EL ESTADO VIGILANTE[1]

Los archivos de la NSA y la respuesta global

Ben Hayes
Investigador del Transnational Institute y de Statewatch

> «[I]ncluso si no estás haciendo nada malo, te están observando y grabando. Y la capacidad de almacenamiento de estos sistemas aumenta cada año de forma continuadaen varios órdenes de magnitud,* y está llegando al punto en que no hace falta que hayas hecho nada malo. Simplemente tienes que resultarle a alguien sospechoso, incluso por una llamada inapropiada. Y entonces pueden usar este sistema para retroceder en el tiempo e investigar cada decisión que has tomado, cada amigo con quien has debatido algo alguna vez. Y esto sirve para atacarte, para crear sospecha sobre una vida inocente y pintar a cualquieracomo malhechor…».
>
> Edward Snowden, junio 2013

El Estado vigilante al desnudo

Si alguien nos ha dicho algo relevante sobre el poder del Estado en 2013 fue Edward Snowden, que reveló cómo la capacidad de vigilancia de algunos gobiernos democráticos occidentales son de tal magnitud que pueden acceder prácticamente a todo lo que sus ciudadanos hacen *on line* o con un teléfono móvil o fijo, en ausencia de controles democráticos o judiciales significativos.

Estos poderes están especialmente avanzados en la alianza *Five Eyes* [Cinco ojos], liderada por EEUU-Reino Unido (y que también incluye a Australia, Canadá y Nueva Zelanda), pero se sabe o se sospecha que muchos otros países europeos y de la OTAN disponen de estructuras de vigilancia avanzadas y han cooperado estrechamente con la Agencia Nacional de Seguridad (NSA, por sus siglas en inglés) de EEUU y la Sede de Comunicaciones del Gobierno del Reino Unido (GCHQ, por sus siglas en inglés). Con una industria global de vigilancia en

1 Traducción: Nuria del Viso.

* La expresión órdenes de magnitud (by *orders of magnitude*) se refiere a la multiplicación de un número dado por 10 (N. de la T.)

expansión dispuesta a ayudarles, es simplemente inconcebible que gobiernos mucho menos democráticos no estén implicados en las mismas prácticas.

No es noticia que los espías espían, o que los poderosos utilizan la vigilancia y la subversión para mantener su poder y su ventaja comparativa. En este sentido, que EEUU-Reino Unido "pincharan" las llamadas telefónicas de destacados políticos es una especie de atracción secundaria conveniente (la historia real es la facilidad con la que lo hicieron); lo que es nuevo e importante del estado del poder es la simplicidad con la que determinados individuos y poblaciones enteras pueden ser puestas bajo vigilancia, el papel crucial que desempeñan las empresas privadas para facilitar esa vigilancia y la ausencia de poder y autonomía que como sujetos tenemos para decidir cómo nos gobernamos y qué ocurre con la información sobre nosotros.

En respuesta a las revelaciones, los directores de prensa y los que destaparon el asunto de los gobiernos se han unido a más de 300 ONG y 500 destacados autores de todo el mundo para pedir un punto final a la vigilancia masiva e indiscriminada; también está circulando una declaración de Académicos contra la Vigilancia Masiva. Campañas nacionales ya con historia contra la vigilancia han rejuvenecido con las revelaciones de Snowden y un grupo de Parlamentos y organizaciones intergubernamentales están concediendo atención al asunto por primera vez. Pero de ninguna manera estas campañas en alza son garantía de una reforma significativa. Este artículo examina algunos de los principales debates en torno a la reforma sobre la vigilancia y las batallas que nos aguardan.

