UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in Economia Aziendale

VALORE PUBBLICO DEL DATO, SUA TUTELA E COSTITUZIONE

PUBLIC VALUE OF DATA, PROTECTION AND CONSTITUTION

Relatore:
Prof.ssa Marta Cerioni

Rapporto Finale di:
Lorenzo Galantini

Anno Accademico 2023/2024

Indice

1. INTRODUZIONE

Negli ultimi vent'anni, l'avvento delle tecnologie digitali ha completamente rivoluzionato il sistema di comunicazione e informatizzazione, rendendo possibile un'interconnessione, capace di superare le barriere di tempo e spazio. Grazie alle possibilità garantite dal mondo virtuale, le persone accedono e comunicano costantemente con la rete, scambiando dati e informazioni sia attivamente che passivamente, rendendoci così vulnerabili a qualsivoglia malintenzionato abbia la capacità di accedervi. Ed è proprio per questo che le istituzioni, per garantire la sicurezza di ogni internauta, ne tutelano la privacy, attraverso la regolamentazione della raccolta, analisi e utilizzo dei dati. Tuttavia, nonostante le stringenti normative adottate negli anni, emergono costantemente nuove minacce in grado di penetrare i sistemi di sicurezza più complessi, e compromettere la sicurezza dei dati. Talvolta, la riservatezza dei nostri dati può essere compromessa proprio da coloro che si fanno garanti della sicurezza informatica, come ad esempio, le istituzioni. È questo il caso di Edward Snowden, ex analista dell'NSA (National Security Agency), che nel 2013 rivelò, attraverso la divulgazione di documentazione classificata, l'esistenza di programmi di sorveglianza di massa condotti principalmente dagli Stati Uniti in collaborazione con Canada, Australia, Regno Unito e Nuova Zelanda. L'obiettivo di questa tesi è quello di ad analizzare le conseguenze di uno dei più importanti Data Leak della storia contemporanea nel contesto giuridico

internazionale, Europeo e nazionale, misurando gli effetti e l'impatto che questo evento ha avuto sulla società odierna, e se negli anni, il suo eco abbia effettivamente portato a disporre di una normativa adeguata, atta a prevenire il tracciamento, la raccolta, l'analisi e lo sfruttamento dei metadati generati da qualsiasi persona fisica o giuridica. Inizialmente ci si occuperà del caso nello specifico, approfondendo il funzionamento del programma di sorveglianza, dagli effetti che questo ha comportato per la società americana e per il diritto internazionale, all'illiceità e violazioni derivate dal suo utilizzo. Successivamente si andrà a trattare delle reazioni dell'Europa e in particolar modo dell'Italia, dimostrando l'incostituzionalità dell'operato statunitense ed esaminando gli sviluppi giudiziari in merito alla normativa conseguente e vigente. Verrà approfondito inoltre il valore economico e sociale del dato, ricercando nei settori chiave i sistemi che riescano a sfruttarne le potenzialità, presentando così un contesto volto a definire l'importanza nell'investire in un solido sistema di cybersecurity e analizzando le recenti normative in merito. Infine, verranno fondate ipotesi sulle prospettive future riassumendo i principali punti trattati in questa tesi, sviluppando così una riflessione conclusiva nei riguardi dell'argomento.

2. IL PROGRAMMA PRISM: ANTEFATTI ED IMPLICAZIONI

2.1 Edward Snowden

È il 9 Giugno 2013, il giorno in cui i giornalisti Glenn Greenwald, Ewen MacAskill, Barton Gellman e la regista Laura Portrais pubblicheranno sul *The Guardian* e sul *The Washington Post* i primi articoli riguardo "una delle notizie più significative nella storia politica degli Stati Uniti" [1]. Dopo uno scambio di mail durato settimane tra Greenwald ed un utente anonimo della rete, rivelatosi poi essere Edward Snowden, ex analista dell'NSA (National Security Agency), i due riusciranno ad accordarsi per un incontro, poi avuto luogo ad Hong Kong nel maggio 2013 dove vennero condivisi file classificati raccolti a partire dell'aprile del 2012 fino all'inizio del 2013, mentre Snowden lavorava per Dell Inc. come lavoratore a contratto per la NSA. I documenti rivelavano in maniera dettagliata l'esistenza di un complesso programma di sorveglianza denominato PRISM o US-948XN, nato e sviluppatosi negli Stati Uniti (NSA) in collaborazione con Regno Unito (GCHQ), Australia (ASD), Canada (CSEC) e Nuova Zelanda (GCSB), membri di un'alleanza nata nel 1946 sotto il nome di Five Eyes:

[1] G. Greenwald *et al*., "Edward Snowden: the whistleblower behind the NSA surveillance revelations", *The Guardian*, (9 Giugno 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

"I segni rivelatori dei Five Eyes, come la classificazione 'AUS/CAN/NZ/UK/US EYES ONLY' o 'FVEY', compaiono spesso nei documenti della cache di Snowden. Queste indicazioni sottolineano il fatto che la sorveglianza di massa [...] è possibile solo con l'infrastruttura di sorveglianza combinata, le strutture, la manodopera e le procedure di analisi dei dati grezzi condivise dalle istituzioni di intelligence in tutte le giurisdizioni dei Five Eyes, integrate da accordi per un massimo di 30 Paesi terzi"

(Felicity Ruby, Gerard Goggin & John Keane (2017) "Comparative Silence", Digital Journalism, 5:3, 353-367, DOI: 10.1080/21670811.2016.1254568) [2]

Il programma sarebbe stato in grado di ottenere e catalogare dati personali, quali messaggi, conversazioni telefoniche, scambi di mail, media, file, notifiche di accesso relative al sito su cui l'obiettivo sta o stava navigando.

[2] *"Telltale signs of the Five Eyes—such as the classification "AUS/CAN/NZ/UK/US EYES ONLY" or "FVEY"—appear often in Snowden cache documents. These indications underscore the fact that mass surveillance* […] *is only possible with the combined surveillance infrastructure, facilities, labour, and procedures for analysing raw data shared by the intelligence institutions in all Five Eyes jurisdictions, which is supplemented by arrangements with up to 30 Third Party countries"*

2.2 Il PATRIOT Act (2001) [3]

Il progetto iniziò a prendere forma in seguito all'attentato al World Trade Center del 2001. L'obiettivo presentato sarebbe stato quello di intercettare e raccogliere dati provenienti dalle "zone calde", ovvero quelle aree dove le attività terroristiche si sarebbero rivelate più consistenti al fine di sventare possibili attacchi futuri come quelli dell'11 settembre. Difatti, poco più di un mese dopo dall'attentato, l'allora presidente Bush firmò il PATRIOT Act, una legge federale che avrebbe riconosciuto al governo statunitense maggiori autorità sul controllo delle comunicazioni informatiche e non:

"Sec. 201. Autorità di intercettare comunicazioni telefoniche, orali ed elettroniche relative al terrorismo.
Sec. 202. Autorità di intercettare comunicazioni telefoniche, orali ed elettroniche relative a reati di frode e abuso informatico.
Sec. 203. Autorità di condividere informazioni investigative penali.

[3] Il termine "USA Patriot Act" è l'acronimo di Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*;* Division of Banks, "USA Patriot Act", *Official website of the Commonwealth of Massachusetts,* (12/12/2001), https://www.mass.gov/industry-letter/usa-patriot-act

Sec. 204. Chiarimento delle eccezioni di intelligence alle limitazioni di intercettazione e divulgazione di comunicazioni telefoniche, orali ed elettroniche." [4]

(H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, H.R.3162, 107th Cong. (2001), https://www.congress.gov/bill/107th-congress/house-bill/3162/text/pl.)

Per poter ottenere l'accesso a queste informazioni non è richiesta un'autorizzazione da parte di un giudice. Attraverso l'emissione di National Security Letters (NSLs), ossia una richiesta scritta da parte dell'Federal Bureau of Investigation, si autorizza l'accesso alle informazioni personali, tra cui i tabulati telefonici, le registrazioni del computer, l'affidabilità finanziaria e l'estratto conto bancario dell'obiettivo. In particolare, la *Section 505* del PATRIOT Act *"Miscellaneous national security authorities"* si occupa della rimozione degli ostacoli, ampliando l'autorità dell'FBI nelle indagini sulle attività di terrorismo internazionale, eliminando il requisito che le informazioni richieste in una NSL debbano riguardare una potenza straniera o un

[4] *"Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism. Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses. Sec. 203. Authority to share criminal investigative information. Sec. 204. Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.* "

agente di una potenza straniera. [5] [6] l'esclusione di questo presupposto, estende significativamente il controllo detenuto dal governo statunitense verso i suoi stessi cittadini. Successivamente, nel 2005, attraverso l'USA PATRIOT Improvement and Reauthorization Act venne abrogato il termine di scadenza del PATRIOT Act, rendendone permanenti gli effetti. [7]

2.3 Il Protect America Act (2007)

Attraverso il Foreign Intelligence Surveillance Act del 1978 (FISA) il governo mirava a stabilire le procedure per la sorveglianza dell'intelligence straniera ma con importanti limitazioni per le intercettazioni riguardanti obiettivi statunitensi [8], limitazioni che, del resto, presentava lo stesso emendamento dello USA PATRIOT Act, nonostante le agevolazioni concesse all'FBI dalla *Section 505*. Ed è così che nel 2007, sotto l'amministrazione Bush, venne approvato il Protect America Act, grazie al quale si riuscì a trovare una soluzione tecnica volta a colmare la lacuna nelle capacità di sorveglianza degli Stati Uniti, assicurandosi in questo modo il

