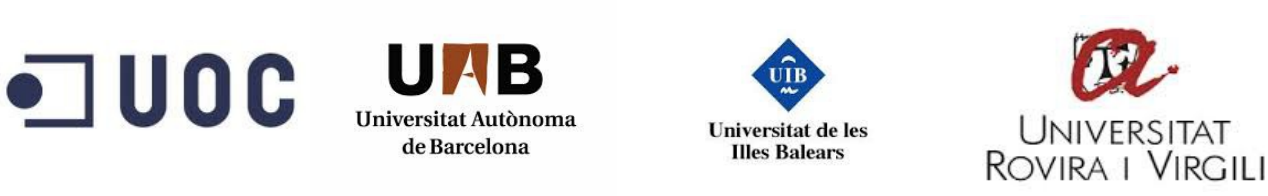

Máster interuniversitario de Seguridad de las tecnologías de la información y las telecomunicaciones, MISTIC

Programas de vigilancia masiva y contramedidas aplicables

Alfonso Sánchez Cañestro

Directora: Dña. Cristina Pérez Solà

Universitat Oberta de Catalunya
12 de junio de 2015

Resumen

Las revelaciones de Snowden han arrojado luz sobre un conjunto de programas de vigilancia masiva que recogen grandes cantidades de datos personales, consistentes en información de metadatos, así como contenido de comunicaciones de personas de todo el mundo.

Este informe pretende revisar los programas de la NSA más renombrados y las contramedidas asociadas. Previamente, se describirá el contexto legal e histórico que llevó a esta situación.

Abstract

Snowden's revelations have shed light on a large set of secret mass surveillance programs that were and are collecting huge amounts of personal data, consisting of metadata information and communications contents from people around the world.

This report aims to review the most renowned NSA programs and the associated countermeasures. Previously, the legal and historical context that led to this situation will be described.

"La telepantalla recibía y transmitía simultáneamente. Cualquier sonido que hiciera Winston superior a un susurro, era captado por el aparato. Además, mientras permaneciera dentro del radio de visión de la placa de metal, podía ser visto a la vez que oído. Por supuesto, no había manera de saber si le contemplaban a uno en un momento dado". 1984, George Orwell

Contenido

i. Lista de abreviaturas

11S: 11 de septiembre, en referencia a los atentados de Nueva York y el Pentágono en 2001
AES: Advanced Encryption Standard, estándar de cifrado
AISE: Agenzia Informazioni e Sicurezza Esterna, Servicio de Inteligencia de Italia
AIVD: Algemene Inlichtingen- en Veiligheidsdienst, Servicio de Inteligencia de Holanda
ASD: Australian Signals Directorate, Servicio de Inteligencia de Australia
AT&T: American Telephone and Telegraph, multinacional de telecomunicaciones
BND: Bundesnachrichtendienst, Servicio de Inteligencia de Alemania
BRUSA: Acuerdo precursor de UKUSA
CALEA: Communications Assistance for Law Enforcement Act
CIA: Central Intelligence Agency
CNI: Centro Nacional de Inteligencia, Servicio de Inteligencia de España
CSE/CSEC: Communications Security Establishment Canada, Servicio de Inteligencia de Canadá
DES: Data Encryption Standard, algoritmo de cifrado
DGSE: Direction générale de la sécurité extérieure, Servicio de Inteligencia de Francia
DIME: Dark Internet Mail Environment, proyecto FOSS
DMTP: Dark Mail Transfer Protocol, protocolo de Dark Mail
DMAP: Dark Mail Access Protocol, protocolo de Dark Mail
DNI: Digital Network Intelligence, datos vinculados a tráfico de internet
DNR: Dial Number Recognition, datos vinculados a llamadas telefónicas
DSA: Digital Signal Algorithm, algoritmo para firma digital
DSS: Digital Signature Standard, estándar para firma digital
E2EE: End to End Encryption, cifrado extremo a extremo
EFF: Electronic Frontier Foundation
ETSI: European Telecommunications Standards Institute
FAA: Foreign Intelligence Surveillance Amendment Act de 2008
FBI: Federal Bureau of Investigations
FISA: Foreign Intelligence Surveillance Act
FISC: Foreign Intelligence Surveillance Court, Tribunal de Vigilancia de Inteligencia Extranjera
FOSS: Free Open Source Software
FVEY: Five Eyes; asociación de las Agencias NSA, GCHQ, ASD, CSEC y GCSB
GCHQ: Government Communications Headquarters, Servicio de Inteligencia de Reino Unido
GCSB: Government Communications Security Bureau, Servicio de Inteligencia de Nueva Zelanda
GNU: GNU's not Linux
GPL: General Public License
GPRS: General Packet Radio Service
GSM: Global System for Mobile Communications
IoT: Internet of Things, Internet de las cosas
ISNU: Israel SIGINT National Unit, Servicio de Inteligencia de Israel
ITU: International Telecommunications Union
LOPD: Ley Orgánica de Protección de Datos de carácter personal
LORTAD: Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal
NAACP: National Association for the Advancement of Colored People
NDB: Nachrichtendienst des Bundes, Servicio de Inteligencia de Suiza
NIS: Norwegian Intelligence Service, Servicio de Inteligencia de Noruega
NIST: National Institute of Standards and Tecnology
NSA: National Security Agency
PET: Politiets Efterretningstjeneste, Servicio de Inteligencia de Dinamarca
PGP: Pretty Good Privacy, programa de cifrado/descifrado
RSA: Rivest, Shamir y Adleman, sistema criptográfico
SHA: Secure Hash Algorithm, funciones hash de cifrado
SIGINT: Signal Intelligence
STOA: Science and Technology Options Assessment, tipo de estudio realizado para el Parlamento de la UE
TACS: Total Access Communication System
TELECOM: Proveedor de Telecomunicaciones
TIA: Total Information Awareness, programa de vigilancia de la NSA
TOR: The Onion Routing, proyecto TOR
TTIP: Transatlantic Trade and Investment Partnership, Asociación Transatlántica para el Comercio y la Inversión
UKUSA: Asociación EEUU-Reino Unido para proyectos de vigilancia
UMTS: Universal Mobile Telecommunications System
USA PATRIOT Act: The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
VoIP: Voice over IP

ii. Lista de tablas

iii. Lista de figuras

1. Introducción

"El Gran Hermano te vigila"
1984, George Orwell

Ya no vivimos en un mundo meramente analógico; hoy en día, nuestra vida se ha "digitalizado" y transcurre por "hilos" físicos de cobre y fibra óptica o por el éter... Se ha instalado en territorio *online*. Lejos están los años en que nos enviábamos telegramas cuando había que notificar algo urgente, cartas cuando queríamos mantener el contacto con amigos y familiares que vivían lejos; los teléfonos fijos y los faxes, aunque siguen usándose, están cada vez más relegados a un segundo plano y ya no perdemos tiempo haciendo cola en los bancos o en agencias de viaje.

Inicialmente apareció la telefonía móvil TACS, todavía analógica, seguida de su implementación digital, GSM. Y, aunque las pruebas de concepto datan de principios de los 70, simultáneamente empezaron a aparecer una serie de funcionalidades, al principio solo para *geeks*, como Gopher, Veronica, Archie o Telnet, que eran las primeras manifestaciones de eso que conocemos como Internet y que es ahora una herramienta de uso masivo, "un mecanismo para diseminar información y un medio para la colaboración y la interacción entre personas y sus ordenadores, sin tener en cuenta su ubicación geográfica" [1].

Al principio, el acceso a internet estaba limitado a los ordenadores desde un emplazamiento fijo (ligado a una conexión telefónica fija o a una red local), pero el desarrollo de las tecnologías inalámbricas permitió la conexión sin hilos, WiFi, y las telecomunicaciones evolucionaron desde el GSM – pasando por el UMTS, el GPRS – hasta el 3G y 4G, permitiendo el acceso ubicuo a la Red, mientras nos desplazamos, desde la calle o en un tren.

Ahora "lo digital" está cada vez más presente en nuestras vidas; las barreras de entrada son muy accesibles y lo hemos incorporado a nuestro día a día; consumimos funcionalidades básicas, como el correo electrónico, los *chats* y la mensajería instantánea, las reservas electrónicas de viajes o la banca *online* (y otros sistemas de pago, como las tarjetas de crédito o servicios tipo *paypal*) y estamos protegidos y vigilados por videocámaras en las calles; asumimos las tecnologías más sofisticadas muy fácilmente, como el *Internet of Things*, IoT, que permite que la nevera haga la compra por nosotros o que la lavadora solicite al servicio técnico una visita, los dispositivos *wearables* que nos permiten hacer un seguimiento de nuestro rendimiento deportivo, como las pulseras monitorizadoras Fitbit o Fuelband, o dispositivos médicos de diagnóstico remoto... Los servicios de salud optimizan su rendimiento con la Historia Clínica Electrónica, irrumpen los servicios en la "nube", el *big data* y, por supuesto, nuestra conexión 24x7 con nuestro entorno mediante nuevas tecnologías de telefonía (VoIP, servicios de voz tipo *hangout o skype*), y con nuevos gadgets como *tablets*, *smartphones* y *smart tvs*, haciendo uso de herramientas de mensajería instantánea, redes sociales, de todo tipo, para comunicarnos y con las que nos expresamos y reflejamos nuestra personalidad.

Para todos, y especialmente para los llamados nativos digitales, internet ya "no es un ámbito separado, autónomo, donde se llevan a cabo unas cuantas funciones vitales.[...] Es el epicentro del mundo, el lugar en el que ocurre prácticamente todo. Donde se hacen amigos, donde se escogen libros y películas, donde se organiza el activismo político, donde se crean y almacenan los datos más privados. Es donde se desarrolla y expresa nuestra verdadera personalidad y la identidad de la persona." [2]

El acceso, y eventual acopio, a toda esta información supone una invasión radical de nuestra privacidad. Y es que ahora existen medios que permiten explotar esa ingente cantidad de información. Para que una sociedad pueda seguir llamándose democrática es imprescindible la tutela efectiva de la privacidad de manera que el comportamiento de los individuos no se vea condicionado.

A raíz de las revelaciones del analista y antiguo empleado de la CIA y NSA, Edward Snowden, a partir del mes de junio de 2013, se hicieron evidentes y vieron la luz pública los programas de vigilancia de la NSA, *National Surveillance Agency* o Agencia de Seguridad Nacional, que iban mucho más allá de los objetivos, *a priori* legítimos, de la *Patriot Act*, normativa estadounidense para enfrentar los desafíos de defensa resultantes de los fatídicos sucesos del 11-S.

Se puso de manifiesto que programas como PRISM o XKeyscore y las agencias de los "Cinco Ojos" (NSA y GCHQ entre ellas) sobrepasaron de manera sistemática los más elementales límites a la

vigilancia y tenían acceso a prácticamente cualquier comunicación electrónica al alcance de los operadores, independientemente de la nacionalidad de los comunicantes, de la existencia de una causa probable para monitorizar las comunicaciones, etc. Asimismo, se hizo pública la colaboración ilimitada de los grandes operadores de telecomunicaciones e internet con las citadas agencias – voluntaria o involuntariamente.

En paralelo, se ha conocido la consecución de un faraónico centro de datos en Utah [3] que pretendería albergar todas las comunicaciones bajo vigilancia de la NSA para eventuales accesos *a posteriori*. La facilidad y la falta de rendición de cuentas con la que cualquier operador de las citadas agencias de un rango medio podría acceder a esta información agravaría aún más la situación.

Así pues, el mundo ha conocido que sus comunicaciones electrónicas, sus relaciones personales, su actividad diaria, sus transacciones económicas son transparentes ante la omnipresente vigilancia electrónica de sus *emails*, sus llamadas telefónicas, sus geoposicionamientos mediante el teléfono móvil, etc. Y no solo los ciudadanos particulares deben estar preocupados; los altos cargos de conglomerados económicos, industriales y financieros, así como los mandatarios de las naciones que pensaban haber quedado al margen de este monumental espionaje han conocido que también han podido ser vigilados en sus conversaciones.

1.1. Objetivos

El **objetivo principal** de este trabajo es reflejar el contexto legal e histórico en el que se ha desarrollado este nuevo escenario, describir algunos de esos programas de vigilancia y ofrecer las alternativas y herramientas a disposición de los ciudadanos, empresas y gobiernos para contrarrestar ese ambiente “hostil” a la privacidad de la ciudadanía.

Este trabajo tendrá las limitaciones propias de tratar una temática que, en condiciones normales, es secreta y difícilmente contrastable; solo mediante la revelación voluntaria de los gobiernos (algo de por sí inédito, ya que la revelación invalidaría la vigilancia) o intrusiva de *whistleblowers,* como Snowden, y ciberactivistas de todo tipo, será posible conocer los programas de vigilancia.

Las alternativas para contrarrestar la intromisión de gobiernos hostiles, competidores corporativos y *hackers* a sueldo malintencionados deben cubrir amplios rangos de tipos de comunicación electrónica, por lo que las herramientas deberán ser variadas y adaptadas a cada uno de los escenarios a bastionar.

1.2. Metodología

El enfoque de este trabajo ha sido fundamentalmente de documentación; identificación de documentación fiable seguida de un análisis crítico y un esfuerzo de síntesis para plasmarlo en un documento de extensión limitada.

La metodología para llevar a cabo todo este trabajo ha sido la identificación de las fuentes bibliográficas, periodísticas, de video y audio necesarias, el análisis de la información hallada para sintetizarla de manera comprensible.

El resultado es un repaso de los diferentes programas de vigilancia y de los medios y recursos que se están poniendo en marcha de cara a hacer frente a esa vigilancia omnipresente. Estas iniciativas tienen que tener, a la fuerza, una génesis descentralizada que permita evitar su control por los grandes poderes. Así, casi la totalidad de las respuestas viene del mundo o*pen source*. Se hace un repaso de algunas de las herramientas que han ido apareciendo y también de algunas que, por diversas causas, han visto interrumpido o aplazado su desarrollo.

1.3. Planificación inicial

El listado de las tareas realizadas para alcanzar los objetivos descritos puede desglosarse como sigue:

- Tarea 1: Búsqueda e identificación de la documentación relevante
- Tarea 2: Lectura de los contenidos
- Tarea 3: Análisis y síntesis

- Tarea 4: Elaboración del índice del informe-memoria
- Tarea 5: Redacción del informe-memoria
- Tarea 6: Elaboración de la videopresentación

La planificación temporal detallada de estas tareas fue la siguiente:

				PAC1					PAC2					PAC3		PAC4			
Semana	23/02	02/03	09/03	16/03	23/03	30/03	06/04	13/04	20/04	27/04	04/05	11/05	18/05	25/05	01/06	08/06	15/06	22/06	29/06
Tarea 1																			
Tarea 2																			
Tarea 3																			
Tarea 4																			
Tarea 5																			
Tarea 6																			
Entrega PAC				**16/03**					**20/04**					**29/05**		**12/06**	**19/06**		

Fig. 1 – Planificación de las tareas del proyecto

Una vez leídos los contenidos de la descripción del proyecto, tal y como lo planteaba la Dirección del Proyecto, se comenzó a trabajar en el Plan de Trabajo, para delimitar, básicamente, los objetivos del mismo, la metodología que se iba a seguir y las tareas que se iban a afrontar, dentro de un marco temporal. Este Plan de Trabajo constituía la primera PAC. Las tareas descritas en el mismo se habían hecho coincidir con los hitos de entrega de cada PAC, cuyo punto final era la entrega del 12 de junio. El Plan de Trabajo no ha sufrido grandes cambios, con excepción de la tarea 1, de búsqueda de información relevante, que estuvo programada inicialmente para finalizar mucho antes (20 de abril); sin embargo, a medida que se iban priorizando los posibles contenidos del trabajo, estos iban aumentando, lo que tenía como consecuencia que era necesario identificar más documentación. Así, fue necesario prolongar esta tarea hasta la fecha de entrega de la PAC3. Si bien este cambio ha sido beneficioso, pues ha permitido documentar mejor el contenido más relevante, también es cierto que la configuración final del trabajo no se ha podido fijar completamente hasta fechas muy avanzadas.

1.4. Estructura del documento

La memoria comienza con un apartado dedicado a describir el contexto histórico y legal que ha derivado en el escenario que ahora conocemos. Será interesante ver el enfoque diferente de la protección de la intimidad que se da en la Unión Europea y Estados Unidos. También se hará un repaso de la normativa relevante de España en este contexto. Más allá del desarrollo normativo, también se repasarán los hitos de la vigilancia en Estados Unidos, país que ha determinado con sus prácticas, la situación de vigilancia global. Se comienza en la Segunda Guerra Mundial hasta llegar a la situación posterior a los atentados del 11S, pasando por los acontecimientos intermedios, como las revelaciones a raíz del caso Watergate o el programa ECHELON.

Posteriormente se hará un breve repaso de las revelaciones de Edward Snowden para, a continuación, detallar y clasificar, en la medida de lo posible y con las limitaciones que tiene una información filtrada, los programas de vigilancia desvelados por el exagente de la CIA.

El capítulo siguiente detalla algunas de las herramientas que se están utilizando para contrarrestar los abusos de las Agencias de Inteligencia; hablamos de programas de cifrado, programas de ocultación de la navegación, etc.

Posteriormente, se dedica un breve capítulo a intentar desgranar qué depara el futuro próximo, qué oportunidades, pero sobre todo, qué riesgos; las previsibles iniciativas de la NSA para tumbar las contramedidas que pone el ciudadano para que no se le espíe (intentos conocidos de las Agencias de quebrar los sistemas de cifrado existentes, los programas impulsados por estas Agencias para infectar aplicaciones y obtener puertas traseras a nuestros dispositivos, etc), la irrupción de empresas en este tablero de juego con evidente ánimo de lucro, las previsibles iniciativas legislativas de la Unión

Europea o los avances tecnológicos y cómo pueden influir en el nuevo escenario.
Por último, se dedica un capítulo para cerrar el trabajo y recoger conclusiones.

2. Contexto histórico y contexto legal

Para ser capaces de valorar los programas de vigilancia masiva de los que se ha tenido conocimiento desde 2013 es preciso establecer el contexto legal e histórico que ha hecho posible llegar a donde estamos y cómo y cuándo tuvo lugar este salto cualitativo y cuantitativo.

2.1. Contexto legal

Los hechos descubiertos por Snowden tienen una significación distinta según se miren desde una óptica americana o europea; en parte, por la normativa europea de carácter más garantista frente al cuerpo jurídico estadounidense más sectorial y autorregulado, pero también por la diferenciación establecida desde EEUU entre ciudadanos americanos y personas del resto del mundo como objetos de vigilancia. El contexto legal puede aclarar cómo los mismos hechos pueden ser observados como legítimos o ilegítimos según la perspectiva legal.

2.1.1. La protección de la intimidad como derecho fundamental

El derecho a la intimidad [4], a la protección de datos y al secreto de las comunicaciones están reconocidos en la **Declaración Universal de Derechos Humanos** [5], proclamada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948, y el **Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales** de 1950. Este último señala en su artículo 8 que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia" y, explícitamente, advierte que "no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás" [6].

Este derecho es protegido de manera desigual a ambos lados del Atlántico, en Estados Unidos de América y en la Unión Europea, como veremos a continuación.

2.1.2. Unión Europea

A nivel europeo, la primera referencia a la protección de los datos de carácter personal se incluye en el **Convenio número 108 del Consejo de Europa** [7]**, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal**, que viene a establecer como requisito para la existencia de una adecuada regulación del derecho fundamental a la protección de datos, la existencia de una o varias autoridades en cada Estado, encargadas de velar por el cumplimiento de los principios establecidos en el Convenio. Actualmente, toda la materia relativa a la protección de datos personales emana de la **Directiva 95/46/CE** [8], del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta norma fue la primera disposición con rango de Directiva promulgada en el ámbito europeo en materia de protección de datos de los ciudadanos. Sin embargo, no contaba con medidas especificas para regular y controlar los riesgos y peligros que iban a ir apareciendo paulatinamente con las nuevas tecnologías y los nuevos usos y costumbres que estos llevan aparejados.

Es por ello que se elaboró, también para el ámbito europeo, una primera norma que aportara las medidas adecuadas a este nuevo mundo que estaba emergiendo. Para proteger los datos y la intimidad de los ciudadanos en el sector de las telecomunicaciones, se elaboró la **Directiva 97/66/CE** [9], del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, complementando así a la Directiva 95/46/CE [8] en las disposiciones jurídico-técnicas para el ámbito de las telecomunicaciones.

Unos pocos años después, se promulgó la **Directiva 2002/58/CE** [10], del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, y conocida como “Directiva sobre la privacidad y las comunicaciones electrónicas” para garantizar un nivel equivalente de protección de las

libertades y los derechos fundamentales en los estados miembros. Se trataba de fijar el derecho a la intimidad en lo tocante a las telecomunicaciones, concretar la protección de datos personales en el sector de las telecomunicaciones y facilitar la libre circulación de los datos personales en la Unión Europea.

Por último, está la **Directiva 2006/24/CE** [11] del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre conservación de datos de tráfico en las comunicaciones electrónicas. Esta norma nace al amparo de la nueva situación creada con los atentados terroristas del 11 de septiembre de 2001 en Nueva York y el Pentágono y del 11 de marzo de 2004 en Madrid; se pretendía poner a disposición de los estados miembros de la Unión una herramienta eficaz de lucha contra el terrorismo y el crimen organizado. La idea central de la Directiva es demandar a los operadores de telecomunicaciones la conservación de los datos del tráfico de las comunicaciones que gestionaban por un mínimo de seis meses y un máximo de dos años. La información del tráfico de las comunicaciones podía resultar muy importante en investigaciones de prevención de terrorismo, intentando hacer compatible esta "especial" vigilancia con las libertades y los derechos fundamentales de los ciudadanos. Sin embargo, cabe indicar que, años después, el 8 de abril de 2014, el Tribunal de Justicia de la Unión Europea [12] declaró inválida esta Directiva, al dictaminar que se estaban reteniendo datos de personas de las que no se podía siquiera sugerir que pudiesen estar involucradas en delitos graves; esto tuvo como consecuencia una marcha atrás y la necesaria modificación de todas las transposiciones nacionales de los Estados miembros de la norma.

También deben reseñarse los esfuerzos que se están haciendo para promulgar una nueva Directiva [13] de protección de datos de carácter personal más adaptada a la realidad sociológica y tecnológica de nuestros días, esfuerzo que ya lleva "encallado" algunos meses.

2.1.3. El caso de España

A nivel nacional, el derecho a la intimidad y al secreto de las comunicaciones está protegido expresamente por la **Constitución Española** [14] de 1978, que recoge la relación entre la protección de datos de carácter personal de los ciudadanos, el derecho al secreto de las telecomunicaciones y a la intimidad dispuesto en el artículo 18.3 de la Carta Magna ("Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial"). Asimismo, el artículo 18.1 defiende el principio de la intimidad al disponer que "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen", pero el artículo 18.4 va más allá de la mera protección de la intimidad y **consagra un auténtico derecho fundamental a la protección de datos** diferenciado, al afirmar que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Cabe destacar la **sentencia del Tribunal Constitucional STC292/2000** [15] de 30 de noviembre que ha defendido la existencia de un auténtico derecho a la protección de datos de carácter personal, que no solo afecta a los datos de carácter íntimo de los individuos, sino a cualquiera "cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no, fundamentales".