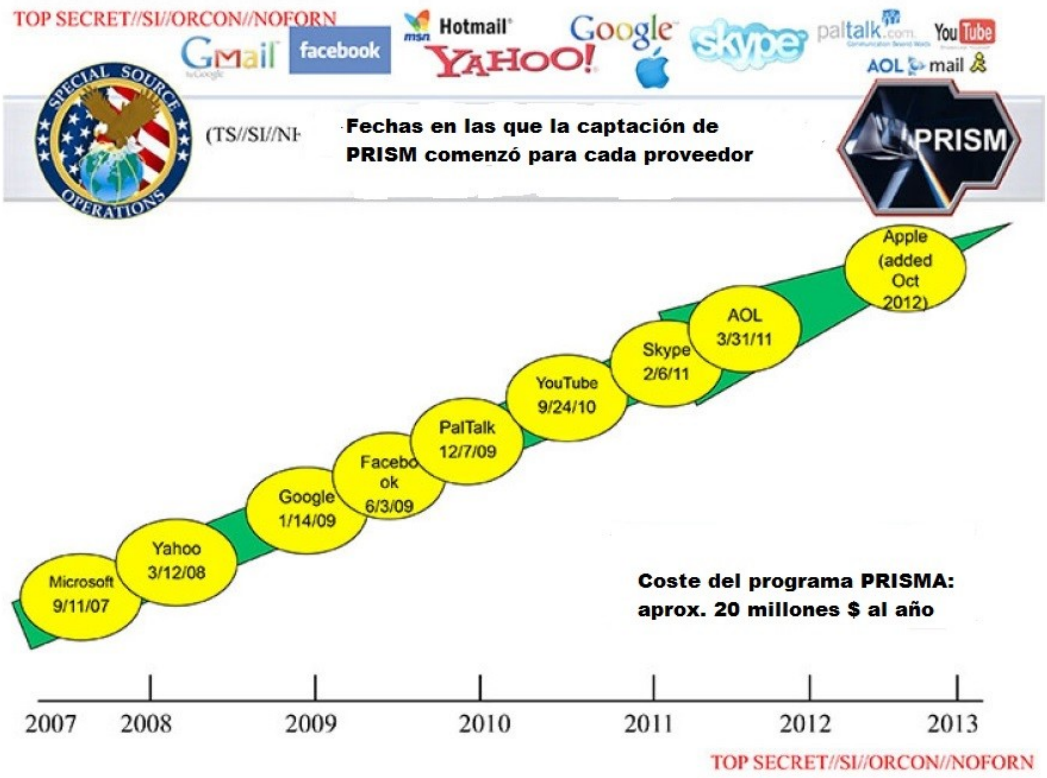
Revelaciones clave

Una mínima fracción de los documentos secretos liberados por Edward Snowden ha sido publicada o ha sido mencionada por los periodistas. Mientras que a Glenn Greenwald y sus compañeros se les ha acusado de todo tipo de delitos, desde apoyar a terroristas y pedófilos a traficar y esconder información peligrosa, ellos han sido tanto sensatos como responsables en la forma en que han revelado la información. Además, las noticias con cuentagotas que revelan la complicidad de un grupo cada vez mayor de empresas y países han garantizado que una de las historias de libertades civiles más importantes de los últimos tiempos ha ocupado la primera plana de los medios de comunicación en todo el mundo durante más de seis meses. Ninguna otra filtración en la historia ha alcanzado esta hazaña. Los "momentos culminantes" de los archivos de la NSA desvelados hasta ahora incluyen:

- La orden judicial *Verizon*: el primero de los filtrajes de Snowden reveló que la NSA guardaba las grabaciones telefónicas de millones de americanos.

Aunque la iniciativa fue lanzada por la administración Bush, mucha gente creía que Obama la había suprimido.

- Programa PRISM: permite a la NSA y al GCHQ “recabar” información de los servidores de algunas de las mayores empresas tecnológicas de EEUU (Google, Apple, Microsoft, Facebook, AOL, PalTalk y Yahoo). Un programa similar llamado Muscular interceptaba millones de registros al día de Yahoo y Google.
- Tempora, parte del programa Mastering the Internet: el GCHQ intercepta y almacena la mayor parte de los datos que entran y salen del Reino Unido a través de los cables de fibra óptica submarina, que son las venas de la World Wide Web. Programas similares de “interceptar a bulto” gestionados por la NSA (Blarney, Fairview, Oaksatar y Stormbrew).
- Xkeyscore: un sistema de recuperación de datos utilizado por la NSA y usado para acceder a emails, llamadas telefónicas, registros de uso de internet y documentos transmitidos en internet.
- Boundless informant: un sistema de análisis y visualización de datos que proporciona una visión de conjunto de las actividades de vigilancia de la NSA por país o programa. Casi 3.000 millones de “unidades de datos” del interior de EEUU fueron capturados por la NSA durante un periodo de 30 días en marzo de 2013, según informaciones.
- Bullrun y Edgehill: un programa de 250 millones de dólares al año bajo el que la NSA y la GCHQ (respectivamente) rompieron la mayor parte dela tecnología deencriptación, que es la base de la seguridad de internet.
- Ciberguerra, espionaje y conspiración: revelaciones posteriores han detallado hasta qué punto EEUU está preparado para utilizar ciberataques internacionalmente «para impulsar los objetivos de EEUU en todo el mundo», el seguimiento de llamadas telefónicas a 35 líderes mundiales y la complicidad en la vigilancia NSA-GCHQ de los servicios de inteligencia de, entre otros, Bélgica, Dinamarca, Francia, Alemania, Italia, Japón, Holanda, Noruega, Singapur, Corea del Sur, España y Suecia.



