Revista de Pensamiento Estratégico y Seguridad CISDE

Recibido: 25-01-2017 / Revisado: 12-03-2017
Aceptado: 12-03-2017 / Publicado: 30-05-2017

CISDE Journal, 2(1), 2017

ECHELON y la vigilancia masiva: entre la seguridad y la protección de la privacidad

ECHELON and mass surveillance: between security and privacy protection

Antonio Pinel Mañas[1]

[1] Investigador independiente. Máster en Ciberseguridad y Ciberdefensa, España

antop@protonmail.com

RESUMEN. En 1980 se daba a conocer el nombre de una red de vigilancia masiva e indiscriminada, centrada en las comunicaciones del ámbito civil, y operada principalmente por la Agencia Nacional de Seguridad de los EE.UU: ECHELON.
En los años siguientes, en parte gracias a una investigación oficial realizada por el Parlamento Europeo, se corroboró su existencia, se detalló su funcionamiento y extensión y se cuestionó su legitimidad.
En 2001, tras los atentados de las Torres Gemelas y la aprobación de la ley USA PATRIOT, esta red alcanzó una magnitud que tan sólo se ha comenzado a vislumbrar al divulgarse algunos de los documentos de Snowden.
Ante la probable existencia de otros sistemas similares operados por otros países, posiblemente con intereses globales más lesivos, es imperativo reflexionar sobre su necesidad, su eficacia y su encaje con la defensa de los derechos básicos de privacidad.

ABSTRACT. In 1980, an indiscriminate mass surveillance system specialized in intercepting civil communications, was disclosed to the public under the name ECHELON.
The following years, in part due to an official investigation led by the European Parliament, this system was deemed as real, being its operating mode further detailed while calling onto question its legitimacy.
In 2001, following the World Trade Centre terror attacks and the subsequent passing of the USA PATRIOT Act, the mass surveillance system reached a magnitude that has only just begun to appear in sight after the disclosure of several Snowden documents.
Given the probable existence of similar systems run by other countries, perhaps with more harmful intentions, it is imperative to consider appropriately the real need for these systems, their effectiveness and monitor the protection of the right to privacy.

PALABRAS CLAVE: Echelon, Vigilancia masiva, Interceptación, Privacidad, Snowden, Xkeyscore, Seguridad.

KEYWORDS: Echelon, Mass Surveillance, Interception, Privacy, Snowden, Xkeyscore, Security.

1. Introducción

A raíz de las revelaciones publicadas en diversos medios a partir de junio de 2013 acerca de un sistema de interceptación de comunicaciones a nivel global liderada por los EE.UU., se procede en el presente trabajo a realizar una valoración sobre este sistema y sobre su encaje en las sociedades democráticas.

Para ello, en primer lugar se realiza una revisión de los antecedentes históricos de este sistema de vigilancia global, desde 1980, cuando se reveló su existencia bajo el nombre ECHELON, hasta la actualidad.

En segundo lugar, se recoge y evalúa el contenido de algunas de las sucesivas filtraciones de los documentos sustraídos por Edward Snowden cuando trabajaba como contratista para la NSA norteamericana, por parte de diversos medios de comunicación en varios países.

Finalmente, se agregan algunas reflexiones adicionales acerca de la veracidad de las filtraciones, su encaje con el derecho a la privacidad, y la proporcionalidad y naturaleza de estas interceptaciones indiscriminadas de las comunicaciones, para alcanzar un mayor entendimiento de la situación actual y obtener algunas recomendaciones futuras.

2. Vigilancia masiva sobre las comunicaciones

2.1. Periodo 1980-1995

Una de las primeras alusiones públicas a un sistema de vigilancia masiva que actuara sobre las comunicaciones internacionales se da en el año 1980, de forma simultánea, en el libro Policing the Police Volume 2 (Kettle, Campbell, Rollo y Hain, 1980), y en la revista británica New Statesman and Policy (Campbell y Melvern, 1980) En ambas publicaciones se desvelaba y denunciaba la existencia de una gran red de interceptación de comunicaciones liderada por la Agencia de Seguridad Nacional (NSA) de los EE.UU., llevada a cabo con la colaboración de agencias de inteligencia especializadas en la interceptación de señales de otras naciones.

A nivel europeo, y siempre de acuerdo a estas publicaciones, el protagonismo de la red denunciada recaía especialmente sobre la estación de interceptación de señales de Menwith Hill, en el Reino Unido, que quedaba bajo la responsabilidad de la agencia británica de inteligencia Government Communications Headquarters (GCHQ), y desde la que se interceptarían las señales de radio, teléfono y comunicaciones por satélite y cables submarinos. También destacaba la importancia de Menwith Hill en el control tanto de satélites destinados a la vigilancia como de elementos de vigilancia integrados en satélites comerciales.

Por último, se exponía la existencia de un acuerdo denominado UKUSA, firmado entre los EE.UU. y el Reino Unido y destinado, según los autores, al intercambio de información e inteligencia basadas en señales (SIGINT). Este acuerdo sería extensible a los países integrantes de la Commonwealth, destacando Australia, Canadá y Nueva Zelanda.

Treinta años después, y empezando en mayo de 2010, la NSA ha ido desclasificando parcialmente multitud de documentos relacionados con este acuerdo UKUSA y publicándolos en su página web[1] y en el Archivo Nacional del Reino Unido[2]. A pesar de tratarse de documentos con un número limitado de páginas legibles (el resto permanece clasificado), permiten confirmar sin lugar a dudas la información expuesta por Campbell en 1980.

De acuerdo a estos datos revelados por la NSA, la primera versión completa del acuerdo UKUSA se firmó en 1951, tras una serie de aproximaciones sucesivas y colaboraciones de distinta naturaleza que se iniciaron

[1] https://www.nsa.gov/news-features/declassified-documents/ukusa/

[2] http://www.nationalarchives.gov.uk/ukusa/

Pinel, A. (2017). ECHELON y la vigilancia masiva: entre la seguridad y la protección de la privacidad. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 2(1), 21-42.

con la Segunda Guerra Mundial. En el texto del acuerdo, tal y como sugerían Campbell y Melvern (1980), se resalta que aunque se firmó entre EE.UU. y el Reino Unido, los países de la Commonwealth tendrían un tratamiento especial para el intercambio de información.

En 1988, a raíz de la información clasificada que le había filtrado Margaret Newsham (consultora de Lockheed para la NSA), en una nueva publicación Campbell (1988) reveló la existencia de una red secreta denominada "ECHELON", establecida y operada en el marco del pacto UKUSA, y que constituía la estructura física de interceptación masiva de señales y su filtrado, afectando tanto a ciudadanos nacionales como a extranjeros.

Esta red estaría integrada por diversas estaciones de control de satélites, centros de monitorización y vigilancia, satélites específicos y redes de computadoras, todos ellos trabajando en el análisis y procesamiento de los millones de señales interceptados de forma continuada. De forma paralela, se mencionaba la red P-415 como una versión mejorada de la anterior red ECHELON (Campbell, 1988).

2.2. Periodo 1995-2001

En 1996 se publicaba el libro Secret Power: New Zealand's Role in the International Spy Network, (Hager, 1996) en el que se recogía una descripción, seguramente la más completa realizada hasta el día de hoy, de la vigilancia masiva ejercida sobre la población en general, y en particular la relacionada con la red ECHELON bajo la dirección de la NSA y con la colaboración estrecha de sus principales socios (Reino Unido y los otros 4 mayores países de la Commonwealth).

Hager (1996) describía un complejo sistema formado por multitud de estaciones secretas de interceptación de señales a nivel global, algunas de ellas especializadas en la interceptación y obtención de inteligencia de comunicaciones (COMINT).

Describía el sistema ECHELON como la red que integraba, aglutinaba y coordinaba todas estas instalaciones y que permitía que las computadoras en cada estación (denominadas "diccionarios") buscaran de forma automatizada comunicaciones que contuvieran o estuvieran relacionadas con palabras concretas introducidas por los analistas y operadores (nombres, direcciones, cuentas de correo electrónico...) y las registraran y transfirieran a las centrales de las 5 agencias: Australian Signals Directorate (ASD) de Australia, Communications Security Establishment (CSE) de Canadá, National Security Agency (NSA) de EE.UU., Government Communications Security Bureau (GCSB) deNueva Zelanda y Government Communications Headquarters GCHQ del Reino Unido (Hager, 1996, p. 29).

Las comunicaciones interceptadas abarcaban las señales satelitales (especialmente las realizadas a través de la red Intelsat[3]), las de radio y las terrestres, tanto en cables submarinos como en forma de microondas. Sobre estas últimas, destacaba el protagonismo de las embajadas como centros de interceptación de señales sobre el territorio ajeno, así como el de los satélites espía específicamente designados para interceptar estas ondas que no se reflejaban en la ionosfera (Hager, 1996, p. 38).

En 1987 se creó en el seno de la Unión Europea el Panel STOA (Science and Technology Options Assessment – traducible como Evaluación de Opciones de Ciencia y Tecnología), como un órgano del Parlamento Europeo, cuya primera y principal misión declarada era y es la de "[contribuir] al debate y al examen legislativo de temas científicos y tecnológicos de especial importancia política". Para ello, como se indica en el Artículo 1 del Reglamento STOA (Parlamento Europeo, 2009),

[3] Desde 1964 hasta 2001 Intelsat era una empresa intergubernamental, propietaria y operadora de una gran red de satélites que ofrecía servicios comerciales de comunicaciones a nivel global. A partir de 2001 la empresa Intelsat se privatizó contando en la actualidad con más de 50 satélites. En 2009 anunció un contrato por el cual operaría y pondría en órbita un satélite destinado a proveer comunicaciones a las Fuerzas Armadas de Australia.

> "(…) facilitará a las comisiones y otros órganos parlamentarios interesados estudios independientes, de alta calidad e imparciales desde el punto de vista científico e información para la evaluación de las repercusiones de la posible introducción o fomento de nuevas tecnologías e identificará, desde el punto de vista técnico, las opciones existentes en lo que respecta a la mejor manera de actuar."

