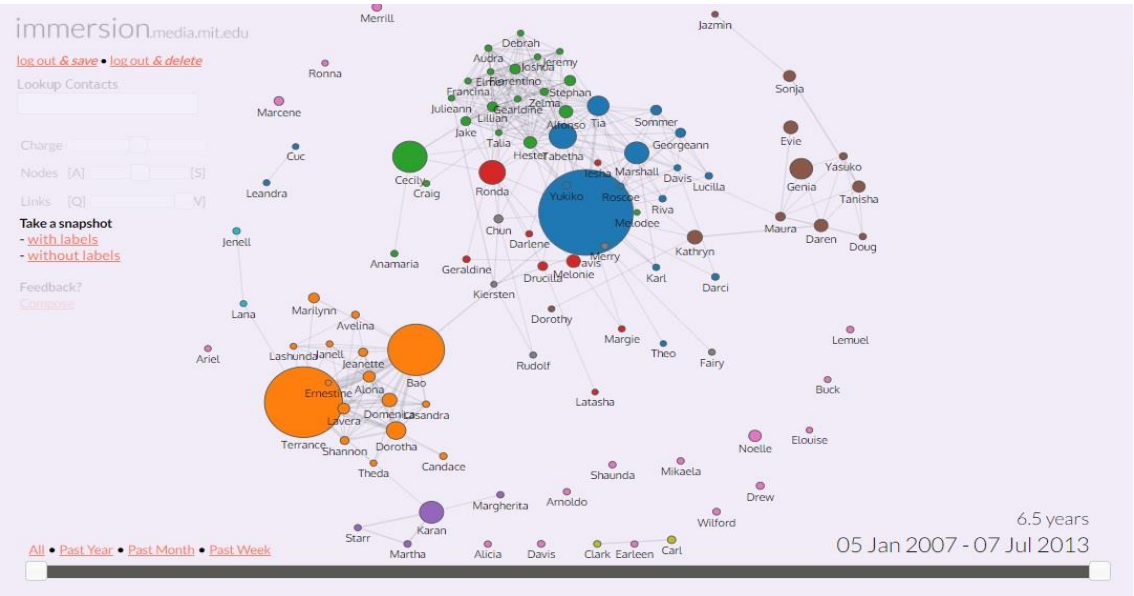

Figura 4: Esempio di Immersion

3.2 Racolta e applizazioni dei metadati

Essendo già a conoscenza dell'importanza che hanno i metadati, possiamo dedurre che la loro raccolta (metadata harvesting) può apportare informazioni molto importanti. Queste informazioni possono avere vari usi e possono essere raccolti in modi diversi.

3.2.1 Open Archives Initiative (OAI)

Uno degli usi più interessanti che è stato dato ai metadati è stato applicato nel progetto Open Archives Initiative (OAI). L'approccio fondamentale dei file aperti è quello di fornire l'accesso ai materiali sul web attraverso i depositi, i quali operando l'uno con l'altro, consentono lo scambio dei metadati, la loro conservazione e la loro pubblicazione. Per chiarire il significato del nome, il termine Archive(archivio) è inteso come un deposito di documenti scientifici o di qualsiasi altro tipo di informazione. Il termine Open(aperto) si riferisce al punto di vista dell'architettura del sistema,

interfacce che consentono l'accesso alle informazioni, per niente relative all'accesso illimitato delle informazioni.

OAI venne creato con lo scopo di sviluppare e promuovere standard di interoperabilità per facilitare la diffusione efficiente dei contenuti di Internet, ossia per incrementare la disponibilità delle pubblicazioni scientifiche. Mano a mano che il progetto veniva sviluppato, si dedusse che avrebbe potuto avere applicazioni che andassero oltre la comunità scientifica e che corrispondessero ad una categoria più ampia di materiali digitali. Pertanto, OAI si occupa della comunicazione dei metadati di qualsiasi materiale immagazzinato in un supporto elettronico.

Il protocollo OAI-PMH (Open Archives Initiative – Protocol for Metadata) è quello utilizzato per questo tipo di trasmissione di dati. Uno dei requisiti necessari per utilizzare questo protocollo è che i metadati trasmessi devono essere codificati in Dublin Core non qualificato, al fine di minimizzare i potenziali problemi legati alle conversioni tra i diversi formati.

Senza addentrarci troppo nei dettagli tecnici del protocollo, possiamo comunque descrivere il suo funzionamento: OAI-PMH usa relazioni HTTP, basandosi su di un'architettura client-server. Il servizio di raccolta dei metadati, che assume il ruolo di client, può chiedere all'archivio (server) l'invio dei metadati secondo questo criterio. Il server restituisce un insieme di registri in formato XML, includendo gli identificatori degli oggetti descritti in ogni registro.
Le petizioni HTTP usano i metodi GET o POST, generando una delle opzioni disponibili, le quali si inviano in coppie del tipo chiave=valore.
Il protocollo supporta diversi formati per esprimere i metadati, ma richiede che i server offrano i registri utilizzando il Dublin Core non qualificato codificato in XML. [22]

3.2.2 Sorveglianza e spionaggio

Un altro uso, probabilmente il più criticato, è quello per la sorveglianza dei cittadini. Questo aspetto si svilupperà in modo più ampio nel seguente paragrafo con la spiegazione del Caso Snowden. In ogni caso, prima delle dichiarazioni di Edward Snowden nel giugno del 2013, giravano già delle notizie sul il governo degli USA che sorveglia i suoi cittadini.

Nel 2006, la Electronic Frontier Foundation, USA Today e altri mezzi di comunicazione, rivelarono che la NSA possiede uno strumento chiamato MAINWAY, creato per registrare a tappeto i metadati delle chiamate dei cittadini degli Stati Uniti, sia nazionali che internazionali. Questa pratica iniziò dopo l'attentato dell'11 settembre del 2001.

Il Database MAINWAY contiene i metadati delle chiamate telefoniche delle 4 maggiori compagnie telefoniche degli Stati Uniti: AT&T, SBC, BellSouth e Verizon.

Questi registri includono i metadati per realizzare le analisi di traffico e le analisi delle reti sociali, ma in ogni caso non includono nessun tipo di informazione riguardante registrazioni o trascrizioni del contenuto delle chiamate. [23]

Il 22 maggio del 206, la rivista Wired rivelò che il programma MAINWAY voleva che la NSA stabilisse *splitters* nei "core routing" di molte compagnie di telecomunicazione e nei principali centri di traffico Internet. Questo permetteva alla NSA di avere accesso diretto alla maggior parte delle telecomunicazioni e del traffico Internet degli USA. La NSA usò questa opportunità per effettuare ascolti e ordinare delle indagini rivolte a milioni di statunitensi senza precedenti. [24]

CAPITOLO 4
CASO SNOWDEN E LA RETE DI SORVEGLIANZA MONDIALE

4.1 Cronologia del Caso Snowden

Il caso Snowden è una notizia riguardante lo spionaggio e la sorveglianza, realizzato dal governo, più scioccante della storia. Edward Snowden, ex tecnico della CIA e della NSA (National Security Agency), rivelò tutta la verità su di una infrastruttura creata degli ultimi anni dal governo statunitense utile a raccogliere sistematicamente ogni tipo di informazione riguardante chiamate, e-mail e traffico internet di milioni di cittadini americani.

Il documentario "Citizenfour", diretto da Laura Poitras, parla di Edwars Snowden e delle sue rivelazioni sulla rete di sorveglianza mondiale. Lì si mostra come Snowden con l'aiuto del giornalista di prestigio del giornale britannico "The Guardian", Glenn Greenwald, pubblicherà gli articoli con tutte le informazioni relative allo spionaggio ai cittadini della NSA.

Il caso Snowden, però, non fu la prima notizia connessa con la sorveglianza del governo. Nel 2006, il tecnico Mark Klein svelò che la NSA aveva accesso alla rete di AT&T, e i clienti sporsero denuncia all'agenzia di sicurezza per aver acquisito dati privati. Si stimava che l'impresa AT&T fornì alla NSA, dal 2001, dopo l'attentato dell'11 settembre, 320 milioni di registri

diari. Il programma avviato era denominato “Stellar Wind”, in italiano “Vento Stellare”. Inizialmente monitorizzava solamente le e-mail scambiate tra i cittadini americani, fin quando non iniziò ad analizzare i metadati, tanto della telefonia quanto di Internet, di cittadini non statunitensi.

Il 3 giugno del 2013, Edward Snowden, si riunì per la prima volta con Laura Poitras e Glenn Greenwald. Questo incontro, avvenuto in un hotel di Hong Kong, ebbe una durata di 8 giorni, durante i quali Snowden raccontò tutta la verità circa la NSA, mostrando documenti confidenziali e di alta segretezza.

Il motivo per cui Snowden decise di mostrare le pratiche della NSA è la violazione della privacy dei cittadini che pensava stesse avvenendo. Ciò che cercò di fare, fu segnalare il potere usato contro delle persone incapaci di difendersi significativamente. Nel documentario parla inoltre dell’inizio di Internet, di come gli usuari erano sicuri si rispettasse la loro privacy. Oggigiorno, la gente fa più attenzione a ciò che cerca in rete, perché cosciente del fatto che da qualche parte c’è qualcuno che li sta controllando, e questo fa sì che le persone limitino la propria formazione intellettuale. Snowden non vuole che tale sorveglianza crei delle frontiere della libertà di ognuno, per questo descrive anche alcune delle tecniche della NSA, come per esempio, la sorveglianza e lo spionaggio realizzato attraverso i droni.

È così come la NSA, insieme alla collaborazione di altri governi, costruì un’infrastruttura a livello mondiale, la quale intercetta ogni tipo di comunicazione digitale, tanto radio quanto analogica. Tutte le comunicazioni sono intercettate in modo automatico, senza nessun obbiettivo concreto. [25]

Durante questi 8 giorni nell’Hotel The Mira, a Hong Kong, i giornali The Guardian e il The Washington Post pubblicarono notizie relative al misfatto. Tutto questo ebbe grandi conseguenze a livello mondiale. Gli USA erano al centro del mirino di tutti i media.

Così, il 7 giugno del 2013, i giornali The Guardian e il The Washinton Post rivelarono due programmi di spionaggio segreto. Uno dei due, di cui abbiamo già parlato in precedenza, riuniva i metadati delle chiamate telefoniche negli

USA. Il secondo programma segreto, denominato PRISM, permette all'intelligenza statunitense di accedere ai server delle principali compagnie di Internet con il pretesto di cercare connessioni con il terrorismo internazionale. Tra queste compagnie, troviamo Microsoft, Apple, Skype, Yahoo!, Google, Facebook e YouTube. Lo strumento che il governo utilizza come motore di ricerca per tutte le informazioni raccolte si denomina UDAQ.

L'11 giugno, The Guardian pubblicò una mappa globale istantanea della NSA, che possiamo vedere nella Figura 5, che rappresentava la raccolta dei dati elettronici nel marzo dello stesso anno. Questo programma è conosciuto come Boundless Informant, e la NSA lo usa per seguire la grande quantità di dati analizzati duranti periodi specifici. Se osserviamo l'immagine, distinguiamo in verde le zone con un livello inferiore di sorveglianza, ovvero dove sono stati raccolti meno dati, e in giallo e arancione le zone di maggiore controllo.