Fuente: Diapositivas de la NSA, *The Washington Post*, junio de 2013

«A través de cualquier medio»

Como Snowden explicó desde el principio, este despliegue desconcertante de programas secretos de vigilancia demuestra la dimensión a la que la "comunidad de inteligencia" llegará para «obtener información donde pueda y por cualquier medio posible».

Se están vigilando redes completas de comunicación, ya sea "legalmente" (en el sentido de que el acceso a los datos que transportan es requisito legal sancionado por orden judicial que ofrece una ámbito de actuación sin límites), bajo acuerdos de cooperación "voluntarios" (entre las agencias de inteligencia y las empresas propietarias de estas redes) o a través de "pinchazos" promovidos por los estados (interceptación de cables de fibra óptica y centros de datos que albergan esas redes).

La NSA también ha estado creando "puertas traseras" en las aplicaciones y software de algunas de las mayores compañías TIC del mundo y utilizando software malicioso para robar información de redes privadas, gubernamentales y empresariales. Existe un documento que sugería que la NSA ha "infectado" más de 50.000 redes de ordenadores en todo el mundo.

Juntos, la NSA y la GCHQ han puesto en peligro la criptografía que permite la transmisión segura de información a través de la mayor parte de internet. Tim Berners-Lee, inventor de la World Wide Web, calificó sus maniobras de

«abominables y estúpidas» porque «beneficiarían a los grupos criminales de hackers y a los estados hostiles», y añadió que él estaba «muy de acuerdo con los intentos de aumentar la seguridad contra el crimen organizado, pero te tienes que distinguir del criminal».

A menos que creas que las actividades reseñadas más arriba son actos totalmente apropiados para los gobiernos democráticos, las acciones de Edward Snowden son la encarnación de la actuación con principios para destapar la olla y le debemos enorme gratitud. El hecho de que se ha visto forzado a pedir asilo en Rusia, no solo de EEUU, sino de los socios europeos, algunos de los cuales mostraron un desprecio sin precedentes por las convenciones diplomáticas al obligar a aterrizar el avión del Presidente de Bolivia para buscar a Snowden, deshonra a todos los involucrados y dice mucho de los valores y los intereses de los actuales gobiernos occidentales.

Grandes bases de datos, mayores problemas

Al considerar cómo la vigilancia encaja en el actual estado del poder, que ha cambiado completamente desde los tiempos en que la Stasi tuviera a poblaciones enteras fichadas, es que infraestructuras privadas se ha convertido en la primera línea de la recopilación de información. A su vez, la vigilancia masiva de la población ya no es solo el elemento que preserva a los regímenes totalitarios, sino un elemento básico de países democráticos.

La revolución en las tecnologías de la información y las comunicaciones (TIC) está transformando nuestras relaciones con todos y con todo. A medida que más y más de nuestras relaciones se desarrollan *on line* −las interacciones con amigos y conocidos se producen a través de las redes sociales; con empresas y proveedores de servicios a través del comercio electrónico; con bancos y con servicios electrónicos de la administración y con campañas políticas−, se recopila más y más información sobre nosotros. Todo se graba, almacena y analiza, mientras que cada año se fortalecen los argumentos económicos y organizativos para guardar esos datos eternamente.

Lo que hacemos en el mundo digital traiciona nuestros pensamientos, intereses, hábitos, atributos y características. Y como especie se pone de manifiesto que somos totalmente predecibles: “embarazosamente”, según un ex consejero general de la NSA. A medida que más y más de las cosas que poseemos están conectadas al mundo digital y utilizamos más y más servicios *on line*, producimos más información sensitiva y completa: dónde estuvimos, qué hicimos y con quién.

Dejamos estos datos por todas partes. Incluye datos personales (información que nos identifica), de contenido (lo que escribimos y decimos) y "metadatos" (datos sobre datos, como registros de llamadas, tráfico de internet, datos de localización, etc.). Muchas innovaciones digitales se basan en la recogida y análisis de esta información, desde los mapas en nuestros *smart phones* a las numerosas aplicaciones a través de las cuales se comparte y consume la información y la cultura. La necesidad de protegernos de las agencias de inteligencia y seguridad, empeñadas en sortear nuestro derecho a la privacidad, constituye solo una parte del problema. También necesitamos saber que estamos protegidos de esas compañías, cuyo balance depende de acceder (y mercantilizar) cuanta información personal sobre nosotros les sea posible.