[5] S0703b – *"A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006"*, US Department of Justice, Office of the Inspector, General, (Marzo 2008)
[6] S0803b – *"A Review of the Federal Bureau of Investigation's Use of National Security Letters"*, US Department of Justice, Office of the Inspector General, (Marzo 2007)
[7] H.R.3199 - 109th Congress (2005-2006): USA PATRIOT Improvement and Reauthorization Act of 2005, H.R.3199, 109th Cong. (2006), https://www.congress.gov/bill/109th-congress/house-bill/3199.
[8] S.1566 - 95th Congress, Report No. 95-1720, Foreign Intelligence Surveillance Act (1978), https://www.intelligence.senate.gov/sites/default/files/publications/951720.pdf, 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871

completo controllo sulle comunicazioni esterne ed interne al paese. [9] La definizione di "intelligence straniera" è fondamentale per l'analisi costituzionale del PAA. La legge non fornisce una definizione di "intelligence straniera" diversa rispetto a quella fornita dal FISA; pertanto, nell'interpretare il PAA, si applica la definizione originale di "intelligence straniera" della FISA del 1978, dove il termine "straniero" si riferisce al contenuto delle informazioni raccolte, e non al luogo in cui (o da cui) esse vengono raccolte, o alla nazionalità delle fonti da cui provengono. Di conseguenza, per "foreign intelligence" si intendono informazioni che a discapito della provenienza, sono necessarie per la capacità degli Stati Uniti di proteggersi da danni o operazioni clandestine contro gli stessi. [10]

Inoltre, la *Section 2* del PAA stabilisce che la definizione di sorveglianza elettronica, precedentemente delineata dal FISA nella *Section 101(f)*, non viene applicata alle attività descritte nel PAA. La definizione del FISA conteneva specifiche relative all'obiettivo e alle procedure di raccolta, definite come "l'acquisizione, mediante un dispositivo di sorveglianza elettronico, meccanico o di altro tipo, del contenuto di qualsiasi comunicazione via cavo o radio inviata o destinata ad essere ricevuta da una persona particolare, persona conosciuta negli

[9] Timothy B. Lee, "How Congress unknowingly legalized PRISM in 2007", *The Washington Post*, (6 Giugno 2013), https://www.washingtonpost.com/news/wonk/wp/2013/06/06/how-congress-unknowingly-legalized-prism-in-2007/
[10] Foreign Intelligence Surveillance Act (FISA) § 101(e), 50 U.S.C. § 1801(e) (2006).

Stati Uniti che si trova negli Stati Uniti, se il contenuto viene acquisito prendendo di mira intenzionalmente tale persona sarebbe necessario un mandato per l'applicazione della legge" [11]. Nel respingere questa definizione, il PAA afferma nella *Section 105A* che "nulla nella definizione di sorveglianza elettronica sotto la *Sec. 101(f)* (FISA) deve essere interpretata in modo da comprendere la sorveglianza diretta a una persona che si ritiene ragionevolmente situata al di fuori degli Stati Uniti" [12]. Pertanto, se la sorveglianza è diretta ad un obiettivo straniero, la definizione di sorveglianza elettronica della FISA non si applica a tale raccolta di informazioni, poichè rientra nelle modifiche apportate nel PAA. Di conseguenza, tale obiettivo non beneficia delle protezioni o delle limitazioni che la FISA pone alla raccolta di intelligence. Inoltre, la *Section 2* non afferma esplicitamente che questa eccezione alla definizione di sorveglianza elettronica si applichi solo alla sorveglianza di un cittadino straniero. Il significato di "diretta a" potrebbe quindi permettere il monitoraggio di persone diverse dall'obiettivo al fine di ottenere informazioni su di quest'ultimo. Pertanto, poiché la sezione 101(f) della FISA non limita la legge PAA, le persone attraverso cui l'intelligence raccoglie informazioni sull'obiettivo potrebbero essere all'interno degli Stati Uniti e/o cittadini statunitensi.

[11] FISA § 101(f)
[12] S.1927 – 110th Congress (2007-2008): Protect America Act of 2007 § 2, S.1927, 110th Cong. (2007), https://www.congress.gov/bill/110th-congress/senate-bill/1927.

2.4 Il programma di sorveglianza PRISM (2007)

Contestualmente all'approvazione del PAA nasce il Planning tool for Resource Integration, Synchronization, and Management ("P.R.I.S.M.") [13], programma reso possibile attraverso la collaborazione tra governo centrale e multinazionali operanti nel settore informatico quali Microsoft, che fu la prima ad entrare nel progetto nel 2007; Yahoo nel 2008 seguito da Google, Facebook e PalTalk; Skype ed AOL nel 2011 ed infine Apple nel 2012. [14]

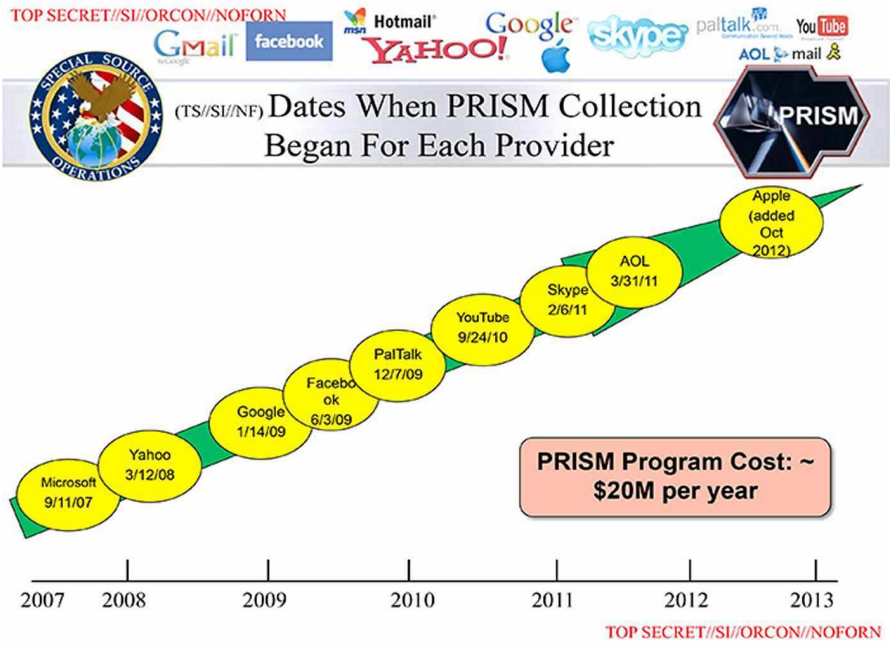


Figura 1. Estratto del documento declassificato "PRISM/US-984XN Overview"

[13] Tariq, Juhi, "The NSA's Prism Program and the New EU Privacy Regulation: Why U.S. Companies With a Presence in the EU Could Be in Trouble" (2014). *American University Business Law Review*, Vol. 3, No. 2, 371, Available at SSRN: https://ssrn.com/abstract=3156725

[14] G. Greenwald, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, (6 Giugno 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Agganciandosi direttamente ai database di quest'ultime, il programma avrebbe avuto accesso a qualsiasi metadato raccolto ed archiviato all'interno dei server aziendali, svolgendo così la funzione di Data Providers per il governo statunitense. Alcune delle aziende coinvolte, come Google e Facebook, hanno acconsentito anche alla richiesta di creare delle vere e proprie sale server dedicate. Principalmente il metodo di condivisione impiegato, prevedeva l'utilizzo di "File Transfer Protocol" (FTP), ossia protocolli crittografati basati sull'architettura client/server volti al trasferimento diretto di dati. [15] I dati raccolti includono e-mail, chat (video e vocali), video, foto, dati salvati, VoIP (come Skype) [16], file trasferiti, video conferenze, notifiche relative alle attività dell'obiettivo (come login, logout, ecc.), dettagli relativi al Social Networking (ogni attività registrata legata alla navigazione ed interazione sui social media) e le "richieste speciali" (non approfondite).

