Espionaje en la red

Jonathan Castro Alberto Fernández Arkaitz Marcos

8 de noviembre de 2013

Índice

Espionaje en la red **3**

Introducción **3**

La primera filtración **3**
PRISM 3
La respuesta del gobierno de EE.UU. 4
Las empresas niegan su participación 4

Posteriores filtraciones **5**
Espiando a líderes mundiales 5
Recopilación de agendas de contactos 5
Espionaje a España y Francia 6
Proyecto MUSCULAR 6

Otras noticias **7**
SIBIOS 7
CIA y AT&T 7

Consecuencias **7**

Protegiendo nuestros datos **8**

Legislación **10**

Legislación de Estados Unidos **10**
Enmienda IV 10
Enmienda IX 10

Legislación de España **10**
Artículo 2 10
Artículo 3 10
Artículo 4 11
Artículo 5 11
Artículo 6 11
Artículo 7 11
Artículo 9 11
Artículo 11 11
Artículo 12 12

Diferencias entre legislaciones **12**

Bibliografía **13**

Glosario **16**

Espionaje en la red

Introducción

Aunque desde los comienzos de Internet se intuía que los diferentes gobiernos del mundo espiaban a sus ciudadanos y empresas, además de aquellas que no son estrictamente de sus países, una filtración nos confirmó lo que todos sospechábamos.

El 5 de junio de 2013, Edward Snowden, ex trabajador de la CIA y empleado para la firma Booz Allen Hamilton, que tiene un contrato con la NSA, hace públicos, mediante los periódicos estadounidenses The Guardian y The Washington Post, documentos clasificados con programas de la NSA, entre ellos PRISM.

La primera filtración

PRISM

PRISM es el nombre que se le dio al programa de vigilancia secreto de la NSA. El objetivo de este programa es el de espiar las comunicaciones personales que se llevan a cabo a través de la red.

Es la última evolución del gobierno estadounidense del esfuerzo de la vigilancia electrónica post 9/11, que empezó en el mandato del presidente G. W. Bush bajo el Acta Patriótica (Patriot Act), y expandida para incluir el Foreign Intelligence Surveillance Act (FISA), promulgada entre 2006 y 2007.

PRISM permite al gobierno, además de la recopilación de la información de las empresas, el acceso directo a sus bases de datos sin necesidad de una orden judicial, lo cual es lo que le diferencia de otros programas de vigilancia. Se espía, entre otra cosas, los correos electrónicos, los chats, los archivos transferidos y el historial de búsqueda de los usuarios.

Cabe destacar que PRISM se centra exclusivamente en vigilar a usuarios extranjeros. "*No puede ser utilizado para tener como objetivo intencional a ningún ciudadano de EE.UU., o a cualquier otra persona de EE.UU., o a cualquiera ubicado en EE.UU.*", declaró el Director Nacional de Inteligencia James Clapper.

Según la filtración, se dicen que las empresas involucradas son las siguientes: Microsoft, Yahoo!, Google, Facebook, Paltalk, YouTube, Skype, AOL y Apple.

The Washington Post informó también que, a diferencia de las otras nueve empresas, la red social Twitter fue la única que rechazó la cooperación con la NSA y el FBI.

La respuesta del gobierno de EE.UU.

El gobierno estadounidense no desmintió PRISM. De hecho, el presidente Obama lo intentó justificar como lucha antiterrorista.

Obama defendió con convicción el programa PRISM: "*Creo que es importante reconocer que no se puede tener el 100 % de seguridad y al mismo tiempo un 100 % de privacidad, además de ninguna incomodidad. Tenemos que tomar ciertas decisiones como sociedad*".

Obama quiso aclarar, no obstante, algunos de los datos revelados por los documentos secretos. En el tema de la recolección de datos de llamadas en móviles, el presidente de los Estados Unidos dejó claro que "*nadie está escuchando vuestras llamadas telefónicas*".

"*Ese no es el objetivo de este programa*", añadió Obama. "*Lo que la comunidad de Inteligencia está haciendo es identificar esas llamadas estudiando los números de teléfono y la duración de las llamadas. No se miran los nombres de la gente, y no se fijan en el contenido de las llamadas*".