Se promulgó, en la línea de lo recogido en la Constitución, la **Ley Orgánica 5/1992** [16] de Regulación del Tratamiento Automatizado de Datos, LORTAD, que se derogó para ser sustituida por la actual **Ley Orgánica 15/1999** [17], de 13 de diciembre, de Protección de Datos de carácter personal, **LOPD**, que resultaba de transponer la **Directiva 95/46/CE** [8]**,** antes mencionada. Estas normas se promulgaron como Leyes Orgánicas para amplificar la trascendencia del bien protegido como derecho fundamental. Posteriormente, se ha promulgado el desarrollo reglamentario mediante el **Real Decreto 1720/2007** [18]. Se trata de una Ley Orgánica y un Real Decreto muy protectores de los derechos de los ciudadanos que, seguramente, han podido quedar obsoletos ante las nuevas realidades tecnológicas y las modificaciones que internet ha supuesto en nuestras costumbres y en los tratamientos que no se limitan ya a territorio nacional. El uso de programas de correo electrónico, como *gmail* o *yahoo*, o servidores de información en "la nube", como *dropbox* o *drive*, supone, en algunos casos, el almacenamiento de nuestros datos fuera del ámbito de la UE; la posible obsolescencia queda patente en el hecho de que la Agencia Española de Protección de Datos, AGPD, debe autorizar las transferencias internacionales de datos de carácter personal con destino a países fuera del ámbito de la Unión Europea que no puedan garantizar los niveles de protección similares a los europeos [19] (o calificados tras una cuidadosa inspección de sus procedimientos como "*Safe Harbour*").

Debe reseñarse, asimismo, que las posibles responsabilidades derivadas de la vulneración de la intimidad de los ciudadanos, pueden llegar a ser castigadas por vía penal, conforme a la **Ley Orgánica 10/1995** [20] del Código Penal (artículo 197, por ejemplo).

Otra legislación relevante, en relación con el derecho a la intimidad es la **Ley Orgánica 1/1982** [21], de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Igualmente, hay que tener en cuenta lo dispuesto en la **Ley 34/2002** [22] de Servicios de la Sociedad de la Información y del Comercio Electrónico y lo referido en la **Ley 9/2014 General de Telecomunicaciones** [23], que establecen el régimen aplicable a las comunicaciones electrónicas, identificando los derechos de los usuarios de telecomunicaciones relacionados con la protección de datos de carácter personal y la privacidad de las personas.

Como vimos más arriba, los atentados de 2001 y 2004 han propiciado un aumento en las medidas de control sobre los medios de telecomunicación, que han podido suponer interferencias en la intimidad y en la vida privada de los ciudadanos, materializadas en la retención de datos por parte los prestadores de estos servicios (cómo y cuándo se han producido las comunicaciones). Este aumento de medidas de control se hizo conforme a la **Directiva 2006/24/CE** [11], tratada antes, y cuya transposición a la normativa española fue la **Ley 25/2007** [24]**, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones**. Esta Ley regulaba los datos que deben retenerse, el periodo de su conservación y las garantías previstas en su cesión, siempre previa autorización judicial, pero fue modificada mediante la **Ley 9/2014** [23], antes mencionada, en respuesta a la sentencia del Tribunal de Justicia de la Unión Europea que declaraba inválida la Directiva 2006/24/CE [11].

2.1.4. Estados Unidos de América

El caso americano sorprende por sus remotos orígenes. La preocupación por el derecho a la intimidad data de la época de la propia creación de los EEUU y jugó un papel reseñable en su proceso de independencia, pues los colonos protestaban contra las leyes que permitían a los funcionarios británicos registrar a voluntad cualquier domicilio; estos admitían que el Estado obtuviese órdenes judiciales específicas para registrar y detener a individuos cuando hubiera indicios de causas probables de actos delictivos, pero no órdenes judiciales de carácter general o registros domiciliarios indiscriminados [25]. La **Cuarta Enmienda a la Constitución** [26] de los EEUU, que consagró estos actos indiscriminados como ilegítimos, pretendía suprimir el poder del gobierno para someter a los ciudadanos a vigilancia generalizada sin una sospecha razonable de por medio.

En EEUU no existe una normativa de protección de datos similar a la Directiva Europea, la **Constitución Federal** [27] no recoge propiamente un derecho fundamental a la protección de datos y la cuestión se rige por un sistema sectorial (registros de crédito o bancarios, registros de alquiler de vídeos, ficheros de salud, etc.) y de autorregulación. Las leyes sectoriales, a menudo se utilizan como complemento de normativas más generales, con la finalidad de otorgar una protección específica a un determinado tipo de datos.

En el sector público existen normas que afectan al tratamiento de los datos, por ejemplo, **The Privacy Act** [28] del 1974 que establece una serie de requerimientos y garantías en el tratamiento y recogida de datos por parte de las agencias federales o gubernamentales o **The Freedom of Information Act** [29] que garantiza, con una serie de excepciones, el derecho de acceso de los ciudadanos a ciertos registros custodiados por las agencias federales.

Por otro lado, también existe otro grupo de normativas que, con la finalidad de cumplir objetivos de vigilancia, establecen la obligación de facilitar información personal en determinados casos; existen cuatro leyes básicas en EEUU [30]: la **Communications Assistance for Law Enforcement Act (CALEA)** [31], el título II de la **USA Patriot Act** [32] de 2001, el **Foreign Intelligence Surveillance Act (FISA)** [33] de 1978 y el título III de la **Omnibus Crime Control and Safe Streets Act** [34] de 1968. Esta última se refiere a la interceptación con fines internos; por contra, la FISA [33] regula interceptaciones con fines de inteligencia a ciudadanos no estadounidenses. La CALEA [31] clarificó los criterios según los cuales deben regirse los operadores de telecomunicaciones para facilitar a los cuerpos de seguridad del Estado la vigilancia electrónica. Por último y al igual que en el caso europeo, los sucesos del 11S motivaron la modificación de la normativa de vigilancia, aumentando los supuestos

legítimos de la FISA [33], mediante la USA PATRIOT Act [32] que añadió a la lista de actividades susceptibles de vigilancia las relacionadas con terrorismo, fraude informático y delitos financieros, se aumentaba la cooperación y el intercambio de información entre las entidades financieras y gubernamentales con el fin de detectar actividades relacionadas con actividades terroristas o de blanqueo de capitales y, por último, facilitaba el seguimiento de ciudadanos no americanos.

La recolección de datos conforme a la FISA [33], que regulaba la interceptación de información de "inteligencia" extranjera, tanto fuera como dentro de EEUU, estaba supervisada por el **FISC** [35], Foreign Intelligence Surveillance Court (Tribunal de Vigilancia de Inteligencia Extranjera) que dictaminaba si la vigilancia estaba justificada. Tras los atentados del 11S, se enmendó la FISA (**FAA, Foreign Intelligence Surveillance Amendment Act** [36] de 2008) para posibilitar la vigilancia en masa a ciudadanos no estadounidenses.

Casualmente, en la fecha en la que se está finalizando este informe, la sección 215 de la USA Patriot Act [32], que habilitaba la recolección de información relevante para investigaciones terroristas (y por la que se justificaba la recolección masiva de datos), expiró el 31 de mayo [37], por lo que desde el 1 de junio las autoridades carecían, temporalmente, de amparo legal para almacenar datos y usar otras herramientas para espiar a sospechosos. Ocurrió en el Senado estadounidense, en el marco de la reforma del espionaje electrónico, por la que se pretendía aprobar la USA Freedom Act [38], una ley que, sin cuestionar la autoridad de los espías para vigilar las comunicaciones privadas, supone el primer intento serio, desde 1978, de limitar los poderes de la NSA [39]. Inicialmente no hubo acuerdo para prorrogar la legislación actual, por lo que la recolección de datos quedó en suspenso durante dos días, hasta que el Senado votó positivamente el martes día 2 de junio.

La USA Freedom Act [38], o Ley de la Libertad de EEUU, busca un término medio entre los defensores de un espionaje opaco y con muy pocos límites y los detractores absolutos del espionaje electrónico. Un elemento central de la ley es que retira a la NSA la capacidad de almacenar los datos sobre las llamadas telefónicas de millones de estadounidenses y coloca estos datos en manos de las compañías telefónicas. Los espías podrán acceder a estos datos caso a caso y previa autorización judicial [40].

2.1.5. Últimas consideraciones

Por último, es preciso dejar bien clara la diferencia entre las interceptaciones "legales" y la vigilancia masiva. La primera sería, de acuerdo a lo establecido por la ITU [41], totalmente legítima, ya que sigue un protocolo bien definido (solicitud de las Fuerzas de Seguridad, evaluación de dicha solicitud por un tribunal competente que, si da el visto bueno, traslada la petición al operador de telecomunicaciones que, a su vez, facilita el acceso a los datos a las Fuerzas de Seguridad) que garantizaría su procedencia. En clara contraposición a este escenario de evaluación "caso por caso" estaría la vigilancia en masa sin diferenciar quiénes son investigados, sin disponer de una causa probable, etc.

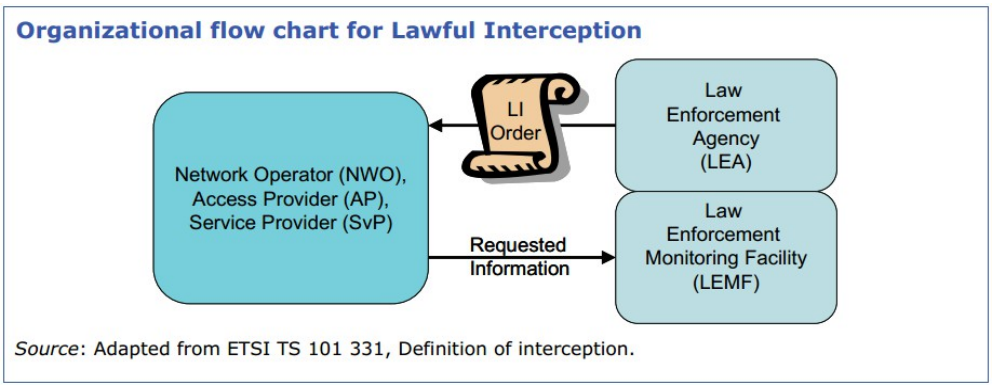

Fig. 2 – Esquema del proceso de interceptación legal de las comunicaciones, Lawful Interception, ETSI

Más adelante veremos que, en el caso de EEUU, el FISC [35], en virtud de la enmienda FAA [36] a la FISA [33], no actuó como ese filtro regulador necesario para un funcionamiento legítimo del sistema y se convirtió en una mera correa de transmisión de las solicitudes, independientemente de que fueran procedentes o no.

Otra aclaración que cabe realizar en este punto es el objeto de la vigilancia. La captación de datos

durante la vigilancia puede referirse a los **contenidos** de la comunicación, pero también a los datos de la propia comunicación, es decir, cuándo se inicia la comunicación, desde dónde, con qué destino, con qué frecuencia, etc.; son los llamados **metadatos**. A las Agencias y a los Estados "vigilantes" les ha interesado devaluar esta segunda opción de datos ante la opinión pública, describiéndolos como de poca importancia y sin un verdadero valor de intromisión. Sin embargo, la experiencia demuestra lo contrario, ya que es posible que el contenido de una comunicación no aporte nada si se utiliza un lenguaje en clave, por ejemplo, pero el análisis automatizado de los metadatos (algo, por otra parte, muy difícil de hacer con los contenidos) puede aportar información de mucho más interés y, probablemente, mucho más veraz.

2.2. Contexto histórico

Así como el contexto legal puede permitirnos entender la legitimidad o ilegitimidad que se otorga al tipo de vigilancia objeto de este estudio, el contexto histórico permite entender, que no justificar, el salto cualitativo que supusieron los atentados al Pentágono y las torres gemelas de Nueva York en la actividad de las Agencias de Inteligencia. Como veremos a continuación, se utilizaron estos actos terroristas como elemento justificativo de unas prácticas de vigilancia masiva que, en realidad, venían realizándose con anterioridad.

2.2.1. El acuerdo UKUSA

La Segunda Guerra Mundial propició un programa de criptoanálisis (cifrado/descifrado) entre EEUU y el Reino Unido para desentrañar las comunicaciones del enemigo (la famosa máquina "Enigma") y proteger las propias en la guerra del Atlántico. Esta colaboración se selló con el acuerdo denominado BRUSA, extendiéndose en los años siguientes, como UKUSA [42], a Canadá, Australia y Nueva Zelanda, que constituyeron el grupo de cinco países, y sus cinco agencias de inteligencia, que se conocería más adelante como Five Eyes, FVEY. Este acuerdo se hizo público recientemente, al desclasificarse sus contenidos. Básicamente, se trataba de intercambiar los resultados obtenidos de actividades de recolección y análisis de tráfico de las telecomunicaciones, así como poner en común los progresos en criptoanálisis. Se utilizaba para ello una red ultrasecreta, denominada STONEGHOST. Más adelante se unieron otros países, que asumían la categoría de "*third parties*", como la antigua República Federal de Alemania, los países nórdicos, Filipinas, etc.

Buena parte de la actividad vinculada a este acuerdo se dirigía, en el marco de la Guerra Fría, a la vigilancia de los países del bloque soviético (Unión Soviética y países de Europa del Este) y la República Popular China.

2.2.2. El programa ECHELON

La colaboración entre Reino Unido y los EEUU fue aumentando y la recolección de SIGINT (SIGnal INTelligence) fue expandiéndose a cables submarinos, enlaces microondas, comunicaciones vía satélite, etc. Aunque ECHELON es un programa específico que data de principios de los 60 y que se estableció formalmente en 1971, se ha convertido en el identificador de la actividad de vigilancia que llevaban a cabo estos dos países conjuntamente. Su objetivo inicial eran las comunicaciones de los países del bloque soviético y China. Posteriormente, se sumaron el resto de Agencias del grupo FVEY. Durante la década de los 90, sus capacidades habían mejorado considerablemente y se había expandido hacia un sistema de interceptación global que también monitorizaba comunicaciones privadas y comerciales. Bajo el nombre de ECHELON se inspeccionaban los contenidos de llamadas telefónicas, faxes, correo electrónico, etc. La actividad de ECHELON suscitó la preocupación de los países europeos y propició la elaboración de dos informes [43]: en 1998 y 1999 el Parlamento Europeo publicó sendos informes de Steve Wright ("An appraisal of technologies of political control" [44]) y el propio Duncan Campbell ("Interception capabilities 2000 – Development of surveillance technology and risk of abuse of economic information" [45]), respectivamente. A la vista de los contenidos de estos informes, el Comité que trató este tema recomendó en su última reunión el uso de criptografía en las comunicaciones para proteger la privacidad de las mismas.

2.2.3. El Comité Church y el programa COINTELPRO

El escándalo Watergate, por el que el presidente Nixon debió dimitir, sacó a la luz una serie de malas prácticas que las agencias de inteligencia y los cuerpos policiales venían desarrollando. Se constituyó

el Comité Church [46] para investigar estos hechos y otros que iban conociéndose y se destaparon una serie de abusos de poder consistentes en el “pinchazo” indiscriminado de teléfonos, la colocación sin orden judicial de micrófonos ocultos, etc., por parte del FBI, en los domicilios y oficinas de líderes de la oposición, de líderes de movimientos civiles, etc. Bajo el programa COINTELPRO [47], figuras destacadas como Martin Luther King Jr., Muhammad Ali o John Lennon y miembros de movimientos como los Panteras Negras, la NAACP o Movimiento Indio Americano fueron objeto de esta invasión de la privacidad, con el argumento de que “socavaban” el orden establecido.

En el marco de los trabajos de este Comité, también se descubrió un programa de vigilancia masiva, no autorizado, sobre telegramas internacionales que databa de los años 40, el proyecto Shamrock [48].

Todos estos descubrimientos suponían un incumplimiento de uno de los pilares de la democracia americana, la Cuarta Enmienda de la Constitución [26]. El Comité se interesó, en particular, por la interceptación “accidental” de información de ciudadanos americanos, cuando se estaban vigilando las comunicaciones de extranjeros y finalmente dictaminó que ésta era tolerable si se habían tomado medidas para minimizar esta captación “errónea”. Este fue el germen de la antes mencionada FISA [33], que pasaba a regular la interceptación de las comunicaciones de agencias de inteligencia extranjeras.

2.2.4. Proyecto Carnivore

Las capacidades de vigilancia iban mejorando y entre 1997 y 1998, el FBI puso en marcha el proyecto Carnivore [49], para monitorizar el correo electrónico y otras comunicaciones electrónicas en los proveedores de Internet. Se basaba en un inspeccionador de paquetes (*packet sniffer*) parametrizable y era necesario instalarlo en las propias instalaciones del proveedor.

El sistema era muy sencillo; su funcionamiento consistía en monitorizar los paquetes que gestionaba el proveedor de internet y se capturaban mediante filtros, aquellos que cumplían los criterios definidos.

Las organizaciones preocupadas por la privacidad, como la Electronic Frontier Foundation, EFF [50], denunciaron el riesgo de este sistema que, en función de los filtros aplicados, puede ser más o menos intrusivo. El FBI abandonó el proyecto en 2005 [51].

2.2.5. Intentos de vulnerar la criptografía

Este tipo de programas que se venían imponiendo en las diferentes Agencias de Inteligencia se encontraban con un rival inesperado; la criptografía [52]. Hasta los años 70, la capacidad de descifrado de la NSA era incuestionable, pero empezaron a aparecer proyectos de investigación públicos que ponían en riesgo este dominio. El primer intento de la Administración por no perder esa situación de preponderancia fue la imposición del chip Clipper, que debía instalarse en todos los sistemas criptográficos, habilitando así para la Administración el acceso a todas las comunicaciones cifradas. Las quejas del sector y de las organizaciones preocupadas por la privacidad hicieron desistir al Gobierno de este proyecto.

El siguiente intento fue imponer el uso de DES y DSS con claves de longitud máxima de 56 bits; el objetivo era que la NSA pudiera acceder a todos los contenidos cifrados cuando lo considerara necesario; nuevamente el intento fracasó. Empezaron a aparecer proyectos fuera del control de la Administración (RSA y PGP). La Administración intentó poner de acuerdo a sus aliados para prohibir la distribución de criptografía por internet [53].

La Administración cambió su estrategia y decidió no imponer una longitud máxima para las claves criptográficas, siempre que se almacenasen las claves en fideicomiso (*key escrow*) para cuando fuera necesario, dejando fuera de la ley a aquellas compañías que no funcionaran bajo este principio, pero finalmente también tuvo que abandonar este proyecto [54].

En paralelo, se llevaban a cabo iniciativas más “agresivas”. En 1997, la NSA llegó a un acuerdo con IBM para que usase en su producto Lotus Notes un algoritmo con una clave de cifrado generada por la propia NSA. De esta forma, "solo" la NSA podía descifrar los datos [55]. Posteriormente, en 1999, un experto en seguridad de Cryptonym encontró en Windows NT 4 Service Pack 5 una clave denominada _NSAKEY, lo que disparó las alarmas de una posible instalación de puertas traseras para la NSA en los productos de Microsoft [56].

2.2.6. Escenario tras los atentados del 11S

En el apartado dedicado a la legislación, se ha descrito brevemente lo que supusieron los atentados de septiembre de 2001 para la vigilancia y el espionaje electrónicos. Se enmendó la FISA [33] y se aprobó la USA Patriot Act [32], normativas que en la práctica abrían las puertas a la vigilancia masiva.

Unas semanas después de los atentados, en medio de un fervor patriótico que soslayaba las dudas éticas y, en parte, para contrarrestar supuestos problemas de descoordinación entre las agencias en vísperas de los atentados, la Administración puso en marcha numerosos programas de espionaje [57] y se empezaron a recopilar en secreto registros de llamadas telefónicas, como parte de las medidas antiterroristas que se estaban empezando a adoptar, sin cuestionarse la legalidad de las mismas.

En este contexto, algunos, como el analista William Binney, se atrevían a denunciar en 2002 programas [58], como el Trailblazer que costó “millones y millones de dólares” para analizar los datos que circulaban por redes de comunicación como Internet, cuando se había vetado uno mucho más barato, el ThinThread, poco tiempo antes de los atentados.

En 2008 se conoció de la existencia del programa "Quantico circuit", que databa de 2003 y que proporcionaba a la Administración una puerta trasera a la red del operador Verizon [59].

La proliferación de programas [57] de recopilación de las comunicaciones era imparable; programas como Stellarwind, que consistía en la colocación de *splitters* o derivadores de fibra óptica en centros de conmutación de Internet, filtrando y almacenando el tráfico que cumpliera ciertos criterios (palabras clave, origen, destino, etc.), o el famoso caso de la “habitación 641A”, historia que el New York Times conocía y ocultó durante un año [60] y que consistía en el “pinchazo” de la red troncal de AT&T, en las propias dependencias de esta empresa.

Fig. 3 – Habitación 641A, en una central de conmutación de AT&T de San Francisco (foto filtrada por Mark Klein)

En 2006 el periódico USA Today [61] desveló la existencia de una base de datos masiva de la NSA con registros de llamadas telefónicas de millones de americanos, suministrados por AT&T, Verizon y BellSouth.

Incluso se conoció una propuesta para trabajar en un proyecto denominado TIA (*Total Information Awareness*) que consistía en la recolección masiva de datos digitales que serían procesados con complejos algoritmos para identificar posibles planes terroristas; sin embargo, la opinión pública encajó mal este programa y, aparentemente, quedó fuera de los presupuestos. Sin embargo, quedaron dudas de que el programa estuviera siendo financiado secretamente [57].

En paralelo, sobre el año 2007, se dio a conocer WikiLeaks, la organización sin ánimo de lucro que comenzó a hacer públicas las filtraciones que les hacían llegar diversas fuentes anónimas y que provocó fuertes controversias.

Este era el contexto en el que se hicieron públicas las revelaciones de Snowden en el año 2013.

3. Revelaciones de Edward Snowden

Después de describir el contexto legal e histórico que estaba propiciando el nacimiento y proliferación del espionaje electrónico, se hará un breve repaso de las circunstancias bajo las que Edward Snowden se animó a filtrar los documentos que probaban el alcance de la feroz vigilancia a la que están sometidas las comunicaciones en internet, así como los aspectos más relevantes de dichos documentos.

Edward Snowden tenía 18 años el día en que se produjeron los atentados del 11S. En ese ambiente de patriotismo exacerbado también él sintió la llamada a la revancha y se alistó en el ejercito con el objetivo de ir a luchar a Irak; después de un accidente, en el que se partió las piernas, tuvo que abandonar el ejército y empezó a trabajar como vigilante en las instalaciones de la NSA. Mientras tanto, se estaba formando en Tecnologías de la Información y muy pronto empezó a trabajar para la CIA como técnico informático inicialmente (las Agencias de Inteligencia necesitaban urgentemente especialistas en todos los terrenos). Aprovechó la oportunidad y fue especializándose en seguridad informática y acabó trabajando para la NSA a través de contratistas (como Dell y Booz Allen Hamilton); tuvo varios destinos (Suiza, Japón...) en los que empezó a tener acceso a documentos cada vez más confidenciales y comenzó a ver cosas que no le gustaron. En un momento dado se plantea que el nivel de injerencia de la Administración es tan grande como escasa la necesaria rendición de cuentas para los accesos a esta información. Ve que hay muchos técnicos de alto nivel que tienen acceso a todo tipo de información muy invasiva para la privacidad de los ciudadanos, sin mayor justificación que la que da tener el perfil de acceso autorizado [62].