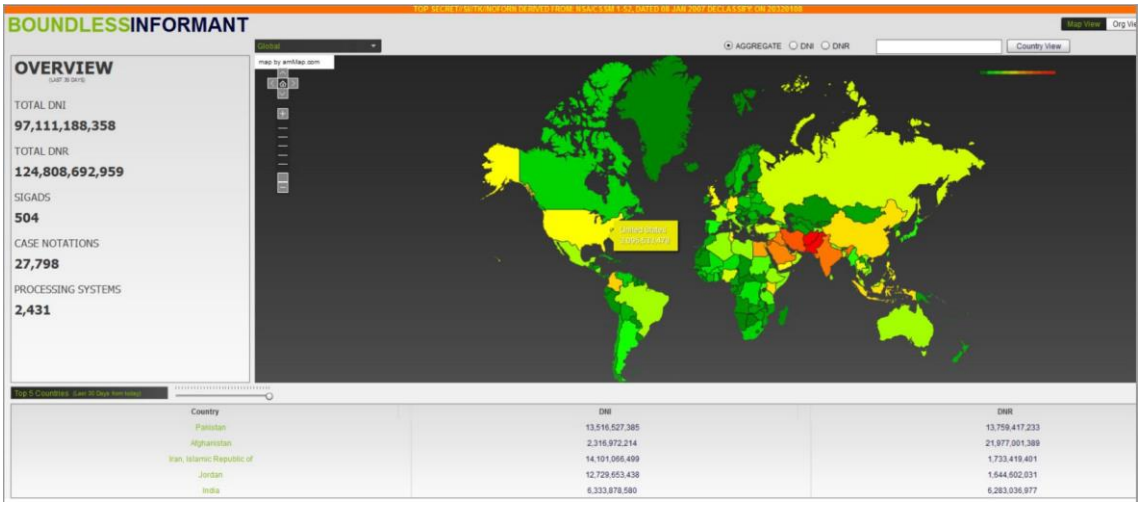

Figura 5: Instantanea di Boundless Informant

Nel giugno 2013, il giornale brasiliano *O Globo* segnalò alla NSA che aveva spiato milioni di e-mail e chiamate del proprio Paese [27], mentre Australia e Nuova Zelanda parteciparono all'operazione congiunta del sistema analitico globale XKeyScore della NSA. Secondo Snowden, la NSA creò accordi segreti di intelligenza con molti governi del mondo occidentale. Così, tra le numerose installazioni degli alleati occidentali che contribuirono a

XKeyScore, troviamo quattro installazioni in Australia e una in Nuova Zelanda:

- Pine Gap
- Stazione di ricezione di Shoal Bay
- Stazione di comunicazioni satellitari per la difesa dell'Australia
- HMAS Harman
- Stazione Waihopai

Le prime quattro appartengono al Paese australiano, le ultime corrispondono alla Nuova Zelanda. [28]

Durante il mese di luglio, il giornale The Guardian continuò a rivelare sempre più dettagli riguardanti l'XKeyScore della NSA, il quale permetteva agli analisti del governo di realizzare una ricerca attraverso gli ampli Database che contengono e-mail, conversazioni in linea e la cronologia delle ricerche di milioni di persone. Tutto questo succedeva senza nessun tipo di autorizzazione previa. Nella Figura 6 possiamo osservare una delle diapositive che include il programma di istruzione per il XKeyScore. Questo programma si distribuiva agli impiegati della NSA per imparare ad usare tale strumento. Come possiamo notare dall'immagine, gli analisti realizzavano ricerche relative ai numeri di telefono, e-mail ecc., sui Database. [29]

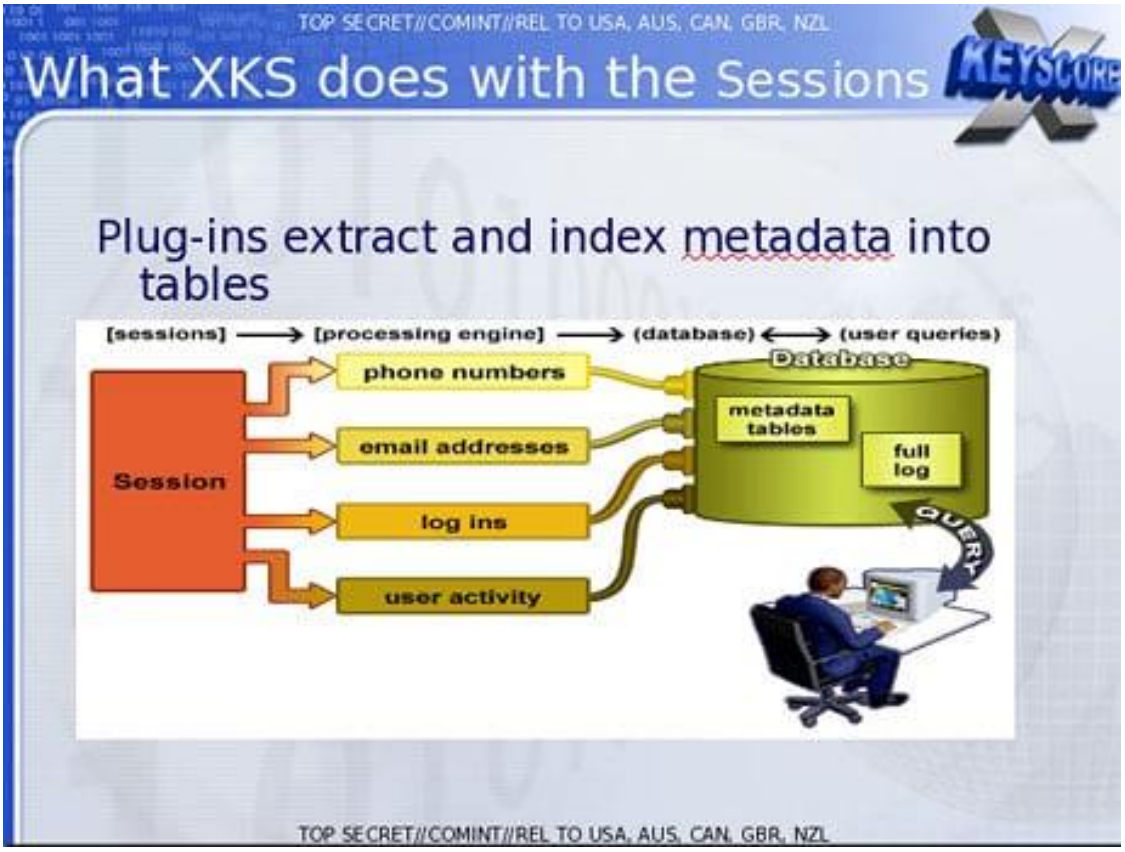

Figura 6: Diapositiva del programma di istruzioni del Xkeyscore

Nell'agosto del 2013, i documenti filtrati da Edward Snowden furono esaminati dai giornali tedeschi Süddeutsche Zeitung e Norddeutscher Rundfunk, i quali pubblicarono articoli rivelando la messa in scena di varie compagnie di telecomunicazioni che aiutarono la GCHQ (Government Communication Headquarters) britannica, dandogli accesso alle comunicazioni della fibra ottica. Gli operatori delle telecomunicazioni sono:

- Verizon Business
- British Telecommunications
- Vodafone Cable
- Global Crossing
- Level 3
- Viatel
- Interoute

A ognuno di loro venne assegnata un'area specifica della rete di fibra ottica della quale era responsabile. [30]

Si stima che la rete di sorveglianza della NSA fornì, durante quell'anno, il 75% di tutto il traffico Internet degli Stati Uniti al governo del Paese americano. [31]

Nel settembre del 2013, The Guardian e The New York Times continuarono a informare usando come loro fonte i documenti filtrati da Snowden. Rivelarono che la NSA collaborò con le imprese tecnologiche per cercare di distruggere i codici cifrati incorporati nei software commerciali. Inoltre fu specificato che il GCHQ aveva a disposizione una equipe per cercare di creare aperture nel traffico dati di Hotmail, Google, Facebook e Yahoo!. [32]

Successivamente rivelarono che Israele, Svezia e Italia collaborano con le agenzie di intelligenza statunitensi e britanniche. Attraverso la firma di un trattato segreto, le agenzie di intelligenza francesi trasferirono milioni di registri e metadati alla NSA. [33]

Così le analisi dei registri che la NSA applicava alle chiamate telefoniche, ai messaggi e alle e-mail per creare rappresentazioni grafiche, erano condivisi con l'intelligenza israeliana, senza eliminare previamente i dati riguardanti i cittadini statunitensi. [34]

Durante il mese di ottobre del 2013, videro la luce altri scandali riguardanti lo spionaggio degli USA. Pertanto, The Whashington Post e The Guardian insieme informarono la popolazione dei ripetuti tentativi della NSA e del GCHQ di spiare usuari anonimi che comunicavano tra loro attraverso la rete TOR. Molte di queste operazioni di sorveglianza includono l'inserimento di codici maligni all'interno dei computer degli usuari di TOR che visitavano pagine web specifiche. La NSA e il GCHQ riuscirono a bloccare l'accesso a questa pagina anonima reindirizzando gli utenti ad altre pagine non sicure. Le agenzie governative riuscirono quindi a scoprire l'identità di alcuni usuari anonimi di Internet. [35], [36].

La presentazione Power Point che pubblicò The Washington Post mostrava come la NSA avviava un plug-in di JavaScript per poter scoprire l'identità degli usuari della rete criptata TOR. Nella Figura 7, osserviamo una diapositiva di questa presentazione che spiega come gli usuari di tale rete potrebbero essere nemici dello Stato o terroristi.

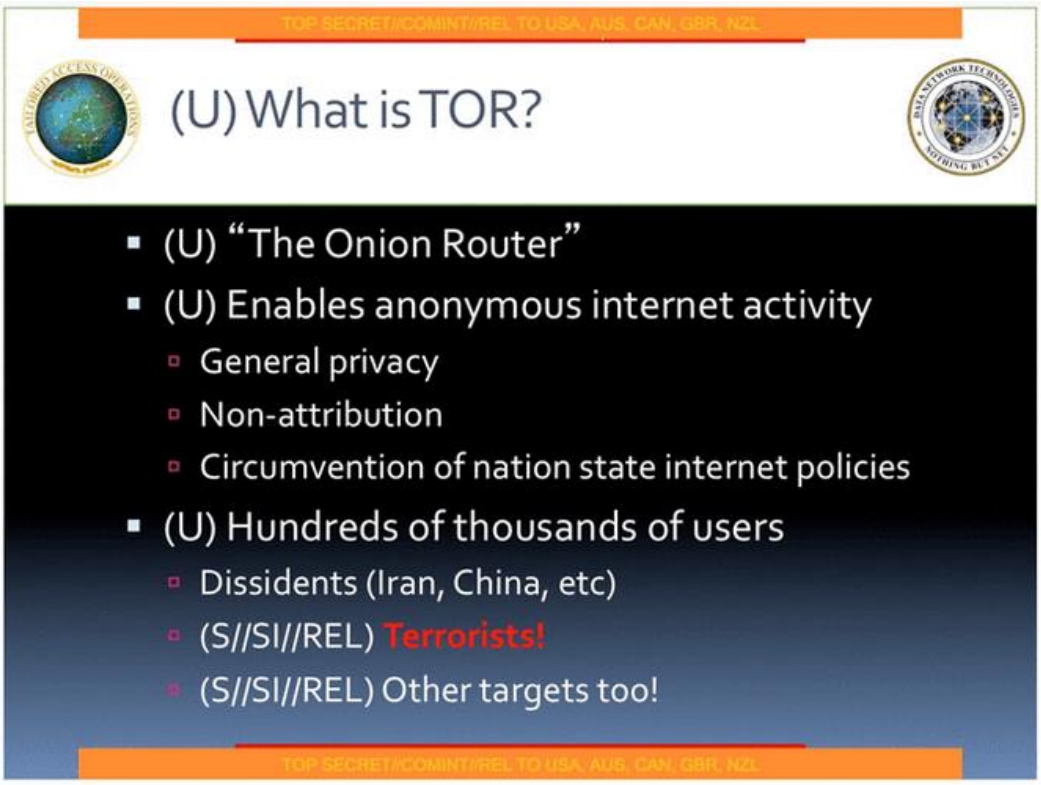

Figura 7: Diapositiva della presentazione su Tor della NSA

Successivamente rivelarono anche che la NSA monitorava gli account di posta elettronica dell'ex presidente messicano Felipe Calderòn Hinojosa, così come le e-mail dei vari membri di alto rango delle forze di sicurezza del Paese e i messaggi dell'attuale presidente Enrique Peña Nieto. La NSA cerca di raccogliere la maggior parte dei numeri di telefono fissi dei funzionari stranieri. Il contenuto delle chiamate telefoniche viene archiviato in Database di PC che possono essere analizzati periodicamente attraverso parole chiave. [37], [38]