Por otra parte, según el Director Nacional de Inteligencia James Clapper, mencionado anteriormente, PRISM no es un "*programa de recolección o minería de datos no divulgado*", sino una herramienta para monitorizar las comunicaciones de ciudadanos no estadounidenses a través de sus metadatos, es decir, la información sobre quién envía una comunicación, a quién va destinada y cuándo se produce, sin llegar a acceder al contenido.

Además, afirmó que la información se utiliza para proteger al país de amenazas terroristas: "*Discutir programas como este públicamente tendrá un impacto en el comportamiento de nuestros adversarios y hará más difícil para nosotros comprender sus intenciones. [..] La información recolectada bajo este programa está entre la inteligencia más importante y valiosa que podemos reunir, y es usada para proteger a nuestra nación de una variedad de amenazas*".

Las empresas niegan su participación

Todas las empresas mencionadas anteriormente escribieron comunicados al de poco tiempo, negando haber concedido a los servicios de espionaje estadounidenses acceso a los datos de sus usuarios ni el acceso directo a sus servidores, asegurando que sólo cedieron información cuando la justicia se lo requirió. Dichos comunicados fueron los siguientes:

Apple: "*Nunca hemos oído hablar de PRISM; no aportamos, a ninguna agencia del gobierno, el acceso directo a nuestros servidores y cualquier departamento del gobierno que nos pide datos de nuestros clientes tiene que presentar una orden judicial*".

Facebook: "*Cuando se le pide a Facebook datos o información sobre individuos determinados, examinamos tal solicitud detenidamente para asegurar que concuerde con las leyes y entonces aportamos información sólo en la medida que la ley nos lo exija*".

Google: "*Google se preocupa mucho por la seguridad de los datos de sus usuarios. Proporcionamos información al Gobierno de acuerdo a la ley y revisamos*

toda petición cuidadosamente. De vez en cuando, algunas personas dicen que hemos creado una puerta trasera en nuestros sistemas, pero Google no tiene tal acceso para que el Gobierno acceda a los datos privados de nuestros usuarios".

Microsoft: "*Nosotros proveemos datos de los clientes cuando recibimos una orden judicial o una citación para hacerlo y nunca de forma voluntaria. Adicionalmente, sólo cumplimos con peticiones acerca de cuentas o identificadores específicos. Si el Gobierno tiene un programa nacional de seguridad para recopilar datos de clientes voluntariamente, nosotros no participamos en él*".

Yahoo!: "*Para Yahoo! la privacidad de los usuarios es un asunto serio. Nosotros no proveemos al gobierno con accesos directos a nuestros servidores, sistemas o redes*".

Paltalk: "*No hemos oído hablar de PRISM. Desde Paltalk hemos protegido de manera extremo los datos de los usuarios, respondiendo solamente a las órdenes judiciales requeridas por la ley. Paltalk no provee acceso directo de nuestros servidores a ninguna agencia gubernamental.*"

AOL: "*No tenemos ningún conocimiento sobre el programa PRISM. Nosotros no revelamos información de los usuarios a las agencias del gobierno sin una orden judicial, citación u otra forma legal, además de no proveer acceso directo a ninguna agencia gubernamental de nuestros servidores.*"

Incluso Dropbox, que no aparecía en la lista anterior, quiso negar también su participación: "*Hemos visto informes de que Dropbox pudo haber sido requerido para tomar parte en un programa gubernamental llamado PRISM. Nosotros no somos parte de tal programa y seguimos comprometidos a proteger la privacidad de los usuarios*".

Posteriores filtraciones

Espiando a líderes mundiales

The Guardian hizo público que la NSA estuvo espiando las conversaciones telefónicas de 35 líderes mundiales, siendo el caso más sonado el de Angela Merkel, cuyo móvil, se dice, llevaba pinchado desde el año 2002, tres años antes de ser elegida Canciller de Alemania. Angela Merkel afirmó que estas prácticas son "*totalmente inaceptables*", mientras Estados Unidos negó haberle espiado sin dejar claro si intervino su número de teléfono o no.

En el caso de España, se teme que entre los afectados hayan estado Mariano Rajoy o José Luis Rodríguez Zapatero —el candidato más probable a las escuchas— en su etapa como presidente del país.