Cuando ve que la llegada de Obama a la Administración no solo no detiene estos programas, sino que los incrementa [62], es cuando decide dar un paso adelante para denunciar esta situación que, a su juicio, está poniendo en peligro la libertad, la democracia y la pervivencia de internet. Sabe que la decisión le costará, como mínimo, el modo de vida de que disfruta y, en el peor de los casos, que se le aplique la Ley de Espionaje de 1917, que puede acarrear la pena de muerte, pero eso no le detiene.

Empieza a recopilar información concienzudamente, escogiendo aquella que expresamente no pone en riesgo la vida de agentes de campo. También escoge documentos cuyo fin no es ser publicados, sino ofrecer un contexto para enterder mejor los que él consideraba que sí debían publicarse. En paralelo, se pone en contacto con los periodistas Laura Poitras y Glenn Greenwald, después de un intento fallido con el periodista del Washington Post, Barton Gellman, que retrasaba la publicación de la información que Snowden le había proporcionado.

Snowden queda con Greenwald y Poitras (a los que se une Ewen MacAskill) en un hotel de Hong Kong para una serie de encuentros, casi novelescos, en los que les va desgranando el contenido de los documentos que les ha entregado y las implicaciones que estos tienen.

Los primeros documentos se publican en junio de 2013 simultáneamente en el The Washington Post y The Guardian. Posteriormente, la cobertura fue global con otros medios como The New York Times, la Canadian Broadcasting Corporation, la Australian Broadcasting Corporation, Der Spiegel (de Alemania), O Globo (de Brasil), Le Monde (de Francia), NRC Handelsblad (de Holanda), L'espresso (de Italia), Dagbladet (de Noruega), la Sveriges Television (de Suecia) y, en España, el diario El País.

A pesar de no querer protagonismo, Snowden quiso que se conociera que los documentos los había filtrado él para evitar que otros agentes pudieran verse señalados como la fuente y para animar a otros, que estuviesen en su misma situación, a que dieran el paso de revelar aquello que consideraran un abuso.

El volumen de la información fue brutal y el impacto fue el que esperaba el propio Snowden; la vigilancia electrónica se había convertido en un tema de debate global (sus últimas consecuencias las hemos visto en este mismos mes de junio de 2015, en el que se ha aprobado la USA Freedom Act [40] que pone freno a la NSA, al menos, formal y públicamente).

Por último, comentar que Edward Snowden, después de un año como asilado, vive actualmente en Rusia con un permiso de residencia temporal por tres años.

A modo de resumen, se repasan algunos de los datos más relevantes e impactantes de las

revelaciones de Snowden:

- Después de haber publicado 26 documentos, The Guardian tuvo que destruir los discos donde almacenaba los documentos a instancias del Reino Unido. El editor de The Guardian, Alan Rusbridger, declaró haber visto unos 58,000 documentos [63]. Se calcula que Snowden pudo descargar más de 1.700.000 documentos [64].
- El caso Verizon desveló la inoperancia real del tribunal FISC; desde el año 1978 al 2002 aprobó todas la peticiones que se le hicieron sin rechazar ni una sola. En los diez años posteriores, solo denegó once solicitudes, cursando más de 20.000 [65].
- El caso PRISM desveló la colaboración de los grandes de internet, aunque cada compañía defendió de manera desigual su comportamiento; algunos que la información que entregaron no tenía verdadero valor, otros que se vieron obligados a entregarla o que nunca llegaron a dar información [66].
- El conocimiento del sistema Boundless Informant reveló que el jefe de la NSA y otros funcionarios mintieron al Congreso cuando fueron cuestionados acerca de las cifras de la vigilancia; estos respondieron que no eran capaces de dar cifras concretas, cuando, en realidad, el citado programa daba cuenta pormenorizada de todos los datos obtenidos [67].
- Una diapositiva también reveló la estrategia de la NSA de recabar toda la información posible, sin límites. Esta filosofía es una de las razones de la construcción del famoso data center de Utah [68].
- Las capacidades de pinchar los troncales de Internet, puntos de interconexión, conmutadores, enlaces microondas, comunicaciones por satélite, etc. conforme a los programas de Upstream [69].
- Las brutal capacidad de recolección de datos y la no menos brutal capacidad de búsqueda en esos almacenes de datos de I-Creach y X-Keyscore [70].
- La existencia del programa Computer Network Exploitation y la división Tailored Access Operations que permite infectar y tomar el control de ordenadores, servidores, dispositivos móviles y de red, mediante técnicas sofisticadas hardware y software, imposibles de detectar [71].
- La existencia de un espionaje económico, como el programa Olympia que obtenía información del Ministerio de Minas y Energía de Brasil [72]. Otros objetivos eran el sistema interbancario SWIFT, la petrolera Gazprom, la aerolínea Aeroflot [73] y, más recientemente, se tuvo conocimiento del espionaje al que fue sometida Airbus [74].
- La existencia de un espionaje político, cuyos objetivos fueron la presidenta Dilma Rouseff o el, por aquel entonces, candidato a la presidencia de México, Enrique Peña Nieto. Incluso se llegó a espiar al secretario general de la ONU para “preparar” su encuentro con el presidente Obama [75].
- A pesar de las notas de condena de países europeos, como Alemania, Francia o España, se comprobó posteriormente su colaboración en programas puntuales. Además de las Agencias de los Cinco Ojos (NSA, GCHQ, ASD [76], CSEC [77] y GCSB), colaboraron el BND de Alemania [78], el PET de Dinamarca [79], la DGSE Francia [80], ISNU de Israel [81], NIS de Noruega [82], AISE de Italia, NDB de Suiza, AIVD de Holanda, el CNI español [83].

4. Programas

Una vez llegados a este punto, es el momento de repasar algunos de los programas desvelados por Edward Snowden.

Antes, es importante hacer notar que los datos relativos a los programas de vigilancia masiva desvelados se basan en los documentos que el propio Snowden "liberó" y en las explicaciones que él mismo ha dado a los periodistas que cubrieron la noticia para poder poner en contexto las funcionalidades de los mismos. Por tanto, se trata de información que proviene de una única fuente y que es difícilmente contrastable. Asimismo la profundidad y exactitud de los datos hechos públicos están limitadas a lo que el propio Snowden ha querido desvelar y a lo que periodistas e investigadores han podido averiguar a partir de su información. La mayor parte de la información descrita en este apartado proviene del libro “Snowden. Sin un lugar donde esconderse” de Glenn Greenwald [84].

Las revelaciones de Snowden describen una constelación de programas que, por diferentes medios, recolectan información de manera masiva; en algunos casos, la delimitación está clara, en otros, es difícil establecerla y se pueden intuir relaciones de jerarquía entre los diferentes programas, englobando unos a otros. Asimismo, algunas de estas actividades no tienen asociado un nombre en clave ni están identificadas por un programa específico, pero no por ello resultan menos intrusivas.

Dicho esto, podemos pasar a describir brevemente la naturaleza de los diferentes tipos de vigilancia y los cuerpos y agentes involucrados.

4.1. Introducción

Durante esta descripción, detallaremos todos los elementos a tener en cuenta en los programas para, posteriormente, entrar en las características de algunos de ellos.

Actores involucrados: El actor principal de la vigilancia es, sin duda, la NSA, Agencia de Seguridad Nacional. Sin embargo, veremos que en algunos casos están involucradas otras agencias norteamericanas, como el FBI o la CIA, que teóricamente tienen otro foco de actuación. En colaboración “de primer nivel” con la NSA, estarían los participantes de esa agrupación conocida como los “Cinco Ojos”, “**Five Eyes**”, compuesta por, además de la NSA, la **GCHQ** (Government Communications Headquarters) de Reino Unido con una relación bilateral con la NSA privilegiada, la **ASD/DSD** (Australian Signals Directorate) de Australia, la **CSE** (Communications Security Establishment) de Canadá y la **GCSB** (Government Communications Security Bureau) de Nueva Zelanda. Existen colaboraciones en un segundo nivel, normalmente negadas, de los países tradicionalmente aliados de EEUU, como la **BND** de Alemania y las agencias de inteligencia de Austria, Italia, Dinamarca, Holanda, etc. En el polo opuesto, estarían los países que suelen ser objetivos, pero nunca socios, como China, Rusia, Irán, Venezuela y Siria, por poner algunos ejemplos. A continuación se muestran dos clasificaciones de países distintas filtradas en los documentos de Snowden:

CONFIDENTIAL//NOFORN//20291123

TIER A **Comprehensive Cooperation**	Australia Canada New Zealand United Kingdom
TIER B **Focused Cooperation**	Austria Belgium Czech Republic Denmark Germany Greece Hungary
	Iceland Italy Japan Luxemberg Netherlands Norway

Fig. 4 – Países que cooperan con la NSA (diapositiva filtrada)

Fig. 5 – Clasificación de países colaboradores de la NSA (diapositiva filtrada)

Asimismo, la NSA se apoya en empresas de telecomunicaciones (como en el famoso caso Verizon) y en proveedores de servicios de Internet (como veremos para el caso PRISM):

Fig. 6 – Acuerdos estratégicos de la NSA (diapositiva filtrada)

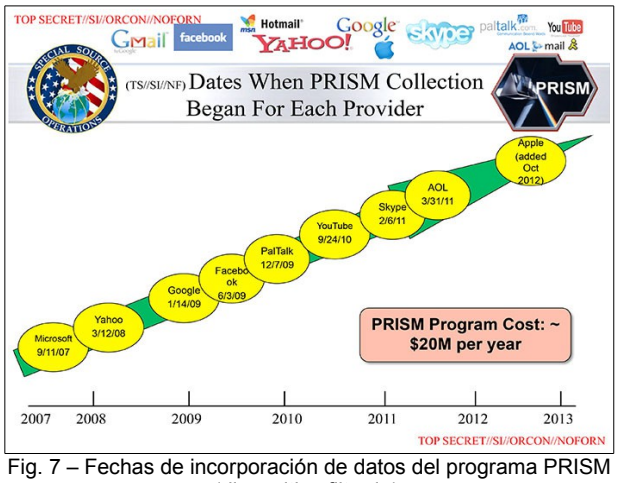

Fig. 7 – Fechas de incorporación de datos del programa PRISM (diapositiva filtrada)

Por último, en relación con este apartado de actores involucrados, cabe reseñar la proliferación de empresas o "contratistas" en el sector de la seguridad de la NSA, la CIA o el FBI, para las que el propio Snowden trabajó en el área de "inteligencia", como Booz Allen Hamilton, por ejemplo, y las empresas que desarrollan sistemas de vigilancia (y, en algunos caso, de ataque) que ponen en el mercado, como Gamma Group, Hacking Team, Bull Amesys o Blue Coat [85].

Divisiones de trabajo: A la hora de entrar a describir los diferentes programas que impulsa la NSA, vendrá bien conocer dos o tres líneas de trabajo de la NSA. Por un lado, están las **SSO** (Special Source Operations) dedicadas a los programas que recolección de información de cables de fibra y switches en las redes de comunicación. Por otro lado, está el **SCS** (Special Collection Service), una iniciativa conjunta de la NSA y la CIA dedicada a insertar equipos de escucha en lugares de difícil acceso, como centros de comunicaciones, instalaciones y embajadas, etc. Por último está la actividad **CNE** (Computer Network Exploitation) que lleva a cabo operaciones **TAO** (Tailored Access Operations) ejecutadas por unidades de hackers [71].

Sistemas de búsqueda e indexación: La información recolectada por todos los programas de vigilancia es tan prolija que la NSA ha tenido que construir un *Data Center* en Utah de capacidades nunca vistas en el pasado [68]. Por otro lado, esa ingente cantidad de información sería inútil si no se pudiese encontrar lo que se desea; para ello, se han tenido que crear herramientas de búsqueda en ese maremágnum de información; **ICREACH**, el *google* de la NSA o el propio programa **X-Keyscore** [70], que veremos más adelante, como herramienta de recopilación, indexación y búsqueda. El programa **BOUNDLESSINFORMANT** es una herramienta analítica de Big Data [67].

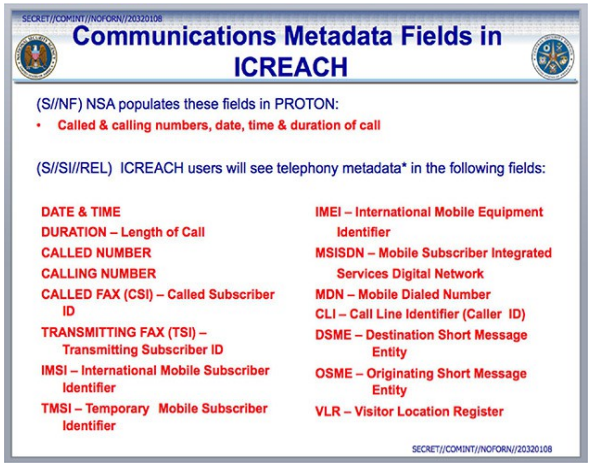

Fig. 8– Metadatos de Icreach (diapositiva filtrada)

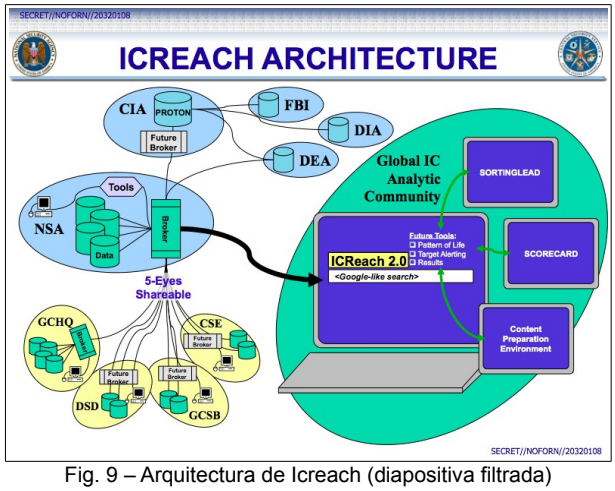

Fig. 9 – Arquitectura de Icreach (diapositiva filtrada)

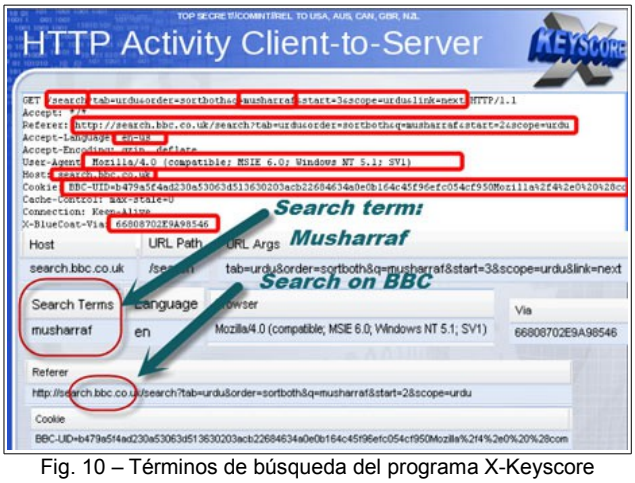

Fig. 10 – Términos de búsqueda del programa X-Keyscore (diapositiva filtrada)

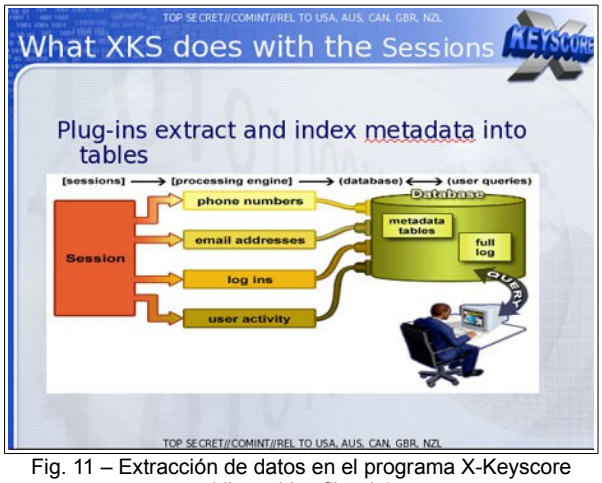

Fig. 11 – Extracción de datos en el programa X-Keyscore (diapositiva filtrada)

Fuentes de recolección: Según se trate de datos de telefonía o de datos de redes de comunicaciones, especialmente internet, se estará hablando de **DNR**, Dial Number Recognition, o de **DNI**, Digital Network Intelligence, respectivamente.

Tipo de recolección: También se puede diferenciar entre la recolección de información en tránsito y la de información ya almacenada. Una clasificación muy importante es la de los datos recolectados como **contenido** de la comunicación frente a la información que rodea la comunicación y que hemos venido llamando a lo largo del documento **metadatos**. El contenido consistiría en las conversaciones de llamadas telefónicas interceptadas, el texto de los *emails*, las conversaciones de un chat, el historial de navegación, las búsquedas realizadas, etc. Por contra, como adelantábamos más arriba, el metadato es la información que rodea una comunicación, por ejemplo, los metadatos de un correo electrónico serían quién envió el correo, a quién, el asunto o la ubicación del remitente; los de una llamada telefónica serían la identidad del que llama y del que recibe la llamada, la duración de la conversación, los emplazamientos y aparatos usados.

Tradicionalmente, se le ha querido quitar trascendencia a este tipo de datos, pero su acumulación y explotación puede resultar muy provechosa para el espía. Las llamadas a un centro de planificación familiar, a una clínica de VIH; llamadas a altas horas de la noche, a líneas de ayuda, tipo el Teléfono de la Esperanza, pueden revelar mucho de una persona. Asimismo, se puede trazar la conexión entre los contactos de una persona y los de otra, permitiendo conocer intereses comunes, etc. A veces, este tipo de datos puede resultar más útil que los propios contenidos, por ejemplo, en el caso de que en la conversación se utilicen palabras en clave, códigos secretos o incluso en aquellos casos en los que se está mintiendo. Los metadatos permiten un tratamiento automatizado y estadístico (tipo Big Data) que difícilmente podrá realizarse sobre algunos contenidos (los de voz, por ejemplo).

4.2. Caso Verizon

El caso Verizon [86] es famoso porque fue el primero de los documentos revelados por Snowden, pero su relevancia estriba en que desvela cómo el propio tribunal FISC autoriza la recolección masiva de **metadatos** de telefonía (**DNR**) para el FBI, independientemente de si se trata de llamadas internacionales o locales, en virtud de la sección 215 de la Patriot Act [32]. El FBI compartía estos datos con la NSA. El caso Verizon es el exponente de aquellos operadores de telecomunicaciones que colaboran con las Agencias, bien por mandato judicial, como este caso, bien con contrapartidas económicas.

De manera similar, Vodafone ha revelado [87] la existencia de cableado secreto que permite a las Agencias interceptar todas las conversaciones en sus redes, de acuerdo a la legislación de cada país donde operan.

Veremos a continuación la colaboración que prestaba AT&T en el contexto del programa BLARNEY. Si bien el caso Verizon consistía en entregar metadatos de las comunicaciones telefónicas, AT&T, según

las filtraciones del Snowden y el Wall Street Journal [88], entregaba a la NSA datos de las comunicaciones de países en los que prestaba servicio, de manera directa o indirecta, como por ejemplo, Alemania, Brasil, Francia, Israel, Italia o Japón [89].

4.3. Upstream - FAIRVIEW, BLARNEY, OAKSTAR, STORMBREW

La recolección de datos Upstream [69], está gestionada por la SSO, Special Source Operations, y su objetivo es la recolección de datos desde el propio troncal de internet, la infraestructura de las telecomunicaciones y los medios de transmisión, esto es, cables submarinos, enlaces de microondas, cableado de fibra óptica, puntos de interconexión o dispositivos de red (switches, routers, etc.). Al igual que en el caso Verizon, la información se recaba con la colaboración de los propios operadores de telecomunicaciones norteamericanos e incluye información global gracias al acceso que estos tienen a los sistemas internacionales en virtud de los contratos de mantenimiento suscritos con las compañías extranjeras. También colaboran Agencias de Inteligencia extranjeras.

Según el Senador Thomas Drake [90], el programa FAIRVIEW sería el programa “paraguas” de los otros tres, pero Snowden lo describe como uno más. En cualquier caso, se trata de la recolección de datos de tipo **DNR y DNI**. El programa BLARNEY, por ejemplo, es fruto de la información suministrada por AT&T y está enfocado a la obtención de **metadatos**. Sin embargo, el acceso físico a los medios de transmisión hace intuir que también se debe estar obteniendo contenido en tránsito. Los cuatro programas son muy similares y difieren en cuál es la TELECOM o Agencia proveedora de los datos y los países de los que se recaba la información.

La contrapartida de estos programas en el Reino Unido es TEMPORA, operado por la GCHQ. También se basa en el acceso directo al nodo troncal de internet (canales de fibra, conmutadores, etc.). Sin embargo, según los artículos de Ewen MacAskill [91], TEMPORA incluye, además de registros de llamadas telefónicas, los contenidos de correos electrónicos, entradas en Facebook o el historial de páginas web visitadas, lo que hemos dado en llamar **contenido**.

4.4. PRISM

El programa PRISM [92] suscitó una gran preocupación cuando vió la luz; las compañías más prominentes de servicios de internet estaban facilitando el acceso ilimitado al contenido de sus servidores a la NSA, es decir **contenidos** y **metadatos (DNI)**. Los datos de los usuarios de Facebook, Google, Yahoo!, Skype, Apple, Microsoft, AOL, Youtube y Paltalk estaban a disposición de la NSA, algo que las citadas empresas negaban estar facilitando de manera masiva. Dada la variedad que proporcionan estas empresas, el tipo de contenidos que se obtenían era muy considerable; correos electrónicos, chats, videos, fotos, datos almacenados, etc. En la documentación hecha pública, la NSA se felicitaba por la gran cantidad de información útil que se podía obtener de este programa y recomendaba a sus agentes usar PRISM en conjunción con Upstream:

Fig. 12 – Comparativa de los programas PRISM vs Upstream (diapositiva filtrada)

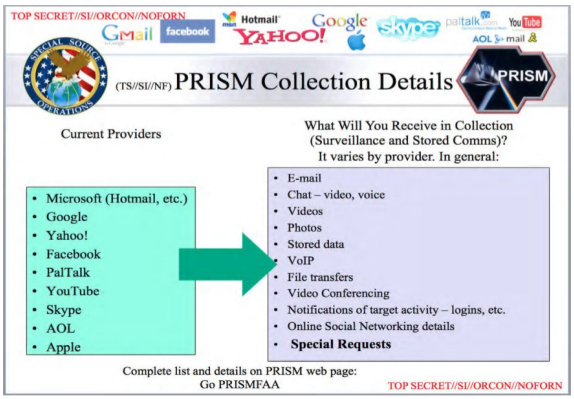

Fig. 13 – Empresas “proveedoras” y detalle de los datos recogidos del programa PRISM (diapositiva filtrada)

El caso de la colaboración de Microsoft con la NSA es paradigmático; mientras incluía en su página de SkyDrive lo importante que consideraban el control de acceso a los datos personales de sus usuarios, uno de los documentos desvelados por Snowden detallaba los meses de trabajo que dedicó Microsoft para facilitar el acceso de la NSA a los mismos. Ejemplos similares valen para Skype (cuando fue

adquirido por Microsoft) o el sistema de correo electrónico Outlook.com [93].

4.5. X-Keyscore

Una de las razones de lo apremiante de construir el centro de datos de Utah [68] es este programa que recopila, contextualiza, organiza y permite buscar en los datos electrónicos. Según los documentos de Snowden, X-Keyscore [94] abarca casi todo lo que hace en internet un usuario típico, incluyendo los textos de sus correos electrónicos, las páginas web visitadas o sus búsquedas en *google*. Además de la recolección masiva de datos, permite hacer un seguimiento individualizado en tiempo real.