[15] C. C. Miller, "3 Tech Giants Want to Reveal Data Requests", *The New York Times*, (11 Giugno 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

[16] VoIP: Sigla di Voice over IP, tecnologia per la comunicazione vocale che utilizza una rete dati per la gestione della conversazione, anziché una rete telefonica dedicata; *Enciclopedia Treccani*, https://www.treccani.it/enciclopedia/voip_(Lessico-del-XXI-Secolo)/

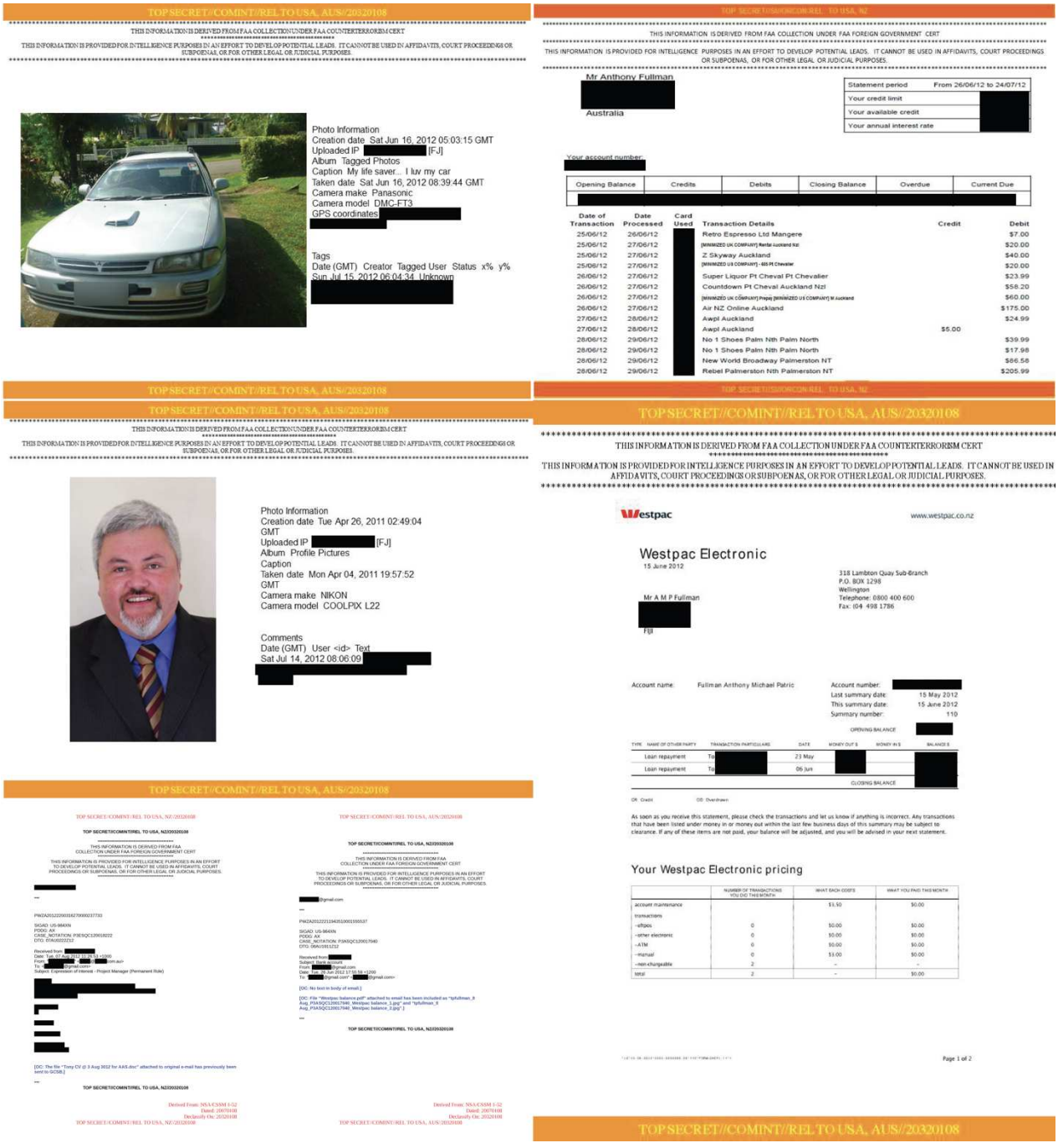


Figura 2. Esempio di informazioni derivanti dall'estrazione di dati relative al FISA Amandment Act Counterterrorism Cert, quindi provenienti dai metodi di sorveglianza utilizzati dal 2007 in poi.

Inoltre, gli USA possiedono un importante vantaggio, presentato nei file declassificati, dal momento che buona parte dell'infrastruttura di Internet si sviluppa proprio negli Stati Uniti. Difatti, dalla documentazione si evince come il programma PRISM sia stato concepito come elemento complementare all'acquisizione di dati attraverso i Transatlantic Communication Cable comunemente chiamati TAT, ossia cavi sottomarini ad altà capacità in fibra ottica. Del resto, il compito assegnato all'AT&T dal governo statunitense, sarebbe quello di effettuare una sorveglianza "a monte" collegandosi, copiando e filtrando tutti i dati che transitano nei TAT. [17]

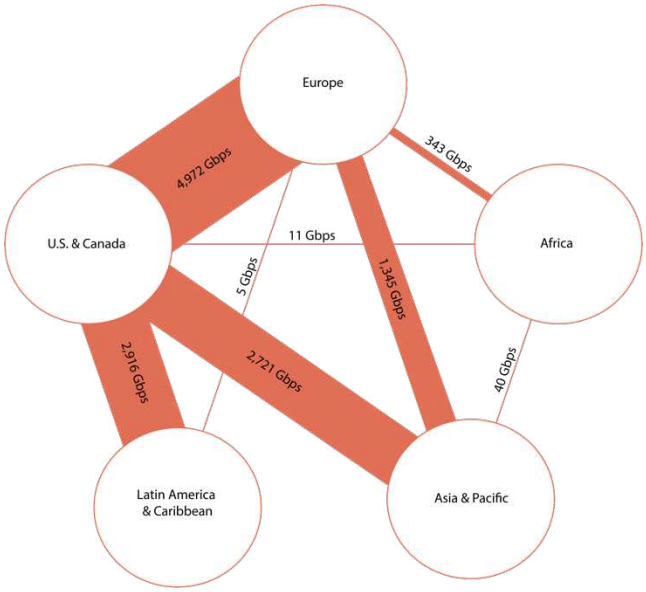


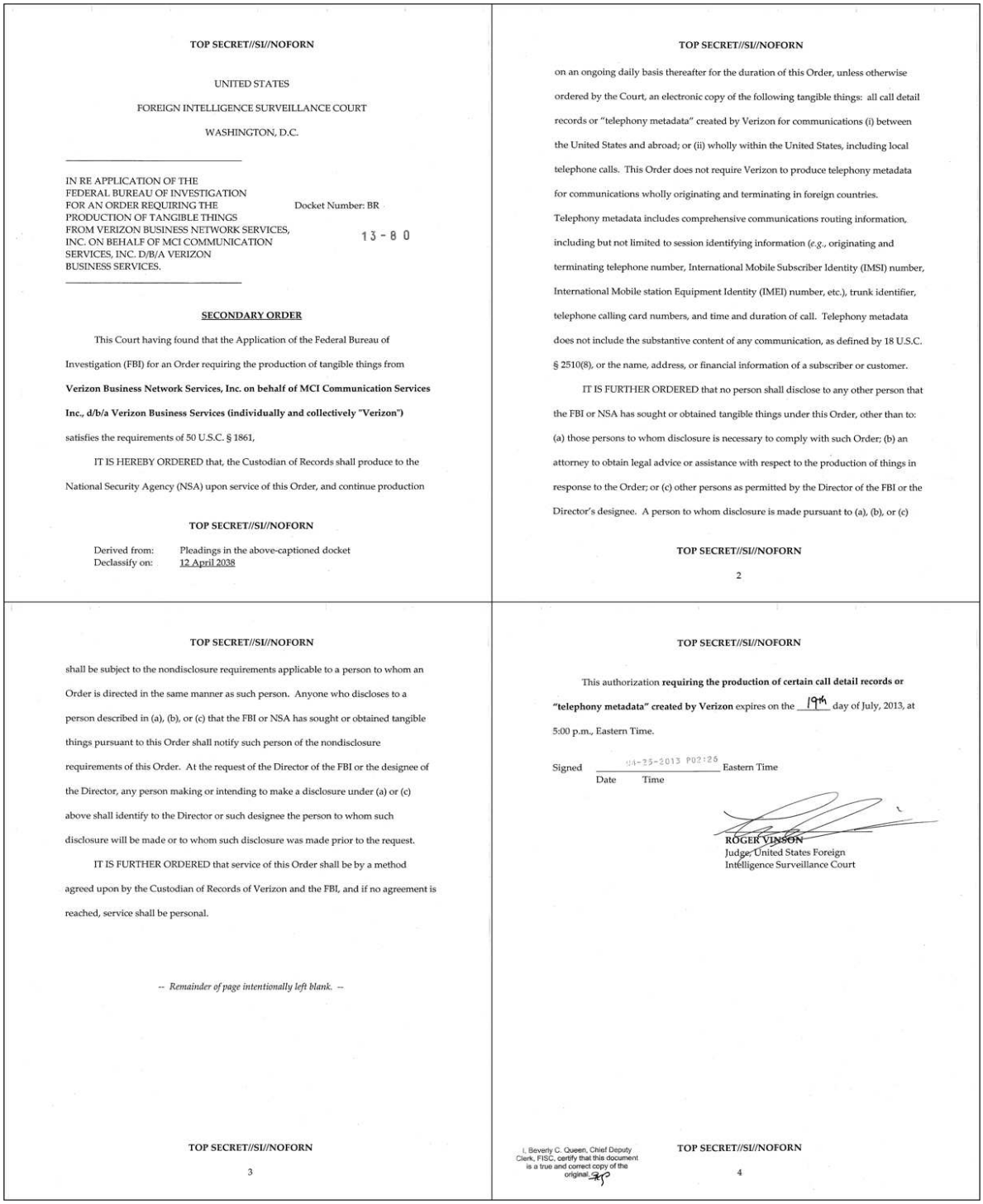
Figura 3. "International Internet Regional Bandwidth Capacity in 2011"

[17] "Upstream vs. PRISM." (19 Ottobre 2017), *Electronic Frontier Foundation*, https://www.eff.org/am/pages/upstream-prism

Il documento "PRISM/US-984XN Overview" mostra inoltre che l'FBI fungeva da intermediario tra l'NSA e le aziende tecnologiche sopracitate, sottolineando la dipendenza del Federal Bureau alla partecipazione delle suddette aziende informatiche, affermando che "l'accesso dipende al 100% dalla fornitura degli Internet Service Provider (ISP)", [18] quali ad esempio AT&T e in particolar modo Verizon, uno dei maggiori fornitori di servizi di telecomunicazione in America, al quale è stato imposto, attraverso un'ordinanza top secret emessa ad Aprile 2013, di condividere, su base "continua e quotidiana" per tutta la durata del presente ordine, informazioni su ogni chiamata effettuata attraverso i suoi sistemi, sia all'interno degli Stati Uniti che tra Stati Uniti e altri Paesi. [19]

[18] Greenwald G. & MacAskill E., (29 Dicembre 2017), "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[19] *Id.*



TOP SECRET//SI//NOFORN

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR 13-80

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

TOP SECRET//SI//NOFORN

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

TOP SECRET//SI//NOFORN

on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries. Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c)

TOP SECRET//SI//NOFORN

2

TOP SECRET//SI//NOFORN

shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

IT IS FURTHER ORDERED that service of this Order shall be by a method agreed upon by the Custodian of Records of Verizon and the FBI, and if no agreement is reached, service shall be personal.