Por el momento, se desconocen las identidades de esos 35 líderes mundiales.

Recopilación de agendas de contactos

Posteriores filtraciones de documentos secretos demostraron que el programa de recolección de direcciones de correo electrónico de la NSA lleva recolectando datos a nivel global durante años.

Junto con el robo de direcciones, se apropiaron de agendas electrónicas, lo cual les ha aportado información respecto al propietario de las mismas, permitiendo a la NSA establecer relaciones entre personas, aparentemente inconexas, sobre personas de todo el mundo.

Espionaje a España y Francia

Por otro lado, en la recogida de datos en otros países no habría tomado parte la propia NSA. Según filtraciones, en el caso del espionaje en Francia y España, se habrían encargado las propias agencias de inteligencia nacionales.

En España, la intercepción de comunicaciones, se llevó a cabo entre 10 de diciembre de 2012 y el 8 de enero de 2013 de la mano del CNI (Centro Nacional de Inteligencia), hizo que la NSA registrara 60 millones de llamadas telefónicas.

Esta misma organización, el CNI, colaboró junto con otros países en un programa, impulsado por el GCHQ británico, para intercambiar información y consejos de cara a labores de espionaje que se llevaban a cabo mediante interceptaciones directas de cables de fibra óptica o mediante acuerdos con compañías de telecomunicaciones.

Sin embargo, el caso de Francia es distinto, puesto que parece que no espió a sus propios ciudadanos, sino que espió a países vecinos.

Proyecto MUSCULAR

Una exclusiva de The Washington Post reveló que la NSA se infiltró en las redes privadas de Google y Yahoo! para obtener información de sus usuarios.

Todo este mecanismo de espionaje se hacía bajo un proyecto denominado MUSCULAR, que se realizaba en colaboración con la agencia británica GCHQ.

Para entender cómo funciona, hay que saber que tanto Google como Yahoo! cuentan con diferentes centros de datos repartidos por el mundo. Estos centros de datos están conectados por canales, o enlaces, propios que no están conectados a ninguna red abierta, es decir, no están conectadas directamente a Internet.

Como por estos enlaces pasan datos que deben utilizar los diferentes centros de datos, es primordial la velocidad, por lo que ni Google ni Yahoo! tiene cifradas las conexiones entre estos enlaces. Y ese es el punto débil.

La NSA y el GHCQ lograrían el acceso secreto a un cable o conmutador de red por el que pasa el tráfico de Google y Yahoo!. Es un punto de acceso localizado fuera de Estados Unidos. Dicho acceso lo daría un proveedor de telecomunicaciones desconocido.

Que el acceso esté localizado fuera de los EE.UU. implica que la NSA puede espiar también a ciudadanos estadounidenses, puesto que, por legislación, la NSA no tiene permitido espiar a sus propios ciudadanos en suelo estadounidense sin una orden judicial.

Ni la Casa Blanca ni la Oficina del Director de Inteligencia Nacional hicieron declaraciones sobre la infiltración en las redes de Google y Yahoo!.

En cambio, Google tuvieron sospechas de que podría estar ocurriendo. Ahora

trabajan en cifrar las conexiones entre sus propios centros de datos e incluso en las redes internas entre servidores en un mismo centro.

Por otro lado, desde Yahoo! explicaron que tienen controles estrictos para proteger sus centros de datos y que no han dado acceso a ninguna agencia a ellos. Los enlaces de su red privada seguirán estando sin cifrar.

Otras noticias

SIBIOS

Si bien esta noticia no trata exactamente sobre el tema del que nos hemos centrado en este documento, la añadimos para demostrar que EE.UU. no es el único país que intenta registrar todos los datos que puede. Como bien se podrá leer a continuación, Argentina está tratando de recopilar todos los datos de sus propios ciudadanos.

SIBIOS, acrónimo de Sistema Federal de Información Biométrica para la Seguridad, es una base de datos centralizada en la que se registran datos personales de las personas como su nombre y apellido, estado civil, grupo sanguíneo, fotografía, huella dactilar y demás recursos y herramientas relacionados para la identificación digital y automática de cualquier ciudadano argentino.