Ambos problemas se agudizan por un tercero: los "*big data*", o grandes bases de datos, que es menos un concepto que un lema del *marketing* para encapsular una nueva industria. «¿Tiene una gran base de datos? Le ayudamos a entender a sus clientes, usuarios, empleados, redes, amenazas, riesgos, oportunidades, etc.». Aquí es donde la "cara oculta" de las TIC –lo que Naomi Klein describió atinadamente como la «fusión entre el centro comercial y la prisión secreta»– se muestra sin tapujos. Los mismos algoritmos y herramientas de análisis que usa Facebook para entender tus intereses y deseos, y que Amazon utiliza para calcular (y calcular erróneamente) qué más puedes querer comprar, pueden ser utilizados por gobiernos y compañías de seguridad privadas para calcular (y calcular erróneamente) si puedes ser una amenaza, ahora o en el futuro. Y es precisamente la naturaleza de "doble uso" de esta tecnología lo que la hace tan difícil de regular. «No es un sistema de vigilancia, es un conjunto analítico de datos», es el discurso en el que se basa este pujante comercio internacional en un formato verdaderamente orwelliano.

Cuestionar las redes de vigilancia que desveló Edward Snowden es relativamente sencillo: se trata de agencias de inteligencia y seguridad que actúan sin freno en una infraestructura digital insegura y utilizan poderes fuera de control heredados de la era analógica, parafraseando a Human Rights Watch. Lograr reformas de relevancia que aborden adecuadamente este problema es mucho más difícil en virtud de los intereses que existen para mantener el *status quo* y los problemas jurisdiccionales que surgen frente a cualquier intento de restricción de las redes de vigilancia transnacionales. Estas cuestiones remiten a cambios profundos en las relaciones entre la ciudadanía, los Estados y las corporaciones.

¿Silicon Valley vs NSA?

En diciembre de 2013 ocho de las firmas tecnológicas de más éxito de Silicon Valley –Aol, Apple, Facebook, Google, Linkedin, Microsoft, Twitter y Yahoo–

hicieron un llamamiento a favor de «cambios a gran escala» de la vigilancia del Gobierno de EEUU basado en cinco principios de reforma: i) “límites razonables” a la recogida de información del Gobierno y el fin de la “captura masiva de datos”; ii) mayor control y rendición de cuentas de las agencias de inteligencia; iii) transparencia sobre las demandas del gobierno y poderes de vigilancia; iv) respeto al “libre flujo de información” y v) un “marco robusto, transparente y basado en principios” para regular peticiones lícitas de datos a través de las jurisdicciones.

Esta iniciativa se basa en pasos tentativos anteriores a favor de una mayor transparencia en la vigilancia en virtud de la cual algunas de estas compañías han publicado información comparativa sobre las demandas del Gobierno y autoridades competentes de los datos de sus usuarios, mientras pedían al Gobierno de EEUU que les permitiera publicar información de los −hasta entonces− tratos secretos con la NSA. Es de destacar que las compañías de telefonía fija y móvil, muchas de las cuales han estado facilitando información al Estado sin cuestionarlo durante mucho más tiempo que sus contrapartes de internet, no han intervenido en el debate de la misma manera; aunque tampoco se pronunciaron nunca a favor de la democracia.

Dice mucho sobre el estado del poder el hecho de que lo que preocupara y moviera a la acción a la Casa Blanca fuera que las revelaciones pudieran perjudicar especialmente a algunas de las corporaciones más poderosas de EEUU. Pero también plantea cuestiones más generales sobre cómo se ejerce el poder corporativo. Algunas de estas compañías han colaborado (en muy distintos niveles) en la vigilancia estatal, pero algunas también han resistido ferozmente la tentativa de una legislación diseñada para dar a los individuos mayor control el destino de sus los datos personales, datos de los que dependen los márgenes de beneficio de tales corporaciones, incluidas las aportaciones al borrador de la UE sobre Regulación de la Protección de Datos.

«Te ayudaremos a protegerte de la vigilancia gubernamental, pero no hace falta que te protejas de nosotros» es una propuesta para un grupo de compañías que, según *Forbes*, destinaron más de 35 millones de dólares a actividades de *lobby* el año pasado. Google absorbió la mitad del total (18,2 millones de dólares); si se excluyen las asociaciones patronales y grupos de presión, solo General Electric admite gastar más en *lobby* (Microsoft, 8,1 millones de dólares; Facebook, 3,9 millones; Yahoo; 2,8 millones y Apple, 2 millones, conforman casi la totalidad del resto hasta el total de 35 millones).