Non solo vigilò gli importanti del Messico, la NSA monitorò le conversazioni telefoniche di 35 lider mondiali, notizia conosciuta grazie ad un articolo di Wall Street Journal, il 28 ottobre del 2013. Dal canto suo, il GCHQ cercò di mantenere segreti i suoi programmi si sorveglianza di massa, dato che temeva un dibattito pubblico dannoso che potesse condurre ad azioni legali contro l'agenzia e le sue attività. The Guardian rivelò che la NSA iniziò a monitorare le conversazioni telefoniche si questi lider dopo che gli vennero forniti i numeri di telefono da un funzionario di un altro dipartimento del governo statunitense. Un promemoria confidenziale della NSA animava gli alti funzionari della Casa Bianca, dello Stato e del Pentagono a condividere le proprie agende elettroniche, ciò che avrebbe permesso alle agenzie di avere accesso ai numeri di telefono dei principali politici e impresari stranieri di tutto il mondo al fine di migliorare i sistemi di sorveglianza. [39]

Nel novembre del 2013, si pubblicarono notizie su di un'operazione dal nome *Ironavenger*. La NSA intercettava e-mail provenienti da paesi alleati con gli USA e indirizzate ai paesi «avversari». Le e-mail alleate includevano un malware che la NSA usò per riunire documenti, password e credenziali di accesso appartenenti ai paesi nemici. [40]

Con il titolo *3G impact and update*, una presentazione di alta segretezza, filtrata da Snowden, rivelò i tentativi della CIA e del DDS per cercare di penetrare la tecnologia 3G in Indonesia e nel sudest asiatico. Insieme alla leggenda ASD/DDS, inserita nella parte inferiore della pagina, è possibile leggere: «Reveal their secrets—protect our own» ('rivelare i loro segreti, proteggere i nostri'). [41]

Il 23 novembre del 2013, il telegiornale neerlandese NRC Handelsblad pubblicò una presentazione segreta della NSA, filtrata da Snowden, dove si mostrano le cinque «classi di accesso» che la NSA utilizza nelle sue operazioni mondiali di intelligenza. Possiamo vederlo nella figura 8.

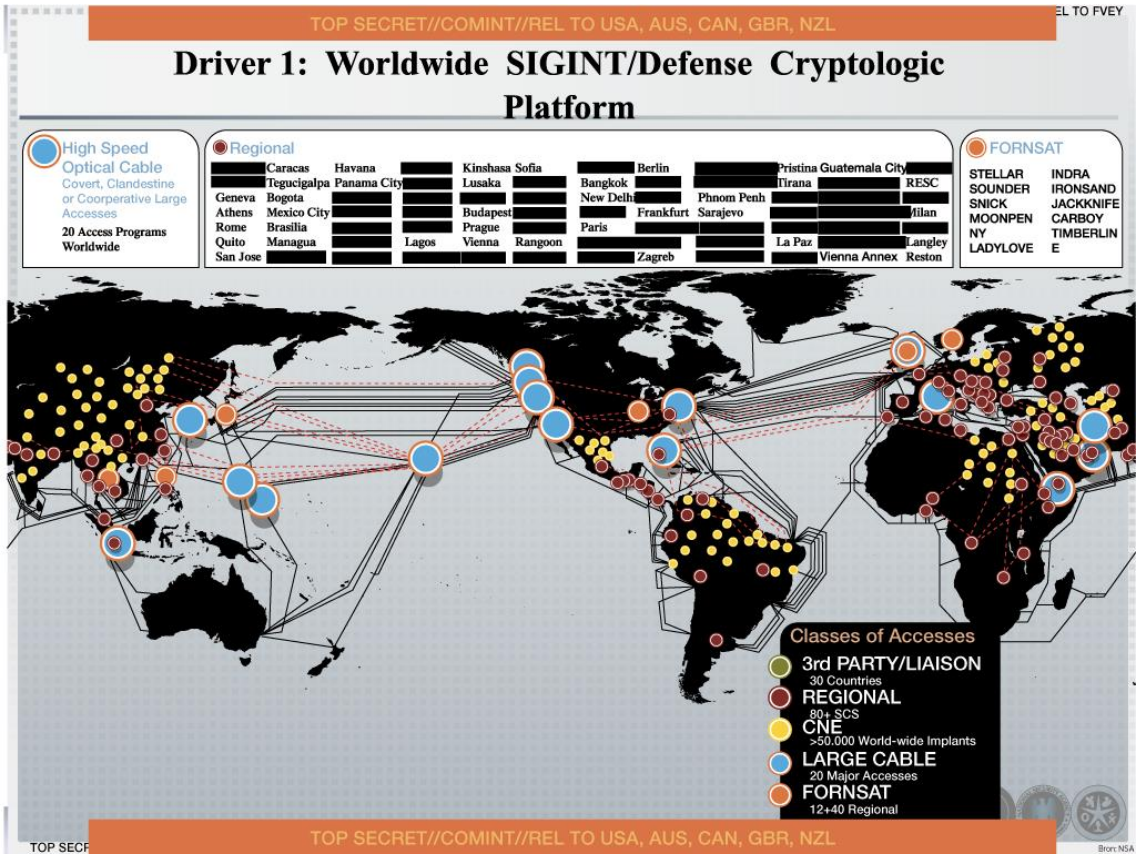

Figura 8: Mappa mondiale con le operazioni di intelligenza

Queste sono le cinque «classi di accesso»:

- 3rd PARTY/LIASON: dati forniti dai soci internazionali della NSA. A questi soci li si conosce come «terzi».
- REGIONAL: si riferisce a più di 80 servizi regionali speciali di raccolta (SCS). Il SCS è un programma segreto finanziato con fondi non dichiarati o di dubbia provenienza applicato dalla NSA e dalla CIA, con vari centri in diverse città come Atene, Bangkok, Berlino, Brasilia, Budapest, Francoforte, Ginevra, Lagos, Milano, Nuova Delhi, Parigi, Praga, Vienna e Zagabria, oltre che in altri posti come America Centrale, la penisola arabica, l'est asiatico e l'Europa continentale.
- CNE (Computer Network Exploitation). Il PDF rivelava che la NSA usava un sofisticato malware che infettò più di 50000 reti. Il malware aveva la capacità di rimanere nascosto durante diversi anni potendo essere attivato in qualsiasi momento per iniziare la raccolta di massa

di informazioni confidenziali. Secondo le rivelazioni, il malware sarebbe stato sviluppato da Tailored Access Operations (TAO), uno dei dipartimenti dell'elite della NSA che assume milioni di hacker altamente qualificati. I suoi centri di direzione si trovano in Brasile, China, Egitto, India, Messico, Arabia Saudita, e in altri paesi dell'Europa dell'est.

- LARGE CABLE: i 20 principali punti di accesso, la maggior parte si trovano negli USA.
- FORNSAT: abbreviatura di Foreign Satellite Collection (Raccolta di satelliti stranieri). Si riferisce ai dati che la NSA intercettava da una serie di satelliti spaziali di paesi come la Gran Bretagna, la Norvegia, il Giappone o le Filippine.

Nel dicembre del 2013, The Guardian pubblicò, d'accordo con i documenti filtrati da Snowden, che l'Australian Signals Directorate offrì la possibilità di condividere informazioni sui cittadini australiani con il resto degli organismi dell'intelligenza dell'UKUSA, la quale era un'alleanza delle nazioni anglofone formata nel 1946 con il proposito di raccogliere informazioni sull'intelligenza. UKUSA è formata da:

- Stati Uniti, attraverso la NSA
- Regno Unito
- Canada
- Australia
- Nuova Zelanda

I dati sarebbero stati condivisi con questi Paesi stranieri senza che fossero stati precedentemente controllati. Inoltre, i dati contenevano informazioni mediche, legali e religiose (private) dei cittadini. [42]

Nello stesso mese, The Washington Post rivelò che la NSA aveva seguito la localizzazione dei cellulari di tutto il mondo grazie ai cavi che connettono le reti mobili a livello mondiale e che danno servizio ai telefoni cellulari degli USA e di tutto il mondo. In questo processo, la NSA raccoglie al giorno più di

5000 milioni di registri di localizzazione. Questo permette agli analisti della NSA di mappare i movimenti dei proprietari dei telefoni attraverso sensori di movimento e attraverso i dati incrociati con i milioni di dati di altri usuari. [43]

The Washington Post informò ancora del fatto che la NSA fa uso dei dati di localizzazione e degli archivi tracciati della pubblicità generata attraverso strumenti di navigazione Internet. Questi strumenti permettono agli annuncianti di Internet di seguire i consumatori che utilizzano motori di ricerca come Google. La NSA usa questi dati per ottenere informazioni su possibili obbiettivi, stabilire chiaramente gli obbiettivi per il governo e sorvegliare possibili pirati informatici. Con questi cookies pubblicitari usati da Google inoltre, e d'accordo con i documenti filtrati da Snowden, la NSA ha riunito informazioni sugli accessi attraverso la TAO (Tailored Access Operations) in collaborazione con il GCHQ britannico. [44], [45]

La NSA è stata capace di rompere anche la tecnologia criptata telefonica, la A5/1. D'accordo con un documento classificato filtrato da Snowden, l'agenzia riuscì a rompere il codice senza ancora conoscere le password. Inoltre, la NSA usa diversi tipi di infrastrutture mobili, tali come vincoli tra le reti degli operatori, utili a determinare la posizione degli usuari. [46]

Negli anni precedenti al 2013, tanto il governo degli Stati Uniti, così come le agenzie dell'intelligenza britannica, si focalizzarono sul sorvegliare 1100 obbiettivi. Tra questi obbiettivi si trovava il primo ministro di Israele, vari impresari di imprese energetiche straniere e un pezzo grosso dell'Unione Europea che in quel momento si trovava di fronte a varie compagnie telefoniche statunitensi accusate di monopolio. [47]

Il 4 dicembre del 2013, The Washington Post pubblicò un documento interno della NSA filtrato da Snowden che possiamo vedere nella Figura 9. Questo diagramma illustra la raccolta di massa di metadati proveniente da telefoni cellulari che arrivò a circa 5000 milioni di registri in un solo giorno. [43]