Este sistema tiene como usuarios iniciales, entre otros, a la Policía Federal Argentina, Gendarmería nacional, Prefectura Naval Argentina, Policía de Seguridad Aeroportuaria, Registro Nacional de las Personas y Dirección Nacional de Migraciones.

No podemos concluir que este sistema sea malo, España a la hora de realizar el DNI también guarda todos nuestros datos, foto y huella dactilar. Sin embargo, muchos ciudadanos argentinos están preocupados por lo que puedan hacer con sus datos y, sobre todo, con quienes tengan acceso a los mismos.

CIA y AT&T

Esta otra noticia la hemos puesto para que se vea que las compañías son capaces de vender nuestro datos, en este caso, a cualquier agencia gubernamental por una buena cantidad de dinero.

El New York Times asegura que la compañía telefónica estadounidense AT&T habría vendido los registros de llamadas internacionales a la CIA. La compañía le cobra más de 10 millones de dólares anuales a la agencia de inteligencia a cambio de acceso a los metadatos de llamadas de supuestos terroristas en el extranjero.

Consecuencias

El espionaje por parte de los EE.UU. ha generado un malestar generalizado entre los usuarios de servicios de comunicación electrónicos.

Según informa The Washington Post, la NSA recoge millones de registros cada día de Yahoo! y Google. Sólo en el mes de octubre de 2013 se han enviado 181.280.466 nuevos registros, con contenido tan diferente como audio, texto y vídeo, además de metadatos.

En la parte política, en la Unión Europea, los gobiernos de Alemania y Francia han hecho que sus embajadores en EE.UU. presionen al gobierno estadounidense para conseguir respuestas. A pesar de que éstas hayan sido las únicas reacciones reales del mundo político, el espionaje de EE.UU. ha sufrido el rechazo verbal por parte de toda la comunidad política de Europa.

En contra de la UE podemos decir que, tal y como han mostrado diferentes filtraciones, ellos también han espiado, espían y seguirán espiando. Por eso cada país tiene su fuerza de inteligencia, en España el CNI, en Reino Unido el GCHQ o en Alemania el Bundesnachrichtendienst.

Además, que las filtraciones hayan dicho que estas fuerzas de inteligencia hayan colaborado con la NSA dice mucho. Todas las naciones tienen algo que esconder, de la misma forma que sobreactúan cuando una noticia tan jugosa y tan importante como el monitoreo de personas aparece en la prensa.

La única diferencia entre EE.UU. y UE es que a la agencia a la que han destapado ha sido a la NSA y no a cualquiera de la UE. De haber sido al contrario, no sabremos cómo habría actuado EE.UU.

Por otra parte, dejando el tema político de lado, empleados de Google manifestaron su frustración tras reconocer datos internos de la empresa en las diapositivas de la NSA. La frase más usada por estos empleados ha sido "*Que se jodan estos sujetos*".

A día de hoy, Edward Snowden llama a la ciudadanía a manifestarse en contra de los programas de vigilancia. Mientras, desde Estados Unidos llegan las declaraciones de varios oficiales que le recuerdan que no habrá "*clemencia*" con su persona.

Protegiendo nuestros datos

Al estar involucradas las empresas informáticas más populares y cuyos servicios son los más usados, nuestro único método de protección es pasar a utilizar software y proveedores de servicios alternativos. La mejor alternativa será, en la mayoría de los casos, utilizar software libre.

En los siguientes puntos trataremos de explicar cuáles podrían ser algunos cambios que podemos hacer para tratar de proteger nuestros datos de la mejor manera posible. Es casi imposible, por no decir imposible totalmente, de protegerlos.

- Cambiar de sistema operativo en nuestros ordenadores. Cambiar Windows o Mac OS por GNU/Linux o FreeBSD/OpenBSD.
- Utilizar los navegadores Firefox o Tor Browser en vez de Chrome, Safari o Internet Explorer. Además, podemos añadir complementos a nuestro navegador para mejorar nuestra privacidad:

  - HTTPS Everywhere.
  - BetterPrivacy.
  - DoNotTrackMe.