Como se vio en las diapositivas de más arriba, el sistema permite además realizar búsquedas en las bases de datos de la NSA de direcciones electrónicas, números de teléfono, direcciones IP, etc. Más abajo, se ve el ejemplo de alguna de estas bases de datos (Traffichief, Marina, Pinwale). Se trata de un programa que recopila sobre todo **contenido** de red, **DNI**, y que permite realizar búsquedas conforme a los **metadatos**. Se trata de contenidos de todo tipo, tanto en tránsito, como almacenados. Es un conglomerado de cientos de servidores a lo largo del mundo que están recopilando información y sobre el que se pueden realizar búsquedas. Las fuentes de información van desde el SCS F6 (una iniciativa conjunta de operaciones clandestinas de la CIA y la NSA) interceptaciones de satélites (FORNSAT), SSO, así como operaciones TAO, autorizaciones FISA y contrapartidas de Agencias de terceros países.

Es tal la profundidad y calidad de la información recolectada, que las búsquedas pueden realizarse tanto con los llamados “strong selectors”, como, por ejemplo, una dirección de correo electrónico, como con “soft selectors”, palabras clave del cuerpo del correo o el chat.

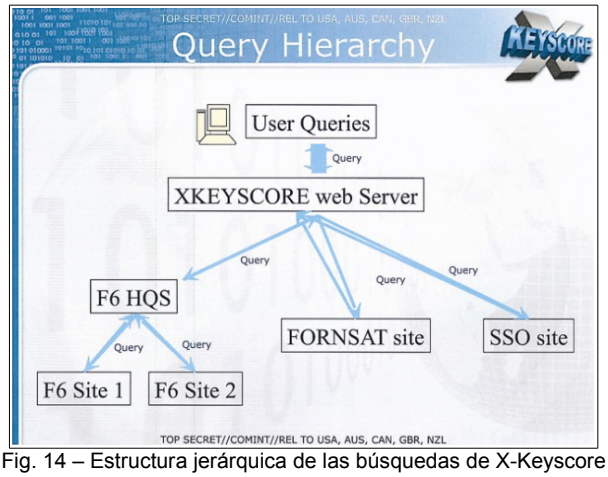

Fig. 14 – Estructura jerárquica de las búsquedas de X-Keyscore (diapositiva filtrada)

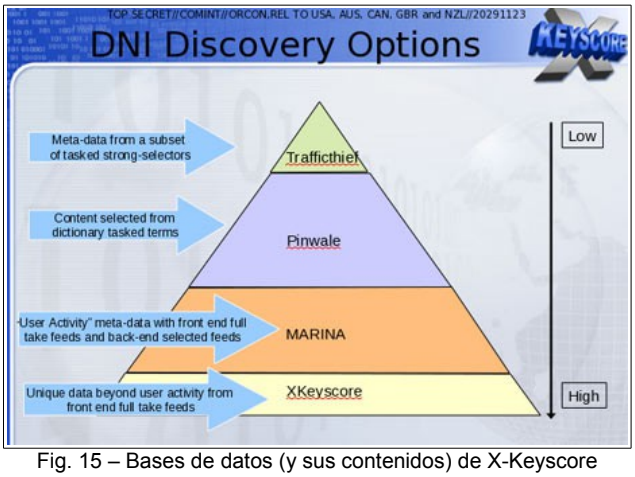

Fig. 15 – Bases de datos (y sus contenidos) de X-Keyscore (diapositiva filtrada)

4.6. Computer Network Exploitation, CNE

Bajo este epígrafe, Computer Network Exploitation [71], se incluyen un conjunto de programas y actividades proactivas llevadas a cabo por la unidad de Tailored Access Operations, TAO, cuyo fin es obtener información de los objetivos mediante:

- Intrusión en las redes o sistemas del objetivo: Se trataría de explotar vulnerabilidades de los dispositivos de red o bien de su configuración, obteniendo acceso a entornos, en teoría, seguros. El programa MUSCULAR podría ser un ejemplo de este tipo de táctica.
- Infección de los sistemas, redes o dispositivos con puertas traseras que permitan el acceso posteriormente; en esta categoría podría incluirse, entre otras, el gusano Stuxnet o la infección denominada “Quantum Insertion”.
- Ruptura mediante técnicas de hacking de estándares de encriptación generalmente aceptados como seguros. Dentro de esta categoría podría incluirse el programa BULLRUN.
- Modificación física de componentes hardware que habilitan puertas traseras para el atacante.

A continuación se detallan algunos de los programas que podrían englobarse en esta categoría, dedicando un punto al llamado “catálogo” ANT:

4.6.1. MUSCULAR y TURMOIL

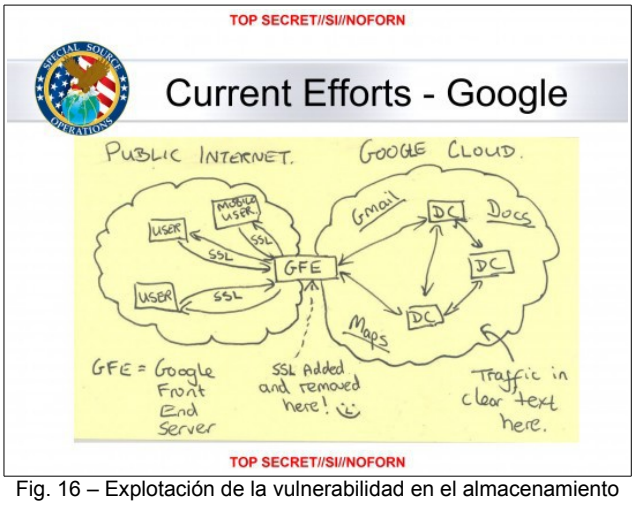

Fig. 16 – Explotación de la vulnerabilidad en el almacenamiento de Google, vinculado a los programas MUSCULAR y TURMOIL (diapositiva filtrada)

MUSCULAR es un programa de la GCHQ, pero operado conjuntamente con la NSA.

El programa consiste en la irrupción dentro de los centros de datos de Google y Yahoo! lo que ha generado una cantidad ingente de información; en particular, se trataría de **contenido** de los citados servicios de internet, **DNI**.

Al parecer, en el caso de Google se aprovechó el hecho de que la transmisión de datos dentro de su nube privada se hacía de manera no encriptada.

La NSA ha trabajado en el sistema TURMOIL para poder procesar la información recogida.

4.6.2. Infecciones de toma de control

Un exponente de este tipo de infecciones es Stuxnet [95], un *worm* o gusano que data de junio de 2010 y que se diseñó para atacar PLCs, unos dispositivos programables que permiten controlar maquinaria industrial de manera automatizada. La manera de acceder a los equipos que se pretende infectar es mediante tarjetas USB infectadas. Una vez se ha usado uno de estos dispositivos USB, la infección se propaga por la red y alcanza su objetivo. El caso que se hizo público fue el de las centrifugadoras de uranio iraníes que resultaron dañadas por esta infección. Snowden ha confirmado que se trataba de un programa conjunto entre la NSA e Israel [96].

Curiosamente, el investigador Michael Heerklotz hizo público a primeros de enero [97] que frente a lo que se daba por hecho, Microsoft no había corregido la vulnerabilidad con el parche de agosto de 2010. Ha sido en el conjunto de parches publicado en marzo de 2015 (actualización MS15-020) que se ha terminado de solucionar este fallo. Por tanto, todo el parque de equipos Windows ha sido vulnerable durante estos cinco años (los sistemas operativos posteriores como Windows Server 2012 o Windows 8.1. habían heredado la vulnerabilidad).

Según los datos revelados por Snowden [98], en el marco de un programa denominado **“Quantum Insertion”**, las agencias NSA y GCHQ han conseguido infectar al menos 50.000 ordenadores individuales con este *malware*. La táctica consistió en crear una página web que emulara la página de LinkedIn, a la que se añadió una funcionalidad inédita, un *malware* que infectó aquellos ordenadores, cuyos usuarios “picaron”. Una vez desplegado el malware, los citados ordenadores estaban bajo control de la GCHQ, obteniendo así acceso a su contenido y a todo aquello que se tecleara, chats, correos electrónicos, incluso las contraseñas del usuario. Se conoce una de las víctimas, la TELECOM Belgacom.

La NSA ha conseguido hacer algo similar con la red social Facebook [99]. También ha logrado obtener acceso a la cámara y micrófono de los ordenadores atacados mediante correo spam y el malware adecuado.

Según el Hufftington Post [100], la NSA ha conseguido infiltrar un código espía en discos duros de Western Digital, Seagate y Toshiba, entre otros fabricantes, teniendo acceso así a la mayoría de ordenadores del mundo. Esto habría sido descubierto por investigadores de Kaspersky Lab, que han encontrado este software espía en al menos 30 países. La infección podría remontarse al año 2001.

4.6.3. BULLRUN y EDGEHILL

El programa BULLRUN [101] es una iniciativa de la NSA para acceder a contenidos cifrados. EDGEHILL es el programa equivalente de la GCHQ. No se han revelado muchos detalles de estos programas, pero los documentos internos de la NSA dan por hecha la posibilidad de acceder a los contenidos cifrados que utilizan protocolos seguros, como https y Secure Sockets Layer (SSL). Wikileaks publicó, en su día, los llamados "Spy Files" [102] que incluyen, a modo de catálogo, un buen número de herramientas comerciales que son capaces, por ejemplo, de escuchar comunicaciones, incluso cuando están cifradas (p.e. ACCESSDATA).

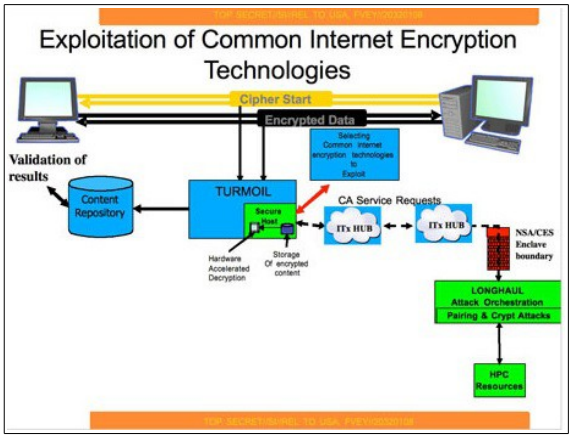

Fig. 17 – Explotación de las tecnologías de cifrado en Internet (diapositiva filtrada)

Estos programas forman parte de una tradición recurrente para intentar acceder a los contenidos cifrados o, incluso, prohibir la posibilidad de cifrar contenidos sin puertas traseras.

Sin ir más lejos, Edward Snowden hizo público el presupuesto de la NSA [103] correspondiente al año 2013, en el que su autor, James Clapper, Director de Inteligencia Nacional, destaca que "estamos invirtiendo en innovadoras capacidades criptoanalíticas para derrotar la criptografía adversa y poder explotar el tráfico de internet [104]." El documento muestra que el 21% del presupuesto aproximado de inteligencia – unos 11.000 millones de dólares – está dedicado al *Consolidated Cryptologic Program*. Fruto de estos esfuerzos, se han llevado a cabo los siguientes programas secretos:

- El profesor Eric Roberts de la Universidad de Stanford sugiere que la NSA introdujo una puerta trasera en noviembre de 2007 en los generadores de números aleatorios que se usan para el cifrado [105]. Lo habría hecho mediante la guía 800-90 del *National Institute of Standards and Technology* (NIST) de aquel año (y sustituida en enero de 2012). Este instituto es el responsable de aprobar las tecnologías para el sector público y privado de EEUU. Hay que tener en cuenta que la generación de estos números de manera realmente aleatoria es fundamental para la creación de claves de cifrado y descifrado; si no se hace correctamente, el sistema estará comprometido [106].
- En el mismo sentido, otra información reciente desvela que la NSA habría pagado 10 millones de dólares a la compañía de seguridad RSA para incluir un RNG trucado en su software Bsafe, usado precisamente para mejorar la seguridad de ordenadores y otros productos [107].
- En los últimos años han aparecido múltiples vulnerabilidades de SSL como, por ejemplo, el Heartbleed Bug [108], que permitía acceder a los datos que habían sido cifrados con OpenSSL. El hecho de que se haya publicado que la NSA sabía de este bug dos años antes de su conocimiento por el público general [109], ha suscitado suspicacias lógicas de que quizás haya estado beneficiándose del problema o que, incluso, fuera su promotor. Otras vulnerabilidades similares han sido "go to fail" [110] o poodle [111].

4.6.4. Intrusiones de hardware

Esta es otra de las líneas de trabajo de los equipos TAO. Según techdirt [112], The Intercept reveló en febrero de 2015 que la NSA junto con la GCHQ habían *hackeado* al mayor proveedor de tarjetas SIM, Gemalto, con la intención de hacerse con el control criptográfico de miles de teléfonos.

Paradójicamente, el gobierno de Estados Unidos llevaba años avisando de que la electrónica de red procedente de China suponía una amenaza por estar fabricada con una funcionalidad de vigilancia encubierta que les proporcionaría la capacidad de espiar las comunicaciones de aquellos que la usaran [113]. Paradójicamente, porque las revelaciones de Snowden iban a poner a la luz pública un programa de la NSA según el cual, se interceptaban dispositivos de red (routers, servidores, etc.) en la cadena de suministro, antes de ser enviados a sus compradores internacionales, para implantar en

ellos instrumentos de vigilancia encubiertos, reempaquetándolos con sello de fábrica, para que el destinatario no pudiese sospechar esta maniobra. De esta manera, la NSA lograba precisamente aquello que le achacaba a las empresas chinas (ZTE y Huawei).

La alarma que planteaba la NSA parece que era razonable, pues en alguno de los documentos desvelados se habla, efectivamente, de este riesgo ("There is also concern that Huawei's widespread infrastructure will provide de PRC with SIGINT capabilities and enable them to perform denial of service type attacks"). Sin embargo, es curioso que esta alarma tuviera como consecuencia que el mercado de este tipo de productos volviera la espalda a los productos chinos para volcarse en la adquisición de los productos norteamericanos más "seguros".

Fig. 18 – Preocupación de la NSA por los productos Huawei (diapositiva filtrada)

La noticia resulta más sorprendente, si cabe, al desvelarse que uno de los objetivos de la NSA fue implantar sus propias puertas traseras en los productos Huawei [114], según el NY Times.

Existen evidencias de que, entre otros equipos, la Agencia intercepta y altera routers y servidores fabricados por CISCO y Juniper para dirigir grandes cantidades de tráfico de internet a los almacenes de la NSA. Der Spiegel [115] publicó que la NSA habría conseguido, además, implantar *backdoors* en servidores Dell y HP.

Entre los documentos de Snowden, hay incluso una fotografía del proceso de adulteración de los dispositivos de red CISCO [116]:

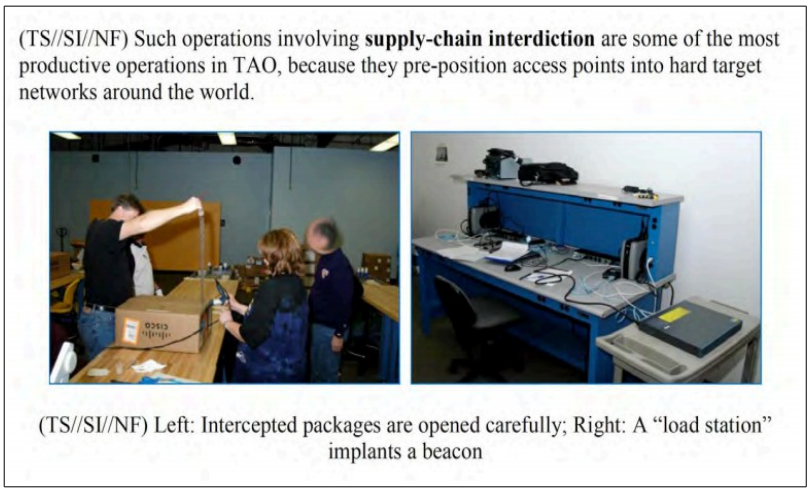

Fig. 19 – Detalles de la interceptación de productos en la cadena de suministro para incluir dispositivos de escucha (fotos de una diapositiva filtrada)

Por último, indicar que existen sospechas fundadas, aunque no vinculadas con las Agencias de Inteligencia, de que existe una técnica que permite alterar el comportamiento de los circuitos integrados, modificando la estructura de los transistores [117].

Según IEEE Spectrum [118], el Departamento de Defensa de Estados Unidos impulsó el programa "Trust in Integrated Circuits" con el objetivo de verificar la integridad de los circuitos integrados, valga la redundancia, que forman parte de sistemas militares. La preocupación consistía en la posibilidad de que se hubieran construido sistemas militares con chips que pudieran tener una puerta trasera que diera entrada a las fuerzas enemigas para control remoto o sabotaje.

Según informaciones del eldiario.es, esto se ha achacado a países como China y tiene su reflejo en teorías que miran hacia la NSA. Es un hecho probado que procesadores como los que desarrollan empresas Intel o AMD disponen de utilidades especiales que permiten a los fabricantes encontrar fallos; un 'acceso controlado' que algunas voces apuntan a que la NSA podría haber aprovechado [119].

4.6.5. Catálogo ANT

El "catálogo" ANT [120], al que tuvo acceso el semanario Der Spiegel [115], podría entenderse como un resumen de las capacidades de la NSA en el campo de la Computer Network Exploitation, CNE. ANT significaría Advanced o Access Network Technology y se trataría de la división de élite, compuesta por agentes especialistas TAO que acuden en ayuda cuando las técnicas habituales no han funcionado.

El catálogo, de unas 50 páginas, incluye incluso los precios (desde gratuidad hasta los 250.000 dólares) de los dispositivos – hardware y software – que están disponibles para los ataques dirigidos.

La mayoría se trata de puertas traseras para dispositivos de red de la práctica totalidad de fabricantes (Juniper, Cisco, Huawei, etc.), pero también hay estaciones GSM, código malicioso para BIOS, programas para infectar el firmware de discos Western Digital, Seagate, Maxtor o Samsung, etc.

No queda claro si los fabricantes implicados habrían colaborado en la creación de estas herramientas.

A continuación se incluyen algunos ejemplos, con sus nombres en clave:

- Cottonmouth – Dispositivos USB que ofrecen acceso wireless a los objetivos
- Deitybounce – Tecnología que permite instalar software en servidores PowerEdge de Dell
- Dropoutjeep - Software para capturar información de teléfonos iPhone (fotografías, lista de contactos, ubicación, etc.)
- Headwater - Software para enviar spyware a través de routers Huawei
- Howlermonkey – Transmisor de radiofrecuencia para copiar datos o tomar control de un oordenador
- Jetplow - Firmware que crea una puerta trasera en cortafuegos de Cisco
- Monkeycalendar - Software que envía la ubicación de un teléfono móvil como mensaje de texto
- Somberknave - Software que permite a los agentes tomar el control de ordenadores con WindowsXP

El catálogo data del año 2008 y algunos de los programas incluidos en él ya no estarían disponibles; por otro lado, durante todos estos años habrán aparecido nuevos productos adecuados a las medidas de seguridad actuales.

4.7. Tabla resumen

Categoría de programas	Programas	DNI Internet	DNR Telefonía	Información en tránsito	Información almacenada	Contenido	Metadatos	Aplicaciones afectadas
Caso Verizon			X	X	X		X	Comunicaciones telefónicas
Upstream	FAIRVIEW	X		X		X	X	Tráfico por internet
	BLARNEY	X		X		X	X	
	OAKSTAR	X		X		X	X	
	STORMBREW	X		X		X	X	
PRISM		X			X	X		Datos de yahoo, google, etc.
X-Keyscore		X	X	X	X	X	X	Recopilación masiva
CNE – Intrusión	MUSCULAR	X			X	X		Datos de yahoo y google
CNE – Infección	QUANTUM				X	X		Control de sistemas
CNE – Decryption	BULLRUN	X	X	X	X	X		Criptografía
CNE – Intrusión HW					X	X		Control de sistemas
CNE – ANT program					X	X		Gran variedad

Tabla 1 – Resumen de los programas NSA

5. Herramientas de defensa ante la vigilancia

En este apartado, se van a repasar las herramientas que el ciudadano tiene a su disposición para poder hacer frente a la invasión de la intimidad que supone la vigilancia masiva.

Tal como hemos visto en los apartados anteriores, los programas revelados por Snowden se podrían categorizar en:

- Programas en que los operadores de telecomunicaciones dan acceso a la información a las Agencias o les proporcionan directamente la información de sus clientes (Caso Verizon y similares)
- Programas en que los proveedores de servicios de Internet dan acceso a la información a las Agencias o les proporcionan directamente la información de sus clientes (PRISM y programas similares)
- Programas de recopilación de la información en tránsito desde la infraestructura de telecomunicaciones (Upstream)
- Programas que inspeccionan toda nuestra actividad en internet y que son capaces de ver el contenido de las comunicaciones, qué sitios web visitamos, qué búsquedas hacemos, etc. (programas tipo X-Keyscore)
- Programas CNE, consistentes en explotación de vulnerabilidades de dispositivos de red, infección de sistemas con puertas traseras, operaciones para romper la protección criptográfica o modificación física de dispositivos.

Si queremos evitar los efectos de la vigilancia y a la vista de las informaciones reveladas por Snowden, un principio básico de prudencia nos debe hacer evitar incluir información sensible en redes sociales, servicios de correo gratuito, de almacenamiento en la nube, etc., tener especial cuidado con las cookies que instalamos en el navegador o con las apps que instalamos en los *smartphones*, etc. Aparte de estas precauciones, que algunos podrían calificar de autocensura, hay una serie de principios básicos a seguir para evitar perder el control sobre nuestros datos.

Por un lado, se ha comprobado que las compañías de servicios de Internet han colaborado, voluntaria o involuntariamente, con las Agencias de Inteligencia, dándoles acceso a los contenidos de los usuarios almacenados en sus servidores. Ante esta amenaza, la herramienta apropiada es aplicar criptografía a los archivos y ficheros que podamos almacenar en sus repositorios; por ejemplo, si almacenamos información en *dropbox* o *drive*, sería aconsejable haberla cifrado previamente con las herramientas que veremos a continuación; lo mismo aplicaría a los documentos que enviemos por servicios de correo web, tipo *gmail* o *yahoo*. Otra respuesta, quizás más radical, será evitar este tipo de servicios, basados en un acuerdo EULA, por el que consentimos en que nuestros datos sean almacenados por el proveedor del servicio, acuerdo que muchas veces se ha convertido en papel mojado ante las presiones y/o arreglos de las Agencias de Inteligencia.

También hemos visto que el conjunto de programas Upstream “pincha” la infraestructura de internet; los cables de fibra, los dispositivos de red, los puntos de interconexión, etc., obteniendo directamente los contenidos que circulan por la red. Ante esta amenaza, lo apropiado será aplicar herramientas que cifren la información en tránsito.

Lo dicho aplicaría, análogamente, al tráfico de voz por las redes de telefonía; visto que las empresas de telecomunicaciones facilitan el acceso de las Agencias de Inteligencia a esta información, habrán de buscarse alternativas que dificulten que un tercero escrute nuestras comunicaciones. También veremos algunas de estas alternativas.