Es decir, la función de STOA era facilitar a los europarlamentarios aquella información actualizada, objetiva y de calidad, relacionada con las nuevas tecnologías, necesaria para que dispusieran de las herramientas adecuadas en sus funciones parlamentarias.

En respuesta a una solicitud realizada a este panel en 1996 por Glyn Ford (diputado británico al Parlamento Europeo), el 6 de enero de 1998 se publicó un documento STOA titulado An appraisal of technologies for political control, firmado por Steve Wright y dirigido a analizar el estado del arte de las tecnologías utilizadas para el control político a nivel europeo e internacional. El capítulo 4 de dicho documento se destinó específicamente a la evaluación del desarrollo de las tecnologías de vigilancia.

En dicho capítulo se exponía cómo, tras la caída de la Unión Soviética, aquellas tecnologías electrónicas desarrolladas a finales la década de los ochenta para interceptar comunicaciones en el marco de la Guerra Fría, junto con los abultados presupuestos de defensa asociados, se transfirieron a los cuerpos y fuerzas de seguridad internos para actuar contra el crimen, las drogas y el terrorismo (Wright, 1998).

El texto recogía esencialmente la información expuesta en los años precedentes por Campbell (1980 y 1998) y por Hager (1996), afirmando que la totalidad de las comunicaciones dentro de Europa, en forma de correos electrónicos, comunicaciones telefónicas y fax, eran interceptadas de forma rutinaria e indiscriminada por parte de la NSA, para después de ser procesadas, ser derivadas a los EE.UU. a través del nodo de Menwith Hill (Wright, 1998, p.19).

Es destacable que dicha publicación, auspiciada por el Parlamento Europeo, es la primera con respaldo oficial en la que se exponía de forma específica este sistema ECHELON. Describía cómo, a diferencia de los sistemas con origen en el ámbito militar, ECHELON se había diseñado para controlar objetivos no militares (gobiernos, organizaciones y negocios) en todo el mundo, interceptando de forma indiscriminada y persistente cantidades ingentes de comunicaciones, extrayendo luego todo aquello considerado valioso.

En respuesta al documento, varios europarlamentarios formularon preguntas escritas tanto al Consejo de la UE como a la Comisión Europea. Las respuestas de ambas entidades fueron evasivas, posiblemente para no enturbiar las relaciones del resto de los países de la UE con el Reino Unido, protagonista europeo de la red ECHELON de acuerdo al informe STOA (Unión Europea, 2014, p. 13).

Tras la publicación de ese documento, la Comisión Permanente de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo realizó una solicitud oficial al panel STOA para investigar más en profundidad esta supuesta red de interceptación masiva dirigida por los EE.UU., llegando la respuesta un año después, en octubre de 1999, con la publicación del documento "Development of surveillance technology and risk of abuse of economic information" (Parlamento Europeo, 1999).

Dicho trabajo se dividía en 5 volúmenes:

El primero de ellos (Pegger, 1999) presentaba el estudio completo, un resumen de los cuatro estudios subsiguientes y además hacía una evaluación preliminar de la situación de la protección de datos y de los derechos humanos en el marco de la UE y del Parlamento Europeo.

El segundo (Campbell, 1999), más conocido por el nombre "Interception Capabilities 2000", describía en mayor profundidad la interceptación masiva en general, y la red ECHELON en particular, exponiendo las tecnologías existentes en el ámbito de las comunicaciones, tanto en su transmisión como en su interceptación.

A continuación, pasaba a formular por un lado cuestiones sobre la vulnerabilidad de las leyes y los derechos humanos relacionados con la privacidad y la intimidad, y por otro, cuestiones sobre el potencial beneficio comercial y económico de los EE.UU. al interceptar de forma masiva cualquier tipo de comunicación internacional en países o corporaciones de interés.

Exponía también algunos casos en los que estas actividades de interceptación supuestamente se habían utilizado para beneficiar a corporaciones norteamericanas frente a otras extranjeras en concursos o licitaciones internacionales, tales como Panavia, Thompson y Airbus (Campbell, 1999, p. 18).

Destacaba también una convergencia de cuerpos de seguridad e inteligencia de multitud de países, al menos desde 1993, auspiciada por el FBI norteamericano, bajo el paraguas de un seminario denominado International Law Enforcement Telecommunications Seminar (ILETS). Dichas reuniones, celebradas anualmente y sin supervisión parlamentaria, estaban destinadas a homogeneizar los requerimientos de los organismos responsables del cumplimiento de la ley de cada país en lo relativo a la interceptación de comunicaciones (Campbell, 1999, pp. 16-17).

El tercer volumen (Leprevost, 1999) se estructuraba en tres partes. La primera, contenía una revisión somera de las técnicas de criptografía y las tecnologías de encriptación disponibles, especialmente en el campo digital y electrónico. En la segunda, se exponían los riesgos existentes para la Unión Europea y sus ciudadanos asociados tanto a la imposición de restricciones a la libre difusión de tecnologías seguras de encriptación (como los relacionados con el Acuerdo Wasenaar), como a la utilización de tecnologías norteamericanas por parte de entidades o individuos no norteamericanos que, de forma desconocida para estos usuarios, facilitarían la obtención de comunicaciones y datos por parte de la NSA. Finalmente, en la tercera parte se planteaban una serie de recomendaciones al Parlamento encaminadas a revisar los riesgos mencionados.

El cuarto volumen (Elliot, 1999) exponía un estudio sobre los instrumentos legales que afectan a la interceptación de las comunicaciones en el marco de los tres intereses principales que identificaba como confluyentes: la privacidad de los individuos como derecho humano fundamental; las necesidades de los cuerpos de seguridad para el cumplimiento de las leyes y la seguridad nacional; y los requerimientos del comercio electrónico. En este documento se destacaba también el protagonismo de los operadores de las redes de comunicaciones en la provisión de servicios de forma que se garantizaran las necesidades de estos tres factores.

En el quinto y último volumen (Bogolikos, 1999), se realizaba un análisis de los estudios precedentes (volúmenes 2, 3 y 4), procediendo a extraer una serie de datos de partida. A continuación, mediante un procedimiento de prospectiva basado en la metodología Delphi, a través de un panel de 30 expertos, valoraba estos datos de partida para extraer finalmente unas conclusiones en forma de recomendaciones a la UE, buscando mejorar la protección de los intereses económicos de los países integrantes de la UE y de la privacidad de sus ciudadanos, sin perjudicar el trabajo de los organismos encargados del cumplimiento de las leyes y de la seguridad nacional de cada país.

Poco después de la presentación del informe completo, el 25 de febrero de 2000 la Presidenta del Parlamento Europeo, Nicole Fontaine, reconocía en unas declaraciones que,

> "(…) uno puede sentirse legítimamente escandalizado con el hecho de que este espionaje, que ha ocurrido durante años, no haya llevado a protestas oficiales. Para la Unión Europea, intereses esenciales están en juego. Por una parte, parece probado que ha habido violaciones de los derechos fundamentales de los ciudadanos; por otra, el espionaje económico puede haber tenido consecuencias desastrosas, en empleo por ejemplo" (como se citó en Piodi y Mombelli, 2014, p. 14).

El 30 de marzo de 2000 se trató este asunto en el Parlamento Europeo, acudiendo a dicho debate representantes de la Comisión y del Consejo, para exponer sus posiciones sobre la existencia del sistema

ECHELON. Nuevamente, las posturas oficiales de ambos órganos no fueron determinantes salvo para incluir dos respuestas escritas procedentes de los gobiernos del Reino Unido y de EE.UU. y dirigidas a la Comisión, en las que el primero negaba actuar fuera de las leyes comunitarias, y el segundo negaba participar en ningún tipo de espionaje industrial[4].

Los europarlamentarios no quedaron satisfechos con estas explicaciones y solicitaron a la Presidencia del Parlamento la creación de una comisión para investigar la existencia y el funcionamiento de ECHELON, y sus efectos sobre los países de la UE. Si bien se presentó una solicitud para crear una comisión de investigación, finalmente se optó por crear una Comisión Temporal, a instancias del europarlamentario español Enrique Barón[5].

La comisión, informalmente conocida como "Comisión Echelon", se constituyó formalmente el 6 de junio de 2000 y con una duración definida de 12 meses, el máximo permitido. Carlos Coelho fue nombrado presidente, mientras que Gerhard Schmid fue nombrado el responsable de organizar y presentar en un informe los trabajos llevados a cabo. La comisión entrevistó a multitud de investigadores, expertos, tecnólogos y funcionarios para tratar de entender la magnitud de la red de vigilancia, los efectos del posible espionaje industrial relacionado y también para definir el papel de la encriptación en la seguridad de las comunicaciones en el seno de la UE.

De entre todos los documentos y declaraciones que se consideraron, merece la pena destacar las declaraciones de un antiguo director de la CIA, William Webster, como se cita en Piodi y Mombelli (2014): "Nuestros aliados políticos y militares también son nuestros rivales económicos, y la habilidad de una rival económico para crear, ganar o controlar mercados en el futuro tiene implicaciones para los EE.UU." (p. 23).

Cuando le llegó el turno a la Comisión Europea de exponer su postura ante la Comisión Echelon, su respuesta se mantuvo en la línea de las respuestas dadas a las preguntas escritas realizadas por los parlamentarios con anterioridad. Dos de las declaraciones no hicieron ninguna referencia a la red ECHELON, mientras que la de Christopher Patten, Comisionado de Asuntos Externos, sí mencionaba ECHELON de forma tangencial, explicando que la CE estaba en proceso de definir un nuevo marco legal bajo el que tratar la información confidencial (Piodi y Mombelli, 2014, p. 26).