-- Remainder of page intentionally left blank. --

TOP SECRET//SI//NOFORN

3

TOP SECRET//SI//NOFORN

This authorization **requiring the production of certain call detail records or "telephony metadata" created by Verizon** expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

I, Beverly C. Queen, Chief Deputy Clerk, FISC, certify that this document is a true and correct copy of the original.

TOP SECRET//SI//NOFORN

4

Figura 4. Ordinanza emessa in merito alla produzione di "cose tangibili" da parte di Verizon Business Network Services Inc.

L'ordine specifica che i registri da produrre includono “informazioni di identificazione della sessione”, come il “numero di origine e di terminazione”, la durata di ogni chiamata, i numeri delle carte telefoniche, i “trunk identifiers” [20], il numero IMSI (International Mobile Subscriber Identity) e “informazioni complete sull'instradamento delle comunicazioni”. Le informazioni sono classificate come metadati, o informazioni transazionali, piuttosto che comunicazioni, e quindi non richiedono mandati individuali per l'accesso. Il documento specifica inoltre che tali metadati non sono limitati agli elementi sopra menzionati. Sebbene l'ordine in sé non includa né il contenuto dei messaggi né le informazioni personali legate al detentore di un particolare numero di cellulare, la raccolta delle informazioni sopracitate consentirebbe all'NSA di costruire facilmente un quadro retrospettivo completo di chi ogni individuo ha contattato, come, quando e dove.

Tornando alla documentazione declassificata relativa al PRISM, si evidenzia che nel 2012 il numero di comunicazioni ottenute è aumentato del 248% per Skype, del 131% per Facebook e del 63% per Google, desumendo inoltre dalla documentazione, l’intenzione di aggiungere Dropbox tra i collaboratori del programma di sorveglianza. In data Giugno 2013, sono stati riportati più di 77.000

[20] Trunk Identifiers: una sequenza di cifre da comporre prima di un numero di telefono allo scopo di selezionare un circuito di telecomunicazioni appropriato con cui la chiamata deve essere instradata; Wikipedia contributors, (1 marzo 2024), “Trunk prefix”, *Wikipedia The Free Encyclopedia*, https://en.wikipedia.org/w/index.php?title=Trunk_prefix&oldid=1211267764

rapporti di intelligence citanti il programma, con un'emissione di circa 2.000 rapporti al mese. Nel 2012 sono stati 24.005, con un aumento del 27% rispetto all'anno precedente.

La richiesta di raccolta massiva di tutti i tabulati telefonici nazionali di Verizon, il libero accesso ai database delle più importanti aziende informatiche e lo sfruttamento delle infrastrutture di rete (quali i TAT o le torri di trasmissione), suggeriscono come l'NSA, a partire dagli eventi dell'11 settembre, abbia continuato ad ampliare il programma di data-mining iniziato dall'amministrazione Bush, sviluppando ed aggiornando i sistemi utilizzati al fine di adattarli alle tecnologie più moderne. Di fatto, conseguentemente alla crescita esponenziale del settore digitale negli ultimi vent'anni, non risulterebbe strano ipotizzare che attualmente esistano più sistemi capaci di rendere la ricerca, l'intercettazione e la sorveglianza dell'obiettivo ancora più efficaci. Basti pensare allo Spyware Pegasus, software di recente fattura, prodotto da un'azienda di sicurezza israeliana (*Nso Group*), concepito per varcare con facilità i tradizionali sistemi di sicurezza di diversi dispositivi come Smartphone, Tablet e Pc. Pur lasciando pochissime tracce, Pegasus può insinuarsi nel device appropriandosi indebitamente di file multimediali, dati

relativi alla geo localizzazione, password oppure leggere chat criptate o modificare il registro delle chiamate. [21]

2.5 FISA Amendments Act (2008)

Giorno particolarmente significativo fu il 10 luglio 2008, ove coerentemente agli atti ed emendamenti approvati sotto l'amministrazione Bush nel campo della sorveglianza, fu avallato il FISA Amendments Act, emendamento volto ad indebolire le limitazioni alla sorveglianza, già precedentemente compromesse dal PAA, permettendo al governo di acquisire le comunicazioni internazionali di cittadini e residenti statunitensi senza richiedere di identificare le persone da monitorare; di specificare le strutture, i luoghi, i locali o le proprietà da sorvegliare; di rispettare limitazioni significative sulla conservazione e la diffusione delle informazioni acquisite; di ottenere mandati individualizzati basati su una causa probabile criminale o di intelligence estera; o anche di ricorrere alla determinazione preventiva per via amministrativa, facendo si che gli obiettivi della sorveglianza governativa possano essere considerati agenti stranieri anche solo se ritenuti collegati in qualche modo, per quanto tenue, al terrorismo. Difatti, secondo l'emendamento, il governo non è tenuto ad identificare gli obiettivi della

[21] "Pegasus: che cos'è e come funziona", (12 August 2021), CoreSistemi, https://coresistemi.it/pegasus-che-cose-come-funziona/

sorveglianza, consentendogli di condurre un monitoraggio intrusivo senza esplicitare alla Foreign Intelligence Surveillance Court (FISC) chi intende sorvegliare, quali linee telefoniche e indirizzi e-mail intende monitorare, dove si trovano gli obiettivi della sorveglianza o perché la sta conducendo. Di fatto il ruolo della FISC è limitato alla verifica iniziale di qualsiasi nuovo programma di sorveglianza, non avendo l'autorità di supervisionarne l'attuazione nel tempo [22], e alla revisione delle procedure di "targeting", "minimizzazione" del governo ed "interrogazione" (come aggiunta recente) che regolano la profilazione dei cittadini statunitensi, come nomi, numeri di telefono e indirizzi e-mail, per cercare informazioni precedentemente raccolte ai sensi della *Section 702*. Sebbene la *Sezione 702* proibisca il "reverse targeting" (ossia la raccolta di comunicazioni diretta, con obiettivo una persona specifica negli Stati Uniti), le "interrogazioni" vengono eseguite a fronte di informazioni già raccolte. [23]

Le sopracitate procedure revisionate dalla FISC riguardano l'acquisizione, conservazione, l'uso e la diffusione di informazioni non pubblicamente disponibili riguardanti persone statunitensi non consenzienti, acquisite prendendo di mira persone non statunitensi che si ritiene ragionevolmente si trovino al di fuori degli

[22] ACLU. (n.d.), "Why the FISA Amendments Act is unconstitutional", *ACLU,* https://www.aclu.org/sites/default/files/images/nsaspying/asset_upload_file578_35950.pdf

[23] Aaron, D., "Unpacking the FISA Section 702 Reauthorization Bill", *Just Security*, (10 Giugno 2024), https://www.justsecurity.org/94771/unpacking-the-fisa-section-702-reauthorization-bill/

USA, in osservanza del Quarto Emendamento della costituzione ed in conformità con la *Section 702* del FISA. [24] [25] Peraltro nella medesima sezione è presente una clausola di decadenza incorporata in base al quale le autorità acquisite dall'emendamento scadono periodicamente. Non per nulla, alla fine dello scorso anno fu approvato dal Congresso e firmato dal Presidente Biden il National Defense Authorization Act (NDAA), [26] legge che includeva una disposizione enstensiva della *Section 702*, prorogandone la scadenza al 19 aprile 2024. Tuttavia, nel testo del NDAA non è inclusa alcuna disposizione esplicita volta ad impedire all'amministrazione Biden di continuare liberamente la sorveglianza fino al 2025.

2.6 Il "BoundlessInformant" ed "XKeyscore"

Tra i numerosi strumenti collegati al programma PRISM, ne risaltano due in particolare. Il primo è il "*BoundlessInformant*", un potente sistema di elaborazione di Big Data nato per registrare e analizzare la provenienza delle informazioni

[24] H.R.6304 - 110th Congress (2007-2008): FISA Amendments Act of 2008, H.R.6304, 110th Cong. (2008), https://www.congress.gov/bill/110th-congress/house-bill/6304.

[25] NSA/CSSM 1-52, "*Minimization procedures used by the National Security Agency in connection with acquisitions of foreign intelligence information pursuant to section 702 of the Foreign Intelligence Ssurveillance Act of 1978, as amended*", pp 1-13, 8 Gennaio 2007.