Al haberse puesto de manifiesto la existencia de puertas traseras en dispositivos físicos y herramientas de software, debería optarse por herramientas – soft y hardware – que, en la medida de lo posible, estén basadas en open source, en contraposición a las herramientas propietarias que suponen, de alguna manera, una caja negra de la que desconocemos su contenido. Las herramientas open source están abiertas al escrutinio público y, por lógica, serán menos susceptibles de contener una backdoor. En el caso del software es bastante probable que encontremos herramientas open source para

cualquier ámbito de trabajo, pues se trata de un campo de trabajo en franca expansión; por el contrario, el alcance del open source en el hardware está bastante limitado al campo lúdico y de investigación y son pocas, si no ningunas, las opciones reales de disponer de un sistema informático profesional y completo basado en open source.

En resumen, la respuesta estará enfocada al uso de la criptografía (que protegerá nuestra información en tránsito o almacenada) y en la elección de aplicaciones transparentes, tipo open source, sobre las que toda una comunidad de programadores tiene los ojos puestos y ejerce un papel auditor que detectaría cualquier desviación de los fines legítimos de estos proyectos.

Antes de entrar a describir algunas de las herramientas que dan respuesta a estas necesidades, cabe indicar que existen diferentes iniciativas de las Agencias de Inteligencia para socavar los proyectos cuyo fin es fortalecer la privacidad de los ciudadanos. Ya lo vimos en los puntos 2.2.5 y 4.6.3, en relación con la criptografía, pero hay otros casos, en los que se presiona directa o indirectamente a los operadores de estos servicios de privacidad que, en algunos casos, acaban discontinuando sus proyectos.

Uno de estos casos es el de Lavabit; Lavabit era un servicio de correo electrónico fundado en 2004 que ofrecía cifrado de extremo a extremo (E2EE) y que llegó a tener más de 410.000 usuarios. En agosto de 2013 su propietario, Ladar Levison, anunciaba en una carta que abandonaba el proyecto, de más de 10 años, para “no convertirse en cómplice de crímenes contra el pueblo americano”. Añadía que, por razones legales, no podía dar los detalles de su decisión, lo que nos remite a los casos ya tratados de Verizon y PRISM que son fruto de decisiones del tribunal FISC, secretas por naturaleza. Recordemos que en aquellos casos, las empresas involucradas entregaron – voluntaria o involuntariamente –


Lavabit

My Fellow Users,

I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know what's going on--the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.

What's going to happen now? We've already started preparing the paperwork needed to continue to fight for the Constitution in the Fourth Circuit Court of Appeals. A favorable decision would allow me resurrect Lavabit as an American company.

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would _strongly_ recommend against anyone trusting their private data to a company with physical ties to the United States.

Sincerely,
Ladar Levison
Owner and Operator, Lavabit LLC

Defending the constitution is expensive! Help us by donating to the Lavabit Legal Defense Fund here.

Fig. 20 – Carta de cierre de Lavabit (agosto 2013) [121]

datos de los usuarios a los servicios de inteligencia de Estados Unidos; en el caso de Lavabit, la petición hubiera implicado desvelar las claves privadas de cifrado de sus usuarios, tal y como explica en la nueva carta de mayo de 2014 [121].

Levison terminaba su carta de agosto diciendo que “esta experiencia me ha enseñado una lección muy importante; sin una acción del Congreso o un fuerte precedente judicial, desaconsejo a cualquiera confiar sus datos privados a compañías con vínculos físicos con Estados Unidos.”

Sin más, se repasan a continuación un conjunto de herramientas anti-vigilancia:

5.1. Navegación segura

Cuando estamos navegando por internet, cada enlace sobre el que pulsamos, cada página web que visitamos es útil para ciertas compañías. Google, Apple, Amazon, Facebook o Yahoo hacen acopio de nuestra actividad online y usan esta información para conocernos mejor, para conocer nuestros hábitos... En principio para bien (para ofrecernos en sus anuncios los productos que nos pueden interesar, para hacernos llegar ofertas asociadas al lugar donde estamos, etc.), pero, en el contexto de este trabajo, la información recolectada puede construir un perfil de nuestras vidas que, según cómo sea usado o en manos de quién caiga, puede resultar perjudicial.

Las capacidades de recolección de información durante la navegación son tan amplias y variadas que existen empresas que se han especializado en ofrecer sus servicios en este campo concreto; por poner un ejemplo, Baynote [122] ofrece sus servicios al canal de distribución web para proporcionar al cliente una experiencia de navegación personalizada multicanal. De esta manera, los comerciantes entienden qué busca el comprador y cuál es la manera en que pueden captarlo y retenerlo para la compra. Esto lo hacen analizando su comportamiento en la web, dónde se detiene más tiempo, en qué *frames* fijan su atención o hacen click, etc. Esta empresa concreta estaría proporcionando una ventaja

a la empresa y al consumidor y lo hace, aclara, evitando capturar datos que permitan identificar al cliente para preservar su privacidad. Sin embargo, esto no siempre es así y este anuncio nos desvela la amplitud de información que se puede averiguar de una persona navegando por la web.

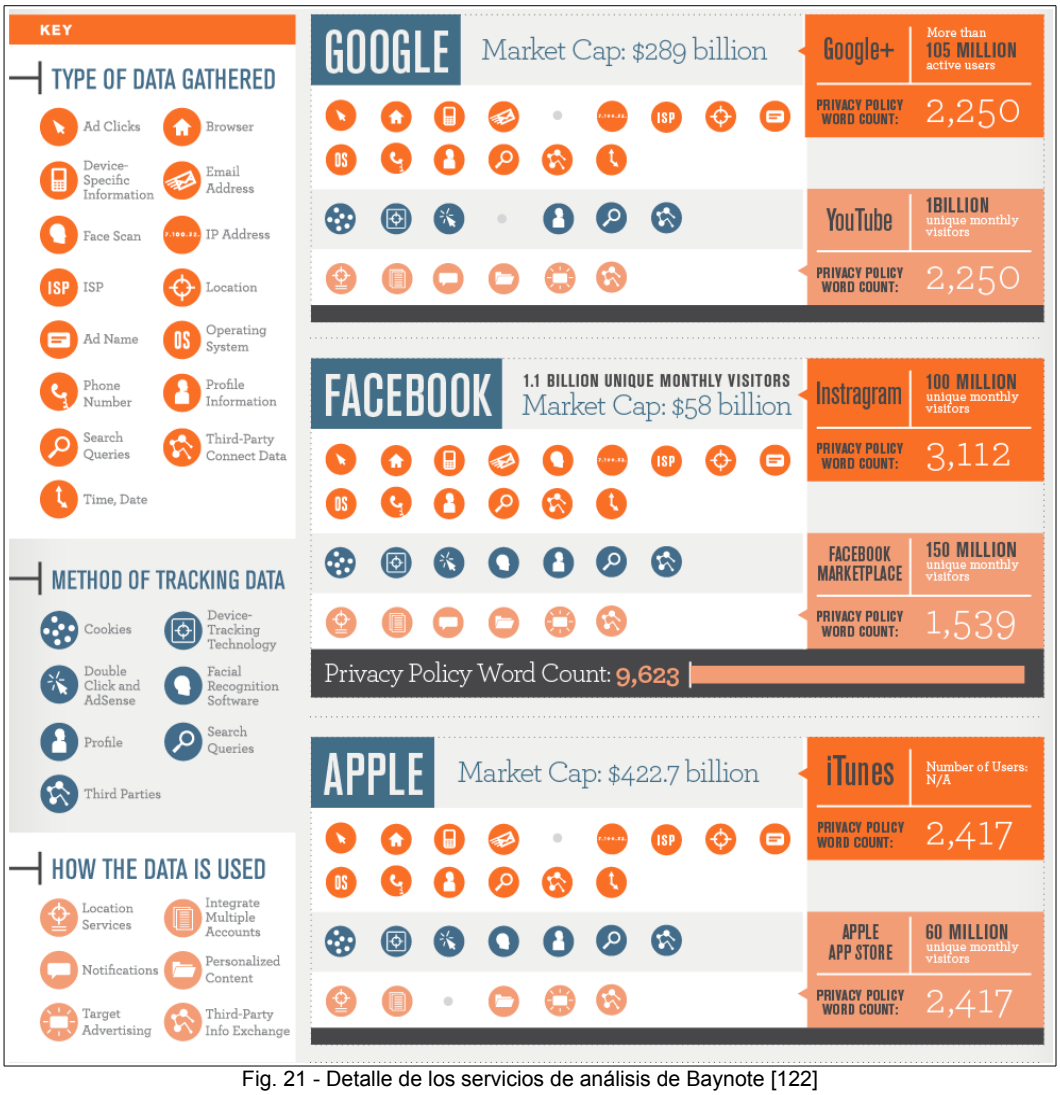

Fig. 21 - Detalle de los servicios de análisis de Baynote [122]

El objetivo de las herramientas que se describen a continuación es que el contenido de la navegación no pueda ser escrutado y que el anonimato del usuario esté garantizado.

5.1.1. Navegador TOR

El navegador TOR [123] es uno más de los componentes del proyecto TOR [124] (The Onion Router) que incluye otras herramientas para asegurar la privacidad y seguridad de sus usuarios en Internet. Antes de describir el navegador, sería conveniente repasar el proyecto TOR.

El proyecto TOR está compuesto por un numeroso grupo de servidores operados a lo largo del mundo por voluntarios que construyen una red de túneles virtuales encriptados a través de los cuales es posible conectar dos puntos, de manera indirecta, sin dejar rastro.

Cuando se establece una comunicación cifrada a través de Internet, logramos que un intruso sea incapaz de conocer el contenido de la comunicación, ya que los paquetes que se transportan por esta red tienen su *payload* cifrado; sin embargo, un análisis del tráfico en la red sí podría averiguar qué dos puntos se están poniendo en contacto, durante cuanto tiempo, etc. Es decir, averiguaría los metadatos de la comunicación analizando las cabeceras de los paquetes de una ruta directa. Esto lo evita la red TOR enrutando cada uno de los paquetes de una comunicación, de manera aleatoria, a través de

distintos nodos (relays en la terminología de TOR) que sólo conocen el relay origen inmediato del paquete y su relay destino inmediato; por tanto, sería altamente complicado y costoso seguir toda una comunicación que se descompone en múltiples paquetes y que discurre por varias rutas que ningún nodo conoce en su totalidad.

Así pues, las dos características principales que ofrece la red TOR son (i) el cifrado de los datos entre los nodos de la red, garantizando la privacidad, y (ii) el anonimato de las comunicaciones, haciendo que el cliente no sepa en qué dirección IP se encuentra realmente el servidor y que el servidor no sepa en qué dirección IP se encuentra el cliente.

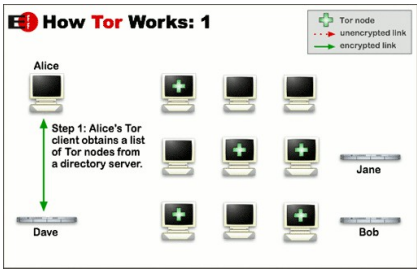

Fig. 22 – Esquema funcionamiento TOR (1), (fuente EFF)

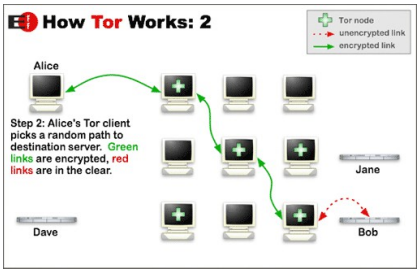

Fig. 23– Esquema funcionamiento TOR (2), (fuente EFF)

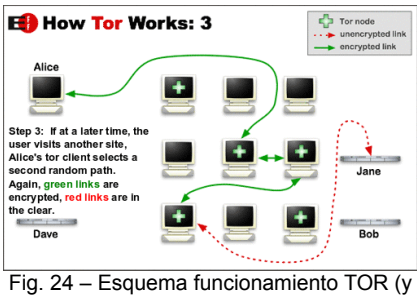

Fig. 24 – Esquema funcionamiento TOR (y 3), (fuente EFF)

Otra buena razón para usar TOR, pero ajena a los objetivos de este TFM, es que permite a sus usuarios evitar limitaciones de navegación impuestas por un Estado o por el proveedor de Internet. Sería el caso de regímenes dictatoriales que suprimen la posibilidad de acceder a ciertas páginas consideradas “subversivas” o “no aptas” para sus ciudadanos; el uso de la red TOR permite eludir esos controles.

El navegador TOR es software libre disponible para Windows, MacOS X, Linux/Unix, y Android. También es posible usarlo sin instalar ningún software, ejecutándolo, por ejemplo, desde un pendrive.

5.1.2. I2P

Es una alternativa a la red TOR; también se la conoce como “el proyecto de internet invisible”. Según la página web del proyecto [125], “I2P es una red anónima que proporciona una capa sobre la que diversas aplicaciones pueden enviarse mensajes entre sí de forma anónima y segura”. Así, tal y como veíamos en el caso del navegador TOR dentro de la red TOR, I2P es una plataforma que ofrece múltiples usos para diferentes aplicaciones. I2P ofrece mensajería IP, pero también da soporte a datagramas TCP. La comunicación está cifrada extremo a extremo.

La red no tiene un punto central en el que las Agencias de Inteligencia puedan ejercer presión para comprometer la seguridad o el anonimato del sistema. Además, la red es capaz de reconfigurarse dinámicamente como respuesta a posibles ataques. El equipo de desarrollo es un grupo abierto y todo el código del proyecto es open source.

I2P está diseñado para permitir que ambos peers que se comunican, lo hagan anónimamente (tanto entre ellos, como frente a terceros). Por ejemplo, existen páginas web en la red I2P “interna” que permiten la publicación anónima, así como proxies HTTP hacia la web normal que facilitan la navegación anónima.

La red está compuesta por múltiples nodos (routers, en terminología I2P) con túneles virtuales unidireccionales entrantes y salientes. Los routers se comunican mediante protocolos TCP, UDP, etc. Las aplicaciones “cliente” hacen uso de estos túneles virtuales, asignando autorizaciones dinámicamente. I2P dispone de una base de datos de la red para distribuir la información de contacto y enrutado de manera segura.

La red hace uso de un número significativo de técnicas y algoritmos criptográficos; 2048bit ElGamal, firmas 1024bit DSA, hashes SHA256...

Aunque en muchos aspectos, muy similar al proyecto TOR, I2P destaca algunas ventajas frente al

primero: diseñado para servicios ocultos, servicios totalmente distribuidos, selección dinámica de los peers en función de su rendimiento actual, basado en tecnología peer-to-peer, mensajes distribuidos a través de múltiples peers, frente a una única ruta, arquitectura resiliente ante fallos al ejecutarse múltiples túneles en paralelo, túneles unidireccionales frente a los birireccionales de TOR, basado en Java... Sin embargo, su base de usuarios es todavía mucho menor que la de TOR.

5.2. Búsquedas en web seguras

Cuando hacemos una búsqueda en google estamos diciendo mucho de nosotros mismos; qué nos interesa, si estamos buscando trabajo o si buscamos a alguien, si necesitamos información sobre determinada patología, una compra prevista... Google guarda incluso esas búsquedas que tecleamos pero que no llegamos a hacer... Aquí se propone una de las alternativas a los buscadores más extendidos que ofrecen garantía de no almacenar y procesar esta información personal.

5.2.1 DuckDuckGo

DuckDuckGo [126] es un buscador que no recoge información personal ni *cookies* de los usuarios y, por tanto, todos obtienen el mismo resultado de una búsqueda.

Según la propia página web DuckDuckGo [127], otros buscadores, además de guardar nuestras palabras de búsqueda, las envían al sitio web sobre el que hemos hecho click. Asimismo, debe tenerse en cuenta que, al visitar un sitio web, el ordenador está enviando información propia del equipo (por ejemplo, el *user agent* o su dirección IP), que puede identificar al usuario. El texto de búsqueda combinado con esta información es un riesgo para la privacidad del usuario. DuckDuckGo no envía, por defecto, los términos de búsqueda al sitio web destino.

Asimismo, DuckDuckGo se basa en HTTPS Everywhere (herramienta que veremos más adelante) para forzar, cuando estén disponibles, los enlaces hacia páginas cuyo protocolo sea HTTPS, evitando así que el contenido de la búsqueda sea accesible en tránsito.

Otra ventaja en el uso de este buscador es que puede utilizarse conjuntamente con un proxy Tor para obtener una búsqueda anónima y encriptada extremo a extremo.

Por último, indicar que DuckDuckGo tampoco guarda un historial de búsquedas, algo que sí hacen otros buscadores. Esta información supone también un riesgo para la privacidad del usuario; puede ser desvelada por el proveedor (caso AOL [128]) o puede ser requerida por las autoridades.

5.3. Protección del correo electrónico

El correo electrónico juega un papel fundamental en las comunicaciones hoy en día; disponer de un correo seguro y confidencial es el objetivo de las herramientas que se describen a continuación:

5.3.1. Dark Mail

Dark Mail [129] surge como alternativa al cierre de Lavabit. Lo puso en marcha el propio Ladar Levison en noviembre de 2013. Se trata de un proyecto de software libre – Dark Internet Mail Environment (DIME) – que, apoyado en la experiencia adquirida con Lavabit, pretende sustituir los servidores de correo actuales con los nuevos protocolos DMTP (Dark Mail Transfer Protocol) y DMAP (Dark Mail Access Protocol) que ofrecen comunicaciones cifradas "extremo a extremo".

El sistema aplica distintas capas de cifrado al correo electrónico para que, durante su viaje desde el remitente al destinatario, el mensaje solamente muestre la información que es necesaria para cursar la comunicación (de manera análoga a la estructura de cebolla – onion – de Tor), dejando siempre oculto el contenido del mensaje.

El servidor de correo electrónico del remitente del mensaje solamente puede descifrar la parte del mensaje que contiene la dirección de correo destino y el servidor del destinatario solamente puede ver la dirección del destinatario (para entregar el mensaje en su buzón) pero no puede ver ni el contenido ni tampoco el correo electrónico del remitente (solamente puede saber del servidor del que procede). Para que este esquema funcione, DIME se apoya sobre un sistema de claves federado (algo parecido al funcionamiento de los servidores DNS) dado que cada sistema que forme parte del proceso de envío y recepción de correos electrónicos tiene sus propias claves públicas y privadas de cifrado.

En estos momentos, el sistema sigue siendo experimental y aún no es posible implementar un servicio de correo electrónico basado en DIME. La idea es que el protocolo Dark Mail se extienda en el mayor número de servicios posible para garantizar la confidencialidad de las comunicaciones.

Juegan a su favor, los pesos pesados que se han involucrado en el proyecto; Jon Callas, Mike Janke y Phil Zimmermann. Si finalmente el proyecto alcanza sus objetivos, DIME podrá ofrecer a Google o Yahoo! un protocolo transparente al usuario que le ofrecerá comunicaciones seguras "extremo a extremo" sin tener que recurrir a componentes externos, como PGP.

5.3.2. Mailvelope

Si, a pesar de lo dicho en el preámbulo, se quiere seguir usando herramientas de uso gratuito como *gmail* o *yahoo!*, Mailvelope [130] es una sencilla extensión para el navegador que proporciona cifrado OpenPGP para este tipo de servicios de correo web. Su interfaz se integra perfectamente y proporciona seguridad instantánea extremo a extremo a la comunicación vía correo electrónico.

Es un proyecto open source, basado en OpenPGP y está disponible en la Chrome Web Store desde agosto de 2012.

OpenPGP es un sistema de criptografía de clave pública que está basado en que cada usuario dispone de una clave pública, que conoce todo el mundo y que usa para cifrar la información, y una clave privada, que solo conoce su propietario y que sirve para que, únicamente él, pueda descifrar los mensajes.

Su funcionamiento es bastante simple y permite leer y escribir los mensajes tanto en la propia página del proveedor de correo (en un sandbox no accesible por el proveedor) o en una ventana emergente. Asimismo, como elemento de seguridad adicional, proporciona el uso de un token que está permanentemente visible y que nos garantiza que el entorno es seguro.

Como punto negativo, indicar que actualmente no permite enviar archivos adjuntos cifrados.

5.4. Cifrado de los datos almacenados en disco

Anteriormente en este apartado se ha repasado la herramienta Truecrypt; se describen a continuación dos de las alternativas para almacenar información de manera segura y confidencial.

5.4.1. DiskCryptor

DiskCryptor [131] es una solución open source para el cifrado en Microsoft Windows que permite encriptar, de manera transparente, el disco completo o solo particiones escogidas (incluidas las particiones de sistema), así como almacenamiento externo, como memorias USB, tarjetas SD, DVDs y CDs, etc.

Como algoritmos de cifrado pueden usarse AES-256, Twofish y Serpent, o cualquier combinación de estos. Además de la protección por contraseña, también permite el uso de *key files*.

Aunque se trata de un proyecto *open source* (Open license GNU GPLv3) y por tanto abierto al escrutinio público, no dispone aun de documentación completa.

5.4.2. Truecrypt

Se trata de un proyecto muy potente que interrumpieron sus impulsores.

Según su guía de uso, TrueCrypt es software libre open source (FOSS), multiplataforma disponible para Windows, OSX y Linux, que crea y gestiona volúmenes encriptados sobre la marcha; esto quiere decir que los datos son cifrados justo antes de ser almacenados y descifrados justo cuando se invocan por el usuario, de manera automática. Sin la clave o *keyfile* correcto no se puede acceder a la información. También se podían encriptar particiones o sistemas completos. Trabajaba con una gama muy amplia de algoritmos de encriptación; AES, Serpent, Twofish, etc. y su uso estaba muy extendido a nivel empresarial y personal, debido a su buen rendimiento y facilidad de uso.

Según Forbes [132], el propio Snowden la usaba y la recomendaba (en una *CryptoParty* en Hawaii en diciembre de 2012).

TrueCrypt interrumpió el soporte y desarrollo de la aplicación inesperadamente en mayo de 2014. Anunciaba en su página web [133] que “el uso de Truecrypt no es seguro y puede contener agujeros de seguridad no resueltos”. El cierre coincidió con el fin de la primera fase de una auditoría de seguridad, de la que salió airoso. Se ha especulado con un cierre similar al de Lavabit, con que el proyecto hubiese sido hackeado o que la NSA estuviese detrás de este proyecto.

Las auditorías de seguridad, realizadas en el marco del Open Crypto Audit Project [134] por nccgroup, se han completado sin evidencia de vulnerabilidades de diseño críticas o puertas traseras deliberadas en su código. "La auditoría no encontró evidencia de puertas traseras u otro tipo de código malicioso deliberado. […] Las vulnerabilidades encontradas parecen ser no intencionadas y serían resultado de bugs”. Hay iniciativas, basadas en Suiza, para continuar con el proyecto y seguir prestando soporte [135].

5.5. Cifrado de los datos almacenados en la nube

Uno de los proveedores de almacenamiento en la nube más populares es dropbox; sin embargo, tiene algunas contraindicaciones por las que es aconsejable optar por otras alternativas. Según dropbox [136], los datos en tránsito están cifrados con Secure Sockets Layer (SSL) y mientras están almacenados la cifra es con AES-256bit, sin embargo las claves las almacena la propia dropbox. Esto recuerda a las *key escrow* del apartado 2.2.5. De esta manera, los datos almacenados en este proveedor estarían a disposición de una petición de la NSA prácticamente sin impedimento. Frente a las soluciones propietarias como dropbox, existen opciones open source que almacenan el contenido cifrado en la nube y cuya clave de cifrado solo conoce el dueño de los datos; esto permite asegurar, con un alto grado de certidumbre, que el acceso a los datos estará solo a disposición de él.