Con respecto a la postura del Consejo Europeo, quedó básicamente definida con la comparecencia de Hervé Masurel, representante de la presidencia francesa en ejercicio, el 28 de noviembre de 2000, donde resaltaba que la interceptación de señales era importante para la lucha contra el crimen, pero se consideraba inaceptable su uso para obtener ventajas económicas. Respecto a ECHELON, declaró no conocer evidencias de que se utilizara para estos fines (Piodi y Mombelli, 2014, p. 26).

Poco después, el 6 de febrero de 2001, compareció Desmond Perkins, director de la unidad responsable de encriptación en la Comisión Europea, en calidad de experto en asuntos de cifrado. De su declaración, es destacable el momento en que dijo, como se cita en Piodi y Mombelli (2014): "Siempre he tenido muy buenos contactos con la Agencia Nacional de Seguridad en Washington, y habitualmente revisan nuestros sistemas [de encriptación] para comprobar si están correctamente mantenidos y no son utilizados de forma incorrecta" (p. 36).

Esta desconcertante declaración, en la que un representante de la Comisión Europea reconocía abiertamente y ante una comisión temporal del Parlamento Europeo que la NSA tenía acceso al sistema de

[4] Parlamento Europeo. (30 de marzo de 2000) Transcripción del debate ante el Parlamento Europeo, Bruselas. Disponible en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20000330+ITEM-002+DOC+XML+V0//ES

[5] Parlamento Europeo. (13 de abril de 2000). Minuta de la Conferencia de Presidentes, Estrasburgo. Pág. 18. Disponible en http://www.europarl.europa.eu/RegData/organes/conf_pres_groupes/proces_verbal/2000/04-13/CPG_PV(2000)04-13_EN.pdf

cifrado del principal órgano ejecutivo de la UE, provocó un considerable revuelo que llevó a la Comisión Europea a enviar a dos oficiales para desmentir y matizar la información, asegurando que se trataba de un malentendido.

Como parte de las investigaciones llevadas a cabo por la Comisión Echelon, se organizaron tres misiones internacionales: una a Londres, otra a Paris y la última a Washington. Las dos primeras permitieron a los parlamentarios reunirse con funcionarios de alto nivel de los ministerios de defensa, interior y exteriores.

La tercera, del 6 al 11 de mayo de 2001, fue en cierta forma un fracaso, dado que diversas agencias de inteligencia y seguridad (CIA y NSA) y los organismos de exteriores (Department of State) y comercio (Department of Commerce) de los EE.UU. rehusaron en el último momento recibir a los europarlamentarios que integraban la misión.

El 13 de julio de 2001 se aprobó el informe definitivo liderado por Gerhard Schmid, que fue posteriormente sometido a debate en el Parlamento el 5 de septiembre de 2001 y aprobado con 2 enmiendas menores. Las conclusiones de dicho informe (Parlamento Europeo, 2001, pp. 133-136) se pueden resumir en:

- No hay ninguna duda de que existe un sistema para interceptar comunicaciones a nivel global, operado por EE.UU, el Reino Unido, Canadá, Australia y Nueva Zelanda bajo el acuerdo UKUSA. Ese sistema, o partes de él, se llaman o llamaron en algún momento ECHELON.
- El objetivo de dicho sistema es el de interceptar comunicaciones privadas y comerciales, pero no militares.
- Sin embargo, las capacidades técnicas de dicho sistema son mucho menores de lo que algunos sectores han sugerido.
- Hay evidencias de que otros países, como Rusia, operan sistemas similares.
- Una interceptación permanente y arbitraria de las comunicaciones no es compatible con el Convenio Europeo de Derechos Humanos (CEDH), y en especial con el Artículo 8 sobre el derecho al respeto de la vida privada y familiar, que dice "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia" (Consejo de Europa, 1950).
- Un parte de la actividad de los servicios de inteligencia de los EE.UU. se centra en la obtención de inteligencia económica exterior, para evaluar el seguimiento de embargos, el suministro de bienes de uso dual, las tendencias de los mercados de mercancías, etc. Por ello, se somete a vigilancia a empresas extranjeras y se interceptan sus comunicaciones, justificando estas acciones además en la lucha contra la corrupción, y esa información obtenida corre el riesgo de ser utilizada como inteligencia competitiva. Sin embargo, no existen evidencias de que el sistema ECHELON se haya utilizado en ese sentido.

Adicionalmente, hacía un llamamiento a Alemania y al Reino Unido al respecto de la actividad de las bases integrantes de ECHELON existentes sobre su territorio, operadas por los servicios de inteligencia de los EE.UU., para poder dar cumplimiento al CEDH (Parlamento Europeo, 2001, p. 139).

Finalmente, de cara a incrementar la seguridad, se recomendaba encarecidamente tanto el uso de sistemas de encriptación de las comunicaciones, como el uso de programas cuyo código fuente fuera abierto y público, a diferencia de otros sistemas como Microsoft Windows o Microsoft Office (Parlamento Europeo, 2001, p. 128).

Es destacable que en el Informe Final se recogían más de una decena de casos de espionaje industrial y/o de obtención de inteligencia competitiva analizados por la comisión, destacándose siete en los que había intervenido la NSA o la CIA, tales como los casos de Thomson-Alcatel vs. Raytheon, Airbus vs. McDonnell-Douglas, Enercon vs. Kenetech Windpower, o Volkswagen vs. General Motors (Parlamento Europeo, 2001, pp. 103-106). Este último caso, Volkswagen vs. General Motors, involucraba directamente a un ciudadano

español, José Ignacio López de Arriortúa, conocido coloquialmente como Superlópez[6].

Si bien el documento final aprobado por el Parlamento no fue especialmente contundente contra los EE.UU. o sus socios en la red de vigilancia masiva, ni daba al sistema el tamaño que se intuía, al menos reconocía su existencia e instaba a los países miembros de la UE a reflexionar sobre este asunto y a desarrollar marcos legales específicamente destinados a tratar con este tipo de acciones.

Invitaba también a todos los países de la UE a promover la creación de organismos parlamentarios que supervisaran las acciones de los servicios de inteligencia, y destacaba la necesidad para los individuos y empresas de utilizar una adecuada encriptación y a utilizar sistemas operativos y programas de código abierto.

2.3. Periodo 2001-2012

El informe fue aprobado el 5 de septiembre de 2001, pero 6 días después tuvieron lugar en suelo norteamericano los atentados de las Torres Gemelas, dirigidos contra el Pentágono, el World Trade Center y el Capitolio (o la Casa Blanca).

El 26 de octubre de 2001 se aprobó por mayoría absoluta tanto en la Cámara de Representantes como en el Senado de los EE.UU. la ley denominada USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism –traducible por "Uniendo y Reforzando América mediante la Provisión de las Herramientas Apropiadas para Interceptar y Obstruir el Terrorismo"). Esta ley, que en la práctica implicaba un incremento enorme del poder de los organismos de seguridad e inteligencia para actuar sin respaldo judicial, inédito en tiempos de paz, en detrimento de los derechos y libertades individuales, se mantuvo vigente hasta junio de 2015. Unos meses antes de su vencimiento, el presidente Obama en una rueda de prensa[7], a la vez que aseguraba que había que limitar las capacidades de interceptación indiscriminada de la NSA, decía que recebar estos datos, específicamente los metadatos de las llamadas, servía para prevenir ataques terroristas con bombas sobre suelo americano, por ejemplo. Un día después de la fecha de vencimiento se aprobó la nueva ley USA Freedom Act, que renovaba hasta 2019 las partes de la ley PATRIOT que habían quedado sin cobertura legal, a excepción de la Sección 215 (recogida de metadatos de llamadas telefónicas), que fue enmendada para restringir en parte a la NSA las capacidades que tenía para realizar vigilancia masiva sobre las comunicaciones telefónicas sin orden judicial. A pesar de ello, pocos meses después, el 27 de octubre de 2015 se aprobó en el Senado de los EE.UU. la ley Cybersecurity Information Sharing Act (CISA), que nuevamente otorgaba mayor poder a las agencias de seguridad e inteligencia para acceder a información personal de ciudadanos dentro y fuera de los EE.UU.

Un año después de los atentados de las Torres Gemelas, el 23 de octubre de 2002, en una comparecencia de la Comisión y del Consejo ante el Parlamento Europeo para tratar el tema del terrorismo, no se logró identificar ninguna acción concreta tomada tras la resolución adoptada el 5 de septiembre de 2001.

De entre multitud de temas tratados en ese debate, hubo un concepto recurrente que apareció en las comparecencias de varios parlamentarios, incluyendo la del Presidente del Consejo, Haager, y que se puede resumir en las palabras del eurodiputado portugués Sousa Pinta: "La determinación para erradicar el terrorismo y la urgente necesidad de establecer nuevos y efectivos instrumentos para lograrlo, no pueden, bajo ninguna circunstancia, afectar de forma desproporcionada a los derechos, libertades y garantías de los individuos" [8].

[6] El caso de Superlópez se analiza en mayor profundidad en la publicación: García, I. (2003). Libertad Vigilada: El Espionaje de las Comunicaciones. Barcelona. Ediciones B, S.A. Capítulo 27: "Echelon" contra "Superlópez".

[7] Disponible en https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

[8] Parlamento Europeo. (23 de Octubre de 2002). Transcripción del debate parlamentario. Estrasburgo. Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20021023+ITEM-003+DOC+XML+V0//EN&language=RO

Sin embargo, la sucesión de atentados graves ocurridos a escala global desde 2001 y de índole yihadista (EE.UU. en 2001, Indonesia en 2002, Rusia en 2002 y 2004, España en 2004, el Reino Unido en 2007, India en 2006 y 2008…), y la denominada "Guerra contra el terrorismo", campaña liderada por los Estados Unidos y apoyada por varios miembros de la OTAN y otros aliados, tuvo el suficiente peso como para impedir o apaciguar cualquier debate o actividad destacable en el marco de la lucha contra vigilancia masiva.