- Reemplazar los buscadores de Google, Yahoo! o Bing y utilizar DuckDuckGo, puesto que es un buscador que no registra quién lo usa y qué se busca. Además, ellos mismos dicen "*Busca anónimamente. Encuentra inmediatamente.*".
- Evitar los DNS de Google, ya que guarda nuestras búsquedas. Hay alternativas muy buenas como OpenDNS. Además, OpenNIC puede ayudarnos en esta tarea.
- Utilizar herramientas para cifrar el correo electrónico y clientes de correo libres para el escritorio, como Thunderbird, si no podemos prescindir de otros correos basados en web como Outlook o Gmail.
- Intentar evitar las redes sociales basadas en modelos abiertos, por ejemplo, Diaspora.
- Utilizar el mapa mundial colaborativo y libre OpenStreetMap para evitar hacer uso de los mapas de Apple, Google o Bing.
- Buscar alternativas a las aplicaciones más populares en Android e iOS.

Siempre deberemos cumplir las recomendaciones anteriores para mantener nuestra privacidad; a fin de cuentas de nada sirve utilizar un sistema GNU/Linux o FreeBSD si seguimos utilizando las DNS de Google o Gmail.

Por otro lado, vemos que es muy difícil dejar de usar servicios y programas que llevamos usando desde hace mucho tiempo. Por lo tanto, como conclusión, la mejor opción es no escribir en la red aquellas cosas que no queremos que se sepan acerca de nosotros mismos, es decir, no digas aquello de lo que no quieres que se entere nadie.

Legislación

Legislación de Estados Unidos

A diferencia de los países europeos, EE.UU. no cuenta con una ley específica para la protección de datos; la Enmienda IV de su Constitución es la encargada de "garantizarles privacidad".

Enmienda IV

El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas.

Enmienda IX

A pesar de que en la Constitución no se mencione explícitamente el derecho a la privacidad, no significa que el Gobierno pueda violarlo.

Es decir, salvo que haya un motivo "justificado" no se puede investigar personas, domicilios, papeles y objetos.

Legislación de España

La legislación aplicada en España en los temas de protección de datos es la "*Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal*", que se encuentra disponible para cualquier persona en la página web de la Agencia Española de Protección de Datos.

Esta ley especifica la forma en que se deben guardar los datos de carácter personal garantizando de esta forma las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo 2

Aclara el ámbito de aplicación de la ley.

Artículo 3

Define los distintos participantes en la ley, datos, ficheros, tratamientos de datos, responsables de datos, etcétera.

Artículo 4

Define que los datos recogidos deben ser exactos y, en caso de no serlos, deben ser cancelados o corregidos. Cuando no sean necesarios para la actividad para la que fueron recogidos deben ser cancelados, salvo que vayan a ser utilizados para fines históricos o estadísticos, en cuyo caso será aplicada otra ley. No pueden ser recogidos de manera fraudulenta y deben ser almacenados de forma que aseguren el derecho de acceso.

Artículo 5

Especifica de forma explícita que los interesados a los que se les soliciten los datos deben ser informados de la existencia de un fichero, del tratamiento que recibirán sus datos, así como de la finalidad de la recogida de datos. Además, deben ser informados de la obligatoriedad de dar los datos, así como de la identidad y dirección del responsable de los datos recogidos. Si los datos son aportados por terceras persona,s el informado debe ser informado en un plazo de 3 meses por el responsable del fichero o su representante.

Artículo 6

Obliga a solicitar permiso inequívoco del afectado para su tratamiento de los datos, aunque no será necesario solicitarlo cuando sea en el ámbito de las administraciones públicas.

Artículo 7

Dice que los datos de carácter personal que revelen la ideología, afiliación sindical, religión, origen racial, salud, vida sexual y creencias, solamente pueden ser recogidos con el consentimiento expreso y escrito del afectado. El afectado nunca puede ser obligado a revelar estos datos.

Artículo 9

Especifica que el responsable de los datos debe tomar medidas para garantizar la alteración, pérdida, tratamiento o acceso no autorizado de los datos. Tanto el responsable del fichero como aquellos que intervengan en el tratamiento de los datos están obligados al secreto profesional.

Artículo 11

Expresa la imposibilidad de ceder datos de una persona a terceros que no tengan nada que ver con las funciones del cedente, es decir, el responsable de los datos, obligando a tener una autorización por parte de la persona en cuestión. La autorización se considerará nula en el caso de que la persona reciba información que no le permita conocer la finalidad de la cesión de sus datos.