[26] H.R.7900 - 117th Congress (2021-2022): National Defense Authorization Act for Fiscal Year 2023, H.R.7900, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/7900.

raccolte dall'Agenzia, dettagliando e mappando per ogni Paese l'enorme quantità di informazioni raccolte dalle reti informatiche e telefoniche. Il software si concentra sul conteggio e sulla categorizzazione delle registrazioni delle comunicazioni, e non sul loro contenuto. Può identificare quante conversazioni vengono fatte e dove, ma le email e i messaggi di testo non vengono tracciati. I documenti di *BoundlessInformant* mostrano che l'agenzia ha raccolto quasi 3 miliardi di dati dalle reti informatiche statunitensi in un periodo di 30 giorni, terminato nel marzo 2013. Il suo scopo è stato quello di fornire ai funzionari dell'NSA informazioni riguardo il tipo di copertura relativa ad un paese, una sorta di dashboard riepilogativa per tenere traccia della sorveglianza effettutata fino ad allora. Un'istantanea dei dati di *BoundlessInformant*, contenuta in una heat map declassificata dell'NSA, mostra che nel marzo 2013 l'agenzia ha raccolto 97 miliardi di informazioni dalle reti informatiche di tutto il mondo. [27] L'Iran è stato il Paese in cui è stata raccolta la maggior quantità di informazioni, con oltre 14 miliardi di rapporti nello stesso periodo, seguito dai 13,5 miliardi del Pakistan. La Giordania, uno dei più stretti alleati arabi dell'America, si è classificata terza con 12,7 miliardi, l'Egitto quarto con 7,6 miliardi e l'India quinta con 6,3 miliardi. La mappa di calore assegna a ogni nazione un codice colore in base all'estensione della sorveglianza. La scala

[27] Greenwald G. & MacAskill E., (2017a, July 14), "Boundless Informant: the NSA's secret tool to track global surveillance data", *The Guardian*, https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

cromatica va dal verde (meno sottoposto a sorveglianza) al giallo e all'arancione, fino al rosso (maggiore sorveglianza). [28] [29]

Figura 5, Il "BoundlessInformant"

Il Secondo è *XKeyscore*, il sistema di "più ampia portata" dell'NSA per lo sviluppo di intelligence dalle reti informatiche (ciò che l'agenzia chiama Digital Network Intelligence o DNI). Una presentazione sostiene che il programma copre "quasi tutto ciò che un utente tipico fa su Internet", difatti lo scopo di XKeyscore è quello di consentire agli analisti di ricercare e-mail, chat, traffico di navigazione web, immagini, documenti, chiamate vocali, foto da webcam, ricerche web, traffico su social media, traffico di botnet (rete di computer infettata da malware), sequenze di

[28] "L'informatore senza limiti della Nsa", (5 Aprile 2017), *Internazionale*, https://www.internazionale.it/notizie/2013/06/10/l-informatore-senza-limiti-della-nsa

[29] Garber, M., "Meet 'Boundless Informant, the NSA's Secret Tool for Tracking Global Surveillance Data", (9 Giugno 2013), *The Atlantic*, https://www.theatlantic.com/technology/archive/2013/06/meet-boundless-informant-the-nsas-secret-tool-for-tracking-global-surveillance-data/276686/

tasti registrate, targeting di reti informatiche (CNE), coppie di nomi utente e password intercettate, upload di file su servizi online, sessioni Skype e altro ancora. Tutto in tempo reale. [30] Anche quando non esiste un account di posta elettronica noto (definito dall'NSA come "selettore") associato all'individuo obiettivo, gli analisti possono effettuare ricerche in base al nome, al numero di telefono, all'indirizzo IP, alle parole chiave, alla lingua in cui è stata condotta l'attività su Internet o al tipo di browser utilizzato.

Figura 6. Estratto del documento "XKeyscore presentation from 2008" - The Guardian - https://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

[30] Greenwald, G., Lee M., & Marquis-Boire M., (20 settembre 2019). "NSA's Google for the World's Private Communications", *The Intercept*, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

Il software fornisce la capacità tecnologica, se non l'autorità legale, di sottoporre a sorveglianza elettronica estensiva anche persone statunitensi, come visto precedentemente, senza un mandato, a patto che l'agente sia a conoscenza della mail o dell'indirizzo IP dell'obiettivo. I documenti della NSA affermano che nel 2008, circa 300 terroristi sono stati catturati utilizzando le informazioni di XKeyscore. [31] [32]

2.7 The Fourth Amendment

In questo capitolo cercheremo di stabilire se il programma di spionaggio della NSA violi o meno il Quarto Emendamento, esaminando la letteratura legale al riguardo. Costruiremo ed esamineremo le ramificazioni di due diversi modelli funzionali del programma della NSA, al fine di valutarne la costituzionalità nel suo complesso. La divisione tra gli studiosi di diritto indica che la questione della validità legale del programma della NSA è tutt'altro che chiara e che si tratta di una questione legale piuttosto complessa, divergendo riguardo alla corretta interpretazione. Prenderemo in esame il modello "ristretto" ed il modello "espansivo". Il modello

[31] Greenwald G. , (14 Luglio 2014), "XKeyscore: NSA tool collects "nearly everything a user does on the internet." *The Guardian*, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[32] "Report on a certain NSA Uses of XKEYSCORE for Counterterrorism Purposes", (2020), *Privacy and Civil Liberties Oversight Board*, https://documents.pclob.gov/prod/Documents/OversightReport/ee4c139b-1674-4bfa-9b6a-5b591b648090/NSA%20XKEYSCORE%20REPORT.pdf

espansivo del programma (senza mandato) comprende i seguenti due elementi importanti. In primo luogo, la NSA può piazzare un'intercettazione telefonica, situata all'estero, su un sospetto terrorista straniero che risiede in un Paese straniero. In secondo luogo, la NSA può effettuare un'intercettazione telefonica negli Stati Uniti su un cittadino statunitense. Il modello ristretto invece, comprende un unico elemento importante. L'NSA piazza una cimice, situata all'estero, su un sospetto terrorista straniero che risiede in un Paese straniero per monitorare tutte le chiamate da e verso la sua linea telefonica. Secondo il modello ristretto del programma, la NSA non va ad effettuare intercettazioni senza mandato delle telefonate internazionali in uscita o in entrata di un sospetto terrorista che vive negli Stati Uniti. L'unico modo in cui la telefonata di un cittadino statunitense che vive negli Stati Uniti verrebbe registrata è se questa persona effettua/riceve una telefonata internazionale al/dal sospetto terrorista straniero che risiede all'estero. [33]

Per stabilire se il Quarto Emendamento sia stato violato, occorre innanzitutto determinare se sia stata effettuata una "perquisizione", condotta da o per conto del governo. Se il modus operandi adottato dal governo non costituisce una perquisizione, la protezione dell'Emendamento non viene attivata. In secondo luogo, l'emendamento prevede sia un requisito di mandato (emesso su causa

[33] Randy E. Barnett, "Why the NSA data seizures are unconstitutional", *Georgetown University Law Center*, 38 Harv. J.L. & Pub. Pol'y 3-20 (2015), https://scholarship.law.georgetown.edu/facpub/1659

probabile) che un requisito di ragionevolezza. Entrambi i requisiti rappresentano due approcci distinti al Quarto Emendamento, il che significa che in alcune situazioni i tribunali applicheranno il requisito del mandato escludendo il requisito della ragionevolezza e viceversa.

"[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures [34]*, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath* [35] *or affirmation* [36]*, and particularly describing the place to be searched* [36]*, and the persons or things to be seized* [37]*."* [38]

[34] "Una perquisizione e un sequestro irragionevoli sono una perquisizione e un sequestro eseguiti 1) senza un mandato di perquisizione legale firmato da un giudice o da un magistrato che descriva il luogo, la persona o le cose da perquisire o sequestrare o 2) senza una probabile causa di credere che una certa persona, un luogo specifico o un'automobile abbiano prove criminali o 3) estendendo l'ambito autorizzato della perquisizione e del sequestro." (unreasonable search and seizure", *LII / Legal Information Institute.*)

[35] "Il giuramento è un'attestazione o una promessa fatta dalla persona che lo presta, in base a un senso immediato di responsabilità nei confronti di Dio. In senso lato, la parola "giuramento" comprende tutte le forme di attestazione con cui una persona dichiara di essere obbligata in coscienza a compiere un atto in modo fedele e veritiero, e in questo senso include l'"affermazione"." *(22 CFR § 92.18 - Oaths and affirmations defined. LII / Legal Information Institute.)*

[36] "Un'affermazione è una dichiarazione o asseverazione solenne e formale, avente la natura di un giuramento, che attesta la veridicità di una dichiarazione o di una serie di dichiarazioni. Quando il giuramento è richiesto o autorizzato dalla legge, una dichiarazione sostitutiva può essere fatta da chiunque abbia scrupoli di coscienza contro il giuramento. Come regola generale, un'affermazione ha la stessa forza ed effetto legale di un giuramento." *(22 CFR § 92.18 - Oaths and affirmations defined, LII / Legal Information Institute.)*

[37] "Il termine "perquisizione e sequestro", nel diritto penale, indica l'esame da parte di un agente delle forze dell'ordine dell'abitazione, del veicolo o dell'azienda di una persona per trovare le prove che è stato commesso un reato. Una perquisizione comporta che le forze dell'ordine esaminino una parte o l'intera proprietà di un individuo, alla ricerca di oggetti specifici che siano collegati a un reato che hanno motivo di ritenere sia stato commesso. Il sequestro avviene se gli agenti entrano in possesso di oggetti durante la perquisizione." (*search and seizure, LII / Legal Information Institute)*