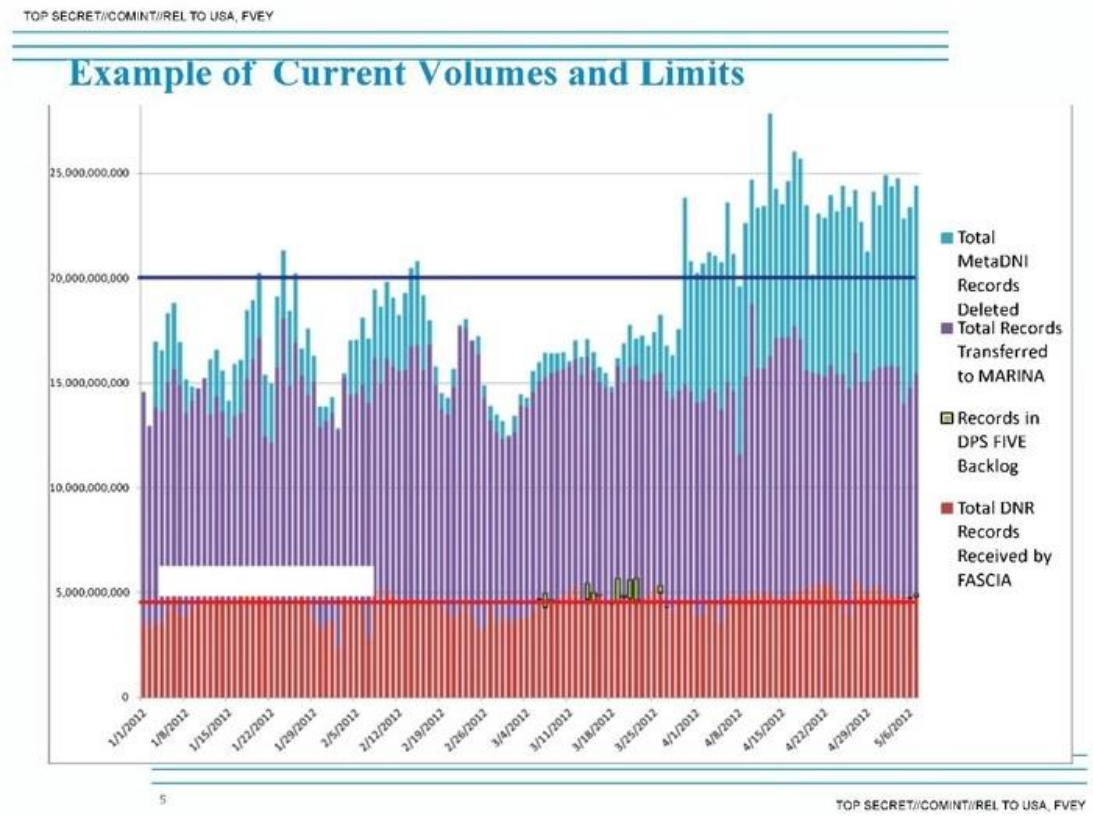

Figura 9: Diagramma con la quantità di metadati raccolti durate il 2012

A parte i programmi segreti attivi negli USA, Snowden informa di TEMPORA, un sistema informatico segreto usato dal GCHQ, uno dei tre servizi di intelligenza del Regno Unito. Questo sistema intercetta le comunicazioni nei cavi in fibra ottica, i quali costituiscono la colonna vertebrale delle compagnie di Internet. A differenza degli Stati Uniti, questo sistema riuniva sia i metadati di massa sia l'informazione completa delle telecomunicazioni senza avere obbiettivi ben definiti. Snowden affermò che i dati raccolti dal programma TEMPORA sono condivisi con la NSA. A differenza che negli Stati Uniti, nel Regno Unito la NSA poteva usare TEMPORA senza limiti. [48], [49], [50]

La prima persona che pagò le conseguenze di tali dichiarazioni fu, ovviamente, lo stesso Edward Snowden. Il paese si divise in due parti: quelli che lo accusavano di aver tradito il Paese e quelli che lo difendevano per aver confessato un segreto nazionale che violava la privacy di milioni di persone.

Una settimana dopo le pubblicazioni, le autorità degli Stati Uniti presentarono tre accuse di spionaggio e frode di proprietà del governo contro Snowden, temendo che potesse filtrare i dati alla Cina. Gli USA richiedono la cattura di Snowden a Hong Kong. Prima che riuscissero a prenderlo, però, Snowden abbandonò il Giappone scappando a Mosca in un volo commerciale. Il Governo americano annullò il suo permesso di soggiorno così da obbligarlo a rimanere nell'aeroporto di Mosca durante 20 giorni, ma il Governo russo si rifiutò di trasferirlo dato che non c'era nessun trattato bilaterale con gli Stati Uniti, in questo modo Snowden si convertì in clandestino per la sua sicurezza.

Barack Obama, presidente degli Stati Uniti, dovette esporsi e parlare avanti ai media per poter dare spiegazioni sul caso Snowden. Accusò quest'ultimo di aver filtrato informazioni confidenziali difendendo il lavoro della NSA, definendolo a favore della sicurezza e contro il terrorismo. Mesi dopo, il Governo tedesco scopre che il Governo americano durante anni spiò il cellulare della cancelliera tedesca Angela Merkel. Quest'ultima chiese informazioni al presidente Americano, il quale negò totalmente il controllo delle reti tedesche da parte dell'intelligenza. [51]

Un'altra persona che fu coinvolta nelle dichiarazioni fu il direttore dell'Intelligenza Nazionale degli USA, James Clapper. Nel marzo del 2013, dichiarò che la NSA non raccoglieva nessun tipo di informazione dei cittadini americani, o almeno non volontariamente. Quando però le dichiarazioni di Snowden vennero fuori, due rappresentanti degli Stati Uniti accusarono Clapper di spergiuro e esigerono le dimissioni per aver testimoniato il falso sotto giuramento e aver ostruito la giustizia.

Così, il caso Snowden rivelò al mondo l'infrastruttura della sorveglianza e dello spionaggio a livello mondiale che i governi usano contro i loro cittadini attraverso le telecomunicazioni. L'atto di Snowden, pur avendo messo a rischio la sua vita e la sua libertà, servì per dimostrare al mondo i controlli ai quali siamo sottomessi senza esserne a conoscenza. [52]

4.2 Rivelazione dopo sul la rete de sorveglianza mondiale

Durante la seconda metà dell'anno 2013, le filtrazioni di documenti segreti da parte di Snowden e le pubblicazioni sul The Guardian e sul Washington Post danneggiarono gravemente l'immagine del governo e dei servizi di intelligenza degli USA. In quel periodo, abbiamo potuto vedere pubblicazioni e notizie della stampa internazionale che fecero uscire alla luce un'impalcatura che dimostra la vigilanza che, principalmente le agenzie di intelligenza degli Stati Uniti, insieme alla collaborazione di altri paesi alleati, stavano esercitando in forma massiccia sulla popolazione mondiale.

Ma, quando finì il 2013, non fermarono le rivelazioni su questa impalcatura di vigilanza mondiale.

Secondo dei dati di Gennaio di 2014, la NSA stava lavorando con un computer quantico, capace di rompere ogni tipo di cifrato e qualunque codice di sicurezza simile. Questo importante progetto fa parte di un programma di investigazione che il governo degli USA ha dotato con 80 milioni di dollari di presupposto, chiamato Penetrating Hard Targets. È un'estesa investigazione che si è sviluppato in abitacoli blindati chiamati Gabbie da Faraday. Questo tipo di stanze sono progettate affinché non penetri o esca nessun tipo di radiazione elettromagnetica. Attualmente, la NSA è vicina ad ottenere questi computer quantici. Una volta che saranno completamente sviluppati, le agenzie di intelligenza potranno sbloccare ed avere accesso a tutti i dati di banche, carte di credito, governi, etc.. [52]-[55]

Giorni dopo, il New York Times pubblicò che la NSA starebbe controllando quasi 100000 calcolatrici in tutto il mondo, grazie ad un software spia chiamato Cuanto. Questo malware permette alla NSA di controllare e vigilare queste squadre, potendo realizzare con essi attacchi cibernetici. Tra gli obiettivi di questi attacchi ci sono gli eserciti cinesi e russi. Altri obiettivi distaccati da questi attacchi sono istituzioni dell'Unione Europea. In questo

stesso articolo, si parla anche di una nuova tecnologia segreta, che la NSA usa dal 2008, per potere accedere e manipolare computer che non siano connessi ad Internet. Questo metodo consiste nell'inserzione fisica di un hardware della radio di alta frequenza per un fabbricante, un spia o perfino una persona in maniera involontaria. Questo hardware invia onde di radio per un canale segreto e può trasmettersi delle placche di circuiti piccoli a biglietti o dispositivi USB inserito nel computer. Anche le ordine potrebbero inviarsi ad una stazione ricevente stabilita per i servizi di intelligenza a chilometri di distanza. Anche questo metodo serve per trasmettere già un nuovo malware al computer infettato. [56]

Channel 4, durante questo mese, rivelò una parte ancora più segreta della NSA, il database Dishfire che redige giornalmente cento milioni di messaggi di testo. L'intelligenza britannica, GCHQ, avrebbe accesso totale al database che utilizza per ottenere informazioni private della popolazione britannica per l'esistenza di una laguna legale nelle leggi del paese. Questo enorme database ha un complemento, l'attrezzo chiamato Prefer Program. Questo attrezzo fu creato per estrarre i distinti tipi di informazione addizionale dei messaggi di testo, come chiamate perse dei contatti. [57]

Alla fine del mese di gennaio, pubblicarono sui periodici New York Times, ProPublica e The Guaridan la notizia che la NSA degli USA ed il GCHQ britannico cominciavano a lavorare uniti per redigere ed immagazzinare dati grazie all'uso di software installati nelle applicazioni degli smartphones. Secondo documenti filtrati per Snowden, questa pratica sarebbe cominciata nel 2007. In questi documenti si legge che qualsiasi persona che utilizzi Google Maps in un Smartphone sta appoggiando i sistemi del GCHQ. La NSA e la GCHQ utilizzano distinti metodi per raccogliere dati di localizzazione, piani di viaggi, contatti e dati geolocalizzati di immagini edite nelle versioni mobili di reti sociali come Twitter o Facebook. In un documento del GCHQ si spiega l'applicazione come spia, a partire dal gioco Angry Birds, redige dati

degli utenti. I dati raccolti di questo tipo di applicazioni permettono alle agenzie di intelligenza di creare un profilo di una persona, sapere il suo modo di vita e tutta la sua informazione personale. [58],[59]

Nella Figura 10, localizzata sotto a queste linee, possiamo osservare una diapositiva di una presentazione della NSA, filtrata per Edward Snowden. Questa diapositiva rivela la portata delle agenzie di intelligenza, sulla vigilanza in smartphones. I dati spiati per la NSA includono l'informazione del suo telefono, le sue connessioni di rete, curriculum di ricerca nella web, contatti e perfino i documenti scaricati. [60]

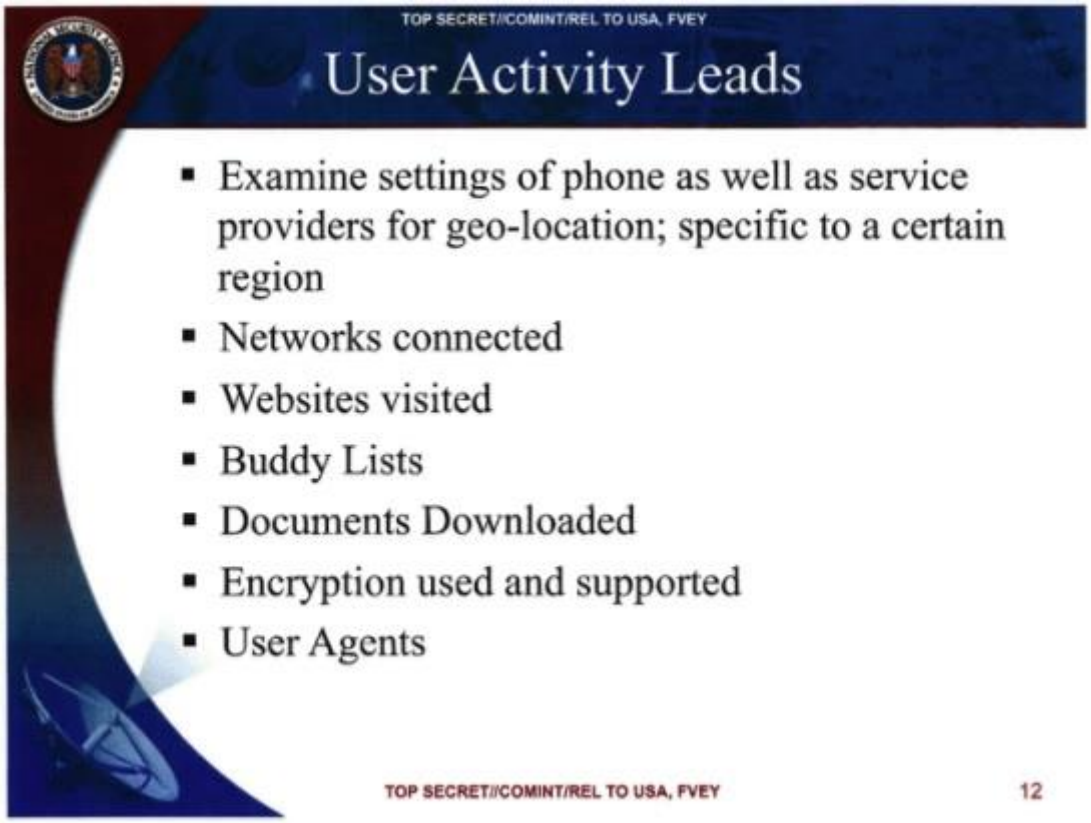

Figura 10: Diapositiva della NSA su spionaggio in smartphones [60]