2.4. Periodo 2013-Actualidad

El 6 de junio de 2013, casi doce años después de aprobarse el informe de la Comisión Echelon, aparecía en el periódico The Guardian un artículo (Greenwald, 2013a)[9], en el que se filtraba una orden judicial emitida por el juez Roger Vinson del Tribunal de Vigilancia de la Inteligencia Extranjera (Foreign Intelligence Surveillance Court), por virtud de la cual se obligaba a la operadora de telecomunicaciones Verizon (una de las mayores de los EE.UU.) a proporcionar a la NSA a demanda, de forma continuada y diaria, la información en forma de "metadatos telefónicos" de todas las llamadas realizadas bajo su sistema, tanto las originadas como las destinadas dentro del territorio de los EE.UU.

De acuerdo a esta orden, los metadatos debían incluir, al menos, los números de teléfono de origen y destino, los identificadores IMSI e IMEI, la ubicación de la antena más cercana y la hora y duración de las llamadas (Tribunal de Vigilancia de la Inteligencia Extranjera de los EE.UU., 2013).

Con esta publicación quedaba expuesta la facilidad con la que el FBI, a través de la NSA podía acceder de forma continuada e indiscriminada a los registros de las llamadas telefónicas de los millones de usuarios de la red Verizon, con el respaldo de los tribunales de su país.

El día siguiente se publicó de forma simultánea en los periódicos The Washington Post y The Guardian una segunda noticia (Gellman y Poitras, 2013; Greenwald y MacAskill, 2013), esta vez relativa a PRISM, un programa que permitía a la NSA y al FBI obtener información directamente desde los servidores de varias empresas de internet, confirmándose así el inicio de la mayor filtración conocida de documentos altamente confidenciales de la NSA, que aún continúa a principios de 2017. La mayor parte de dichos documentos fueron sustraídos por Edward Snowden desde la red interna de la NSA mientras trabajaba para ellos como consultor con Booz Allen Hamilton.

El número de periódicos y portales que tuvieron acceso a los documentos de Snowden fue incrementando progresivamente, llegando a incluir a Der Spiegel, Zeit, El Mundo, El País, Le Monde, The New York Times y a The Intercept, entre otros.

3. Contenido de las filtraciones sobre la vigilancia masiva

3.1. Grupo Five Eyes

De entre dichos documentos publicados, aparecen multitud de referencias al grupo Five Eyes, a menudo abreviado como FVEY, principalmente en los encabezados o pies de documentos donde se indica el grado de clasificación, el tipo de información contenida y las personas o grupos con los que se puede compartir la información.

Uno de los documentos filtrados por Snowden es un boletín interno de la NSA llamado SIDtoday, del que aporta publicaciones que abarcan un período comprendido entre marzo de 2003 y octubre de 2005. En el número correspondiente al 5 de agosto de 2003[10], se hace referencia a un encuentro histórico mantenido

[9] A Glenn Greenwald se le otorgó el prestigioso premio Pulitzer en 2014 por el servicio público llevado a cabo al investigar sobre la NSA a lo largo de 2013, siendo esta su primera publicación al respecto.

[10] NSA. (5 de agosto de 2003). SIGINT Directors Set Strategic Direction for 5-Eyes SIGINT Enterprise. SIDtoday. Disponible en https://theintercept.com/snowden-sidtoday/3008302-sigint-directors-set-strategic-direction-for-5/

entre los directores SIGINT de los cinco países, en el que buscaban dar a su cooperación una nueva visión y establecer unas nuevas metas estratégicas.

En una entrevista a Edward Snowden (NDR, 2014), explicaba que Five Eyes consistía en una asociación de las agencias de inteligencia de EE.UU, Reino Unido, Canadá, Australia y Nueva Zelanda, que esencialmente constituyen el acuerdo UKUSA. En dicha entrevista Snowden definía el acuerdo FVEY como "una organización de inteligencia supra-nacional que no responde a las leyes de sus propios países" (como se cita en NDR, 2014).

3.2. Sistemas de interceptación expuestos

En la información publicada por Snowden, aparecen referencias a multitud de sistemas utilizados por la NSA y el GCHQ para la interceptación y vigilancia de las comunicaciones.

De ellos, por su magnitud, se destacan los siguientes:

3.2.1. PRISM - UPSTREAM

En la publicación de documentos sustraídos por Snowden del 7 de Junio de 2013, se incluía la descripción del programa denominado PRISM. En una de las imágenes de la presentación interna de la NSA[11] se describe un sistema doble (Gellman y Poitras, 2013):

- Una parte, denominada UPSTREAM, actúa sobre las redes físicas de comunicaciones de internet (incluyendo cables de fibra) a medida que la información es transmitida desde ellas o fluye por ellas a la salida y entrada de los EE.UU.
- La segunda, denominada PRISM, recoge información directamente desde los servidores de proveedores de servicios de internet ubicados en los EE.UU. como Google, Skype, Apple, Microsoft o Yahoo, en forma de correos electrónicos, chats, videos, fotos, credenciales de acceso, información almacenada, llamadas VoIP, intercambio de archivos, redes sociales... (Gellman y Poitras, 2013).

Como muestras de inteligencia concreta generada con este sistema, se exponen temas como el comercio de petróleo y de material militar en Venezuela; narcóticos, energía, seguridad interna y asuntos políticos en México y por último, tráfico ilícito y FARC en Colombia (Greenwald, 2014)[12].

Si bien el grado de clasificación de la presentación excluye la divulgación a agentes extranjeros (codificación NOFORN o NF), en otras láminas de la presentación se puede comprobar el acceso que se dio a los agentes británicos del GCHQ al sistema PRISM durante las olimpiadas de 2012 en Londres (Gallagher, 2014).

La relación entre ambas agencias de inteligencia no se limitó a este acceso puntual, existiendo otras láminas en que se describe el trasvase de información desde la NSA hacia el GCHQ a través de una base de datos en la nube denominada GHOSTMACHINE (Gallagher, 2014).

Es destacable que a raíz de estas revelaciones varios grupos de defensa de los derechos humanos entre los que se encontraban Privacy International y Amnistía Internacional, denunciaron el acceso del GCHQ (entidad británica) a los datos privados almacenados en los servidores de los gigantes de internet como Microsoft, Google o Apple a través de PRISM (sistema norteamericano). La Comisión de Inteligencia y Seguridad del

[11] En el blog ELECTROSPACES (http://electrospaces.blogspot.com/2014/04/what-is-known-about-nsas-prism-program.html) se puede encontrar un análisis más detallado del programa, que complementa lo descrito en el artículo de The Washington Post.

[12] Los documentos originarios del archivo de Snowden que han sido utilizados en el libro están disponibles en: http://us.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf. También en: https://web.archive.org/web/20130712225535/http://oglobo.globo.com/infograficos/big-brother-am-latina/

Parlamento británico inició una investigación que culminó con una atípica sentencia del Tribunal Especializado en Asuntos de Vigilancia declarando ilegal el acceso secreto a este sistema, "contraviniendo" principios de privacidad y libertad de expresión recogidas en la Convención Europea para los Derechos Humanos, no en tanto por la naturaleza de los datos, sino en cuanto a la forma de acceder a ellos (Gallagher, 2015a).

Con todo ello quedaba expuesta la magnitud del sistema PRISM, que en definitiva permitía a los principales organismos de inteligencia de los EE.UU. acceder directamente a los servidores de algunos de los principales fabricantes y proveedores de servicios de internet.

3.2.2. XKEYSCORE

Otro de los sistemas expuestos es XKEYSCORE (Greenwald, 2013b), también iniciado por la NSA, que según la presentación filtrada tenía como objetivo la creación de una base de datos mediante la captación de comunicaciones en internet, ralentizando de alguna forma la velocidad de estas comunicaciones y permitiendo así a los analistas tiempo adicional para separar información de interés de la irrelevante antes de ser desechada.

La cantidad de información obtenida cada día era enorme y abarcaba la mayor parte de lo que un usuario medio podía hacer en la red: mensajes instantáneos, historiales de navegación, correos electrónicos, metadatos… Esto se lograba almacenando la totalidad de los paquetes de comunicaciones durante 2-3 días, y sus metadatos asociados durante al menos 30 días, contando con 700 servidores dedicados distribuidos en países de todo el mundo (incluyendo en España, Brasil, China y Rusia) (Greenwald, 2013b).

La información considerada relevante era luego redirigida a otros sistemas de archivo o bases de datos donde la información se pudiera almacenar durante años.

La presentación filtrada expone algunos ejemplos concretos de utilización que demuestran la potencia del sistema (Greenwald, 2013b):

- Identificar movimientos anómalos en la red (uso de un idioma distinto del usado en el país en que se encuentra, uso de encriptación, búsqueda en la web de elementos sospechosos o marcados…).
- Identificar quién está utilizando encriptación PGP en un determinado país, o identificar todos los documentos Word encriptados en la web de ese país.
- Mostrar todos los inicios de sesión en VPN en un país determinado y obtener los datos necesarios para descifrar esa comunicación e identificar a los usuarios.
- Encontrar a un objetivo que habla un idioma pero está oculto en una región otro.
- Obtener información que me permita averiguar la dirección de correo electrónico de una persona que usa Google Earth para observar determinados objetivos.
- Averiguar quién ha escrito un documento jihadista que está circulando por internet.
- Obtener una base de datos en Excel que incluya todas las direcciones MAC y los registros de conexión para las computadoras utilizadas en una región de internet desde un determinado país.
- Averiguar todas las computadoras que pueden ser explotables en un determinado país.

El 23 de marzo de 2015, en The New Zealand Herald se filtraba un documento según el cual se habría utilizado el sistema X-KEYSCORE por parte de la agencia de inteligencia GCSB de Nueva Zelanda para investigar a los nueve candidatos a la posición de Director General de la Organización Mundial de Comercio –WTO, uno de los cuales era en un ministro neozelandés (Hager y Gallagher, 2015).

Con todo ello, quedaba expuesta la magnitud y potencia del programa X-KEYSCORE, que por la propia naturaleza de su estructura, actuaba a escala global profundizando en las redes de computadoras en general, y en Internet en particular.