Artículo 12

Estipula que no se considerará comunicación de datos al acceso de un tercero, siempre que ese acceso sea necesario para la prestación de un servicio al responsable del tratamiento. Este acceso deberá estar regulado en un contrato escrito en el que se indica que este tercero solamente seguirá las instrucciones del responsable de los datos y se le obliga a que esos datos no sean utilizados para nada más. En caso de incumplirse el contrato se le considerara responsable de datos y deberá responder a las infracciones que hubiera cometido.

Diferencias entre legislaciones

Para un estadounidense, el derecho a la privacidad es, literalmente, "*the right to be let alone*", es decir, que tiene el derecho a que nadie le moleste, incluido el gobierno. No es un derecho fundamental reconocido por su Constitución, como podría ser la libertad de expresión recogida en la "*Primera Enmienda*". Dicho derecho, por tanto, fue creado y perfilado por la propia jurisprudencia americana suponiendo, en la práctica, una protección muy parecida a nuestro derecho a la intimidad.

Por el contrario, para un europeo la privacidad es algo muy distinto. Dado que nuestra legislación reconoce y protege todos estos aspectos mediante el derecho a la intimidad, la privacidad ha surgido como una esfera de protección más amplia. Dicha esfera abarca todos los datos que cualquier entidad, privada o no, tenga sobre un ciudadano.

En Europa, por tanto, el derecho a la privacidad no es otra cosa que el derecho que protege a las personas físicas en relación al tratamiento de sus datos por parte de terceros o, dicho de otro modo, el derecho a la protección de datos de carácter personal.

También, a diferencia de Estados Unidos, en Europa el derecho a la privacidad se protege como un derecho fundamental, recogido tanto en el artículo 18.4 de nuestra Constitución como en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, además de desarrollado tanto por la LOPD como por la Directiva Europea 95/46/CE.

Bibliografía

Softpedia. *Obama sobre PRISM: El programa no se aplica a los ciudadanos estadounidenses* [en línea]. Gabriela Vatu, traducido por Elvis Bucatariu, 8 de junio de 2013. Disponible en: `http://news.softpedia.es/Obama-sobre-PRISM-El-programa-no-se-aplica-a-los-ciudadanos-estadounidenses-359497.html`

Engadget. *EEUU desclasifica PRISM al tiempo que se filtra su herramienta de catalogación de datos* [en línea]. Alberto Ballestin, 9 de junio de 2013. Disponible en: `http://es.engadget.com/2013/06/09/eeuu-desclasifica-prism-catalogador-boundless-informant-filtrado/`

Gizmodo. *What Is PRISM?* [en línea]. Brian Barrett, 7 de junio de 2013. Disponible en: `http://gizmodo.com/what-is-prism-511875267`

The Verge. *Everything you need to know about PRISM* [en línea]. 17 de julio de 2013. Disponible en: `http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet`

TechCruch. *Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program* [en línea]. Frederic Lardinois, 6 de junio de 2013. Disponible en: `http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/`

FayerWayer. *Gobierno de EE.UU. dice que PRISM es para recolectar datos de extranjeros* [en línea]. Cony Sturm, 7 de junio de 2013. Disponible en: `http://www.fayerwayer.com/2013/06/gobierno-de-ee-uu-dice-que-prism-es-para-recolectar-datos-de-extranjeros/`

TechCruch. *U.K. Security Agency Also Tapped Into The NSA's PRISM Surveillance Program* [en línea]. Frederic Lardinois, 7 de junio de 2013. Disponible en: `http://techcrunch.com/2013/06/07/u-k-security-agency-also-tapped-into-the-nsas-prism-surveillance-program/`

Genbeta. *Proyecto MUSCULAR: La NSA se habría infiltrado en las redes privadas de Google y Yahoo* [en línea]. Guillermo Julián, 30 de octubre de 2013. Disponible en: `http://www.genbeta.com/actualidad/proyecto-muscular-la-nsa-se-habria-infiltrado-en-las-redes-privadas-de-google-y-yahoo`