[38] Fourth Amendment. *LII / Legal Information Institute.* https://www.law.cornell.edu/wex/fourth_amendment

I Padri Fondatori chiesero l'approvazione del Quarto Emendamento per impedire al Presidente degli Stati Uniti e ad altri membri del ramo esecutivo di utilizzare "mandati generali" per violare i diritti alla privacy dei coloni, sottoponendoli a perquisizioni arbitrarie basate su una discrezionalità illimitata. Il testo della legge è stato redatto in base al disprezzo per i mandati generali, ma includendo anche il requisito di ragionevolezza nel testo. Il requisito è stato probabilmente aggiunto per creare uno standard legale (cioè la "ragionevolezza") per le perquisizioni senza mandato condotte dalle forze dell'ordine come difesa contro la responsabilità civile.[39] L'intercettazione governativa (o qualsiasi altra forma di intercettazione elettronica) di una conversazione tra due o più individui che comunicano telefonicamente, costituisce una perquisizione ai sensi del Quarto Emendamento. Pertanto, nel modello ristretto, l'intercettazione elettronica viene classificata, in ogni sua forma, come una perquisizione nei confronti della persona che è stata oggetto dell'intercettazione. Va sottolineato il ruolo cruciale del giudice neutrale, che rilasciando al governo solo mandati basati su causa probabile (dichiarati dalla Corte come inequivocabilmente necessari, salvo strette eccezioni), sostiene e salvaguarda i diritti alla privacy che il Quarto Emendamento garantisce a tutti gli americani. Di contro, il modello espansivo del programma dell'NSA è molto simile

[39] L. Rush Atkinson, "The Fourth Amendment's National Security Exception: Its History and Limits", *66 Vanderbilt Law Review xi* (2013) https://scholarship.law.vanderbilt.edu/vlr/vol66/iss5/1

a un mandato generale. Sono i funzionari della NSA, piuttosto che un giudice neutrale, a decidere se intercettare, quando intercettare, chi intercettare, per quanto tempo e così via. Il programma della NSA mette a rischio i diritti alla privacy degli americani, che conducono conversazioni altamente private su linee telefoniche internazionali controllate dall'Esecutivo. Questo è costituzionalmente inaccettabile secondo la giurisprudenza del Quarto Emendamento, in quanto il giudice neutrale deve frapporsi tra il governo e i cittadini, per garantirne il diritto alla privacy. In conclusione, potremmo sostenere che il modello "ristretto" del programma NSA sia costituzionale e verrebbe confermato dai tribunali, mentre il modello "espansivo" del programma NSA sarebbe giudicato incostituzionale, in quanto violerebbe il Quarto Emendamento conformemente alla mancata emissione di mandati e alla mancata mediazione di un giudice di pace. Le conseguenze di questa incertezza giuridica e la mancanza di tutela del Quarto Emendamento per i cittadini non statunitensi, rappresentano un chiaro segno di come le autorità statunitensi non riconoscono alcun diritto alla privacy per i non americani. [40]

[40] Norvell B., "THE CONSTITUTION AND THE NSA WARRANTLESS WIRETAPPING PROGRAM: a FOURTH AMENDMENT VIOLATION?", (1 Gennaio 2009), http://hdl.handle.net/20.500.13051/7763

3. RISPOSTA DELL'EUROPA ED EVOLUZIONE DELLA NORMATIVA

3.1 La reazione dell'Europa

La Commissione Europea espresse preoccupazione per PRISM subito dopo la diffusione dei documenti relativi al programma di sorveglianza. La dichiarazione evidenziava le differenze tra gli approcci degli Stati Uniti e dell'UE sulla protezione dei dati, in particolare il fatto che gli Stati Uniti "garantivano" ai cittadini statunitensi la tutela della privacy, mentre ai cittadini dell'UE non venivano assicurate le tutele costituzionali o un'adeguata supervisione della raccolta dei dati, affinché questa avvenisse entro i limiti della legalità. La dichiarazione della Commissione Europea sottolineava come il programma PRISM sarebbe dovuto essere limitato a singoli casi e basato su sospetti concreti, se finalizzato all'applicazione della legge. In particolare, una successiva riforma della protezione dei dati avrebbe dovuto affrontare la questione dell'ambito territoriale per imporre

alle aziende non appartenenti all'UE di rispondere alle normative europee in materia di protezione dei dati mentre operano in Europa. [41]

Successivamente, il 4 Luglio 2013, venne approvato il testo P7_TA(2013)0322 come risposta all'impatto causato dal Datagate di Edward Snowden. Nel testo, il parlamento europeo si espresse con seria preoccupazione in merito al programma di sorveglianza, poiché si sarebbe potuta configurare "una grave violazione del diritto fondamentale alla privacy e alla protezione dei dati ai danni dei cittadini e dei residenti dell'UE, nonché del diritto al rispetto della vita privata e familiare, della riservatezza delle comunicazioni, della presunzione di innocenza, della libertà di espressione, della libertà di informazione e della libertà di esercitare un'attività economica." [42] Si invitarono poi le autorità statunitensi a fornire ogni informazione concernente il programma PRISM (ed ulteriori ed eventuali programmi analoghi di raccolta dati) all'UE, in particolare quelle riguardanti la loro base giuridica, la necessità e la proporzionalità, nonché le garanzie adottate per proteggere i diritti fondamentali dei cittadini dell'UE, come le limitazioni sulla portata e la durata, le

[41] Andreas Geiger, "EU Will Ramp Up Data Protection in Wake of Snowden", *THE HILL* (14 Agosto 2013), http://thehill.com/blogs/congress-blog/foreign- policy/317061-eu-will-ramp-up-data-protection-in-wake-of-snowden-.

[42] "Testi approvati - Programma di sorveglianza della NSA negli Stati Uniti, servizi segreti in diversi Stati membri e impatto sulla privacy dei cittadini dell'UE" (Giovedì 4 luglio 2013), © *Unione Europea*, *Parlamento Europeo*, https://www.europarl.europa.eu/doceo/document/TA-7-2013-0322_IT.html#ref_1_1

condizioni di accesso e la supervisione indipendente, come previsto dalla *Convenzione sulla criminalità informatica* che mira a contribuire "alla lotta contro i reati che possono essere commessi solo attraverso l'uso della tecnologia, in cui i dispositivi sono allo stesso tempo lo strumento per commettere il reato e l'obiettivo del reato, e i reati in cui la tecnologia è stata utilizzata per favorire un altro reato, quali frodi. La Convenzione fornisce orientamenti per qualsiasi paese che sviluppi leggi nazionali sulla criminalità informatica e serve come base per la cooperazione internazionale tra le parti contraenti della convenzione." [43] Proprio in quest'ultimo punto, la Commissione invitava le autorità statunitensi a riprendere quanto prima i negoziati concernenti la protezione dei dati personali trasferiti e trattati ai fini della cooperazione di polizia e giudiziaria, e che i negoziati rispettassero il diritto all'informazione dei cittadini UE qualora i dati fossero stati elaborati negli USA, l'accesso al sistema giudiziario statunitense pari a quello previsto per i cittadini statunitensi ed il diritto di ricorso. [42] Inoltre, venne sottolineato che le società soggette alla giurisdizione di un paese terzo avrebbero dovuto fornire agli utenti stabiliti nell'UE un'avvertenza chiara e ben visibile della possibilità che i dati personali fossero elaborati dai servizi incaricati dell'applicazione della legge e dalle agenzie di intelligence per effetto di ordini segreti o ingiunzioni.

[43] "Convenzione sulla criminalità informatica", *EUR-Lex*, https://eur-lex.europa.eu/IT/legal-content/summary/convention-on-cybercrime.html

3.2 Il "Safe Harbour"

Per quanto concerne il trasferimento stesso dei dati da parte delle aziende coinvolte presenti in Europa, viene sottolineata nel n. 36 del Testo approvato P7_TA(2014)0230 (12 marzo 2014) la loro adesione all'accordo di "Safe Harbour", [44] che autorizza i trasferimenti di dati personali dal territorio dello Stato membro verso organizzazioni aventi sede negli Stati Uniti effettuati sulla base e in conformità ai "*Principi di approdo sicuro in materia di riservatezza*". [45] Prendendo in esame due punti fondamentali dalla "*Decisione della Commissione a norma della direttiva 95/46/CE del Parlamento Europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di Approdo Sicuro"*, ossia:

1) *"[…] gli Stati membri sono tenuti a consentire il trasferimento verso un paese terzo di dati personali soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato e se vengono rispettate, prima*

[44] Testi approvati - Programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti e impatto sui diritti fondamentali dei cittadini dell'UE - Mercoledì 12 marzo 2014. (n.d.). © Unione Europea, 2014 - Fonte: Parlamento Europeo. https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_IT.html

[45] Autorizzazione al trasferimento verso gli Stati Uniti d. (n.d.). https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/30939

del trasferimento stesso, norme di attuazione delle altre disposizioni della direttiva adottate dagli Stati membri;" [46]

2) *"La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. In tal caso è possibile trasferire dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie;"* [47]

si desume il timore espresso dall'UE riguardo la mancata codificazione dei dati trasferiti e la necessità di effettuare controlli sulla liceità e correttezza dei trasferimenti e delle operazioni di trattamento anteriori ai trasferimenti medesimi, nonché sul rispetto dei principi sopraindicati, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento in mancata osservanza di tali criteri. [44]

3.3 Miglioramento della normativa Europea

Negli anni, la crescente preoccupazione generata dall'esponenziale sviluppo dei sistemi informatici, ha comportato una serie di adeguamenti da parte dell'Unione Europea e degli Stati membri. Tra questi il più significativo è sicuramente il

[46] Decisione della Commissione circa l'adeguatezza della protezione dati offerta dai principi dell'Approdo sicuro ("Safe Harbor"). (n.d.). https://www.privacy.it/archivio/com2000-520.html

[47] Id.