Al respecto de las acusaciones emitidas por las autoridades norteamericanas sobre el involucramiento de

servicios de inteligencia rusos en el acceso no autorizado a servidores asociados con el Partido Demócrata[13] antes de las elecciones nacionales de los EE.UU. de 2016, Edward Snowden aseguraba por Twitter el 25 de julio de 2016 que, de haber realmente ocurrido, la herramienta idónea para rastrear los datos sustraídos sería precisamente X-KEYSCORE, como él aseguraba haber hecho desde la NSA con una operación similar contra China[14].

3.2.3. MUSCULAR

El programa MUSCULAR, cuya existencia se expone al público inicialmente en octubre de 2013, es operado de forma conjunta por la NSA y GCHQ, y supone la infiltración en las redes privadas de enlace entre los distintos centros de datos tanto de Yahoo como de Google repartidos por el mundo (Gellman y Soltani, 2013).

La NSA ya disponía del sistema PRISM, antes indicado, que les permitía acceder directamente de forma masiva a datos guardados en los servidores de muchas empresas operadoras de servicios de internet como Google y Yahoo dentro de los EE.UU., pero como muchos centros de datos de estas empresas se encuentran repartidos por el mundo, es probable que la obtención de información en el extranjero, al no tener los mismos condicionantes legales que PRISM en los EE.UU., requiriera un enfoque tecnológicamente distinto. Al interceptar directamente los flujos completos de información que circulan entre los centros de datos, el programa MUSCULAR es de más amplio alcance.

En una presentación filtrada (Gellman y DeLong, 2013), se expone que la cantidad de datos obtenidos con el sistema era inmanejable y en muchas ocasiones obstaculizaba más que ayudaba la labor de los analistas.

En la presentación no se describe cómo esta infiltración o interceptación tenía lugar, pero podría ocurrir en las redes de comunicaciones por fibra entre los centros de datos, en los nodos de salida de los cables submarinos o en los propios centros de datos compartidos.

3.2.4. TEMPORA, BLACK HOLE, y otros sistemas del GCHQ

El sistema TEMPORA, originado y operado por el GCHQ, es una versión británica y agrandada del sistema X-KEYSCORE norteamericano, y va dirigido a recopilar cantidades ingentes de información de comunicación originada tanto en internet como en llamadas de voz, principalmente a través de los cables de fibra óptica (MacAskill, Borger, Hopkins, Davies, y Ball, 2013).

En una presentación secreta del sistema TEMPORA es definido como un sistema masivo que utiliza 1000 centros de computación para procesar y presentar a los analistas más de 40 mil millones de paquetes de datos al día, siendo su tamaño mayor que el de los demás sistemas X-KEYSCORE existentes juntos (Stöcker y Horchert, 2013).

El 25 de septiembre de 2015 se revelaron además dos docenas de documentos relacionados con otras actividades y capacidades de vigilancia masiva del GCHQ (Gallagher, 2015b).

Basados en un enorme sistema de archivos planos denominado BLACKHOLE[15], que entre 2007 y 2012 contaba con más de un billón de entradas, y que incrementaba su tamaño en 10 mil millones de archivos al día, se describían multitud de sistemas como Mutant Broth, Karma Police, Infinite Monkeys, Marbled Gecko, Social Animal, Goob, Moose Milk, Lightwood, Autoassoc…

[13] La mayor parte de la información filtrada correspondiente a este acceso no autorizado se encuentra en forma de correos electrónicos, y se han publicado en la web Wikileaks (https://wikileaks.org/dnc-emails/).

[14] https://twitter.com/Snowden/status/757577131912208384?ref_src=twsrc%5Etfw

[15] Disponible en https://theintercept.com/document/2015/09/25/qfd-blackhole-technology-behind-inoc/

De entro ellos, es destacable el programa KARMA POLICE, cuyo objetivo, de acuerdo a una presentación del 29 de febrero de 2008, es:

"correlacionar cada usuario visible por [procedimientos] pasivos SIGINT, con cada página de internet que visita, proporcionando de ese modo bien (a) un perfil de navegación de internet para cada usuario visible en internet, o (b) un perfil de usuarios para cada página web visible en internet"[16].

Es decir, disponer de un inventario completo del comportamiento y los hábitos en internet de todas las personas visibles por el sistema.

En marzo de 2012, GCHQ registraba 50 mil millones de metadatos al día[17], previendo ampliar esta capacidad a finales de ese mismo año hasta los 100 mil millones al día.

Juntando las ambiciones declaradas con las capacidades expuestas, las filtraciones reflejaban que la vigilancia masiva del GCHQ poco tenía que envidiar a la de la NSA.

3.2.5. STATEROOM

El programa STATEROOM, operado bajo, entre otros, el Special Collection Service (unidad de acción conjunta entre la NSA y la CIA), y que se filtró con la noticia de la interceptación de las comunicaciones de la canciller alemana Angela Merkel, consistía en la utilización de embajadas y consulados de varios de los países Five Eyes para instalar en ellos de forma encubierta dispositivos especiales de interceptación y descifrado de comunicaciones telefónicas y digitales (Der Spiegel, 2013).

Las imágenes filtradas en el artículo[18] incluían, entre otros, mapas con la localización de estas unidades de interceptación de señales y una descripción de sus capacidades. Las señales interceptadas incluían microondas, WiFi, WiMAX, GSM, CDMA, satélite…

A raíz de la información expuesta por Der Spiegel, la canciller Angela Merkel realizó una llamada al presidente Obama para pedirle explicaciones. Si bien no se conoce el contenido de la conversación, una portavoz del Consejo de Seguridad Nacional de los EE.UU. envió al diario Der Spiegel un comunicado indicando que en dicha conversación el "presidente le había comunicado a la canciller que ni monitoreaba las comunicaciones de la canciller Merkel ni lo haría en el futuro" (como se cita en Appelbaum, Stark, Rosenbach y Schindler, 2013). No indicaba nada acerca de haberlo hecho en el pasado o no.

A finales de junio y principios de julio de 2015, el portal Wikileaks filtraba una serie de documentos[19] con los que confirmaba la interceptación de comunicaciones por parte de la NSA a diversos ministros y altos funcionarios del gobierno de Alemania, incluyendo a Angela Merkel, durante al menos una década.

Si bien la actividad del programa STATEROOM, interceptando de forma indiscriminada señales de comunicación de ciudadanos desde instalaciones diplomáticas, tiene un dudoso encaje tanto en el marco legal de su propio funcionamiento en territorio extranjero, como en el marco legal de la protección de privacidad, en la actualidad no es excesivamente complicado interceptar las comunicaciones de forma indiscriminada desde elementos que pueden ser ubicados en maletines, oficinas o en aeronaves (tripuladas o no).

Un ejemplo son los denominados "captadores de IMSI", que son dispositivos que simulan ser estaciones base de telefonía, atrayendo con mayor intensidad a los teléfonos que están en su radio de acción que las

16 Presentación disponible en https://theintercept.com/document/2015/09/25/pull-steering-group-minutes/

17 Presentación disponible en https://theintercept.com/document/2015/09/25/gchq-analytic-cloud-challenges/

18 Imágenes disponibles en http://www.spiegel.de/fotostrecke/photo-gallery-spies-in-the-embassy-fotostrecke-103079-2.html

19 Documentos disponibles en https://wikileaks.org/nsa-germany/

estaciones base auténticas, y que permiten a los operadores de estas bases simuladas interceptar y extraer datos individuales de los suscriptores, información sobre los teléfonos, metadatos de las comunicaciones y, en los modelos más avanzados, registrar a demanda conversaciones completas o mensajes enviados. La señal emitida desde el teléfono luego es remitida a la estación base genuina.

A este respecto, es destacable una investigación llevada a cabo por el equipo del medio noruego Aftenposten en diciembre de 2014 (Johansen, 2014).

En ella, el equipo trabajó en campo durante 6 semanas para tratar de averiguar si en la ciudad de Oslo había en funcionamiento algún dispositivo como el mencionado. Tomaron cincuenta mil mediciones a lo largo de 100 km, y llegaron a la conclusión de que al menos 122 de las incidencias detectadas en la red de telefonía móvil correspondían a artefactos de este tipo, encontrándose multitud de ellos en las proximidades de la oficina del Primer Ministro, el Parlamento, el ministerio de Defensa y el Banco Central.

Con los sorprendentes resultados obtenidos, y tras la ausencia de respuesta obtenida de los operadores de telefonía y la propia Policía cuando les comunicaron estos datos, los investigadores contactaron entre otros con dos firmas de seguridad y tecnología (Aeger Group y CEPIA Technology), quienes tras realizar averiguaciones por su cuenta, llegaron a una conclusión similar (Johansen, 2014).

Ante la falta de justificación oficial sobre este asunto, unos meses después los investigadores de Aftenposten requirieron a la empresa británica de seguridad Delma realizar un análisis forense sobre los hallazgos de su investigación del año 2014 (Foss, 2015).

Delma contó con una serie de expertos internacionales para elevar el documento a estándares de plena validez ante los tribunales y una de sus conclusiones fue que "[e]l trabajo de investigación en esta etapa mostró de forma concluyente que la interceptación [de comunicaciones de telefonía] móvil está ocurriendo en la Ciudad de Oslo" (McKay, 2015). Otra conclusión fue que de los lugares indicados en la investigación inicial, al menos 6 albergaban con muy alta probabilidad estaciones de interceptación como las descritas, siendo el resto de media o baja probabilidad.

La policía noruega (Police Security Service) publicó en julio de 2015 un informe de 17 páginas (CRNA, 2015) en el cual consideraba que la información publicada por Aftenposten y refrendada por la empresa Delma era inconcluyente.