Genbeta. *Según Estados Unidos, la inteligencia española colaboró en el espionaje de llamadas* [en línea]. Guillermo Julián, 29 de octubre de 2013. Disponible en: `http://www.genbeta.com/actualidad/segun-estados-unidos-la-inteligencia-espanola-colaboro-en-el-espionaje-de-llamadas`

Genbeta. *La cifras del espionaje de la NSA en España: 60 millones de llamadas interceptadas en un mes* [en línea]. María González, 28 de octubre de 2013. Disponible en: `http://www.genbeta.com/actualidad/la-cifras-del-espionaje-de-la-nsa-en-espana-60-millones-de-llamadas-interceptadas-en-un-mes`

FayerWayer. *Agencias de España y Francia habrían colaborado con la NSA* [en línea]. Cony Sturm, 29 de octubre de 2013. Disponible en: `http://www.fayerwayer.com/2013/10/agencias-de-espana-y-habrian-espiado-a-los-espanoles-y-franceses-no-la-nsa/`

Genbeta. *La NSA interceptó las comunicaciones del Gobierno español y de otros 35 líderes mundiales* [en línea]. María González, 25 de octubre de

2013. Disponible en: http://www.genbeta.com/actualidad/la-nsa-intercepto-las-comunicaciones-del-gobierno-espanol-y-de-otros-35-lideres-mundiales

Xataka. *La NSA recolecta millones de direcciones de correo electrónico a nivel global* [en línea]. Javier Pastor, 15 de octubre de 2013. Disponible en: http://www.xataka.com/otros/la-nsa-recolecta-millones-de-direcciones-de-correo-electronico-a-nivel-global

La Primera Plana. *MUSCULAR es el proyecto de espionaje de EU en servidores de Google y Yahoo* [en línea]. 31 de octubre de 2013. Disponible en: http://laprimeraplana.com.mx/2013/10/31/muscular-el-proyecto-de-espionaje-de-eu-en-servidores-de-google-y-yahoo/

RTVE. *Berlín y París convocan a los embajadores de EE.UU. para pedir explicaciones por el espionaje* [en línea]. Agencias, 1 de julio de 2013. Disponible en: http://www.rtve.es/noticias/20130701/berlin-califica-inaceptable-espionaje-entre-socios-aliados/702520.shtml

The Washington Post. *Edward Snowden comes forward as source of NSA leaks* [en línea]. Barton Gellman, Aaron Blake y Greg Miller, 9 de junio de 2013. Disponible en: http://articles.washingtonpost.com/2013-06-09/politics/39856642_1_extradition-nsa-leaks-disclosures

El Blog de Carlos Tena. *Estos son algunos de los métodos y sistemas que la N.S.A. utiliza para obtener información* [en línea]. Carlos Tena, 31 de octubre de 2013. Disponible en: http://tenacarlos.wordpress.com/2013/10/31/estos-son-algunos-de-los-metodos-y-sistemas-que-la-n-s-a-utiliza-para-obtener-informacion/

Alt-Tab. *PRISM: qué es, posibles consecuencias, cómo evitarlo* [en línea]. Felipe, 17 de junio de 2013 . Disponible en: http://alt-tab.com.ar/prism-que-es-posibles-consecuencias-como-evitarlo/

Alt1040. *Estados Unidos a Snowden: "no habrá clemencia"* [en línea]. Santi Araujo, 4 de noviembre de 2013. Disponible en: http://alt1040.com/2013/11/edward-snowden-clemencia

FayerWayer. *Europa: Doble moral de espionaje* [en línea]. Manu Contreras, 4 de noviembre de 2013. Disponible en: http://www.fayerwayer.com/2013/11/europa-doble-moral-de-espionaje/

FayerWayer. *Snowden: "Quienes dicen la verdad no están cometiendo un crimen"* [en línea]. Fabrizio Ballarino, 4 de noviembre de 2013. Disponible en: http://www.fayerwayer.com/2013/11/snowden-afirma-que-las-reformas-propuestas-justifican-sus-filtraciones/

La voz de Galicia. *De la nube de ceniza a la nube de datos: Europa bloqueada* [en línea]. Víctor Salgado, 20 de abril de 2010. Disponible en: http://blogs.lavozdegalicia.es/victorsalgado/2010/04/20/de-la-nube-de-ceniza-a-la-nube-de-datos-europa-bloqueada/