Regolamento UE 2016/679, meglio noto come *Regolamento Generale Sulla Protezione dei Dati* (GDPR) entrato in vigore 25 Maggio 2016. Esso è volto a colmare le lacune riguardanti la raccolta ed il trattamento dei dati da parte del settore pubblico e privato, mirando a rafforzare i diritti individuali e a facilitare le attività economiche con regole chiare per le imprese nel mercato unico digitale, eliminando la frammentazione e gli oneri amministrativi superflui. Di fatto, come recita l'Art. 1 del regolamento:

"1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali." [48]

Esso viene applicato al trattamento interamente o parzialmente automatizzato e al trattamento, non automatizzato, di dati destinati o contenuti in archivio.

[48] Regolamento - 2016/679 - EN - GDPR - EUR-Lex., https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679

L’inapplicabilità del regolamento riguarda principalmente il trattamento da parte delle autorità competenti, approfondito in una direttiva ulteriore. Essa stabilisce norme per la protezione delle persone fisiche nel trattamento dei dati personali da parte delle autorità competenti per la prevenzione, indagine, accertamento e perseguimento di reati, oltre alla salvaguardia e prevenzione di minacce alla sicurezza pubblica. Gli Stati membri garantiscono che lo scambio dei dati tra le autorità competenti all'interno dell'Unione non sia limitato né vietato per motivi legati alla protezione dei dati personali, non impedendo agli Stati membri di prevedere garanzie più elevate per la tutela dei diritti e delle libertà nel trattamento dei dati personali da parte delle autorità competenti. [49]

Gli Stati membri dell'UE hanno inoltre istituito autorità nazionali per la protezione dei dati in conformità con la *Carta dei Diritti Fondamentali dell'Unione Europea*. Il *Comitato Europeo per la Protezione dei Dati* (EDPB), organismo indipendente istituito dal GDPR, assicura l'applicazione coerente delle norme sulla protezione dei dati in tutta l'UE. Il regolamento (UE) 2018/1725 stabilisce le norme per il trattamento dei dati personali da parte delle istituzioni dell'UE, in linea con il GDPR.[50] Il *Garante Europeo della Protezione dei Dati* (GEPD) monitora

[49] Direttiva - 2016/680 - EN - EUR-LEX. (n.d.). https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016L0680

[50] Regolamento 2018/1725, EUR-LEX, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32018R1725

l'applicazione delle norme nelle istituzioni europee. La Commissione Europea ha anche nominato un responsabile della protezione dei dati per monitorare internamente l'applicazione delle norme. Inoltre, nel giugno 2021, la Commissione Europea ha adottato due serie di clausole contrattuali per agevolare la conformità al GDPR, una per l'uso tra titolari del trattamento e responsabili del trattamento all'interno dello Spazio Economico Europeo (SEE) e l'altra per il trasferimento di dati personali verso paesi al di fuori del SEE. [51]

4. VALORE DEI DATI IN ITALIA: CONTESTO E DIMENSIONI

4.1 Il GDPR in Italia

In Italia il GDPR è stato accolto l'8 agosto 2017, con l'approvazione da parte del Consiglio dei Ministri del decreto legislativo di armonizzazione del *Codice Privacy* (d.lgs. n. 196/2003) [52] e delle altre leggi dello Stato al GDPR. il Consiglio dei Ministri ha approvato in via definitiva il decreto attuativo, integrandolo però con regole semplificate per le PMI e aggiungendo una moratoria di otto mesi per quanto

[51] "La protezione dei dati nell'UE", *Commissione Europea*, https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_it

[52] Decreto legislativo 30 giugno 2003, n. 196, CODICE INMATERIA DI PROTEZIONE DEI DATI PERSONALI, https://www.privacy.it/archivio/codiceprivacy.html#art1

riguarda i controlli e le sanzioni. Operativamente si tratta dell'attuazione dell'articolo 13 della legge di delegazione europea 2016-2017, che coordina la normativa nazionale con la legge UE, e nello specifico l'Italia ha deciso di adottare una prassi già intrapresa da altri paesi europei. [53] Ha scelto perciò di attivare una prima fase soft, di applicazione del GDPR, dove sono venuti a mancare controlli e sanzioni da parte del garante. Infine, la normativa italiana prevede anche delle semplificazioni per le PMI, affidate ai provvedimenti del Garante. Le imprese hanno avuto tempo, grazie alla moratoria su ispezioni e sanzioni per un periodo di otto mesi, sino al gennaio 2019 per adeguarsi alla nuova normativa sul trattamento dei dati personali o GDPR. [54]

4.2 L'adeguamento dell'Italia al GDPR: la raccolta ed il trattamento dei dati

Il GDPR prevede che il titolare del trattamento dei dati fornisca agli interessati un'informativa chiara e completa prima di iniziare il trattamento dei dati stessi. L'informativa deve rendere l'interessato consapevole delle finalità e modalità del trattamento, garantendo trasparenza e correttezza (principio di accountability). Essa

[53] LEGGE 25 ottobre 2017, n. 163, "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea", Legge di delegazione europea 2016-2017, (17G00177) (GU Serie Generale n.259 del 06-11-2017), https://www.gazzettaufficiale.it/eli/id/2017/11/6/17G00177/sg

[54] "GDPR: cosa dice il decreto italiano sulla privacy", (20 Agosto 2018), *MetalCoop*. https://www.metalcoop.it/gdpr-cosa-dice-decreto-italiano-sulla-privacy/

è necessaria anche per ottenere un consenso valido, se richiesto. L'informativa è obbligatoria quando i dati sono raccolti direttamente dall'interessato o da terzi. Non è richiesta per dati anonimi, di enti o persone giuridiche, o per trattamenti a scopo personale/domestico. Se i dati non sono raccolti direttamente dall'interessato, l'informativa deve essere fornita entro un mese o al momento della comunicazione a terzi. Non è necessaria quando l'interessato dispone già delle informazioni, se la comunicazione è impossibile o sproporzionata, se è prevista dal diritto dell'UE o dello Stato membro, o se i dati devono rimanere riservati per segreto professionale. Il contenuto minimo dell'informativa include: categorie e finalità dei dati trattati, base giuridica del trattamento, obbligatorietà del conferimento dei dati, destinatari dei dati, trasferimenti extra UE, periodo di conservazione dei dati, diritti dell'interessato, dati identificativi del titolare e del responsabile della protezione dei dati, e eventuali processi decisionali automatizzati. Deve anche includere i cookie utilizzati dal sito e come disabilitarli. [55]

L'informativa deve essere chiara, accessibile e intellegibile, soprattutto per i minori, e può essere fornita per iscritto, via elettronica o oralmente se richiesto. Essa è sempre dovuta ogni qual volta vi sia la raccolta ed il trattamento dei dati (es.

[55] "LEGGE SULLA PRIVACY, UNA COMPLETA SINTESI AGGIORNATA", (13 Febbraio 2013), *AB Innovation Consulting*, https://www.abinnovationconsulting.com/blog/legge-sulla-privacy-una-completa-sintesi-aggiornata/

indirizzi IP, mail). Le violazioni dell'obbligo di informativa possono comportare sanzioni da parte dell'autorità di controllo e azioni legali da parte degli utenti. [56] Ulteriore considerazione da fare riguarda il consenso. Se i dati vengono utilizzati ai fini del sito (es. mailing list), occorre solo l'informativa privacy ma non la raccolta del consenso, mentre se usati per fini promozionali o pubblicitari, serve sia l'informativa che il consenso.