Más recientemente, en septiembre de 2016, se publicaron algunos manuales de propietario de dispositivos como los mencionados, aparentemente dirigidos a cuerpos policiales, que mostraban un grado de avance suficiente como para suplantar cuatro estaciones base simultáneamente, monitorear hasta 4 operadores de telefonía de forma simultánea, y operar en las redes 2G, 3G y 4G de forma simultánea (Biddle, 2016).

4. Algunas reflexiones adicionales sobre la vigilancia masiva

4.1. Sobre la veracidad de la información filtrada

Al respecto del sistema ECHELON, el informe final aprobado por el Parlamento Europeo en septiembre de 2001 reconocía de forma inequívoca la existencia de un sistema de vigilancia global operado por los países Five Eyes bajo el acuerdo UKUSA, como se ha mencionado con anterioridad.

Por lo tanto, las filtraciones de los años precedentes, fundamentalmente las de Campbell y Hager, quedaron esencialmente verificadas.

Sin embrago, sobre algunos aspectos asociados a este sistema como la utilización de ECHELON o algún sistema similar para otorgar ventaja competitiva a compañías de los EE.UU. frente a otras compañías

extranjeras en licitaciones internacionales, no se pudieron obtener pruebas concluyentes.

Al respecto de las filtraciones iniciadas en junio de 2013, la respuesta de las administraciones de los países involucrados se centró más en criminalizar a Snowden y en señalar las vulnerabilidades que estas divulgaciones habían introducido en la seguridad frente al crimen y terrorismo, que en desmentir las informaciones publicadas en los medios.

Como ejemplo, una de las primeras respuestas oficiales fue la de James Clapper, responsable de la comunidad de inteligencia para el presidente de los EE.UU. (Director of National Intelligence), quien dijo al respecto del programa PRISM que "la divulgación no autorizada de información sobre este programa importante y completamente legal es reprobable y pone en riesgo protecciones importantes para la seguridad de los americanos" (como se cita en Gilbert, 2013).

Pocos días después, el General Keith Alexander, director de la NSA, expuso que un mes después de iniciarse las filtraciones tenían evidencias de que determinados grupos terroristas ya estaban introduciendo cambios en su forma de operar. Añadió luego que la razón de ser de los programas, y la razón de ser de su secretismo, no era para ocultarlos de los americanos, sino para ocultarlos de aquellos que se ocultan entre los ciudadanos para intentar matarles (Williams, 2013).

En una comparecencia, el jefe de prensa de la Casa Blanca recalcaba la necesidad de mantener vigentes esos programas para salvaguardar la seguridad nacional, señalando dos casos concretos de atentados impedidos por haber sido detectados en fases incipientes[20]. Además, parafraseando unas declaraciones del presidente Obama en la Universidad de Defensa Nacional unas semanas antes[21], indicaba que el presidente reconocía haber encontrado el equilibrio adecuado entre seguridad y protección de la privacidad.

En octubre de 2013, en una rueda de prensa dada en Bruselas, en la sede del Consejo Europeo, David Cameron (primer ministro del Reino Unido) indicó que lo que Snowden y los medios que le ayudaban habían hecho era dificultar mucho más el mantener a los países y a los ciudadanos seguros. Añadió: "…hay mucha gente que quiere dañaros, que quiere hacer explotar a nuestras familias, que quiere mutilar a gente en nuestros países. Eso es un hecho. No es un hecho agradable, pero es cierto"[22].

Por otra parte, la canciller alemana Merkel, seguramente con el respaldo de sus servicios de inteligencia, dio por ciertas las informaciones desveladas acerca de la interceptación y seguimiento de su teléfono por parte de la NSA, considerándolo completamente inaceptable, añadiendo al respecto que "espiarse entre amigos nunca es aceptable"[23].

Finalmente, en septiembre de 2016, la Comisión de Inteligencia del Congreso de los EE.UU. (U.S. House of Representatives Permanent Select Committee on Intelligence) presentó un informe sobre la divulgación no autorizada de información de la NSA por parte de Snowden. En dicho informe, del que únicamente se encuentra desclasificado un pequeño resumen de 4 páginas, aparte de describir más en detalle la forma en que Snowden sustrajo los archivos, la primera conclusión que alcanzan es que las revelaciones de Snowden "… han causado un tremendo daño a la seguridad nacional", siendo los documentos divulgados "(…) de gran interés para los adversarios de América" (U.S. House of Representatives, 2016, p. 1).

20 Nota de prensa disponible en https://www.whitehouse.gov/the-press-office/2013/06/13/press-briefing-press-secretary-jay-carney-6132013

21 Declaración ante la NDU disponible en https://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university

22 Rueda de prensa de David Cameron el 25 de octubre de 2013 tras la cumbre de la UE. Disponible en https://www.gov.uk/government/speeches/pms-european-council-press-conference-october-2013

23 Declaraciones de la canciller disponibles en video en http://www.reuters.com/video/2013/10/24/germanys-merkel-says-spying-among-friend?videoId=274277973

En conclusión, en esta pequeña muestra de respuestas oficiales, y en especial en la de la comisión del Congreso de los EE.UU, no se encuentran dudas o negaciones expresadas por oficiales o funcionarios de alto nivel sobre el contenido de las filtraciones. Tampoco se han encontrado evidencias de que sean falsas o hayan sido manipuladas antes de ser publicadas, por lo que, en ausencia de otras pruebas concluyentes, se consideran veraces.

4.2. Sobre el derecho a la privacidad

La Declaración Universal de Derechos Humanos es un documento de las Naciones Unidas refrendado en 1948 por representantes de todas las regiones del mundo, representando un ideal común para todos los pueblos y naciones. Recoge en su artículo 12 que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"[24].

En el ámbito europeo, pocos años después, en 1953, entró en vigor el Convenio Europeo de Derechos Humanos (CEDH), inspirado expresamente en la mencionada Declaración Universal de Derechos Humanos.

El artículo 8 del CEDH, sobre el derecho al respeto a la vida privada y familiar, recoge y amplía este concepto, incluyendo algunos motivos aceptados para poder quebrantar esta privacidad:

> "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> 2. 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 del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás" (Consejo de Europa; Tribunal Europeo de los Derechos Humanos, 1950).

En el caso de España, por ejemplo, la protección de las comunicaciones se regula con la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD), teniendo por objeto, de acuerdo a su artículo 1, "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

Para los cuerpos y fuerzas de seguridad de España, la Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y el Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, regulan su actividad en materia de interceptación de comunicaciones. En el caso del Centro Nacional de Inteligencia, esta regulación procede de la Ley 11/2002 reguladora del Centro Nacional de Inteligencia y en la Ley Orgánica 2/2002 reguladora del control judicial previo del Centro Nacional de Inteligencia.

En esta misma línea, la mayor parte de las economías avanzadas[25] posee leyes y reglamentos que regulan qué tipo de interceptación de comunicaciones es legal y bajo qué circunstancias puede realizarse, estando estas interceptaciones auspiciadas generalmente por una orden judicial.

4.3. Sobre la proporcionalidad y la naturaleza de la interceptación

En primer lugar, es necesario distinguir entre la interceptación personalizada y la vigilancia masiva, que por naturaleza es indiscriminada.

[24] Declaración Universal de Derechos Humanos de las NN.UU. disponible en http://www.un.org/es/universal-declaration-human-rights/

[25] Terminología utilizada por el Fondo Monetario Internacional, que incluye a los países desarrollados que tienen tanto un elevado PIB como un elevado grado de industrialización. Más información disponible en http://www.imf.org/external/np/exr/key/advanced.htm

Es indudable que los cuerpos de seguridad y las agencias de inteligencia de los Estados deben disponer de las herramientas más adecuadas y de la suficiente capacidad de acción en defensa de los elementos indicados en el artículo 8 del CEDH, como la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden o la prevención del delito. Sin embargo, el control parlamentario y judicial de sus actuaciones es igualmente necesario y deseable para la estabilidad de una estructura democrática, debiendo siempre tratar de buscar la proporcionalidad entre las medidas utilizadas y los objetivos buscados.

Evaluando la información expuesta en las sucesivas filtraciones, se observa una tendencia extendida, en especial por parte de las agencias de inteligencia de los países denominados Five Eyes, a disponer de medios que les permitan interceptar de forma indiscriminada cualquier comunicación de cualquier usuario que se produzca en el campo de acción de sus potentes sistemas.

Esta tendencia, representada inicialmente por el sistema ECHELON y que fue considerada inaceptable por el Parlamento Europeo ya en 2001, se vio agravada e incrementada tras los atentados del 11-S de ese mismo año, a la sombra de la denominada "guerra contra el terrorismo" liderada por los EE.UU.

Ese atentado terrorista y los que han continuado sucediendo de forma persistente hasta la actualidad sobre diversos países de Europa, África y Asia, han favorecido la pérdida de impulso de cualquier iniciativa social o estatal contraria a la vigilancia masiva.

En un momento en que la tecnología invade de forma creciente la vida diaria de millones de personas en todo el mundo y permite obtener cantidades de información ingentes sobre sus costumbres, contactos, afiliaciones, gustos y movimientos, las capacidades de generación de inteligencia por parte de los Estados sobre los ciudadanos también se incrementan de forma exponencial.

Es difícil pensar hoy en día en alguien que considerara aceptable que un investigador que trabajara para el Estado, sin excesivo control judicial, se pudiera pegar a nuestras espaldas día y noche, dentro y fuera de nuestra casa, registrando de forma continua nuestra actividad diaria, dónde estamos en cada momento, con quién hablamos, qué buscamos en internet, qué opinamos y escribimos..., todo por el bien de prevenir un potencial delito o un acto terrorista. Y esto es precisamente de lo que trata la vigilancia masiva en una sociedad con alto grado de desarrollo tecnológico.

Tanto la presunción de inocencia como el requerimiento legal de que un juez, expresamente designado y capacitado para ello, ante una muestra de evidencias o indicios de suficiente peso decida vulnerar el derecho a la privacidad, buscando un bien mayor para el resto de los ciudadanos o el Estado, son aspectos generalmente poco atendidos en el uso de las tecnologías de vigilancia masiva descritas anteriormente.