Nella Figura 11, vediamo gli obiettivi dello spionaggio, cioè, le fonti di

informazione che dovevano essere controllate per ottenere tutti i dati degli smartphones. [60]

Figura 11: Diapositiva della NSA su spionaggio in smartphones [60]

Un'altra delle notizie che ha visto la luce nel gennaio 2014, grazie al giornalista Glenn Greenwald, è quella di un documento del GCHQ britannico, dove si descrive un programma di vigilanza chiamato Squeaky Dolphin che permetteva di seguire, in tempo reale, le attività di una persona. Queste attività potevano essere i video di YouTube che stava vedendo in diretto o perfino i 'Likes' su Facebook. Tutto questo succedeva senza la conoscenza di dette compagnie che prestavano servizi. Questo programma era capace di riunire, analizzare ed utilizzare i dati con fini analitiche. [61]

Il 4 Febbraio del 2014, il The Guardian pubblica la notizia che l'antico cancelliere tedesco era stato monitorizzato dal 2002. Queste rivelazioni hanno la sua origine, un'altra volta, nei documenti filtrati da Snowden. Il motivo di questo spionaggio al cancelliere sarebbe stato dovuto all'opposizione del governo tedesco all'intervento militare in Iraq. In detto documento, esiste una lista che trattiene i nomi dalle persone ed istituzioni che erano sotto vigilanza della NSA. [62]

Anche in quel mese, il servizio di intelligenza britannico GCHQ lanciò un attacco cibernetico alla più famosa rete di attivisti, Anonymous. Realizzarono un attacco di rifiuto di servizio (Dos) per cercare di chiudere una pagina di chat frequentato da membri di questa rete. L'attacco si denominò Rolling Thunder. Questo attacco non riuscì a rivelare le identità di detti membri di Anonymous. [63]

Il 12 Marzo del 2014, Glenn Greenwald va alla ribalta con un altro articolo, svelando pratiche segrete della NSA. Racconta il possesso della NSA di un'infrastruttura che permette di hackerare computer di forma massiccia, grazie a programmi automatizzati che riducono la necessità di intervento umano nel processo. Il sistema si chiama TURBINE e permette di gestire e controllare una gran rete di impianti di malware, trasmettendolo a dispositivi informatici di forma remota. È progettato affinché possa gestire milioni di impianti di malware di forma simultanea. Gli archivi ottenuti per la NSA sono condivisi coi suoi alleati dell'alleanza Cinque Occhi. Questa alleanza lavora in Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti; gli stessi paesi che formano UKUSA.

Le funzioni di TURBINE permettono alla NSA di:

- Infettare archivi e hard disk, potendo avere accesso completo ad essi.

- Registrare audio e video di forma nascosta utilizzando i microfoni e la camera web delle squadre infettate.

- Lanciare attacchi cibernetici, di rifiuto di servizio (Dos), verso determinato posti web.

- Poter infettare unità USB per ampliare la rete di squadre infettate.

Detti impianti di TURBINE sono vincolati ad un'estesa rete di vigilanza clandestina che la NSA controlla in tutto il mondo. Questi sensori controllano i pacchetti di dati che si inviano attraverso Internet.

Quando uno di impiantali identifica in maniera automatica l'informazione, la devia verso la NSA affinché sia analizzata. Nel caso in cui gli obiettivi si stiano comunicando, si inviano vigili a TURBINE affinché cominci l'attacco con malware. Per identificare gli obiettivi da vigilare, si usano una serie di "selettori" progettati man mano che si trasmettono attraverso Internet.[64]-[66]

Questi selettori possono raccogliere direzioni di posta, IP, cookies che contengano nomi di utente o identificazioni provenienti da posti come Google, Facebook, Hotmail, Yahoo! e Twitter. Questi "cookies" di pubblicità di Google raccolgono i curriculum di navigazione, impronte digitali e chiavi che permettono inseguire l'utente ed identificare il computer dal quale si collega ad Internet. [66]

Il 18 Marzo del 2014, il The Washington Post pubblica un programma segreto della NSA, chiamato MYSTIC, il quale si mise in funzionamento nel 2009. Questi programmi, insieme a quelli complementari, permette di registrare il 100% delle chiamate telefoniche provenienti da un paese straniero e dopo recuperare ed analizzare quelle fino a un mese prima. La NSA rivedeva ed analizzava le chiamate ed il suo metadatos. Con questa

capacità di immagazzinamento, la NSA aveva la capacità di rivedere il curriculum per vedere i movimenti di un individuo, piani e persone relazionate con detto individuo. [67]

Alcuni giorni più tardi, The New York Times svela che la NSA starebbe spiando la compagnia di tecnologia cinese Huawei, fabbricante di smartphones, tables ed infrastrutture di telecomunicazioni. La NSA, in un'operazione chiamata Shotgiant, accede ad archivi di posta di Huawei ed ai codici dei suoi prodotti. Il governo degli Stati Uniti temeva che Huawei cooperasse con l'Esercito Popolare di Liberazione, le forze armate della Cina, ed il governo di quel paese per le attività di cyberspionaggio o cyberguerra. Gli obiettivi dell'operazione della NSA erano valutare questa relazione ed imparare ad attuare i piani del governo cinese, ma anche utilizzare i dati ottenuti di Huawei per spiare i suoi clienti, come Iran, Afghanistan, Pakistan, Kenya e Cuba. L'ex presidente della Cina, Hu Jintao, il Ministero del Commercio cinese e le principali banche del paese anche furono sotto vigilanza della NSA. [68],[69]

Alla fine dl marzo 2014, Der Spiegel e The Intercept pubblicarono una serie di documenti segreti, relazionati con gli sforzi del GCHQ e la NSA per spiare alla Germania. Il GCHQ britannico utilizzò fino a tre imprese tedesche di analisi di dati per potere ottenere informazione del traffico di Internet in Germania, come i principali fornitori e le tendenze future nel settore sull'impiego e sulla tecnologia. Il Tribunale di Vigilanza di Intelligenza Straniera autorizzò alla NSA per vigilare in forma continua ed a persone ed istituzioni tedesche, indipendentemente se quelli spiati fossero o no, potenziali sospettati di qualche delitto.

Il cancelliere tedesco, Angela Merkel, era compresa nella lista di persone vigilate, vicino ad altri 121 leader stranieri. I dati raccolti si immagazzinavano in un database chiamato Nymrod. La NSA utilizzava il sistema Nymrod per trovare informazioni relative ad obiettivi che altrimenti sarebbero impossibili

da inseguire. Secondo gli archivi segreti della NSA, il database conta su relazioni segrete, comunicazioni intercettate e trascrizioni complete di fax e chiamate telefoniche. [70],[71]

CAPITOLO 5
SITUAZIONE ATUALE

5.1 Leggi internazionali sulla protezione di dati e la privacy

5.1.1 Electronic Communications Privacy Act (ECPA)

La prima delle leggi che citeremo è la Legge sulla Privacy delle Comunicazioni ettroniche. Questa legge emanata dal Governo degli Stati Uniti stabilisce norme su come il governo può accedere alle informazioni digitali della popolazione. Fu approvata nel 1986, e da allora, nonostante la tecnologia si sia continuamente evoluta, questa legge è rimasta ancora arretrata.

Il Capitolo I de la ECPA protegge le comunicazioni telefoniche ed elettroniche durante la loro circolazione e inoltre stabilisce requisiti molto rigidi in tale ambito piuttosto che in altri.

Il Capitolo II de la ECPA è la Legge di Comunicazioni Memorizzate.

Protegge le comunicazioni registrate nelle Memorie elettroniche e soprattutto i messaggi salvati nei computer. Questa legge è meno rigida del Capitolo I sull'accesso alle informazioni.

Il Capitolo III proibisce l'uso di pendrives registratori o di servizi di pianta per registrare marcature, instradamento o l'indirizzamento del processo di trasmissione di comunicazioni, senza l'ottenimento di un ordine giudiziale previo.

Il movimento che difende la riforma dell'ECPA denuncia la facilità con cui il Governo degli USA ottiene archivi elettronici senza la necessità di nessun ordine giudiziale

Tale legge ha ricevuto critiche per la sua arretratezza e al modo in cui permettesse alle persone di condividere, immagazzinare ed usare l'informazione.

L'ECPA permette al Governo di accedere alle comunicazioni digitali, come la posta elettronica o messaggi di Facebook, con un semplice mandato di comparazione, (e non un ordine del tribunale), una volta che tali archivi siano più vecchi di 180 giorni. [72]

5.1.2 Cyber Intelligence Sharing and Protection (CISPA)

CISPA è un disegno di legge degli Stati Uniti che permette lo scambio di informazioni di traffico di Internet tra io governo degli USA e le imprese.

L'obiettivo di tale progetto è di individuare le minacce cibernetiche e garantire la sicurezza delle reti contro gli attacchi cibernetici.

Questo disegno di legge è stato appoggiato dalle corporazioni come Microsoft, Facebook, e perfino dalla Camera di Commercio degli USA, che vede in questa legge un metodo efficace di condivisione dell'informazione importante sulle minacce cibernetiche con il governo. Al contrario i difensori della privacy in Internet come l'Electronic Frontier Foundation (EFF) criticano questa legge, poiché limita pochissimo il governo sull'ottenimento e la manipolazione dell'informazione della navigazione in Internet.

Sostengono anche che uno dei maggiori problemi sono le ampie definizioni su quello che è una minaccia cibernetica. Mark Stanley, direttore di campagne e comunicazioni del centro Democrazia e Tecnologia (CDT),

assicura che uno degli aspetti preoccupanti di questa legge, è che l'informazione proporzionata al governo degli USA è dedita alla NSA.

Questa, essendo una divisione militare, mantiene nascosto cosa si impadronisce dell'informazione ricevuta.

Il problema si manifesta quando i dati forniti dalle imprese sono dati personali. Non si sa come quell' informazione sarà utilizzata. La CDT sta sollecitando norme che regolino il modo e l'uso di quell'informazione da parte delle organizzazioni del governo.