4.3 Cybersicurezza e disposizioni attuali

Il 19 giugno 2024, il Senato della Repubblica ha approvato in via definitiva il ddl d'iniziativa governativa in materia di rafforzamento della cybersicurezza nazionale e reati informatici, noto come DDL Cybersicurezza, per contrastare il crescente fenomeno del cybercrime as a service, che include attacchi ransomware dannosi per imprese e organizzazioni statali. Il disegno di legge, composto da 24 articoli, introduce significativi aumenti di pena per reati quali l'accesso abusivo a sistemi informatici, la distribuzione di programmi dannosi ed il danneggiamento di informazioni, dati e programmi informatici. Introduce anche l'obbligo di notifica degli incidenti per enti pubblici e aziende di trasporto urbano, supervisionato dall'Agenzia per la Cybersicurezza Nazionale (ACN) con sanzioni fino a 125.000

[56] Capone F., "Cookie 2022: nuove norme dal 10 gennaio", (19 Febbraio 2022), *Ecommerce Legale*, https://ecommercelegale.it/gdpr/cookie-nuove-norme-da-gennaio-2022/#_Cookie_le_novita_dal_10_gennaio_2022

euro per mancate segnalazioni. [57] [58] Inoltre, il DDL affronta l'intelligenza artificiale, armonizzandosi con il recente AI Act europeo, prevedendo norme per garantire la sicurezza dei dispositivi digitali attraverso il Cyber Resilience Act. Quest'ultimo, approvato dal Parlamento Europeo, impone nuovi requisiti per la sicurezza dei prodotti digitali immessi sul mercato dell'UE. Questo regolamento, che prevede un periodo di adeguamento di 36 mesi per i produttori (a partire da marzo 2024), mira a garantire il rispetto delle norme di sicurezza standardizzate per tutti i dispositivi hardware e software. Esso si applica a una vasta gamma di prodotti, escludendo quelli già regolamentati come i dispositivi medici, veicoli a motore e relativi componenti. [59]

Questi sforzi legislativi mirano a migliorare la sicurezza informatica nell'Unione Europea e creare un mercato europeo uniforme per la sicurezza digitale, semplificando le procedure di conformità e migliorando la protezione per

[57] Bruseghin, D., & Bruseghin, D. (2024, March 15). DDL Cybersicurezza: allo studio del Parlamento le nuove regole di difesa nel cyberspazio. Cyber Security 360. https://www.cybersecurity360.it/cybersecurity-nazionale/ddl-cybersicurezza-allo-studio-del-parlamento-le-nuove-regole-di-difesa-nel-cyberspazio/

[58] DISPOSIZIONI IN MATERIA DI RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE E DI REATI INFORMATICI, Dossier XIX Legislatura, A.C. n. 1717, (12 marzo 2024), *Senato della Repubblica, Camera dei Deputati,* https://documenti.camera.it/leg19/dossier/pdf/AC0225.pdf?_1710354256194

[59] DISPOSIZIONI IN MATERIA DI RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE E DI REATI INFORMATICI, (19 Giugno 2024), *Senato della Repubblica,* https://www.giurisprudenzapenale.com/wp-content/uploads/2024/06/messddl-1143__437629.pdf

consumatori e aziende, introducendo standard uniformi e protezioni per prodotti digitali.

5. PROSPETTIVE FUTURE E CONCLUSIONI

Nonostante l'evoluzione nel panorama della privacy, una cosa rimane chiara nel 2024: avere un piano di sicurezza strategico completo è fondamentale per salvaguardare i dati personali dalle sempre crescenti minacce informatiche. È importante tenere a mente che rimanere aggiornati sulla cybersecurity richiede sia un impegno costante che una prospettiva di “ampio respiro”. Sebbene la conformità normativa e le forze geopolitiche possano fornire indicazioni preziose per la pianificazione dei sistemi di sicurezza digitale e per la salvaguardia del diritto alla privacy (come il GDPR per l’Europa), con la crescita esponenziale di dispositivi connessi come smartphone, gadget per la casa intelligente e dispositivi Internet of Things (IoT), la superficie di attacco si è notevolmente ampliata. Se non protetti, i dispositivi possono diventare facili bersagli di attacchi informatici, consentendo agli aggressori di raccogliere metadati sempre più facilmente. Le organizzazioni devono proteggere in modo proattivo i loro ambienti di rete intricati e interconnessi. Ciò implica la correzione tempestiva delle vulnerabilità, l'implementazione di

solide misure di autenticazione e la segregazione delle reti per contenere la propagazione di malware.

Come analizzato in questa tesi, il paradigma odierno si basa sull'estrazione dei dati. Gli internauti navigano sul web e si confrontano con i marchi, mentre le aziende monitorano e registrano questi comportamenti insieme a tutte le informazioni demografiche necessarie per registrarsi o effettuare transazioni con loro. Una volta estratti, questi dati possono essere utilizzati per analisi, marketing e altri scopi come la sorveglianza. Allo stesso tempo questo avviene senza il consenso degli utenti, il che da origine a un mix sempre più complesso di tecnologie e leggi che limitano/auto-limitano il modo in cui le informazioni possono essere acquisite, ospitate e utilizzate. In più la scarsa sensibilità dei consumatori nei confronti dello stato della privacy online rende evidente che qualcosa deve cambiare alla fonte. Ciò troverebbe soluzione nell'educare gli individui e le organizzazioni sull'importanza della protezione delle informazioni personali e di incoraggiarli a prendere provvedimenti per salvaguardare i loro dati attraverso i numerosi strumenti di prevenzione (VPN, Browser con VPN integrata, ADBlocker, estensioni browser per il blocco dei cookie, ecc.). Successivamente, per quanto concerne le autorità governative ed il potere che detengono, esse dovranno tener conto delle necessità delle tecnologie di sorveglianza, che diventando più sofisticate, trovino e mantengano il delicato equilibrio tra sicurezza e privacy. I governi e le

organizzazioni dovranno affrontare un controllo crescente per garantire che le misure di sorveglianza siano proporzionate, trasparenti e rispettino i diritti degli individui.

In Conclusione, la privacy dei dati emerge come un panorama dinamico e in continua evoluzione. I governi debbono dare priorità a piani strategici di cybersecurity completi che si allineino alla conformità normativa ed alla salvaguardia del diritto alla privacy di ogni individuo. I progressi con l'intelligenza artificiale, i cambiamenti normativi e le considerazioni etiche rimodelleranno il nostro approccio alla protezione dei dati personali. Navigare in questo futuro richiede un impegno collettivo, dai singoli alle organizzazioni, dai responsabili politici ai tecnologi, per promuovere un ambiente digitale in cui la privacy non sia solo un diritto, ma una pietra miliare del nostro mondo connesso.

7. BIBLIOGRAFIA E SITOGRAFIA

Felicity Ruby, Gerard Goggin & John Keane (2017) "*Comparative Silence*", Digital Journalism, 5:3, 353-367, DOI: 10.1080/21670811.2016.1254568

Zuboff, S. (2019). "*Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*"

Schneier, B. (2015). "*Data and Goliath: The hidden battles to collect your data and control your world*"

Pasquale, F. (2015). "*The Black Box Society: The Secret Algorithms That Control Money and Information*", Harvard University Press.

Han, B. (2015). "*The transparency society*", Stanford University Press.

Voigt, P., & Von Dem Bussche, A. (2017). "The EU General Data Protection Regulation (GDPR)", In Springer eBooks. https://doi.org/10.1007/978-3-319-57959-7

http://hdl.handle.net/20.500.13051/7763

http://thehill.com/blogs/congress-blog/foreign-policy/317061-eu-will-ramp-up-data-protection-in-wake-of-snowden-

https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_it

https://coresistemi.it/pegasus-che-cose-come-funziona/

https://documenti.camera.it/leg19/dossier/pdf/AC0225.pdf?_1710354256194

https://documents.pclob.gov/prod/Documents/OversightReport/ee4c139b-1674-4bfa-9b6a-5b591b648090/NSA%20XKEYSCORE%20REPORT.pdf

https://ecommercelegale.it/gdpr/cookie-nuove-norme-da-gennaio-

https://en.wikipedia.org/w/index.php?title=Trunk_prefix&oldid=1211267764

https://eur-lex.europa.eu/IT/legal-content/summary/convention-on-cybercrime.html

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016L0680

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32018R1725

https://scholarship.law.georgetown.edu/facpub/1659

https://scholarship.law.vanderbilt.edu/vlr/vol66/iss5/1

https://ssrn.com/abstract=3156725

https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

https://www.abinnovationconsulting.com/blog/legge-sulla-privacy-una-completa-sintesi-aggiornata/

https://www.aclu.org/sites/default/files/images/nsaspying/asset_upload_file578_35950.pdf

https://www.congress.gov/bill/107th-congress/house-bill/3162/text/pl

https://www.congress.gov/bill/109th-congress/house-bill/3199

https://www.congress.gov/bill/110th-congress/house-bill/6304

https://www.congress.gov/bill/110th-congress/senate-bill/1927

https://www.congress.gov/bill/117th-congress/house-bill/7900

https://www.cybersecurity360.it/cybersecurity-nazionale/ddl-cybersicurezza-allo-studio-del-parlamento-le-nuove-regole-di-difesa-nel-cyberspazio/

https://www.eff.org/am/pages/upstream-prism

https://www.europarl.europa.eu/doceo/document/TA-7-2013-0322_IT.html#ref_1_1

https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_IT.html

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/30939

https://www.gazzettaufficiale.it/eli/id/2017/11/6/17G00177/sg

https://www.giurisprudenzapenale.com/wp-content/uploads/2024/06/messddl-1143__437629.pdf

https://www.intelligence.senate.gov/sites/default/files/publications/951720.pdf

https://www.internazionale.it/notizie/2013/06/10/l-informatore-senza-limiti-della-nsa

https://www.justsecurity.org/94771/unpacking-the-fisa-section-702-reauthorization-bill/

https://www.law.cornell.edu/wex/fourth_amendment

https://www.mass.gov/industry-letter/usa-patriot-act

https://www.metalcoop.it/gdpr-cosa-dice-decreto-italiano-sulla-privacy/

https://www.privacy.it/archivio/codiceprivacy.html#art1

https://www.privacy.it/archivio/com2000-520.html

https://www.theatlantic.com/technology/archive/2013/06/meet-boundless-informant-the-nsas-secret-tool-for-tracking-global-surveillance-data/276686/

https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

https://www.treccani.it/enciclopedia/voip_(Lessico-del-XXI-Secolo)/

https://www.washingtonpost.com/news/wonk/wp/2013/06/06/how-congress-unknowingly-legalized-prism-in-2007/