Una idea que se encuentra con frecuencia es que la vigilancia masiva es en cierto modo justificable para prevenir atentados terroristas, y pudiera parecer que la sociedad actual se encuentra ante la tesitura de tener que elegir entre la vigilancia masiva y la prevención efectiva de acciones terroristas o criminales, pero esta es una falacia lógica de falso dilema.

Es difícil pensar que las redes trasnacionales de crimen organizado o terrorismo no sean conscientes de las capacidades de interceptación de comunicaciones que poseen muchas agencias de seguridad e inteligencia estatales, y de las vulnerabilidades que las tecnologías de la información introducen en las estructuras de sus redes.

Los atentados terroristas de noviembre de 2015 en Paris se llevaron a cabo utilizando teléfonos móviles simples activados horas o minutos antes de las acciones operativas, y no se captaron los suficientes indicios digitales en los días y semanas precedentes como para prevenir las muertes de 130 ciudadanos (Stone, 2016). El ex director de la CIA, Paul Brennan, argumentó en unas declaraciones sobre los atentados de Paris que debido a las filtraciones no autorizadas de los últimos años, la habilidad de los gobiernos para encontrar a los

terroristas era un reto mucho más desafiante (como se cita en Beckwith, 2016).

Vincular las filtraciones de 2013 con un incremento de las capacidades de operación de los grupos terroristas no es una relación evidente e inequívoca y requiere de un análisis más profundo y extenso, pero la realidad es que antes de esa fecha muchos grupos criminales ya hacían uso extensivo de la encriptación y de los teléfonos desechables (González, 2001).

En definitiva, para valorar en su justa medida las implicaciones de un sistema de vigilancia masiva internacional, se debe realizar un enfoque más extenso y multidisciplinar, dando cabida a los distintos organismos y necesidades involucrados, pero sin olvidarse de proporcionar respuestas a algunas cuestiones básicas que conciernen a preocupaciones legítimas de los ciudadanos, como pueden ser:

- ¿Es realmente aceptable el enfoque de que si un ciudadano nada tiene que ocultar no debe preocuparse por la vigilancia realizada sobre él por su gobierno? ¿Y si el gobierno cambia y es menos amigable? ¿Qué se hace con toda esa información almacenada? ¿Cómo se custodia? ¿Durante cuánto tiempo?
- ¿Cómo encaja en el marco de supervisión y control parlamentario el hecho de que una determinada agencia decida no realizar la interceptación indiscriminada, pero acceda a esos mismos datos comprando o intercambiando la información a otras agencias de otros países con menos escrúpulos legales? ¿O lo haga utilizando a una agencia militar que se encuentre condicionada por otras restricciones legales?
- ¿Existe algún sistema parlamentario que permita supervisar o debatir de forma efectiva la delgada línea que separa la obtención de inteligencia para garantizar la seguridad económica de un Estado, de la utilizada para otorgar ventaja competitiva a corporaciones o intereses de ese Estado ante terceros?
- ¿Existe igualmente algún sistema, parlamentario o de otra naturaleza, para supervisar el uso de la vigilancia para el control político en un Estado, bajo el pretexto de la seguridad nacional?
- Cuando se detecta en un Estado la ocurrencia de un episodio de interceptación global ejercido por parte de otro, ¿hay alguna medida o posición prevista? ¿Qué encaje tiene la injerencia del sistema liderado por los EE.UU. en los países miembros de la UE, al respecto de acuerdos de intercambio de información existentes, como el Acuerdo de Asistencia Judicial en materia penal entre la UE y los Estados Unidos[26]? ¿Es compatible el papel tan dispar de distintos países de la UE (ver Bigo et al., 2013) en este sistema de vigilancia global, con una defensa común de los intereses europeos frente a terceros?
- ¿Es aceptable y proporcionado implantar o permitir la operación de un programa de vigilancia intrusiva e indiscriminada con la justificación de potencialmente poder prevenir delitos?
- Sólo conocemos el caso de EE.UU. y sus socios Five Eyes por proceder la mayor parte de las filtraciones de sus ciudadanos, pero es evidente que existen otros estados con la capacidad y voluntad de operar sistemas similares, y posiblemente con intereses más lesivos para países de Europa Occidental y Norteamérica. ¿Qué se hace contra esto? ¿Cómo se controla?

Estas cuestiones son tan sólo una muestra de lo amplio que puede llegar a ser este análisis objetivo, razonado y compatible con un estado democrático, realizado sobre los beneficios y perjuicios reales para la sociedad acerca de la existencia de un sistema de vigilancia global.

Y es evidente, como se ha indicado con anterioridad, que la discusión no pasa por mermar las capacidades de las agencias de inteligencia y de los cuerpos de seguridad en el ejercicio de sus funciones para proteger la soberanía y seguridad nacional. De hecho, todos los medios con que cuenten son pocos para incrementar su efectividad ante las amenazas internas y externas que existen en la actualidad en el ámbito global, pero de igual modo es necesario garantizar que el uso que den a estos medios sea plenamente compatible con los requerimientos más básicos de un estado de derecho democrático, sin tener que depender de filtraciones no

[26] Decisión 2009/820/PESC, del Consejo de la Unión Europea de 23 de octubre de 2009. Diario Oficial de la Unión Europea, L 290/40, 07 de noviembre de 2009. Este acuerdo, que entró en vigor en 2010, sienta las bases sobre las que los países beneficiarios de ambos lados del Atlántico pueden reclamar información entre sí en la persecución de crímenes o en la defensa su seguridad pública, por ejemplo. El texto completo está disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:jl0052.

autorizadas o de labores de periodismo de investigación para conocer su adherencia a estos requerimientos.

Es cierto que para ello primero habría que regular el marco legal en que estas agencias desarrollan su trabajo en el plano del ciberespacio, pero en este asunto no se están logrando los suficientes avances que logren aunar a las grandes potencias internacionales. Una indudable dificultad para lograrlo es que a pesar de ser el ciberespacio el plano que recoge una de las mayores amenazas para la seguridad internacional, como lo son el ciberterrorismo o la ciberguerra, también es el plano en el que la población a nivel mundial exige una mayor apertura y desregulación (Domínguez, 2016).

5. Conclusiones

En 1980, un periodista de investigación británico llamado Duncan Campbell publicó unos artículos revelando la existencia de una red de interceptación de comunicaciones liderada por la NSA norteamericana con la colaboración de otros países aliados.

Este programa conjunto de captación indiscriminada de señales de comunicación a escala global, que denominó ECHELON, se estructuraba bajo el acuerdo UKUSA, firmado entre los EE.UU. y el Reino Unido.

Tras la publicación del informe del panel STOA en 1999 titulado Development of surveillance technology and risk abuse of economic information, el Parlamento Europeo ordenó la creación de una comisión temporal de investigación parlamentaria, denominada informalmente Comisión Echelon, para investigar el asunto en mayor profundidad.

La principal conclusión de la comisión de investigación fue que ese sistema global, operado por EE.UU, el Reino Unido, Canadá, Australia y Nueva Zelanda, existía sin ninguna duda, bajo ese nombre u otro, con la finalidad de interceptar comunicaciones del ámbito comercial, no militar, siendo además un sistema como ese incompatible con el artículo 8 del Convenio Europeo de Derechos Humanos ("toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"). Por último, expresaba la Comisión su preocupación con el hecho de que, en defensa de la lucha contra la corrupción y el crimen, los servicios de inteligencia de los EE.UU. interceptaban rutinariamente las comunicaciones de empresas extranjeras, pudiendo luego usar esa información para otorgar ventajas competitivas a otras empresas.

Este movimiento en contra del sistema de vigilancia masiva, liderado por representantes de países europeos, se detuvo casi totalmente con los atentados de las Torres Gemelas de 2001 y los que siguieron y afectaron a multitud de países como España, Reino Unido, India, Indonesia, Francia y Alemania.

En junio de 2013, Edward Snowden, un contratista de la NSA que había robado multitud de documentos clasificados de la red interna de la NSA mientras trabajaba allí, los entregó a varios periodistas para su divulgación.

Desde aquel momento ha habido una divulgación progresiva y continuada de esta información por parte de varios medios, mostrando de forma global la magnitud de las actividades de la NSA y de sus socios.

A la vista de esta información, se puede comprobar que queda un largo camino por recorrer en lo que concierne a la defensa de los derechos más elementales de privacidad de los ciudadanos, en especial en la relacionada con los sistemas digitales, que en la actualidad no parece estar alineada con la forma de operar de multitud de agencias y cuerpos de inteligencia y seguridad tanto civiles como militares.

Es recomendable que se abra un debate a todos los niveles acerca del control realizado sobre esta forma de operar, y también sobre si esta es la forma más responsable y efectiva de garantizar la seguridad nacional y de luchar contra el crimen y el terrorismo.

Es necesario que en esta discusión participen las agencias y cuerpos de inteligencia y seguridad de modo que se pueda garantizar que todas sus necesidades queden atendidas y no se vean en mermadas sus capacidades frente a las amenazas globales, entendiendo además que la capacidad de una sola nación para hacerles frente es cada vez más limitada, siendo por tanto necesario desarrollar capacidades y alianzas sólidas supranacionales.

Sin ninguna duda, este será un debate complejo y extenso, con multitud de matices, enfoques, marcos legales e intereses distintos, en el que deben también poder participar los ciudadanos, pero para ello primero es necesario que cuenten con información completa, objetiva y veraz, que no puede consistir únicamente en filtraciones a la prensa de datos robados a determinadas agencias.