5.1.3 Computer Fraud and Abuse (CFAA)

Nel 1986 si promulgó la legge CFAA contro la frode e l'abuso dei computer. Questa legge considera un delitto federale l'accedere e il condividere informazioni protette. Inoltre, questa legge proibisce l'accesso a un computer senza autorizzazione

Questo disegno di legge fu promulgato in risposta alle preoccupazioni che i delitti informatici rimanessero impuniti. Tuttavia per anni, associazioni come l'Electronic Frontier Foundation ha chiesto che la legge si riformi, riducendo le sanzioni per violare le CFAA

Non avendo definito in modo chiaro come violare le CFAA. [73]

5.1.4 Trans Pacific-Partnership Agreement (TTP)

Fino ad ora si è parlato delle leggi riguardanti gli Stati Uniti e la sua legislazione. Tuttavia, l'Accordo transpacifico di Cooperazione Economica colpì inizialmente nove Paesi, redatto e firmato nel 2015. Questi Paesi erano Stati Uniti, Perù, Cile, Vietnam, Singapore, Malesia, Australia, Brunei e Nuova Zelanda. Questo accordo è un trattato di libero commercio multilaterale che fu negoziato in gran segreto per cinque anni. [74], [75]

Il TTP potrebbe ampliare gli standard di proprietà intellettuale degli USA ad altri Paesi, e rinforzare le leggi vigenti sulla proprietà intellettuale degli Stati Uniti. I gruppi difensori della tecnologia temono l'impatto che il TTP

possa avere sui diritti digitali di autore tanto negli Stati Uniti come a livello internazionale.

Inizialmente questa legge fu fortemente promossa per il Paese nordamericano. Nel gennaio del 2017, però, il presidente nordamericano Donald Trump ha firmato la ritirata definitiva degli Stati Uniti dal trattato, ed è per questo che virtualmente l'entrata in vigore di tale trattato risulta impossibile. [76]

5.2 Dibattito tra la sicurezza nazionale e la privacy

G Il dibattito tra la primazia della privacy relativo alla sicurezza nazionale e viceversa è un tema cadente. Da quando tutto il mondo ha iniziato ad avere accesso ai dispositivi elettronici, da quando tutti sentiamo la necessità di condividere le nostre vite nelle reti sociali, e soprattutto, a partire dal boom degli Smatphone e dalla facilità di averne uno e poter accedere alla rete, questo dibattito ha preso sempre più piede aumentando la sua importanza.

L'inizio, pertanto, è qualcosa di indefinito: Quando inizio questa guerra? Quando iniziammo ad essere gelosi della nostra privacy? Quando si iniziò a dire che la sicurezza nazionale era superiore a quest'ultima?

Per iniziare a capire questo dibattito, è necessario prima di tutto chiarire due termini chiave che si trovano contrapposti: Privacy e Sicurezza Nazionale.

5.2.1 Privacy

Secondo la Real Academia de la lengua Española – conosciuta come RAE – al cercare "privacy" otteniamo:

Privacy:

1.f Qualità di privato

2.f. Ambito della vita privata che si deve proteggere da qualsiasi intromissione.

Per l'obbiettivo di questo lavoro, sceglieremo il secondo significato. Si dice che abbiamo il diritto di proteggere questa sfera d'intimità, pertanto si può dedurre che esiste un diritto di privacy. Vediamo come raggiungerlo.

Nella Costituzione Spagnola, questo diritto lo troviamo raccolto nella sezione dei diritti Fondamentali, ossia, i basici, i più importanti, gli inalienabili. La Costituzione Spagnola, non lo chiama direttamente "Diritto di Privacy", bensì lo definisce con altri termini:

Articolo 18

1. Si garantisce il diritto all'onore, all'intimità personale e familiare e alla propria immagine.
2. Il domicilio è inviolabile. Nessuna entrata o registro potrà avvenire senza il consenso del titolare o di un mandato giudiziale, tranne in caso di delitto.
3. Si garantisce il segreto delle comunicazioni e, specialmente, delle lettere, telegrafiche e telefoniche, tranne in caso di mandato.
4. La legge limiterà l'uso dell'informatica per garantire l'onore e l'intimità personale e familiare dei cittadini e il pieno esercizio dei suoi diritti.

La Costituzione Spagnola, quindi, si riferisce a questi diritti come diritti all'intimità personale e familiare, al segreto delle comunicazioni ecc. Questi sono solo alcuni componenti basici che costituiscono questo diritto.

Però non è solo nel caso spagnolo che questo diritto resta raccolto, possiamo infatti trovare referenze dello stesso in una delle dichiarazioni più importanti della storia recente, ovvero nella Dichiarazione Universale dei Diritti Umani. [77],[78]

"Articolo 12:

Nessuno sarà oggetto di ingerenze arbitrarie nella vita privata, con la propria famiglia, nel proprio domicilio o nella corrispondenza, né di attacchi al pudore o alla propria reputazione. Tutte le persone hanno diritto alla protezione della legge contro tali ingerenze o attacchi."

Neanche in questo caso, come possiamo notare, si fa riferimento diretto alla privacy; non la si chiama mai per nome. Ma che cos'è la privacy se non poter fare ciò che si desidera nella propria sfera intima e personale?

Anche nella "Carta de los derechos Fundamentales de la Unión Europea" (Lettera dei diritti fondamentali dell'UE) – da questo momento, CDFUE – di cui si discute nell'art.7, di definisce come "ogni persona ha rispetto della propria vita privata e familiare, del suo domicilio e delle sue comunicazioni.

In ogni caso si trovano anche molteplici meccanismi e organi internazionali messi a disposizione per proteggere tale diritto:

- Comitato dei diritti umani delle Nazioni Unite;
- Rappresentante speciale dei difensori dei diritti umani;
- Procedimento 1503;
- Commissione Interamericana sui Diritti Umani e dei Paesi;
- Tribunale Europeo dei Diritti Umani;

Anche il Tribunale della Giustizia dell'Unione Europea fa riferimento a questo termine in varie sentenze:

Sentenza Carolina contro Germania, del 24 giugno del 2004, nella quale si garantisce il rispetto per tutti gli individui: "di uno spazio nel quale sia possibile sviluppare la propria personalità senza intromissioni esterne, che non include solo la sfera privata bensì che in un certo senso proietta allo stesso tempo la protezione in uno spazio pubblico, sempre che non comporti una rilevanza sociale o un interesse generale"

Un altro tema molto relazionato con la privacy, che deriva da essa, è la sicurezza nazionale:

Diritto derivato dalla protezione dei dati. Esistono due strumenti internazionali di protezione di dati: la Convenzione per la protezione delle persone, rispetto al Trattamento Automatizzato dei dati di carattere personale del Consiglio Europeo, del 28 gennaio 1981, e le direttrici della OCDE.

La prima, definita nell'art.8 CDFUE: "ogni persona ha il diritto che i propri dati personali restino protetti così come che i dati si trattino in modo leale, per fini concreti e ricevendo il consenso della persona concreta o in virtù di qualsiasi altro fondamento legittimo stabilito dalla legge".

Una volta definito il termine privacy, passiamo al termine successivo.

5.2.2 Sicurezza Nazionale

Questo è un termine dotato di molti significati, di molti modi di vederlo e di capirne i limiti. Per alcuni, la sicurezza nazionale è tutto, per altri è importante e si deve mettere a bilancio con altri aspetti e altri diritti della vita diaria.

Purtroppo non possiamo dare una definizione corretta di questo fenomeno, il concetto di sicurezza nazionale si è evoluto con le trasformazioni globali, e in questo modo, si vuole posizionare di fronte alle sfide della nostra società attuale, la quale si evolve e cambia di pari passo con il concetto stesso.

La sicurezza nazionale, si riferisce alla nozione di relativa stabilità, calma o predicibilità che si suppone sia beneficiosa per lo sviluppo di un paese, così come alle risorse e alle strategie per ottenerla (attraverso la difesa nazionale).

Possiamo definirlo, a grandi linee, come l'azione dello Stato utile a proteggere la libertà e il benessere dei suoi cittadini, a garantire la difesa di un Paese in concreto e i suoi princìpi e valori.

Così sul sito del governo Spagnolo, nell'appartato della sicurezza nazionale troviamo quest'ultima definita come l'azione dello Stato rivolta a proteggere la libertà e il benessere dei suoi cittadini, a garantire la difesa Spagnola, i suoi principi e valori Costituzionali, come anche a contribuire con i nostri alleati alla sicurezza internazionale compiendo i compromessi assunti.

La sicurezza nazionale si relaziona anche con un altro concetto apparso recentemente, "la sicurezza umana". Questo è un concetto legato alla

definizione di ordina pubblico al punto che molte volte vengono usati come sinonimi.

Se la sicurezza umana si usa nell'ambito di una società concreta, in uno spazio concreto e in un determinato tempo, la sicurezza nazionale consiste in una società, come insieme, come un ente dotato di relazioni esteriori che non si può limitare per assicurare che ci siano "le condizioni di tranquillità e collaborazione necessarie per poter vivere e prosperare in pace". Lo Stato deve controllare le minacce, anche quelle latenti. Per riuscire a raggiungere una sicurezza nazionale maggiore, ogni società deve elaborare una politica di difesa nazionale.

Alcune delle minacce che possono affettare la sicurezza internazionale sono:

- Conflitti armati
- Terrorismo
- Ciber minacce
- Crimine organizzato
- Instabilità economica e finanziaria
- Vulnerabilità energetica
- Proliferazione di armi di distruzione di massa
- Flussi migratori irregolari
- Spionaggio
- Emergenze e catastrofi
- Vulnerabilità dello spazio marittimo
- Vulnerabilità delle infrastrutture critiche e dei servizi essenziali

Alcune tra le precedentemente citate – come terrorismo, narcotraffico e ciber attacchi – sono considerate le nuove minacce della sicurezza internazionale. I loro obbiettivi non sono orientati ai bianchi tradizionali della tipica sicurezza, come il territorio, il potere militare, l'autonomia di decisione di uno stato ola sua sovranità, bensì colpiscono la popolazione civile e l'integrità delle istituzioni. Dato che colpiscono in maniera ostile e deliberata, sono considerate minacce alla pace e alla sicurezza internazionale;

queste differiscono dalle altre perché per natura risulta difficile neutralizzarle attraverso il potere militare. [79]

Tutti i Paesi, indipendentemente dalla loro grandezza o posizione, hanno proprie strategie di difesa internazionali mirate ad impedire tali minacce:

- USA: "Il rapporto sulla strategia della Sicurezza Nazionale è una pubblicazione del ramo esecutivo del governo degli Stati Uniti. Ha l'intenzione di essere una dichiarazione esaustiva di tutto il mondo, l'articolazione degli interessi, mete e obbiettivi degli Stati Uniti che sono importanti per la sua sicurezza. Tra i requisiti di presentazione del rapporto, ci sono le azioni necessarie per dissuadere l'aggressione e per porre in pratica la strategia della sicurezza nazionale" [80]
- España: In questo caso per esempio l'ultimo piano di Sicurezza Nazionale è datato nel 2013: "La strategia della Sicurezza Nazionale del 2013 è un passo trascendente che offre una visione integrale della Sicurezza Nazionale. Continua e controlla la strategia Spagnola di Sicurezza approvata nel 2011, adattando e aggiornando il suo contenuto ai cambi dello scenario strategico, configurando un nuovo Sistema di Sicurezza Nazionale e implicando la società civile negli ambiti di interesse prioritario della Sicurezza Nazionale".[81]
- Regno Unito: il 27 gennaio si presentò al Parlamento Britannico il nuovo piano di attrezzatura di difesa per il periodo che va dal 2017 al 2022. Questo è ampiamente relazionato con i rapporti annuali portati a termine dal governo britannico per ottenere un piano strategico di difesa nazionale e internazionale. Redatto nel 2008 dal partito del lavoro britannico, quasi per la prima volta, questo fu il primo rapporto che ebbe rilevanza pubblica: "Strategia di Sicurezza Nazionale, The National Security Strategy of the United Kingdom: Security in an Interdependent World". Successivamente David Cameron affermava: "La nostra sicurezza nazionale dipende dalla nostra sicurezza economica e viceversa. Pertanto il primo passo nella nostra strategia di Sicurezza Nazionale è assicurare che la nostra economia è, e si

mantiene forte". Strategia che rimase uguale nel "National Security Strategy and Strategic Defense and Security Review 2015". L'ambizioso documento, include tutti i rami dello sviluppo britannico e vuole contribuire con il 2% per la NATO e lo 0,7% per l'assistenza allo sviluppo.