National Archives. *La Constitución de los Estados Unidos de América 1787* [en línea]. Disponible en: http://www.archives.gov/espanol/constitucion.html

University of Missouri. *The Right of Privacy* [en línea]. Disponible en: http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

FayerWayer. *Ingenieros de Google dicen "que se joda" la NSA* [en línea]. Cony Sturm, 6 de noviembre de 2013. Disponible en: http://www.fayerwayer.

com/2013/11/ingenieros-de-google-dicen-que-se-joda-la-nsa/

Security By Default. *Cómo queda la seguridad post Snowden* [en línea]. 7 de noviembre de 2013. Disponible en: http://www.securitybydefault.com/2013/11/como-queda-la-seguridad-post-snowden.html

FayerWayer. *SIBIOS, ¿el PRISM argentino?* [en línea]. Fabrizio Ballarino, 7 de noviembre de 2013. Disponible en: http://www.fayerwayer.com/2013/11/sibios-el-prism-argentino/

FayerWayer. *La CIA le estaría pagando a AT&T para revisar las llamadas internacionales* [en línea]. Cony Sturm, 7 de noviembre de 2013. Disponible en: http://www.fayerwayer.com/2013/11/la-cia-le-estaria-pagando-a-att-para-revisar-las-llamadas-internacionales/

La Kolmena. *PRISM. Vamos a cuidar nuestra privacidad en Internet* [en línea]. Disponible en: http://www.lakolmena.com/blog/prism-vamos-a-cuidar-nuestra-privacidad-en-internet/

Glosario

9/11 Atentados del 11 de septiembre de 2001.

AT&T AT&T es una compañía estadounidense de telecomunicaciones. Provee servicios de voz, vídeo, datos, e Internet a negocios, clientes y agencias del gobierno.

Bundesnachrichtendienst Bundesnachrichtendienst (en español, Servicio Federal de Inteligencia o Servicio Federal de Información) es la agencia de inteligencia policial extranjera del gobierno alemán. Esta institución está bajo el control directo de la Oficina del Canciller.

CIA Central Intelligence Agency (en Español, Agencia Central de Inteligencia) es la agencia gubernamental de Estados Unidos encargada de la recopilación, análisis y uso de inteligencia, mediante el espionaje en el exterior, ya sea a gobiernos, corporaciones o individuos que puedan afectar la seguridad nacional del país.

CNI El Centro Nacional de Inteligencia es el servicio de inteligencia de España. Su función es proporcionar información, estudios y análisis al Gobierno y a su presidente que permitan prevenir y evitar peligros, amenazas o agresiones contra la independencia y la integridad de España.

Conmutador de red Un conmutador, o switch, es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

FBI Federal Bureau of Investigation (en Español, Oficina Federal de Investigación) es la principal rama de investigación del Departamento de Justicia de los Estados Unidos.

FISA Foreign Intelligence Surveillance Act (en Español, Ley de Vigilancia de Inteligencia Exterior) es una ley de los Estados Unidos que establece los procedimientos para la vigilancia física y electrónica y la recopilación de "información de inteligencia extranjera" entre "potencias extranjeras" y "agentes de potencias extranjeras". Esta ley no se aplica fuera de los Estados Unidos.

GCHQ Government Communications Headquarters (en español, Cuartel General de Comunicaciones del Gobierno) es uno de las tres servicios de inteligencia del Reino Unido y pertenece al Ministerio de Asuntos Exteriores británico.

LOPD Acrónimo de Ley Orgánica de Protección de Datos.

NSA National Security Agency (en español, Agenciad de Seguridad Nacional) es una agencia de inteligencia criptológica del Gobierno de los Estados Unidos, administrada como parte del Departamento de Defensa.

Patriot Act Patriot Act (en Español, Ley Patriótica) es un texto legal estadounidense promulgado el 26 de octubre de 2001, cuyo objetivo es ampliar la capacidad de control del Estado en aras de combatir el terrorismo, mejorando la capacidad de las distintas agencias de seguridad estadounidenses al coordinarlas y dotarlas de mayores poderes de vigilancia contra los delitos de terrorismo.

UE Acrónimo de Unión Europea.