En definitiva, este debate debe hacerse y las decisiones que surjan de él deben traducirse en medidas que se implanten de forma efectiva, tanto a nivel nacional como a nivel supranacional, para evitar que queden sin respuesta preguntas fundamentales como la que contenía el informe de la Comisión Echelon de 2001 en su primera página:

"Sed quis custodiet ipsos custodes?"
(Pero, ¿quién vigilará a los vigilantes?)
Juvenal (ca. 60 hasta 130 AD), Sát. 6, 346-348

Cómo citar este artículo / How to cite this paper

Pinel, A. (2017). ECHELON y la vigilancia masiva: entre la seguridad y la protección de la privacidad. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 2(1), 21-42. (www.cisdejournal.com)

Referencias

Appelbaum, J.; Stark, H. ; Rosenbach, M.; Schindler, J. (2013). Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone? Spiegel Online. (www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html)

Beckwith, R. (2015). Read the CIA Director's Thoughts on the Paris Attacks. Time. (http://time.com/4114870/paris-attacks-cia-john-brennan/)

Biddle, S. (2016). Long-secret Stingray manuals detail how police can spy on phones. The Intercept. (https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/)

Bigo, D.; Carrera, S.; Hernanz, N.; Jeandesboz, J.; Parkin, J.; Ragazzi, F.; Scherrer, A. (2013). Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law. (CEPS Papers in Liberty and Security in Europe; No. 62). Brussels: CEPS, 29-30. (www.ceps.eu/publications/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law)

Bogolikos, N. (1999). The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception. PE 168.184 Vol 5/5/EN. Luxemburgo: European Parliament Directorate General for Research. Directorate A. The STOA Programme. (www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf)

Campbell, D., Melvern, L. (1980). America's Big Ear on Europe. New Statesman. 10-14. (www.duncancampbell.org/PDF/America's%20Big%20Ear%20on%20Europe%2018%20July%201980.pdf)

Campbell, D. (1999). The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition. PE 168.184 Vol 2/5/EN. Luxemburgo: European Parliament Directorate General for Research. Directorate A. The STOA Programme. (www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf)

CRNA Centre for Resilient Networks and Applications Simula Research Laboratory. (2015). An investigation into the claims of IMSI catchers use in Oslo in late 2014. Norwegian Police Security Service. (www.pst.no/media/76725/IMSI-report-SimulaResearch-Laboratory.pdf)

Consejo de Europa y Tribunal Europeo de los Derechos Humanos. (1950). Convenio Europeo de Derechos Humanos. (www.echr.coe.int/documents/convention_spa.pdf)

Decisión 2009/820/PESC, del Consejo de la Unión Europea de 23 de octubre de 2009. Diario Oficial de la Unión Europea, L 290/40,

07 de noviembre de 2009. (2009). (http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:jl0052).
Der Spiegel, Editorial. (2013). Embassy Espionage: The NSA's Secret Spy Hub in Berlin. Spiegel Online. (www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html)
Domínguez, J. (2016). La ciberguerra como realidad posible contemplada desde la prospectiva. Revista de Pensamiento Estratégico y Seguridad CISDE, 1(1), 18-32. (www.cisdejournal.com)
Elliot, C. (1999). The legality of interception of interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law. PE 168.184 Vol 4/5/EN. Luxemburgo: European Parliament Directorate General for Research. Directorate A. The STOA Programme. (www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf)
Foss, A. B. (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service. Aftenposten. (www.aftenposten.no/norge/New-report-Clear-signs-of-mobile-surveillance-in-Oslo_-despite-denial-from-Police-Security-Service-61149b.html).
García, I. (2003). Libertad Vigilada: El Espionaje de las Comunicaciones. Ediciones B, Barcelona.
Gallagher, R. (2014). British spy chiefs secretly begged to play in NSA's data pools. The Intercept. (https://theintercept.com/2014/04/30/gchq-prism-nsa-fisa-unsupervised-access-snowden/)
Gallagher, R. (2015a). In historic ruling, UK surveillance secrecy declared unlawful. The Intercept. (https://theintercept.com/2015/02/06/surveillance-uk-gchq-unlawful-human-rights/)
Gallagher, R. (2015b). From radio to porn, British spies track web users' online identities. The Intercept. (https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/)
Gellman, B.; Poitras, L. (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. The Washington Post. (www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html)
Gellman, B.; Soltani, A. (2013). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. The Washington Post. (www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html)
Gellman, B.; DeLong, M. (2013). How the NSA's MUSCULAR program collects too much data from Yahoo and Google. The Washington Post. (http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/)
González, M. (2001). La cooperación de la CIA y el FBI contra ETA es aún 'muy incipiente'. Diario El País. (http://elpais.com/diario/2001/06/15/espana/992556005_850215.html)
Greenwald, G. (2013a). NSA collecting phone records of millions of Verizon customers daily. The Guardian. (www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order)
Greenwald, G.; MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. The Guardian. (www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data)
Greenwald, G. (2013b). XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. The Guardian. (www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data)
Greenwald, G. (2014). No place to hide. EE.UU: Metropolitan Books. Documentos de Snowden disponibles en: (http://us.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf)
Hager, N. (1996). Secret Power: New Zealand's Role in the International Spy Network. Nueva Zelanda: Potton & Burton.
Hager, N.; Gallagher, R. (2015). How spy agency homed in on Groser's rivals. Nzherald. (www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11421370)
Johansen, P. A. (2014). Secret surveillance of Norway's leaders detected. Aftenpost. (www.aftenposten.no/norge/Secret-surveillance-of-Norways-leaders-detected-71828b.html)
Kettle, M.; Campbell, D.; Rollo, J.; Hain, P. (1980). Policing the Police Volume 2. John Calder, Londres.
Leprevost, F. (1999). Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues. PE 168.184 Vol 3/5/EN. Luxemburgo: European Parliament Directorate General for Research. Directorate A. The STOA Programme. (www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf)
Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado, 14 de diciembre de 1999, núm. 298. (www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf)
Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Boletín Oficial del Estado, 22 de julio de 2015, núm. 174, páginas 61593 a 61660. (www.boe.es/diario_boe/txt.php?id=BOE-A-2015-8167)
MacAskill, E.; Borger, J.; Hopkins, N.; Davies, N.; Ball, J. (2013). GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian. (www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa)
McKay, G. (2015). Mobile Network Forensic Analysis. Project "Solo". Delma. Pág. 8. (http://mm.aftenposten.no/2015/06/23-mobilspionasje/pub/MFA-CP-007-D.pdf)
NDR Norddeutscher Rundfunk, Editorial. (2014). Snowden-Interview: Transcript. NDR. (www.ndr.de/nachrichten/netzwelt/snowden277_page-2.html)
NSA (2003). SIGINT Directors Set Strategic Direction for 5-Eyes SIGINT Enterprise. SIDtoday. (https://theintercept.com/snowden-sidtoday/3008302-sigint-directors-set-strategic-direction-for-5/)
Oficina de Prensa de la Casa Blanca (2016). Declaración del Presidente Obama. (www.whitehouse.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity)

Oficina de Prensa de la Casa Blanca (2016). Orden Ejecutiva firmada por el Presidente Obama contra intereses rusos. (www.whitehouse.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency)
Parlamento Europeo (2000) Debate ante el Parlamento Europeo, Bruselas. (www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20000330+ITEM-002+DOC+XML+V0//ES)
Parlamento Europeo (2000). Minuta de la Conferencia de Presidentes, Estrasburgo, 18. (www.europarl.europa.eu/RegData/organes/conf_pres_groupes/proces_verbal/2000/04-13/CPG_PV(2000)04-13_EN.pdf)
Parlamento Europeo. (2009). Reglamento de STOA. PE422.577/BUR. (www.europarl.europa.eu/stoa/webdav/site/cms/shared/1_about/rules/201606/1066262_1_es.pdf)
Parlamento Europeo, Scientific and Technical Options Assessment STOA (1999). Development of surveillance technology and risk abuse of economic information. A Working Document for the STOA Panel, PE 168.184. (www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf)
Parlamento Europeo. Temporary Committee on the ECHELON Interception System (2001). Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), 128, 133-136, 139. (www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%20REPORT%20A5-2001-0264%200%20DOC%20PDF%20V0//EN)
Parlamento Europeo (2002). Debate parlamentario. Estrasburgo. (www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20021023+ITEM-003+DOC+XML+V0//EN&language=RO)
Pegger, B. (1999). Présentation et analyse. 1) Présentation des quatre études. 2) Analyse: protection des données et Droit de l'Homme dans l'Union Européenne et role du Parlement Européen. PE 168.184 Vol 1/5/EN. Luxemburgo: European Parliament Directorate General for Research. Directorate A. The STOA Programme. (www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf)
Piodi, F.; Mombelli, I. (2014). The ECHELON Affair: The European Parliament and the global interception system 1998 – 2002. European Parliamentary Research Service. Historical Archives Unit. PE 538.877, 14, 23, 26, 36. (www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf)
Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado, de 17/09/1882, núm. 260. (www.boe.es/buscar/act.php?id=BOE-A-1882-6036)
Stöcker, C.; Horchert, J. (2013). Alles, was man über Prism, Tempora und Co. wissen muss. Spiegel Online. (www.spiegel.de/netzwelt/netzpolitik/prism-und-tempora-fakten-und-konsequenzen-a-909084.html y en http://www.spiegel.de/media/media-34090.pdf)
Stone, J. (2016). ISIS Terrorists Used Disposable Burner Phones, Activated Just Hours Before, To Carry Out Paris Attacks. International Business Times. (www.ibtimes.com/isis-terrorists-used-disposable-burner-phones-activated-just-hours-carry-out-paris-2340265)
Tribunal de Vigilancia de la Inteligencia Extranjera de los EE.UU. (2013). Orden judicial sobre Verizon. (www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order)
Unión Europea, Directorate-General for Parliamentary Research Services (2014). The ECHELON affair. The European Parliament and the global interception system 1998 - 2002. PE 538.877, 13. (www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf)
U.S. House of Representatives (2016). Executive Summary of Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden, 1. (https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_-_unclass_summary_-_final.pdf)
Wright, S. (1998). An appraisal of technologies for political control. Luxemburgo: European Parliament Directorate General for Research. Directorate B. The STOA Programme, 19. (http://aei.pitt.edu/5538/)