- Francia: Lanciò il conosciuto come "Libro Bianco" nel 2013, con obbiettivi e proposte di sicurezza nazionale per i 15 anni successivi. "Il Libro Bianco combina la volontà di dotare il paese della capacità di poter assumersi tutte le responsabilità di Difesa e Sicurezza, l'adattamento della nostra strategia e una visione ad ampio raggio". Per quanto riguarda gli obbiettivi pianificati, il Libro Bianco cita chiaramente: "La protezione della popolazione e del territorio francese è un elemento chiave della nostra strategia, dovuto all'apparizione di nuovi pericoli oltre a quelli a cui si è generalmente esposti. L'obbiettivo è proteggere la nazione dalle grandi crisi e aumentare la capacità di elasticità. Questa si definisce come la "capacità dei poteri pubblici e della società francese per rispondere a una grande crisi e per stabilire rapidamente il suo normale funzionamento". D'altro canto, questo è stato uno dei paesi più coinvolti dal terrorismo in particolare da quello islamico: "L'assemblea Nazionale francese ha approvato, con 137 voti a favore e 13 contrari, mantenere fino al prossimo 1 lo stato di emergenza nel Paese. Da quando entrò in vigore nel novembre del 2015, dopo gli attentati di Parigi, lo stato di emergenza è stato prorogato sei volte."

5.2.3 Cosa dovrebbe avere maggiore importanza, la sicurezza internazionale o la privacy?

Dopo questo breve riassunto di atmosfera internazionale e dopo aver parlato di alcuni dei Paesi implicati, passiamo ad analizzare la relazione che media tra entrambi i concetti, anteriormente esposti.

Anche se a prima vista questi due concetti non sembrano essere relazionati, nel momento in cui vengono approfonditi e si applicano a un concetto si riesce a percepire la relazione che intercorre tra loro. Che succede se si presenta una minaccia per la sicurezza nazionale e si devono interrompere le comunicazioni? O spiare diversi Paesi? Come si comportano i Paesi? O come dovrebbero comportarsi?

Barack Obama disse: "non possiamo aspirare al 110% della sicurezza e al 100% della privacy. Il culmine immediato di questo approccio è che dobbiamo accettare un ritaglio – sempre noto e inarrestabile – del quadro dei diritti e delle libertà che ci definiscono come società aperte, come unica via per garantire la nostra sicurezza". [82]

Come possiamo vedere, i governi in svariate occasioni antepongono la sicurezza internazionale alla privacy dei loro cittadini intercettando conversazioni o entrando in luoghi privati della sfera personale nei quali non si potrebbe entrare se non con un mandato. Tutto questo, dicono, è applicato nella sicurezza nazionale e internazionale, che come concetto non è male, ma ci fa dimenticare in molte occasioni che ciò che stiamo lasciando in secondo piano è un diritto fondamentale avallato dalla Dichiarazione dei Diritti Umani.

È vero che specialmente dopo gli attentati dell'11 settembre negli Stati Uniti e dopo i recenti attacchi jihādisti contro i paesi europei, si installò una specie di allarme collettivo che ci portò a giustificare ogni tipo di comportamento, ma a che costo?

I diritti umani sono una conquista storica, tra questi diritti c'è anche il diritto di privacy, e ora li stiamo calpestando e ritagliandogli uno spazio inseguendo un concetto tanto astratto come quello della sicurezza nazionale, il quale ammette quasi qualsiasi comportamento.

In base a questo i tribunali di giustizia internazionali in varie occasioni hanno preso posizione di fronte a tale dibattito.

Così nel caso Leander contro la Svizzera, sentenza risolta dal TEDH dove venne considerato che: "oltre ad ottenere e immagazzinare dati, anche la

trasmissione degli stessi o la negazione ad ottenere informazioni sui dati in posso dei poteri pubblici, è capace di supporre una violazione del diritto di privacy". Questo caso lo mettiamo in relazione con la violazione prodotta dagli ascolti e dall'archiviazione di massa di dati prodotto dalla NSA e dalle agenzie europee di sicurezza attraverso i nuovi programmi di spionaggio senza lasciare che i particolari possano accedere alle informazioni raccolte".

In questa come in molte altre sentenze, tutte provenienti da diversi organi, troviamo che i tribunali fanno referenza al problema dell'invasione della privacy in molti ambiti; quello che abbiamo scoperto è che all'essere lo spionaggio una maniera di ottenere dati privati più o meno recenti, nella versione relazionata con la sicurezza nazionale, ci sono sentenze del TEDH che risolvono tali questioni. Si sono però pronunciati contro le violazioni realizzate dalla NSA e dalle agenzie europee dell'intelligenza, le quali ottenevano informazioni dai programmi di spionaggio; in questi nuovi casi si producono intromissioni ingiustificate e illegittime delle autorità pubbliche nella privacy dei cittadini europei, quadro protetto dal CEDH, violandone i diritti umani e lo Stato del Diritto.

Esempio di questo sono i comportamenti di investigazione o di controllo realizzati dagli USA durante il 2013. "Il giornale britannico The Guardian e lo statunitense The Washington Post informarono lo scorso 6 giugno che la NSA prendeva registri giornalieri di chiamate telefoniche di milioni di usuari dell'operatore di telefonia Verizon, in virtù di un mandato segreto. The Guardian spiegava che aveva avuto accesso a una copia di tale disposizione giudiziale, emessa ad aprile, dove si pretendeva dalla compagnia telefonica che fornisse alla NSA, in maniera continua, giornalmente, informazioni di tutte le chiamate telefoniche, tanto interne quanto esterne agli USA."

Ma non tutta la giurisprudenza è a favore del diritto della privacy, il caso Murray contro il Regno Unito, del 28 ottobre del 1994, risolto dal TEDH si considera uno dei primi casi riguardanti questo argomento. Questa sentenza si posiziona all'estremo opposto al considerare che non si produce una violazione della privacy per soddisfare il limite riconosciuto nel secondo

comma dell'art.8 dove si dispone che: "perquisizioni, detenzioni di persone e scattare foto come parte di un'operazione sono cose necessarie per combattere il terrorismo".

In questo modo pensano autori come LA RUE, che non definisce solo il diritto umano della privacy ma che è anche a favore dell'adozione di determinate misure di spionaggio: "per gli stati quando si presentino circostanze eccezionali considerate da questo autore, come l'amministrazione della giustizia criminale, la prevenzione dei crimini o del terrorismo. Queste circostanze si devono rispettare con il CEDH e con le leggi interne di ogni stato, rispettando inoltre il principio di proporzionalità".

Nelle Direttrici del Consiglio Europeo, per quanto riguarda i diritti umani e la lotta al terrorismo, si dispone che per lottare contro questi attacchi, la raccolta e il trattamento dei dati da parte di qualsiasi autorità competente per la sicurezza della sfera personale interverrà nella vita privata delle persone solo quando verranno soddisfatti tre elementi principali: "che siano regolate da apposite disposizioni di legge, siano in proporzione con l'obbiettivo per cui sono state previste e siano suscettibili ad un controllo da parte di un'autorità indipendente".

Per quello che abbiamo potuto vedere, non esiste una giurisprudenza unanime né omogenea relativa a questo argomento; la privacy o la sicurezza nazionale dipenderanno dal singolo caso e non da una corrente uniforme.

5.3 Decisioni del presidente Donald Trump

Il 29 marzo del 2017 veniva annunciata la notizia sulla sparizione della privacy in Internet negli Stati Uniti. La camera di rappresentanti ha approvato una legge che permetterà alle imprese di telecomunicazioni di commercializzare l'informazione degli utenti in Internet senza il loro consenso.

In questo modo le imprese fornitrici di Internet potranno vendere agli annuncianti i dati degli utenti su Internet, come ricerche, applicazioni scaricare e attraverso un dispositivo potranno navigare su Internet.

Questa legge si rivela un trionfo per le compagnie Verizon, Concast o AT&T, le quali erano un disaccordo con le misure prese dall'ex presidente Barack Obama e la Commissione Federale di Comunicazioni (FCC), il cui scopo era garantire la sicurezza e la privacy in rete.

I repubblicani sono convinti che questa legge finirà con regolamenti eccessivi, senza il sostengo e l'apporto di esperti o assessori per la redazione del testo. Non fu discussa con i comitati del settore nemmeno la normativa. Donald Trump, nonostante ciò, ha firmato il testo in cui venivano sciolti i regolamenti del precedente presidente Obama.

Prima dell' approvazione di questa legge, le imprese potevano accedere alle informazioni sui clienti solo se ricevevano il loro consenso esplicito ed erano obbligate ad informare sul tipo di informazione al quale accedevano , come chiedere il permesso per redigere dati riguardanti la cronologia delle ricerche. Attualmente le compagnie possono accedere a tutte queste informazioni senza il consenso degli utenti, i quali devono dichiarare espressamente il loro dissenso nella raccolta dei loro dati. [83]

In questo modo gli statunitensi non saranno totalmente protetti dall'esamizione e la vendita dei loro dati al miglior offerente.

CAPITOLO 6
CONCLUISONI

Con tutto ciò che è stato descritto nel presente lavoro e le notizie relative alla rete di sorveglianza mostrate, è possibile arrivare alle seguenti conclusioni.

Prima di tutto, l'importanza dell'informazione al giorno d'oggi, essendo uno degli obbiettivi principali sia per le imprese sia per i governi. Quello che dimostra tanta evidenza è l'incredibile sviluppo e espansione del Big Data negli ultimi anni. Possiamo quindi affermare che questa tecnologia è uno dei punti fondamentali del futuro dell'informatica.

In secondo luogo, possiamo dire che i metadati degli archivi e delle telecomunicazioni riescono a trasferire molte più informazioni di quanto si possa credere in un primo momento. Si tende a pensare infatti, che tutte le informazioni sono racchiuse in una chiamata, nel testo di un messaggio, o nell'intercambio di messaggi vocali, ma in realtà è stato dimostrato che i metadati possono essere molto più importanti delle informazioni scambiate. Altro concetto descritto, è l'utilità dei metadati, come la creazione e il miglioramento delle biblioteche virtuali.

Infine, investigando sul caso Snowden, sulle rivelazioni riguardanti il governo degli Stati Uniti, e sui metodi applicati da questa rete di sorveglianza mondiale, possiamo dedurre che la NSA e altre agenzie di intelligenza sorvegliano la popolazione segretamente. Forse la cosa più preoccupante

dopo le rivelazioni fatte da Snowden è che non si credeva che le tecniche applicate dalla NSA potessero arrivare a quel punto, violando l'intimità e la privacy di milioni di persone in tutto il mondo.

Riferimenti bibliografici

[1] R. B. Fragoso, “Qué es Big Data.” [Online]. Available: https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/.

[2] D. Boyd and K. Crawford, “CRITICAL QUESTIONS FOR BIG DATA,” *Information, Commun. Soc.*, vol. 15, no. 5, pp. 662–679, Jun. 2012.

[3] IBM, “Relational Database.” [Online]. Available: http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/reldb/.

[4] B. Devlin and P. Murphy, “An architecture for a business and information system.”

[5] D.J. Power, “A Brief History of Decision Support Systems.” [Online]. Available: http://dssresources.com/history/dsshistory.html. [Accessed: 20-Jun-2017].

[6] M. Cox and D. Ellsworth, “Application-Controlled Demand Paging for Out-of-Core Visualization,” 1997.