Por nombrar alguna de ellas, Seafile [137] es un sistema open source multiplataforma de almacenamiento en la nube que permite compartir contenidos por grupos. Los contenidos se almacenan y se transfieren cifrados; se agrupan por “librerías” a elección del usuario, pudiendo sincronizarlas de manera independiente. Cada librería puede ser cifrada con una contraseña diferente, que no se almacena en el servidor, por lo que el administrador no puede acceder a los contenidos cifrados. Es sistema se basa en un servidor central contra el que se sincronizan los ordenadores y dispositivos móviles a través del cliente Seafile. La licencia del escritorio y los clientes móviles de Seafile es GPLv3. La del servidor web es la licencia de Apache. Todo el código fuente está publicado en Github.

Otra opción es SparkleShare [138], una herramienta open source para compartir contenidos de manera segura (protocolo SSH) y sencilla (plataforma Git) y está disponible para distribuciones Linux, Mac y Windows. El soporte para Android y dispositivos iOS está todavía por desarrollar.

Estas herramientas permiten al usuario asumir la labor de *hosting*, lo que supone tener el control absoluto sobre los datos.

5.6. Cifrado de los datos en tránsito

Algunos de los programas de vigilancia descritos en el punto anterior, tienen la capacidad de ver la información en tránsito; solo si la información circula cifrada estará a salvo de miradas indiscretas. Una respuesta clásica a este problema es la implantación del protocolo de navegación seguro https. Sin embargo, ocurre con frecuencia que muchos sitios web ofrecen un servicio https seguro bastante limitado (por ejemplo, la página por defecto no está protegida y opera en http o bien las páginas nos redirigen a enlaces no seguros). Para ello, se han implementado soluciones como la que se describe a continuación, HTTPS Everywhere.

5.6.1. HTTPS Everywhere

Se trata de un proyecto conjunto desarrollado por el proyecto Tor y la Electronic Frontier Foundation, EFF. Se parte de la base. HTTPS Everywhere [139] es un *add-on* para Mozilla Firefox, Google Chrome y Opera que reescribe de manera inteligente las peticiones http para que, allí donde sea posible, redirija el tráfico a páginas securizadas con el protocolo https, garanrizando así la navegación segura. Es importante hacer notar que no todas las páginas web funcionan con HTTPS Everywhere.

Como buena parte de las herramientas sugeridas en este apartado, HTTPS Everywhere está abierto al

escrutinio público y su código fuente está disponible [140] para colaboración y/o estudio.

5.7. Comunicaciones de voz seguras

Según el profesor Esteban Moro, de la Universidad Carlos III de Madrid [141], “el móvil que llevamos en nuestro bolsillo se ha convertido en un sensor ubicuo y muy interesante para conocer cómo se comportan las personas y, por agregación, nuestra sociedad: recoge datos de cómo, cuándo y con quién nos comunicamos, dónde estamos o cómo nos movemos. Esto hace que sea posible estudiar el comportamiento humano y de nuestra sociedad a un nivel espacial, temporal y social sin precedentes”. El profesor pone el foco en los beneficios que este seguimiento puede tener; sin embargo, los actores involucrados en estas tecnologías son una amenaza para la privacidad de los ciudadanos.

La interceptación de llamadas se ha convertido en una industria; tanto las Agencias de Inteligencia como empresas especializadas interceptan llamadas rutinariamente en busca de información de carácter político, económico, etc. El equipo necesario para interceptar llamadas de teléfonos móviles es tan asequible que su uso se ha generalizado en ciertos entornos

Es por ello que se han puesto en marcha varios proyectos para ocultar los contenidos de nuestras comunicaciones. Estas soluciones deben pasar por ofrecer algoritmos abiertos al estudio por expertos; la alternativa son sistemas propietarios cuya calidad no puede ser verificada y cuya potencia de cifrado quizás es ya insuficiente. Por ello, es conveniente no confiar en productos que son una “caja negra” A continuación, destacamos algunos de ellos:

5.7.1. Cryptophone

GSMK es una empresa alemana que ofrece un conjunto de productos para la comunicación y mensajería segura y llamadas de voz cifradas en un dispositivo diseñado a prueba de las técnicas de la NSA; el Cryptophone [142]. Trabaja en entornos GSM, 3G/UMTS, satélite y con líneas de telefonía fija.

La seguridad viene integrada de serie sin tener que preocuparse de su configuración; protege tanto las comunicaciones que se realizan como los datos en el dispositivo mediante algoritmos de cifrado publicados abiertamente para tener la seguridad de su eficiencia y de que no hay puertas traseras. El dispositivo está fuertemente bastionado con un sistema operativo con gestión granular de la seguridad. Además, el sistema de almacenamiento protege mediante cifrado la lista de contactos, los mensajes y, por supuesto, las claves. La información confidencial está almacenada a prueba de pérdida o robo.

Las llamadas se cifran con claves de 256 bits usando AES y Twofish, lo que proporciona una red de protección para el caso improbable que uno de los sistemas tuviera alguna vulnerabilidad o fallo. Para la comunicación vía SMS se trabaja en modo CCM, lo que garantiza autenticación y confidencialidad. Todo ello con intercambio de claves Diffie-Hellman de 4096 bits y hashes de verificación.

Todo ello abierto para su estudio y escrutinio.

Fig. 25 – Distintos productos de GSMK (fotografías extraídas de [142])

5.7.2. RedPhone

RedPhone [143] es un proyecto que permite realizar de manera sencilla llamadas telefónicas cifradas de extremo a extremo en Android, usando VoIP (utiliza SRTP para cifrar la conversación y ZRTP para negociar la clave privada que se intercambian los dos interlocutores para establecer el canal seguro). De esta manera, se pueden realizar llamadas gratuitas seguras a todo el mundo.

Al tratarse de una comunicación sobre VoIP, la llamada telefónica requerirá una conexión de datos, bien a través de la conexión 3G propia de la línea móvil o bien mediante una conexión Wi-Fi.

RedPhone utiliza un servidor central que hace las veces de pasarela y pone en contacto a los usuarios, usando como identificador el número de teléfono habitual.

Se trata de un proyecto FOSS, por lo que el código fuente está accesible (y por tanto auditable) en GitHub [144].

5.8. Mensajería segura

A la hora de proteger las conversaciones online, por mensajería o chat, se puede recurrir a la solución integrada en el Tor Bundle, el TorChat, que utiliza el protocolo onion de Tor y ofrece un entorno anónimo y descentralizado. Otra buena opción es usar una solución basada en el estándar Off-The-Record, OTR. Se trata de un protocolo que proporciona cifrado fuerte para las conversaciones de mensajería instantánea sobre el servicio de mensajería que se elija, siempre que soporte OTR. Utiliza el algoritmo AES de claves simétricas, el protocolo de intercambio de claves Diffie-Hellman y la función hash SHA-1. Además de la autenticación y el cifrado, OTR aporta confidencialidad perfecta.

5.8.1. Off-the-Record Messaging – Pidgin

El protocolo OTR proporciona una biblioteca cliente para que los usuarios que lo deseen, puedan implementar el protocolo. Existe un complemento para Pidgin [145] y un complemento para Kopete que permiten que OTR sea usado sobre cualquier protocolo IM soportado por Pidgin o Kopete, ofreciendo autodetección.

La ventaja de usar OTR es que se oculta la identidad de los participantes y la confidencialidad de la conversación, frente a otras soluciones en las que al salir se genera un registro de la comunicación que podría proporcionar la identidad de los participantes.

Pidgin es un cliente de mensajería instantánea multiplataforma (Windows, Linux, Unix...). Permite conectarse a múltiples redes (AIM, Jabber, MSN, Yahoo!, etc.); es una solución FOSS escrita en C y que usa las librerías Glib y GTK+.

Los mensajes pueden ser cifrados utilizando plugins; si se quiere usar el protocolo OTR, el plugin apropiado es OTR-Plugin11.

5.8.2. TextSecure

WhisperSystems, la empresa que está trás RedPhone, también ofrece a los usuarios el servicio TextSecure [143] (para Android y iPhone) que permite enviar mensajes de texto, SMS, MMS y mensajes de datos mediante un protocolo de cifrado de extremo a extremo, convirtiéndolo así en un modo de comunicación privado y confidencial; como en el caso de RedPhone, su código fuente también está disponible en Github [146]. La comunicación se hace sobre redes WiFi, 3G o LTE

El sistema permite crear grupos, compartir ficheros y archivos multimedia. La comunicación es completamente confidencial, pues los servidores ni almacenan los datos ni tienen acceso a la información (no tienen acceso al contenido ni a los metadatos de la comunicación).

Como RedPhone es un proyecto FOSS.

5.9. Sistemas Operativos seguros

Entendiendo por ello Sistemas Operativos que disponen de diversas funcionalidades de seguridad, como por ejemplo, que previenen la instalación o ejecución de malware y el acceso de atacantes a los programas en ejecución, que ofrecen facilidad para crear VPNs y túneles de acceso seguro a dominios a priori inseguros conexiones, etc.

5.9.1. tails

Tails [147] (The Amnesic Incognito Life System) es un sistema operativo basado en Debian GNU/Linux diseñado específicamente para los que quieren proteger de manera integral su actividad online frente a los intentos de espionaje descritos. Para ello, además de los programas habituales de este tipo de distribuciones (escritorio GNOME, procesador de textos LibreOffice, navegador Firefox, editores de

imagen y sonido, etc.), concentra buena parte de las herramientas para la protección que hemos venido describiendo en este capíitulo, entre las que destacan el navegador Tor, la herramienta de mensajería Pidgin (preconfigurada para Off-the-Record Messaging), el cliente de correo Claws, Aircrack-ng, I2P, un sencillo cliente de bitcoin, la trituradora de documentos Nautilus Wipe, etc.

Tiene la particularidad de que, como está diseñado con la seguridad como principio rector, las aplicaciones que tienen vulnerabilidades han sido eliminadas de la distribución. Además, todas las comunicaciones en todos los programas están cifradas con https y solo pueden tener lugar a través de Tor, siendo bloqueadas si tratan de conectarse a internet sin pasar por Tor. Utiliza el sistema de cifrado Luks, para cifrar discos duros y memorias USB, y GnuPG (la implementación GNU de OpenPGP) para cifrar los correos. Incluye otras herramientas muy útiles como Florence (teclado virtual para evitar keyloggers hardware), PWGen (generador de contraseñas robustas), KeePassX (gestor de contraseñas), etc.

Se trata de una distribución que también permite su uso en modo live; es decir, que puede invocarse desde un DVD, tarjeta SD, memoria USB, etc. pudiendo usarse en cualquier ordenador, independientemente del sistema oeprativo que este tenga instalado. Es muy util cuando necesitamos acceder a un ordenador que no es el nuestro, ya que nos permite operar en él sin miedo a ser "observados", por lo que es una de las herramientas que recomienda Marta Peirano en su libro “El pequeño libro rojo del activista en la red” [148].

5.9.2. Qubes

Qubes [149] es un Sistema Operativo open source, basado en Xen y Linux, especialmente diseñado para proporcionar seguridad, según el principio de la compartimentación. Se trata de un Sistema Operativo que puede ejecutar casi todas las aplicaciones de linux y utilizar la mayoría de sus drivers.

Qubes se rige por el principio de Security by Isolation; esta estrategia se basa en la creación de múltiples dominios de seguridad, implementados como máquinas virtuales ligeras que se ejecutan en el hipervisor Xen; la filosofía consiste en que, si un atacante comprometiera uno de los dominios, no sería capaz de acceder a los otros dominios gracias a esta filosofía de aislamiento.

Los programas se ejecutan en dominios, pero no una aplicación por dominio. Se crean dominios de seguridad que se agrupan por similitud; por ejemplo, podría crearse un dominio de “trabajo”, un dominio “personal” y un dominio “inseguro”. Cada dominio contendrá las utilidades que necesita para operar correctamente, de manera que no se desperdicien recursos. En el escenario descrito, el dominio “trabajo” se equiparía con aplicaciones de ofimática y se le dotaría de unas medidas de seguridad fuertes; el dominio “personal” estaría dotado de herramientas del gusto del usuario en la línea de sus aficiones como el tratamiento de imágenes o de juegos online, aplicando un nivel de seguridad apropiado. Por último, el dominio que hemos denominado “inseguro”, serviría para ejecutar esas aplicaciones que no nos ofrecen confianza o para navegar por sitios de dudosa reputación; eso sí, usaremos este dominio con la tranquilidad de que no tenemos nada valioso en el dominio y de que, en caso de que se viera comprometido, las pérdidas estarían limitadas al dominio “inseguro” y no se propagarían a los otros dominios.

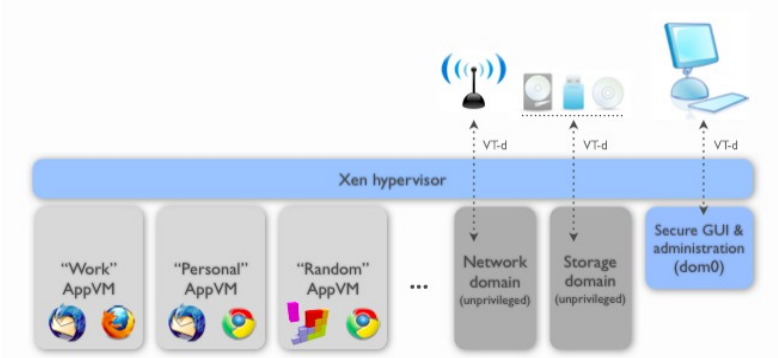

Fig. 26 – Filosofía del principio de “Security by Isolation” de Qubes (gráfico extraído de [149])

5.10. Transacciones económicas *online*

La actividad económica es una dimensión de las actividades diarias que puede revelar mucho de nuestra personalidad, nuestras preferencias ideológicas, políticas y de estilo de vida. Las transacciones económicas electrónicas (banca online, tarjetas de crédito, medios de pago tipo PayPal) están muy centralizadas y son muy susceptibles de seguimiento y tratamiento. Si añadimos además el hecho de que los grandes del sector (VISA, Mastercard, PayPal) son compañías que residen en Estados Unidos, se evidencia que cualquier transacción económica que hagamos con estos medios pasará por sus servidores y, de manera similar a lo que veíamos en los programas Upstream, será susceptible de ser inspeccionada, almacenada y analizada sin límites.

Aquellos ciudadanos celosos de su privacidad, estarán muy interesados en encontrar un medio de pago electrónico que proporcione la privacidad y anonimato que ofrece el dinero en efectivo. Existen varios proyectos trabajando en esta dirección, pero el Bitcoin es quizás el que más se ha extendido y popularizado.

5.10.1. Bitcoin

Bitcoin [150] es una moneda virtual (casi) anónima y descentralizada p2p, sin autoridad central, sin posibilidad de censura o control estatal. Bitcoin apareció en 2009 a partir de un artículo matemático de Satoshi Nakamoto [151] que demostró la posibilidad de un sistema monetario distribuido y robusto basado en el cifrado y una red de intercambio de claves.

Para usar bitcoin es necesario tener instalado el software cliente de Bitcoin con el que se dispone de una cartera de Bitcoins en el ordenador, como por ejemplo, GreenAddress [152] o Bither [153]. Una vez hecho esto, se pueden gastar y recibir bitcoins como si fueran transferencias de o desde una cuenta de banco.

Los bitcoins se pueden crear en un complicado proceso llamado minería que consume una gran cantidad de recursos del ordenador; la otra opción, más sencilla, es comprarlos.

El bitcoin sería lo más parecido a operar con efectivo en la red; sin embargo, bitcoin no es anónimo del todo, ya que genera registros que son públicos. Todas las transacciones de Bitcoin son públicas, rastreables y permanecen almacenadas en la red Bitcoin. Las direcciones Bitcoin son la única información usada para definir donde se encuentran y donde han sido enviados los bitcoins. Estas direcciones son creadas de forma privada por el monedero del usuario. Sin embargo, una vez que se utilizan, quedan marcadas por la historia de todas las transacciones involucradas. Cualquier persona puede ver el saldo y operaciones de cualquier dirección. Dado que los usuarios usualmente tienen que revelar su identidad para recibir bienes o servicios, las direcciones Bitcoin no pueden permanecer completamente anónimas. Es por ello que las direcciones Bitcoin deberían ser usadas una única vez y tener cuidado de no revelarlas.

Por contrapartida, el bitcoin ha demostrado tener una alta volatividad y su contravalor ha experimentado altibajos muy pronunciados que, si bien pueden beneficiarnos, también podrían reducir nuestra cartera al mínimo.

5.11. Videovigilancia

La videovigilancia [154], combinada con técnicas de reconocimiento facial y bases de datos de geoposicionamiento nos pueden situar en un lugar concreto en un momento determinado [155]. La ciudad de Londres [156] es un ejemplo de ciudad extremadamente videovigilada, a pesar de la protección que ofrece la legislación europea de protección de datos. Frente a estos excesos, también se han planteado contramedidas que lindan con el activismo ciudadano y la instalación artística [157]:

- Una de estas iniciativas es la del artista Leo Selvaggio, al que se le ocurrió que, si todo el mundo tuviera la misma cara, el reconocimiento facial sería inútil. Así, diseñó una máscara que es la recreación hiperrealista de sus facciones, pudiendo fabricarse con una impresora 3D. El proyecto se llama URME Surveillance y la idea es que cualquiera pueda llevar esta máscara puesta en la calle. De esta forma, se daría la circunstancia de que hubiera cientos de Leos caminando por las calles. La máscara guarda el suficiente detalle como para confundir a los algoritmos de reconocimiento facial.

Fig. 27 – Máscara del proyecto URME Surveillance (extraído de [157])

Otro proyecto en la misma línea es el de Adam Harvey. Su propósito es evitar, mediante maquillaje, que el software de tratamiento de las imágenes de videovigilancia pueda identificar a una persona al leer su rostro. Harvey estudió el funcionamiento de la tecnología de reconocimiento facial y concluyó que la solución sería camuflar con maquillaje los patrones en los que ésta se basa a la hora de analizar las imágenes para dificultar la identificación.

Fig. 28 – Maquillajes anti-videovigilancia propuestos por Adam Harvey (extraído de [157])

Si bien se trata de proyectos un tanto extravagantes, podría ser el germen de una respuesta a esta realidad.

5.12. Tabla resumen

Programa	Almacenamiento cifrado	Cifrado en tránsito	Anonimato	Open source o similar
Navegador TOR		X	X	X
I2P		X	X	X
DuckDuckGo			X	X
Dark Mail	X	X		X
Mailvelope	X	X		X
Diskcryptor	X			X
Truecrypt	X			X
Seafile	X	X		X
SparkleShare	X	X		X
HTTPS Everywhere		X		X
Cryptophone	X	X		X
RedPhone	X	X		X
OTR-Pidgin		X		X
TextSecure		X		X
tails	X			X
Qubes	X			X

Tabla 2 – Resumen de las aplicaciones anti-espionaje

El hecho de poner “Open Source o similar” es señalar que se trata de código fuente disponible para su escrutinio.

6. Tendencias

Tras la enumeración de algunos de los programas de vigilancia de la NSA y de la selección de herramientas disponibles para intentar evitar estas intromisiones indeseadas, podría parecer que, en algunos casos, se ha alcanzado un punto de equilibrio y, en otros, poco se puede hacer contra el espionaje más invasivo.

Un tema que, sin duda, marcará el futuro de la vigilancia masiva en el mundo es la puesta en marcha de la USA Freedom Act [38], aprobada el día 2 de junio. Será necesario ver las garantías que ofrece para con la privacidad de los ciudadanos – americanos y no americanos – y, por supuesto, el grado de implantación y seguimiento que tenga. En teoría, la legislación previa, si se hubiese acatado correctamente y el tribunal FISC [35] hubiese ejercido su labor de control, era suficiente.

A continuación se detallan algunas tendencias o prosprecciones a futuro de lo que podemos esperar en los próximos años.

6.1. Contramedidas a TOR

En el apartado dedicado a herramientas de defensa hemos visto el Proyecto Tor. Este proyecto ha tenido un doble éxito; su eficacia frente a los intentos de espiar el contenido de las comunicaciones y su popularización entre las personas que valoran su privacidad. Este éxito ha propiciado que la NSA asigne recursos adicionales para vulnerar la seguridad que proporciona Tor; su éxito y el hecho de que esta red se haya convertido en una de las vías principales de entrada a la denominada Deep Web, ese conjunto de páginas de internet no indexadas, cuyos contenidos no siempre son legales.

Este dominio secreto a ojos de las Agencias de Inteligencia es un desafío que quieren desvelar a toda costa; ya han conseguido algunos logros y seguirán poniendo los medios para lograrlo.

La NSA ha logrado avances con el programa denominado “EgotisticalGiraffe” [158], explotando una vulnerabilidad del navegador Firefox que no había sido resuelta en Tor:

Fig. 29 – Diapositivas filtradas del programa EgotisticalGiraffe

Otro éxito contra la red Tor fue una operación internacional conjunta denominada “Onymous” [159] que se jactó de haber hecho grandes progresos de criptoanálisis, al haber logrado romper los mecanismos de seguridad de la red Tor y que los propios desarrolladores de esa red han sido incapaces de identificar [160].

Esta sospecha se confirmó recientemente, cuando investigadores italianos y americanos publicaron un artículo científico, en el que describían cómo pudieron revelar el origen del tráfico anónimo de Tor con un 100% de efectividad en laboratorio y con un 81.4% en la red [161].

Por último, cabe indicar que no solo la NSA pretende acceder al núcleo de Tor y todo lo que esconde; se ha hecho público un anuncio en el que la Administración rusa busca especialistas para la

"investigación técnica" de esta red anónima [162].

Así, frente a lo que se pudiera pensar, la red Tor no es la panacea para la privacidad de las comunicaciones y puede asegurarse que las Agencias seguirán asignando recursos hasta tener acceso fácil e inmediato a la red anónima por antonomasia.

6.2. Open source

En la exposición hecha hasta ahora, cuando se ha hablado de herramientas para contrarrestar los intentos de espionaje de los estados, se ha dado preferencia a las herramientas basadas en open source. Básicamente, por dos razones;

- porque las eventuales vulnerabilidades del software de código abierto quedarían a la vista gracias al escrutinio público al que este está sometido; se tiende a pensar que las vulnerabilidades se descubren antes en sistemas abiertos
- la experiencia ha demostrado que los sistemas propietarios pueden estar albergando puertas traseras para derivar datos a las Agencias; así pues, una eventual puerta trasera en el código abierto sería descubierta por la comunidad; por no hablar del hecho que un eventual atacante descartaría implantar una puerta trasera en uno de estos productos abiertos

Así, parece evidente que es preferible optar por herramientas que hagan bandera de transparencia y al escoger una herramienta FOSS, estaríamos trabajando con software abierto al escrutinio público; una puerta trasera, una vulnerabilidad serían rápidamente identificadas y la versión del programa puesta en cuarentena, pero... ¿seguro que es así?

Hay opiniones bien fundadas que consideran que la creencia de que los proyectos open source son siempre más seguros, más confiables es, en realidad, un mito.

En su estudio "Is open source Security a Myth?" [163], Guido Schryen demostraba empíricamente que esta creencia no tiene fundamento. Después de realizar un análisis comparativo de la seguridad en sistemas open source *versus* sistemas closed source, llegó a la conclusión que no difieren en la severidad de sus vulnerabilidades, el tiempo para identificar la vulnerabilidad o el comportamiento de publicación de parches. Parece que la diferencia estaría más en el comportamiento de cada proveedor concreto que en otra cosa.