[7] N. Smith, “History of Business Intelligence,” 2009. [Online]. Available: https://www.slideshare.net/nicsmith/history-of-business-intelligence-1236862. [Accessed: 20-Jun-2017].

[8] “ProjectDescription - Hadoop Wiki,” 2014. [Online]. Available: https://wiki.apache.org/hadoop/ProjectDescription. [Accessed: 20-Jun-2017].

[9] GilPress, “A Very Short History of Big Data,” 2012. [Online]. Available: https://whatsthebigdata.com/2012/06/06/a-very-short-history-of-big-data/. [Accessed: 20-Jun-2017].

[10] C. Pettey and L. Goasduff, “Gartner EXP Worldwide Survey of More than 1,500 CIOs Shows IT Spending to Be Flat in 2009,” 2009. [Online]. Available: http://www.gartner.com/newsroom/id/855612. [Accessed: 20-Jun-2017].

[11] S. Rogers, “Top 10 Trends in Business Intelligence and Analytics for 2011,” 2011. [Online]. Available:

http://blogs.enterprisemanagement.com/shawnrogers/2011/01/11/top-10-trends-in-business-intelligence-and-analytics-for-2011/. [Accessed: 20-Jun-2017].

[12] M. Hilbert and P. López, “The World’s Technological Capacity to Store, Communicate, and Compute Information,” *Science (80-.).*, vol. 332, no. 6025, 2011.

[13] D. Bestard Delgado, “¿Cómo se explica el crecimiento del BIG DATA la última década? ¿Qué retos nos ha planteado esta ciencia?,” 2013. [Online]. Available: https://evaluacionimpacto.wordpress.com/2013/04/23/como-se-explica-el-crecimiento-del-big-data-durante-la-ultima-decada-que-retos-nos-ha-planteado-esta-ciencia/. [Accessed: 27-Jun-2017].

[14] A. Lafuente, “Sistemas de ficheros distribuidos.” .

[15] “Sistemas Distribuidos : TALLER SISTEMA DE ARCHIVOS DISTRIBUIDOS.” [Online]. Available: http://toquemeque.blogspot.it/2016/04/taller-sistema-de-archivos-distribuidos.html. [Accessed: 03-Jul-2017].

[16] B. Mukherjee *et al.*, “KTK: kernel support for configurable objects and invocations A survey of load sharing in networks of workstations Light-weight process groups in the Isis system Object replacement using dynamic proxy updates Micro-kernel support for migration.”

[17] TechTarget, “¿Qué es Base de datos relacional?,” 2015. [Online]. Available: http://searchdatacenter.techtarget.com/es/definicion/Base-de-datos-relacional. [Accessed: 03-Jul-2017].

[18] R. Stephens and R. Plew, “Alternatives to the relational database model,” 2001. [Online]. Available: http://searchoracle.techtarget.com/tip/Alternatives-to-the-relational-database-model. [Accessed: 03-Jul-2017].

[19] I. Daudinot Founier, “Organización y recuperación de información en Internet: teoría de los metadatos,” *SCIELO*, vol. 14, no. 5, pp. 0–0, 2006.

[20] G. Marilín, “Qué son tus metadatos y por qué pueden ser tan importantes como el contenido de tu email,” *eldiario*, 2013.

[21] “Immersion,” 2013. [Online]. Available: https://immersion.media.mit.edu/. [Accessed: 03-Jul-2017].

[22] J. Barrueco and I. S. Coll, “OAI-PMH: protocolo para la transmisión de contenidos en Internet,” *El Prof. la Inf.*, 2003.

[23] I. Martinez, “Por qué la recolección de metadatos sí importa,” *FaerWayer*, 2014.

[24] Wired, “Whistle-Blower’s Evidence, Uncut,” *Wired*, 2006.

[25] Diario TI, “La NSA vigila el 75% del tráfico digital mundial,” *D. TI*, 2013.

[26] G. Greenwald, “Boundless Informant: the NSA’s secret tool to track global surveillance data,” 2013. [Online]. Available: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining. [Accessed: 04-Jul-2017].

[27] G. Greenwald, “The NSA’s mass and indiscriminate spying on Brazilians,” *Guard.*, 2013.

[28] P. Dorling, “Edward Snowden reveals Australia’s Links To Secret US Spy Program,” *Sydney Morning Her.*, 2013.

[29] G. Greenwald, “XKeyscore: NSA tool collects ‘nearly everything a user does on the internet,’” *Guard.*, 2013.

[30] J. Goetz, H. Leyendecker, F. Obermaier, and J. Cáceres, “British Officials Have Far-Reaching Access To Internet And Telephone Communications,” *Sueddeutsche*, 2013.

[31] S. Gorman and J. Valentino, “New Details Show Broader NSA Surveillance Reach,” *Wall Str. J.*, 2013.

[32] N. Perlroth, J. Larson, and S. Shane, “N.S.A. Able to Foil Basic Safeguards of Privacy on Web,” *New York Times*, 2013.

[33] G. Champeau, “Lustre : la France aurait coopéré avec la NSA,” *Numerama*, 2013.

[34] G. Greenwald, “NSA and Israeli intelligence: memorandum of understanding,” *Guard.*, 2013.

[35] S. Rich and M. DeLong, “NSA slideshow on ‘The TOR problem,’” *Washington Post*, 2013.

[36] B. Gellman, C. Timberg, and S. Rich, “Secret NSA documents show campaign against Tor encrypted network,” *Washington Post*, 2013.

[37] L. Poitras, M. Rosenbach, and J. Glüsing, “NSA Hacked Email Account of Mexican President,” *Spiegel*, 2013.

[38] M. Lander and M. Schmidt, “Spying Known at Top Levels, Officials Say,” *New York Times*, 2013.

[39] S. Gorman, “Obama Unaware as U.S. Spied on World Leaders: Officials,” *Wall Str. J.*, 2013.

[40] S. Shane, “No Morsel Too Minuscule for All-Consuming N.S.A. - The New York Times,” *New York Times*, 2013.

[41] M. Brissenden, “Australia spied on Indonesian president, leaked documents reveal,” *ABC*, 2013.

[42] E. MacAskill, J. Ball, and K. Murphy, “Revealed: Australian spy agency offered to share data about ordinary citizens,” *Guard.*, 2013.

[43] B. Gellman, “NSA tracking cellphone locations worldwide, Snowden documents show,” *Washington Post*, 2013.

[44] A. Soltani and M. DeLong, “NSA signal-surveillance success stories,” *Washington Post*, 2013.

[45] A. Soltani, “Reporter: For NSA, Google cookies allow ‘laser-guided’ targeting,” *Washington Post*, 2013.

[46] A. Soltani and M. DeLong, “How the NSA pinpoints a mobile device,” *Washington Post*, 2013.

[47] J. Glanz and A. W. Lehren, “N.S.A. Spied on Allies, Aid Groups and Businesses,” *New York Times*, 2013.

[48] P. Bump, “The UK Tempora Program Captures Vast Amounts of Data — and Shares with NSA,” *Atl.*

[49] C. Huhne, “Prism and Tempora: the cabinet was told nothing of the surveillance state’s excesses,” *Guard.*, 2013.

[50] E. MacAskill, J. Borger, N. Hopkins, and J. Ball, “GCHQ taps fibre-optic cables for secret access to world’s communications,” *Guard.*, 2013.

[51] 20minutos, “Merkel pide explicaciones a Obama porque cree que EE UU ha espiado su móvil,” *20 minutos*, 2013.

[52] L. Poitras, *Citizenfour*. Estados Unidos, 2014.

[53] S. Rich and B. Gellman, “NSA seeks to build quantum computer that could crack most types of encryption,” *Washington Post*, 2014.

[54] M. Winter, “NSA working to build computer to crack encryption,” *USA Today*, 2014.

[55] T. Lee B., “Confused about the NSA’s quantum computing project? This MIT computer scientist can explain,” *Washington Post*, 2014.

[56] D. E. Sanger and T. Shanker, “N.S.A. Devises Radio Pathway Into Computers,” *New York Times*, 2014.

[57] G. White, “Revealed: UK and US spied on text messages of Brits,”

Channel 4, 2014.

[58] J. Larson, “Spy Agencies Probe Angry Birds and Other Apps for Personal Data,” *ProPublica*, 2014.

[59] J. Ball, “Angry Birds and ‘leaky’ phone apps targeted by NSA and GCHQ for user data,” *Guard.*, 2014.

[60] NSA, “From the National Security Agency,” *New York Times*, 2014.

[61] G. Greenwald, “Snowden docs reveal British spies snooped on YouTube and Facebook,” *NBC News*, 2014.

[62] P. Oltermann, “NSA tapped German ex-chancellor Gerhard Schröder’s phone,” *Guard.*, 2014.

[63] “Snowden leaks: GCHQ ‘attacked Anonymous’ hackers,” *BBC News*, 2014.

[64] R. Gallagher, “Compare the NSA’s Facebook Malware Denial to its Own Secret Documents,” *Intercept*, 2014.

[65] R. Gallagher and G. Greenwald, “How the NSA Plans to Infect ‘Millions’ of Computers with Malware,” *Intercept*, 2014.

[66] G. Corea, “Escándalo de espionaje: qué es el "Club de los cinco ojos",” *BBC*, 2014.

[67] B. Gellman, “NSA surveillance program reaches ‘into the past’ to retrieve, replay phone calls,” *Washington Post*, 2014.

[68] D. E. Sanger and N. Perlroth, “N.S.A. Breached Chinese Servers Seen as Security Threat,” *New York Times*, 2014.

[69] “NSA Spied on Chinese Government and Networking Firm Huawei,” *Spiegel*, 2014.

[70] R. Gallagher, “Der Spiegel: NSA Put Merkel on List of 122 Targeted Leaders,” *Intercept*, 2014.

[71] L. Poitras and M. Rosenbach, “GCHQ and NSA Targeted Private German Companies,” *Spiegel*, 2014.

[72] “Electronic Communications Privacy Act of 1986,” 2013. [Online]. Available: https://www.it.ojp.gov/PrivacyLiberty/authorities/statutes/1285. [Accessed: 26-Jun-2017].

[73] whitehouse.gov, “SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts,” 2015. [Online]. Available:

https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat. [Accessed: 27-Jun-2017].

[74] "¿QUÉ ES EL TPP?" [Online]. Available: http://tppabierto.net/que-es-tpp. [Accessed: 27-Jun-2017].

[75] "Trans Pacific Partnership trade deal signed in Auckland," *BBC News*, 2016.

[76] Redaccion BBC Mundo, "Donald Trump retira a Estados Unidos del TPP, el Acuerdo Transpacífico de Cooperación Económica," *BBC Mundo*, 2017.

[77] "Declaración Universal de Derechos Humanos."

[78] "Título I. De los derechos y deberes fundamentales - Constitución Española." [Online]. Available: http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2. [Accessed: 09-Jul-2017].

[79] "Nuevas amenazas a la paz y seguridad internacionales." [Online]. Available: https://es.slideshare.net/ignacio2794/nuevas-amenazas-a-la-paz-y-seguridad-internacionales. [Accessed: 09-Jul-2017].

[80] "National Security Strategy Archive." [Online]. Available: http://nssarchive.us/. [Accessed: 09-Jul-2017].

[81] "Estrategia de Seguridad Nacional | DSN." [Online]. Available: http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional. [Accessed: 09-Jul-2017].

[82] "Privacidad vs. seguridad, guerra perdida | Internacional | EL PAÍS." [Online]. Available: https://internacional.elpais.com/internacional/2013/06/17/actualidad/1371487237_851726.html. [Accessed: 09-Jul-2017].

[83] "Trump deroga la ley de privacidad en internet: los proveedores ya pueden vender información de los usuarios," *ABC.es*.