Por otro lado, cabe citar a Pablo González, de ElevenPaths, que impartió la charla "Osb-rastreator: easy way for looking for bugs in open source" en el marco de la pasada Hackron 2015 de Santa Cruz de Tenerife. El contenido de su ponencia mostró la implementación de un conjunto de scripts que permiten detectar funciones inseguras en código escrito en C. La detección de estas funciones no significa de manera automática que se haya encontrado una vulnerabilidad en el código, pero sí ayuda a realizar estadísticas del estado o calidad del código disponible en los repositorios utilizados por millones de usuarios. Si tenemos en cuenta que buena parte de los proyectos open source, basados en los diferentes sabores de unix y linux, tienen en su base el código escrito en C, podemos aplicar sus conclusiones al repositorio de aplicaciones open source. Su herramienta le ha permitido encontrar vulnerabilidades en el código, introducidas por el uso de funciones no seguras, muchas de las cuales llevan años sin ser corregidas. Desafortunadamente, muchas de estas vulnerabilidades podrán ser heredadas por nuevas aplicaciones que se basan en estas rutinas "defectuosas" y podrán llegar a convertirse en una puerta de entrada para las amenazas.

En definitiva, el verdadero problema de los sistemas propietarios es que son una caja negra de cara al usuario, lo que impide averiguar si existen puertas traseras o no. La incidencia de vulnerabilidades, la rapidez de publicación de parches no son un factor de elección entre open y closed source. Además, el mito de que el código abierto es más seguro también queda en entredicho por los descubrimientos de González. La verdadera ventaja de los sistemas open source es que están abiertos al escrutinio público.

Así pues, queda claro que la elección de proyectos open source no es necesariamente la opción más segura frente a vulnerabilidades, pero sí da la tranquilidad – relativa – de que el software está siendo analizado y comprobado por cientos o miles de desarrolladores globalmente.

6.3. Contramedidas a la encriptación

En apartados anteriores se han repasado los continuos intentos de los gobiernos y las agencias por controlar la criptografía. Inicialmente se trató de hacer por medios legales, obligando a que todos los sistemas criptográficos incluyeran una puerta trasera a disposición de las Agencias de Inteligencia o prohibiendo longitudes de clave imposibles de romper por la tecnología de la NSA; también se intentó con medios menos legales, como el caso descrito del chip Clipper.

Actualmente, parece que se están reactivando los movimientos gubernamentales en pro de la prohibición [164] o, al menos, en pro de la puerta trasera.

En un discurso ofrecido por David Cameron en París, tras el atentado contra la revista “Charlie Hebdo”, preguntó retóricamente “¿queremos un país que permita medios de comunicación entre personas que no seamos capaces de leer?” y comparó las herramientas de cifrado con las cartas o las llamadas telefónicas que pueden ser inspeccionadas con una orden judicial.

El debate también ha llegado a Australia (por accidente), pero lo cierto es que con la nueva ley aprobada, el personal investigador no podrá usar claves criptográficas de una longitud mayor a 512 bits [165].

Por último hacer mención al artículo de diario.es [166] en el que se hace referencia a esta tendencia; la Casa Blanca estaría maniobrando para exigir a las compañías tecnológicas debilitar la seguridad de sus claves de cifrado para poder leer las comunicaciones, así como reinstaurar el ya comentado *key escrow*.

Así pues, es posible que vayamos hacia un futuro en el que las claves criptográficas estén limitadas para poder ser escrutadas por las fuerzas de seguridad y agencias de inteligencia de los estados o hacia sistemas que, por ley, dispongan de puertas traseras.

6.4. Iniciativas de la UE

La repercusión de la vigilancia y espionaje masivos que reveló Snowden fue extraordinaria en todo el mundo, pero en la Unión Europea el impacto fue aún mayor, pues se hizo patente que el nivel de protección no era el mismo, en función de si se trataba de un ciudadano americano o no. Este agravio comparativo a que estaban siendo sometidos los ciudadanos europeos repercutía, además, en un derecho fundamental altamente valorado en Europa, el de la privacidad.

Los parlamentarios europeos expresaron su preocupación por los programas de vigilancia y condenaron el espionaje a que habían sido sometidos representantes oficiales de la Unión, solicitando se estudiaran las circunstancias en que se habían llevado a cabo estos programas y posible respuesta a los mismos.

Fruto de esta solicitud, se emitió un informe y dos estudios STOA, en los que se analizaron los programas de espionaje y se proponían líneas de trabajo en el medio y largo plazo.

El informe “The US surveillance programmes and their impact on EU citizen’ fundamental rights” [167] concluía con varias recomendaciones, de las que destacaría las siguientes:

- Reducir la exposición a los sistemas de información americanos y promover la creación de la nube europea: Dado que la jurisdicción americana no respeta los derechos de los europeos, ni tan siquiera los vinculados a tratamiento Safe Harbour (FISA y USA Patriot Act no lo tienen en cuenta), el informe aconseja dirigir su actividad online a empresas que se rigen por la normativa europea; como estas son minoritarias en el mercado actual, el informe anima a que se promueva la creación de una nube europea.
- El último borrador publicado del nuevo Reglamento Europeo de protección de datos de carácter personal, cuya aprobación está prevista para este año o el siguiente, había eliminado el artículo 42. A este artículo se le llamaba el artículo anti-FISA, porque protegía expresamente los datos de los ciudadanos europeos frente a accesos desde terceros países. La eliminación del artículo 42 es, en este contexto, inapropiada, por lo que el informe recomienda volver a incluirlo en la redacción definitiva del citado Reglamento.

Por otro lado, los dos estudios STOA [85][168], con sus correspondientes anexos [169][170], hacían también varias recomendaciones, de las que destaco las siguientes:

A corto y medio plazo:

- Que la UE adopte implementaciones de criptografía basadas en open source.
- La promoción de protocolos, implementaciones y sistemas abiertos.
- Regulación de la seguridad de las telecomunicaciones y de los estándares de cifrado.
- Inversión en concienciación de los ciudadanos
- Crear una normativa que exija a las aplicaciones informáticas que la configuración por defecto sea la de máxima protección de la privacidad.

A medio y largo plazo:

- Promover
    - la adopción del cifrado extremo a extremo: con medidas de concienciación y formación al ciudadano, mediante auditorías de seguridad de los productos criptográficos y promoviendo entornos amigables para su uso.
    - la adopción de open source: estableciendo la certificación de este tipo de productos y auditándolos periódicamente.
    - servicios ICT europeos: Cloud, redes sociales, motores de búsqueda... para evitar la dependencia de una internet norteamericana.
    - el desarrollo seguro de software: promoviendo guías de desarrollo seguro (p.e. OWASP) y certificando el producto software.
- Crear confianza con una subred europea en internet
- Acciones de innovación
    - Estimular el I+D en la detección del espionaje y en la reducción de la trazabilidad de las comunicaciones, es decir, mecanismos que hagan más complicado el rastreo de las comunicaciones.
    - Trabajar para modificar los protocolos inseguros de internet - ‘Fix the internet’ (bajo esta expresión, la UE pretende agrupar aquellas iniciativas que promuevan protocolos más seguros y la interrupción regulatoria de aquellos cuyos requisitos de seguridad no puedan ser corregidos).
    - Desplazar la filosofía de la seguridad al dato, abandonando el enfoque de la seguridad en la aplicación, es decir, apostar por tecnologías “*data-centric*”.

La contrapartida a las buenas intenciones de la UE podría estar en el futuro acuerdo TTIP, Transatlantic Trade and Investment Partnership, con Estados Unidos.

Este acuerdo de libre comercio tiene como objetivo ampliar el acceso de la UE al mercado estadounidense, pero su negociación ha venido acompañada de la controversia y una oposición generalizada, originada, en parte, por el secretismo con el que se está llevando a cabo.

Aún no queda claro cómo va a quedar la normativa europea de protección de datos si finalmente entra en vigor el Tratado. Sin embargo, podemos plantearnos varios escenarios: que se mantenga tal y como está ahora; que se endurezca (tal y como prevé el nuevo Reglamento UE); que se armonicen ambas legislaciones; o bien, que no se aplique la normativa europea a las relaciones entre USA y UE. Esto último no parece tan descabellado si tenemos en cuenta que en EEUU la normativa de protección de datos solo se aplicaba a ciudadanos estadounidenses (recientemente se ha planteado extender la protección también a los ciudadanos europeos).

El 65% de los servicios de comercio electrónico online en la Unión Europea proviene de Estados Unidos. Y en todas esas transacciones, hay datos personales. Jan Philipp Albrecht, eurodiputado verde

del Comité de Libertades Civiles, Justicia e Interior, advierte de que Estados Unidos está presionando para incluir provisiones que podrían socavar los estándares de protección de datos en la UE. Este es uno de esos asuntos donde la normativa a ambos lados del océano es completamente diferente, y en este asunto Rodríguez Piñero sí ve preciso que se garantice un alto nivel de seguridad. En EEUU ni siquiera existe regulación al respecto para las empresas.

La comisión de Comercio del Parlamento ha advertido recientemente que las normas de la UE sobre protección de datos no deben ponerse en riesgo por este acuerdo, por lo que tendrá que excluir expresamente todas las reglas vigentes y futuras en la UE sobre protección de datos personales de cualquier concesión. Las cláusulas sobre flujo de datos personales sólo podrán negociarse con Washington si se aplican las mismas reglas de protección “en ambos lados del Atlántico”, subraya el texto. La protección de datos no es negociable.

A la problemática y dudas del TTIP, cabe añadir el nuevo Reglamento UE comentado más arriba y ver cómo encajarán ambos.

6.5. Privatización del espionaje: el espionaje como negocio

La seguridad y los servicios de vigilancia asociados son un sector económico de grandes proporciones. Snowden [171] ha dado algunos datos que justifican la atracción de las empresas para formar parte de este negocio; el presupuesto de la NSA correspondiente al año 2013 superó los 52.000 millones de dólares.

Aunque oficialmente, la NSA es un organismo público, mantiene múltiples asociaciones con empresas del sector privado y ha externalizado muchas de sus funciones. Según los datos del libro de Greenwald [172], la NSA da empleo a unas 30.000 personas, pero tiene contrato con 60.000 más que pertenecen a compañías privadas. Según el analista Tim Shorrock, “el setenta por ciento de nuestro presupuesto de inteligencia se gasta en el sector privado” [173]. Asimismo, se señala que en las inmediaciones de las oficinas de la NSA en Fort Meade, Maryland, se congregan una gran cantidad de contratistas vinculados con la Agencia, como son Booz Allen Hamilton, SAIC, Northrop Grumman, etc.

A este conjunto de empresas contratistas, deben añadirse las empresas de telecomunicaciones y de servicios de internet que, como hemos visto, colaboran con la NSA.

A este conjunto de colaboradores – directos o indirectos – de la NSA habría que añadir aquellas empresas que prestan servicios de vigilancia en todo el mundo; lamentablemente, buena parte de sus clientes lo constituyen regímenes no democráticos (por poner un ejemplo, después de la primavera árabe, se descubrieron en Egipto y Libia [174] dispositivos de vigilancia de telefonía e internet de las empresas Gamma Corporation de Reino Unido, Amesys de Francia, VASTech de Sudáfrica y ZTE Corp de China).

Wikileaks publicó, en su día, los llamados “Spy Files” [102] que incluyen, a modo de catálogo, un buen número de herramientas comerciales que son capaces, por ejemplo, de escuchar comunicaciones, incluso cuando están encriptadas.

En definitiva, el dinero es un acicate para cualquier industria y el sector de la seguridad se beneficia de este interés, innovando y trabajando, sobre todo, en colaboración con las Agencias para llegar siempre más allá.

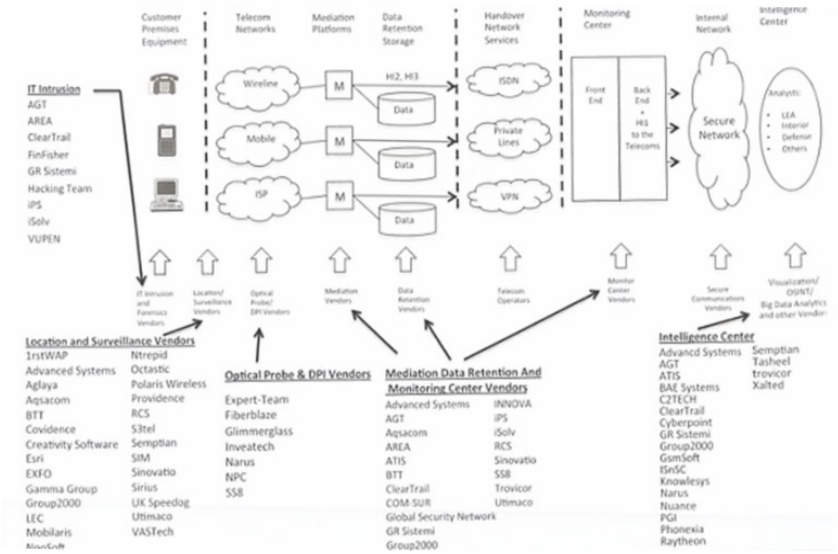

Fig. 30 – Proveedores de servicios de vigilancia y espionaje (gráfico extraído de [168])

6.6. Avances tecnológicos

Los sistemas basados en la criptografía, tal y como la conocemos hoy día, serán vulnerables en cuanto sistemas de computación cuántica empiecen a estar disponibles. Sin embargo, en ese hipotético escenario, las herramientas criptográficas también comenzarán a hacer uso de esta nueva tecnología, adoptando algoritmos que se beneficien de esa nueva capacidad de computación.

Según el Washington Post [175], la NSA ha destinado casi 80 millones de dólares al programa "Penetrating Hard Targets" que incluye investigación sobre el futuro desarrollo del "ordenador cuántico útil para la criptología" que permitiría la ruptura de todo el cifrado de clave pública, incluyendo la RSA. Esta herramienta sería capaz de romper cualquier tipo de cifrado mediante ataques de fuerza bruta, sin necesidad de conocer las claves [176].

Los esfuerzos para descifrar datos sin conocer sus claves de cifrado serán gigantescos, dependiendo de lo fuertes que sean la longitud y fortaleza de las mismas. Disponer de una capacidad de cálculo superior que pudiera ejecutar complejos algoritmos para analizar grandes cantidades de datos es lo que persiguen las Agencias de Inteligencia y, por eso, están invirtiendo en las tecnologías cuánticas y la investigación del grafeno [177]. Sin embargo, quedan todavía al menos cinco años hasta que la idea del ordenador cuántico pueda pasar del concepto teórico a una implementación física real [178].

Otro salto tecnológico cualitativo a tener en cuenta es la implementación física de la idea conceptual del cifrado homomórfico. Esta idea viene trabajándose desde el año 2009. Según el artículo de la wikipedia [179], basado a su vez en varios artículos del investigador Youssef Gahi, "los principios en los que se fundamenta el cifrado homomórfico pueden servir como punto de partida para mejorar los sistemas de seguridad (o aplicaciones) que almacenan y manipulan datos de carácter personal o sensibles. Esta garantía de protección deriva de la capacidad, que tiene el sistema de cifrado homomórfico, de realizar operaciones aritméticas sobre datos cifrados. Basándose en un sistema de cifrado completamente homomórfico, Youssef Gahi desarrolló el esquema básico, y el diseño de unos circuitos genéricos, fácilmente adaptables, que pueden preservar de manera efectiva la privacidad y confidencialidad entre diversos sistemas o aplicaciones. El modelo propuesto por Gahi, acepta datos de entrada cifrados y luego los procesa en función de las directrices marcadas por el usuario, sin llegar a descifrarlos nunca, y ofreciendo la garantía de que sólo el usuario que solicitó el procesado de los datos tiene la capacidad de descifrarlos. De esta manera, el sistema permite a los clientes utilizar determinados servicios, ofrecidos por aplicaciones o sistemas remotos, con la confianza de que no existe riesgo de que sus datos sean revelados, incluso cuando los servidores sean de dudosa reputación".

7. Conclusión

"Probablemente ya ha captado los inconvenientes legales de la metodología precrimen. Estamos deteniendo individuos que no han vulnerado ninguna ley."
"Pero, sin duda, lo harán", afirmó Witwer con convicción.
"Felizmente, no - porque llegamos a ellos antes de que hayan podido cometer un acto de violencia."
El informe de la minoría, Philip K. Dick

El objeto de este trabajo era describir el estado actual del espionaje y vigilancia masiva a los que somos sometidos, teniendo en cuenta lo desvelado por Edward Snowden en 2013, y hacer un repaso de las herramientas a nuestra disposición para hacerles frente.

Las escuchas autorizadas por orden judicial o los seguimientos justificados por sospechas razonables eran hechos aceptados como parte de herramientas de las fuerzas de seguridad de los Estados. Sin embargo, ese escenario tenía como requisito, normalmente, la supervisión de un juez y la proximidad física; había que poner un micrófono en el espacio vigilado, “pinchar” los cables telefónicos en la arqueta correspondiente o seguir al individuo bajo vigilancia en la calle... y una orden judicial.

Sin embargo, Snowden confirmó algo que muchos intuían; la vigilancia va, en muchos casos, más allá de lo razonable; cuantitativamente, porque se recoge toda la información y, cualitativamente, porque se hace sin una legitimación judicial clara; los elementos reguladores se convirtieron en una correa de trasmisión de las fuerzas de seguridad y de las Agencias de Inteligencia, como el propio tribunal FISC que autorizaba por defecto cualquier actuación que se le hacía llegar, incluso las masivas. La combinación de todos los sistemas de vigilancia masiva que hemos repasado recaban contenido y metadatos que, combinados con la videovigilancia masiva, el seguimiento de las transacciones económicas online y las capacidades de obtener datos de geoposicionamiento, suponen una foto muy precisa (e invasiva) de todos los ciudadanos. El propio Keith B. Alexander, director de la NSA hasta principios de 2014, afirmaba “necesito tener todos los datos”, por el mero hecho de tener la capacidad para hacerlo [180].

Los Estados se amparan en intereses legítimos, como la lucha contra el crimen organizado o la pedofilia, contra el tráfico de drogas o el terrorismo [181]; es un hecho que la “*deep web*” ofrece un ecosistema óptimo para los delincuentes... Sin embargo, también se intuyen otros usos ilegítimos de la vigilancia por parte de los Estados... intereses comerciales, intereses ante países rivales (o incluso aliados [182]) o intereses de control de la disidencia. Este trabajo se ha centrado en la actividad de países democráticos como Estados Unidos y la Unión Europea, pero cabe preguntarse ¿cuál será el resultado de este tipo de vigilancia en regímenes dictatoriales?

Los Estados están poniendo medios ilimitados para vulnerar nuestras defensas (recuérdese el centro de datos de Utah); reiterados intentos, a lo largo de los años, para romper la criptografía, instalación de puertas traseras en el software y en dispositivos físicos (electrónica de red, teclados, memorias USB, etc.). Al igual que sucede en la seguridad informática, el atacante (en este caso, las Agencias de Inteligencia) tiene la ventaja de poder poner todos sus medios para explotar una vulnerabilidad concreta, mientras que el que se defiende debe securizar todas las posibles vías de acceso. Si además, como es el caso, los medios no están equilibrados, el atacante las tiene todas consigo. El ciudadano solo tiene a su favor que es mayoría y que puede hacer frente a la amenaza colaborativamente, con herramientas y proyectos open source.

Este panorama se ve agravado por la colaboración de los proveedores de telecomunicaciones y servicios de internet y la incorporación a la vigilancia de grandes corporaciones, al servicio de los Estados, que han visto en la seguridad un gran negocio.

Se han repasado las contramedidas “defensivas” que tiene el ciudadano a su disposición que, bien aplicadas, son de gran utilidad, pero debe tenerse en cuenta que estamos ante la lucha de David frente a Goliath. Las Agencias de Inteligencia y las corporaciones a su servicio disponen de recursos económicos y tecnológicos incomparables a los de la comunidad que intenta hacer frente de manera colaborativa; estos últimos tienen a su favor una amplia base de colaboradores muy motivados, pero que siempre estarán en una posición de desventaja. Sin embargo, también hemos visto que el open source no es la panacea; si bien, proporciona herramientas escrutables y auditables, no son

necesariamente más seguras.

La Unión Europea está trabajando en la respuesta a este fenómeno; por un lado debe cuidar el aspecto normativo y, por otro, prepara una respuesta tecnológica a medio plazo. En el apartado legal, debe reinstaurar el artículo 42 en el borrador de la nueva Directiva de protección de datos... Por otro lado, deberá escrutar con especial cuidado los contenidos del TTIP. En el aspecto técnico, la Unión Europea estaría planificando la creación de un "ecosistema tecnológico" europeo que no nos ponga en manos de la tecnología norteamericana. Estaríamos hablando de soluciones criptológicas en el ámbito europeo, un "*gmail*" o un "*dropbox*" europeos, etc. Estos planes nos protegerían frente a las injerencias de los Estados Unidos, pero, teniendo en cuenta la colaboración que ha obtenido la NSA de agencias europeas, ¿estaríamos a salvo del escrutinio de nuestros propios gobernantes?

Por otro lado, habrá que observar las implicaciones de la reciente aprobación de la USA Freedom Act (Ley de la Libertad de EE UU) que busca un término medio entre los defensores de un espionaje opaco y sin límites y los detractores sin resquicios del espionaje electrónico. El hecho de que se le retire a la NSA la capacidad de almacenar los datos sobre las llamadas telefónicas y que se pongan en manos de las compañías telefónicas, en principio, refuerza las garantías de privacidad para el ciudadano, ya que (en teoría) la NSA solo podrá acceder a estos datos caso a caso y previa autorización judicial.

Ante nosotros, un futuro tecnológico que abre nuevos interrogantes; ¿que sucederá cuando se hagan avances significativos en computación cuántica? ¿cómo afectará a la vigilancia la implantación del cifrado completamente homomórfico?

Todos estos interrogantes deben ser tenidos en cuenta, porque, como el propio Greenwald declara en "Snowden. Sin un lugar donde esconderse", "desde la época en que internet empezó a utilizarse ampliamente, muchos han detectado su extraordinario potencial: la capacidad para liberar a centenares de millones de personas democratizando el discurso político e igualando el campo de juego entre los poderosos y los carentes de poder. La libertad en internet – la capacidad de usar la red sin restricciones institucionales, control social o estatal, ni miedo generalizado – es fundamental para el cumplimiento de esa promesa. Por tanto, convertir internet en un sistema de vigilancia destruye su potencial básico. Peor aún, transforma la red en un instrumento de represión, lo cual ameneza con crear el arma más extrema y opresora de la intrusión estatal que haya visto la historia humana" [183].

8. Bibliografía y fuentes consultadas

[1] Internet Society, “Breve Historia de Internet”, http://www.internetsociety.org/es/breve-historia-de-internet, último acceso junio 2015
[2] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 16
[3] James Bamford, Wired Magazine, “The NSA is building the country’s biggest spy center (watch what you say)”, http://www.wired.com/2012/03/ff_nsadatacenter/all/1, último acceso junio 2015
[4] INTECO, “Guía de privacidad y secreto en las telecomunicaciones”, 26/09/2007
[5] ONU, Declaración Universal de Derechos Humanos, 1948, http://www.un.org/es/documents/udhr/, último acceso junio 2015
[6] Consejo de Europa, Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, 1950, http://www.echr.coe.int/Documents/Convention_SPA.pdf, último acceso junio 2015
[7] Consejo de Europa, Convenio número 108, 1981, http://conventions.coe.int/treaty/en/Treaties/Html/108.htm, último acceso junio 2015
[8] Parlamento Europeo, Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:31995L0046, último acceso junio 2015
[9] Parlamento Europeo, Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:31997L0066, último acceso junio 2015
[10] Parlamento Europeo, Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF, último acceso junio 2015
[11] Parlamento Europeo, Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF, último acceso junio 2015
[12] Tribunal de Justicia de la Unión Europea, http://curia.europa.eu/juris/liste.jsf?num=C-293/12&language=es, último acceso junio 2015
[13] Parlamento Europeo, Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012PC0011&from=ES, último acceso junio 2015
[14] Constitución Española, 1978, https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229, último acceso junio 2015
[15] Tribunal Constitucional, Sentencia de 30 de noviembre de 2000, respecto de los arts. 21.1 y 24.1 y 2 de la LOPD, http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/Sentencia292.pdf, p. 21, último acceso junio 2015
[16] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, https://www.boe.es/boe/dias/1992/10/31/pdfs/A37037-37045.pdf, último acceso junio 2015
[17] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf, último acceso junio 2015
[18] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf, último acceso junio 2015
[19] Agencia Española de Protección de Datos, Transferencias internacionales de datos, https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php, último acceso junio 2015
[20] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, http://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf, último acceso junio 2015
[21] Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, http://www.boe.es/boe/dias/1982/05/14/pdfs/A12546-12548.pdf, último acceso junio 2015
[22] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, http://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf, último acceso junio 2015
[23] Ley 9/2014, de 9 de mayo, de Telecomunicaciones, http://www.boe.es/boe/dias/2014/05/10/pdfs/BOE-A-2014-4950.pdf, último acceso junio 2015
[24] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, http://www.boe.es/boe/dias/2007/10/19/pdfs/A42517-42523.pdf, último acceso junio 2015
[25] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A. 2014, ISBN 978-84-666-5459-3, p. 13
[26] Cuarta Enmienda a la Constitución, 1791, https://www.law.cornell.edu/constitution/fourth_amendment, último acceso junio 2015
[27] Constitución de los Estados Unidos de América, 1789, https://www.law.cornell.edu/constitution, último acceso junio 2015
[28] The Privacy Act, 1974, http://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf, último acceso junio 2015
[29] The Freedom of Information Act, 1967, http://www.gpo.gov/fdsys/pkg/STATUTE-80/pdf/STATUTE-80-Pg250.pdf,

último acceso junio 2015
[30] SS8 Networks, “The ready guide to intercept legislation”
[31] Communications Assistance for Law Enforcement Act (CALEA), 1994, http://askcalea.fbi.gov/calea/, último acceso junio 2015
[32] USA Patriot Act, 2001, http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf, último acceso junio 2015
[33] Foreign Intelligence Surveillance Act (FISA), 1978, http://fas.org/irp/agency/doj/fisa/, último acceso junio 2015
[34] Omnibus Crime Control and Safe Streets Act, 1968, https://transition.fcc.gov/Bureaus/OSEC/library/legislative_histories/1615.pdf, último acceso junio 2015
[35] Electronic Privacy Information Center, EPIC, Foreign Intelligence Surveillance Court (FISC), https://epic.org/privacy/terrorism/fisa/fisc.html, último acceso junio 2015
[36] FISA Amendments Act, 2008, https://www.congress.gov/bill/110th-congress/house-bill/6304, último acceso junio 2015
[37] Marc Bassets, elpais.com, “El bloqueo político fuerza un breve cierre de un programa clave de la NSA”, 2015, http://internacional.elpais.com/internacional/2015/05/31/actualidad/1433081291_336371.html, último acceso junio 2015
[38] USA Freedom Act, 2015, https://www.congress.gov/bill/113th-congress/house-bill/3361, último acceso junio 2015
[39] Marc Bassets, elpais.com, “La NSA ve recortado su poder por primera vez desde el 11-S”, 2015, http://internacional.elpais.com/internacional/2015/06/01/actualidad/1433187787_378714.html, último acceso junio 2015
[40] Marc Bassets, elpais.com, “Obama firma la ley que impone límites a la NSA”, 2015, http://internacional.elpais.com/internacional/2015/06/02/actualidad/1433277585_519201.html, último acceso junio 2015
[41] ITU, “Technical Aspects of Lawful Interception”, ITU-T Technology Watch Report 6, mayo 2008
[42] National Security Agency, https://www.nsa.gov/public_info/declass/ukusa.shtml, último acceso junio 2015
[43] Duncan Campbell, duncancampbell.org, http://www.duncancampbell.org/content/echelon, último acceso junio 2015
[44] Steve Wright, “An appraisal of technologies of political control”, 1998, http://aei.pitt.edu/5538/, último acceso junio 2015
[45] Duncan Campbell, “Interception capabilities 2000 – Development of surveillance technology and risk of abuse of economic information”, 1999, http://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf, último acceso junio 2015
[46] Informes de la Comisión Church, 1975-1976, http://www.aarclibrary.org/publib/church/reports/contents.htm, último acceso junio 2015
[47] Informe de la Comisión Church, Libro III “Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans”, http://www.aarclibrary.org/publib/church/reports/book3/pdf/ChurchB3_1_COINTELPRO.pdf, último acceso junio 2015
[48] Bruce Schneier, “Project Shamrock”, 2005, https://www.schneier.com/blog/archives/2005/12/project_shamroc.html, último acceso junio 2015
[49] Electronic Privacy, Information Center, EPIC, Carnivore FOIA Documents, https://epic.org/privacy/carnivore/foia_documents.html, último acceso junio 2015
[50] Electronic Frontier Foundation, “EFF Position on FBI Carnivore Snooping System”, https://www.eff.org/effector/13/6, último acceso junio 2015
[51] Fox News, “FBI Ditches Carnivore Surveillance System”, 2005, http://www.foxnews.com/story/2005/01/18/fbi-ditches-carnivore-surveillance-system.html, último acceso junio 2015
[52] Michael Schwartzbeck, “The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies (U)”, 1997, http://www.foia.cia.gov/sites/default/files/DOC_0006231614.pdf, último acceso junio 2015
[53] Christiane Schulzki-Haddouti, Telepolis, “USA urges ban on encryption products over teh internet”, 1999, http://www.heise.de/tp/artikel/5/5124/1.html, último acceso junio 2015
[54] ComputerWeekly.com, “US abandons key scrow encryption plan”, 2001, http://www.computerweekly.com/news/2240042808/US-abandons-key-escrow-encryption-plan
[55] Ducan Campbell, Telepolis, “Only NSA can listen, so that’s OK”, 1999, http://www.heise.de/tp/artikel/2/2898/1.html, último acceso junio 2015
[56] CNN.com, “NSA key to Windows: an open question”, 1999, http://edition.cnn.com/TECH/computing/9909/03/windows.nsa.02/index.html?_s=PM:TECH, último acceso junio 2015
[57] Caspar Bowden, “The US surveillance programmes and their impact on EU citizen’ fundamental rights”, 2013, http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf, p.12
[58] Tim Shorrock, The Nation, “Obama’s Crackdown on Whistleblowers”, 2013, http://www.thenation.com/article/173521/obamas-crackdown-whistleblowers#, último acceso junio 2015
[59] Kevin Poulse, Wired Magazine, “Whistle-blower: Feds have a backdoor into wireless carrier – Congress reacts”, http://www.wired.com/2008/03/whistleblower-f/, 2008, último acceso junio 2015
[60] James Risen y Eric Lichtblau, The New York Times, “Bush Lets US Spy on Callers Without Courts”, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0, 2005, último acceso junio 2015
[61] USA Today, “NSA has massive database of American’s phone calls”, http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm, 2006, último acceso junio 2015
[62] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 56-65

[63] BBC News, “Only 1% of Snowden files published – Guardian editor”, 2013, http://www.bbc.com/news/uk-25205846, último acceso junio 2015
[64] Chris Strohm, Bloomberg, “Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers”, 2014, http://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says, último acceso junio 2015
[65] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p.160-161
[66] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 134-140
[67] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 115-116
[68] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 121
[69] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 127-133
[70] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 164, p. 190
[71] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 146, p. 183
[72] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 150-152
[73] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 167-168
[74] Luis Doncel, elpais.com, “El escándalo de espionaje pone en apuros al Gobierno de Merkel”, 2015, http://internacional.elpais.com/internacional/2015/04/30/actualidad/1430392574_182172.html, último acceso junio 2015
[75] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 173-174
[76] Tim Leslie y Mark Corcoran, ABC News, “Explained: Australia's involvement with the NSA, the US spy agency at heart of global scandal”, 2013, http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786, último acceso junio 2015
[77] Greg Weston, Glenn Greenwald y Ryan Gallagher, CBC News, “Snowden document shows Canada set up spy posts for NSA”, 2013, http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886, último acceso junio 2015
[78] Christian Fuchs, John Goetz y Frederik Obermeier, Süddeutsche Zeitung, 2013, http://www.sueddeutsche.de/politik/spionage-in-deutschland-verfassungsschutz-beliefert-nsa-1.1770672, último acceso junio 2015
[79] Online Post, 2013, “Denmark is one of the NSA’s 9-Eyes”, 2013, http://cphpost.dk/news14/international-news14/denmark-is-one-of-the-nsas-9-eyes.html, último acceso junio 2015
[80] Jacques Follorou, Le Monde, “La France, précieux partenaire de l’espionnage de la NSA”, 2013, http://www.lemonde.fr/technologies/article/2013/11/29/la-france-precieux-partenaire-de-l-espionnage-de-la-nsa_3522653_651865.html, último acceso junio 2015
[81] The Guardian, “NSA shares raw intelligence including American’s data with Israel”, 2013, http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents, último acceso junio 2015
[82] Kjetil Malkenes Hovland, The Wall Street Journal, “Norway Reveals It Monitored Phone Data”, 2013, http://www.wsj.com/news/articles/SB10001424052702303985504579207500439573552, último acceso junio 2015
[83] The Guardian, “GCHQ and European spy agencies worked together on mass surveillance”, 2013, http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden, último acceso junio 2015
[84] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.S., 2014, ISBN 978-84-666-5459-3
[85] Arkaitz Gamino García (y otros), European Parliament STOA, “Mass Surveillance Part 1 – Risks, Opportunities and Mitigation Strategies Study”, 2015
[86] The Guardian, “NSA collecting phone records of millions of Verizon customers daily”, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, último acceso junio 2015
[87] The Guardian, “Vodafone reveals existence of secret wires that allow state surveillance”, 2014, http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance, último acceso junio 2015
[88] Siobhan Gorman y Jennifer Valentino-Devries, The Wall Street Journal, “New Details Show Broader NSA Surveillance Reach”, 2013, http://www.wsj.com/articles/SB10001424127887324108204579022874091732470, último acceso junio 2015
[89] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 129
[90] Joe Kloc, The Daily Dot, “Forget PRISM: FAIRVIEW is the NSA’s project to ‘own the internet’”, 2013, http://www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/, último acceso junio 2015
[91] The Guardian, “GCHQ taps fibre-optic cables for secret access to world’s communications”,2013,

http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, último acceso junio 2015
[92] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 133-145
[93] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 140-144
[94] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 189-200
[95] BBC News, "Stuxnet worm hits Iran nuclear plant staff computers", 2010, http://www.bbc.com/news/world-middle-east-11414483, último acceso junio 2015
[96] rt.com, "Snowden confirms NSA created Stuxnet with Israeli aid", 2013, http://rt.com/news/snowden-nsa-interview-surveillance-831/, último acceso junio 2015
[97] Hispasec, Una al día, "Stuxnet o la vulnerabilidad que Microsoft nunca corrigió", 2015, http://unaaldia.hispasec.com/2015/03/stuxnet-o-la-vulnerabilidad-que.html, último acceso junio 2015
[98] Der Spiegel, “Quantum Spying: GCHQ Used Fake LinkedIn Pages to Target Engineers”, http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html, último acceso junio 2015
[99] Ryan Gallagher y Glenn Greenwald, The Intercept, ”How the NSA plans to infect millions of computers with malware”, https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/, último acceso junio 2015
[100] Joseph Menn, The Hufftington Post, “NSA Has Ability To Hide Spying Software Deep Within Hard Drives: Cyber Researchers ”, 2015, http://www.huffingtonpost.com/2015/02/16/nsa-computer-spying_n_6694736.html, último acceso junio 2015
[101] The Guardian, "Revealed: how US and UK spy agencies defeat internet privacy and security", http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security, último acceso junio 2015
[102] Wikileaks, "The Spyfiles", https://www.wikileaks.org/the-spyfiles.html, último acceso junio 2015
[103] National Intelligence Program Summary, 2013, http://www.documentcloud.org/documents/781820-black-budget-excerpts-from-washington-post.html#document/p1, último acceso junio 2015
[104] Kevin Poulsen, The Wired Magazine, "New Snowden leak reports 'groundbreaking' NSA crypto-cracking", 2013, http://www.wired.com/2013/08/black-budget/, último acceso junio 2015
[105] Tony Wu, Justin Chung y otros, “The ethics (or not) of massive government surveillance”, http://cs.stanford.edu/people/eroberts/cs201/projects/2007-08/ethics-of-surveillance/tech_encryptionbackdoors.html, último acceso junio 2015
[106] Bruce Schneier, “Did NSA Put a Secret Backdoor in New Encryption Satandard?”, 2007, https://www.schneier.com/essays/archives/2007/11/did_nsa_put_a_secret.html, último acceso junio 2015
[107] Joseph Menn, Reuters, "Exclusive: Secret contract tied NSA and security industry pioneer", 2013, http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220, último acceso junio 2015
[108] http://heartbleed.com/, último acceso junio 2015
[109] Michael A Riley, Bloomberg, "NSA Said to Have Used Heartbleed Bug, Exposing Consumers", 2014, http://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers, último acceso junio 2015
[110] http://gotofail.com/, último acceso junio 2015
[111] Bodo Möller,Thai Duong y Krzysztof Kotowicz, Google, “This POODLE Bites: Exploiting The SSL 3.0 Fallback”, 2014, https://www.openssl.org/~bodo/ssl-poodle.pdf, último acceso junio 2015
[112] techdirt, "Gemalto: Ok, Yes, We Were Hacked, And Yes Some SIM Cards May Be Compromised, But Not Because Of Us", 2015, https://www.techdirt.com/articles/20150225/07101530138/gemalto-ok-yes-we-were-hacked-yes-some-sim-cards-may-be-compromised-not-because-us.shtml, último acceso junio 2015
[113] The Guardian, “China's Huawei and ZTE pose national security threat, says US committee”, 2012, http://www.theguardian.com/technology/2012/oct/08/china-huawei-zte-security-threat, último acceso junio de 2015
[114] David E. Sanger y Nicole PerlRoth, The New York Times, “N.S.A. Breached Chinese Servers Seen as Security Threat”, 2014, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=1, último acceso junio 2015
[115] Jacob Appelbaum, Judith Horchert y Christian Stöcker, Der Spiegel, "Shopping for Spy Gear: Catalog Advertises NSA Toolbox", 2013, http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html, último acceso junio 2015
[116] Bruce Schneier, "Cisco Shipping Equipment to Fake Addresses to Foil NSA Interception", 2015, https://www.schneier.com/blog/archives/2015/03/cisco_shipping_.html, último acceso junio 2015
[117] Arkaitz Gamino García (y otros), “Mass Surveillance Part 1 – Risks, Opportunities and Mitigation Strategies”, 2015, p. 38
[118] Sally Adee, “The Hunt for the Kill Switch”, 2008, http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch, último acceso junio 2015
[119] Juan Jesús Velasco, eldiario.es, “Las puertas traseras que la NSA nunca reconocerá”, 2014, http://www.eldiario.es/turing/vigilancia_y_privacidad/Vulnerabilidades-puertas-traseras-NSA-reconocera_0_249525793.html, último acceso junio 2015
[120] Catálogo ANT, publicado por la EEF, https://www.eff.org/files/2014/01/06/20131230-appelbaum-

nsa_ant_catalog.pdf, último acceso junio de 2015
[121] www.lavabit.com, último acceso junio 2015
[122] http://www.baynote.com/infographic/big-brother-is-a-tech-company/, último acceso junio 2015
[123] https://www.torproject.org/projects/torbrowser.html.en, último acceso junio 2015
[124] https://www.torproject.org, último acceso junio 2015
[125] https://geti2p.net/es/, último acceso junio 2015
[126] https://duckduckgo.com/, último acceso junio 2015
[127] https://duckduckgo.com/privacy, último acceso junio 2015
[128] Michael Arrington, Techcrunch, “AOL Proudly Releases Massive Amounts of Private Data”, 2006, http://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/, último acceso junio 2015
[129] https://darkmail.info/home.html, último acceso junio 2015
[130] https://www.mailvelope.com/, último acceso junio 2015
[131] https://diskcryptor.net/wiki/Main_Page, último acceso junio 2015
[132] Runa A. Sandvik, Forbes, "That One Time I Threw A CryptoParty With Edward Snowden", 2014, http://www.forbes.com/sites/runasandvik/2014/05/27/that-one-time-i-threw-a-cryptoparty-with-edward-snowden/, último acceso junio 2015
[133] http://truecrypt.sourceforge.net/, último acceso junio 2015
[134] https://opencryptoaudit.org/, último acceso junio 2015
[135] https://truecrypt.ch/, último acceso junio 2015
[136] https://www.dropbox.com/help/28, último acceso junio 2015
[137] http://manual.seafile.com/, último acceso junio 2015
[138] http://sparkleshare.org/, último acceso junio 2015
[139] https://www.eff.org/es/https-everywhere, último acceso junio 2015
[140] https://github.com/EFForg/https-everywhere, último acceso junio 2015
[141]http://portal.uc3m.es/portal/page/portal/repositorio_noticias/noticias_generales/13BFE18760030969E05075A36FB0683B?_template=/SHARED/pl_noticias_detalle_pub, último acceso junio 2015
[142] http://www.cryptophone.de/, último acceso junio 2015
[143] https://whispersystems.org/, último acceso junio 12015
[144] https://github.com/WhisperSystems/RedPhone, último acceso junio 2015
[145] https://pidgin.im/, último acceso junio 2015
[146] https://github.com/WhisperSystems/TextSecure, último acceso junio 2015
[147] https://tails.boum.org/index.en.html, último acceso junio 2015
[148] Marta Peirano, “El pequeño libro rojo del activista en la red”, Roca, 2015, ISBN 978-84-9918-822-5
[149] https://www.qubes-os.org/, último acceso junio 2015
[150] https://bitcoin.org/es/, último acceso junio 2015
[151] Satoshi Nakamoto, “Biticoin: A Peer-to-peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, último acceso junio 2015
[152] https://greenaddress.it/es/, último acceso junio 2015
[153] https://play.google.com/store/apps/details?id=net.bither, último acceso junio 2015
[154] Fran Andradres, eldiario.es, “El avance de una videovigilancia y el análisis biométrico sin garantías ciudadanas”, 2013, http://www.eldiario.es/turing/vigilancia_y_privacidad/videovigilancia-analisis-biometrico-garantias-ciudadanas_0_149435381.html, último acceso junio 2015
[155] Peter Yost, “Nos vigilan”, https://www.youtube.com/watch?v=KjIeQyZlSMQ, último acceso junio 2015
[156] vintechnology.com, “Top 5 Cities with the Largest Surveillance Camera Networks”, 2011, http://www.vintechnology.com/journal/uncategorized/top-5-cities-with-the-largest-surveillance-camera-networks/
[157] Pablo G. Bejerano, eldiario.es, “Contra el reconocimiento facial: entre la protesta y el arte”, 2015, http://www.eldiario.es/turing/movimiento-anti-reconocimiento-facial_0_379712743.html
[158] The Guardian, "Attacking Tor: how the NSA targets users' online anonymity", 2013, http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity, último acceso junio 2015
[159] Europol, "Global action against dark markets on Tor network", 2014, https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network, último acceso junio 2015
[160] Torproject, "Thoughts and Concerns about Operation Onymous", 2014, https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous, último acceso junio 2015
[161] Sambuddho Chakravarty y otros, "On the Effectiveness of Traffic Analysis Against Anonimity Networks Using Flow Records", https://mice.cs.columbia.edu/getTechreport.php?techreportID=1545, último acceso junio 2015
[162] Simon Sharwood, The Register,"Putin: Crack Tor for me and I'll make you a MILLIONAIRE", 2014, http://www.theregister.co.uk/2014/07/25/putin_crack_tor_for_me_and_ill_make_you_a_millionaire/, último acceso junio 2015
[163] Guido Schryen, “Is open source Security a Myth?”, Communications of the ACM, 2011
[164] Andrew Griffin, The Independent, "WhatsApp and iMessage could be banned under new surveillance plans", 2015, http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html, último acceso junio 2015
[165] Richard Chirgwin, The Register, "Australia tries to ban crypto research – by ACCIDENT", 2015, http://www.theregister.co.uk/2015/01/14/australia_tries_to_ban_crypto_research_by_accident/, último acceso junio 2015
[166] Pablo G. Bejerano, eldiario.es, "El pulso que determinará el cifrado de Internet", 2015,

http://www.eldiario.es/turing/cifrado-internet-key-escrow_0_391961676.html, último acceso junio 2015
[167] Caspar Bowden, “The US surveillance programmes and their impact on EU citizen’ fundamental rights”, 2013, http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf
[168] M. van den Berg (y otros), European Parliament STOA, “Mass Surveillance Part 2 – Technology Foresight Study”, 2015
[169] Arkaitz Gamino García (y otros), European Parliament STOA, “Mass Surveillance Part 1 – Risks, Opportunities and Mitigation Strategies Annex”, 2015
[170] M. van den Berg (y otros), European Parliament STOA, “Mass Surveillance Part 2 – Technology Foresight, options for longer term security and privacy improvements Annex”, 2015
[171] Barton Gellman y Greg Miller, The Washington Post, "‘Black budget’ summary details U.S. spy network’s successes, failures and objectives", 2013, http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html, último acceso junio 2015
[172]Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p.126
[173] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p.126
[174] Arkaitz Gamino García (y otros), European Parliament STOA, “Mass Surveillance Part 1 – Risks, Opportunities and Mitigation Strategies Annex”, 2015, p. 57
[175] The Washington Post, "A description of the Penetrating Hard Targets project", http://apps.washingtonpost.com/g/page/world/a-description-of-the-penetrating-hard-targets-project/691/, último acceso junio 2015
[176] Steven Rich y Barton Gellman, The Washington Post, "NSA seeks to build quantum computer that could crack most types of encryption", 2014, http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html, último acceso junio 2015
[177] The Washington Post, "FASCIA: The NSA's huge trove of location records", http://apps.washingtonpost.com/g/page/world/what-is-fascia/637/#document/p1/a135288, último acceso junio 2015
[178] Arkaitz Gamino García (y otros), European Parliament STOA, “Mass Surveillance Part 1 – Risks, Opportunities and Mitigation Strategies Annex”, 2015, p. 99
[179] http://es.wikipedia.org/wiki/Cifrado_homom%C3%B3rfico, último acceso junio 2015
[180] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p.119
[181] Pierluigi Paganini, securityaffairs, "The ISIS advances in the DeepWeb among Bitcoin and darknets", 2015, http://securityaffairs.co/wordpress/36961/intelligence/isis-in-the-deepweb.html, último acceso junio 2015
[182] The Guardian, "GCHQ intercepted foreign politicians' communications at G20 summits", 2013, http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits, último acceso junio 2015
[183] Glenn Greenwald, “Snowden. Sin un lugar donde esconderse”, Ediciones B, S.A., 2014, ISBN 978-84-666-5459-3, p. 17