No cabe duda de que estas compañías se oponen sinceramente a la vigilancia y almacenamiento de datos masivo que lleva a cabo la NSA porque es un riesgo genuino al espíritu de su negocio. Como indica el Consejo General de

Microsoft, «la gente no utilizará tecnología de la que no se fía. Los gobiernos han puesto en riesgo esa confianza y los gobiernos tienen que restaurarla». Pero al mismo tiempo que sus máximos dirigentes se dirigen a Davos para demandar más transparencia y control de la vigilancia para preservar la "integridad de internet", debemos preguntarnos qué más buscan y reciben de nuestros líderes y legisladores. También debemos preguntar al sector tecnológico europeo dónde se sitúan respecto a la reforma en la vigilancia y por qué no ha asumido sus responsabilidades.

¿Europa vs el "Gran Satán"?

La indignación pública ante las revelaciones de Snowden es tal que actualmente hay capital político significativo vinculado a la reforma de la vigilancia. Pero lo que se han considerado críticas y demandas de cambio procedentes de Angela Merkel y Barack Obama no han ido paralelas, al menos hasta ahora, con la acción política. Ciertamente, a pesar de las reformas cosméticas, existe poca evidencia de que haya verdadera voluntad de cambios estructurales más profundos tan notoriamente necesarios.

Los gobiernos de la UE aprobaron una declaración conjunta de crítica a su socio transatlántico y avisando de un derrumbe de la confianza, pero no han anunciado ninguna sanción.

Los gobiernos europeos, que han expresado abiertamente sus críticas a las actividades de EEUU y el Reino Unido, han buscado simultáneamente asegurar que las actividades de sus propios aparatos de seguridad e inteligencia nacionales se mantuvieran fuera del debate. La canciller alemana, Angela Merkel, ha hecho una gran trabajo de interpretación para las audiencias internas (la NSA "como la Stasi", "los amigos no se espían entre sí", etc.) mientras que ignoraba en gran medida la inquietud ampliamente compartida por la vigilancia interna y enviaba un grupo de negociadores de Washington en lo que primero pareció como un intento de garantizar la admisión de Alemania en el club *Five Eyes*. En connivencia con el Reino Unido, el Gobierno alemán también bloqueó la rápida adopción del borrador para regular la protección de datos en la UE, solicitado por el Parlamento Europeo y la Comisión, paralizando unas necesitadas reformas largamente debatidas.

El Gobierno francés describió las prácticas de la NSA como "totalmente inaceptables" antes de incluir en la Ley de Defensa 2014-2019 provisiones que garantiza la expansión de sus poderes a sus propios servicios de seguridad para grabar conversaciones telefónicas, acceder a emails, realizar localización y acceder a otros metadatos sin ninguna supervisión judicial. Mientras tanto el Gobierno británico, cuyo espionaje sobre sus socios comunitarios seguramente

representa una transgresión contra “amigos” de una magnitud mucho mayor a todo lo realizado anteriormente por EEUU, ha sido el más cínico al rechazar cualquier crítica, describiendo a los críticos de la GCHQ como tipos “fantasiosos” y animando a una caza de brujas contra *The Guardian.* El socio de Glenn Greenwald[2] fue detenido en el aeropuerto de Heathrow bajo las leyes antiterroristas y bajo la supervisión de agentes estatales destruyeron un portátil propiedad del periódico. Todo ello no presagia nada bueno sobre el estado de la democracia en ese país.

La Comisión Europea, desprovista de cualquier poder en lo que respecta a las políticas de seguridad nacional de los Estados miembro de la UE, ha sido muy franca sobre el espionaje de la NSA, pero en la práctica se ha reducido a lanzar amenazas y desaprobaciones señalando con el dedo en la dirección de Silicon Valley, lo que es un poco inconsistente, ya que algunos de los acuerdos de vigilancia de las comunicaciones en Europa son igual de problemáticos. El Tribunal de Justicia de la UE ha indicado que muy probablemente anulará una directiva impulsada por la Comisión que obligaba a los servicios de telecomunicaciones y grandes suministradores de internet a conservar por ley los metadatos durante 24 meses con fines de seguridad; esta decisión se debe a que no fue capaz de hacer un seguimiento judicial adecuado (o, de hecho, estipular cualquier restricción sobre el acceso a datos).

El Parlamento Europeo ha completado una investigación sobre la vigilancia de la ciudadanía comunitaria por la NSA y sus homólogos europeos, pero sin el poder para obligar a los testigos a declarar, ha dependido de periodistas, promotores de campañas y expertos independientes. Su borrador de recomendaciones, que no son vinculantes en la UE, incluirían probablemente la suspensión de varios acuerdos para compartir datos con EEUU hasta que se implante la privacidad recíproca y derechos de protección de datos, el desarrollo de una “nube de la UE” y la reforma de los programas europeos de vigilancia masiva.

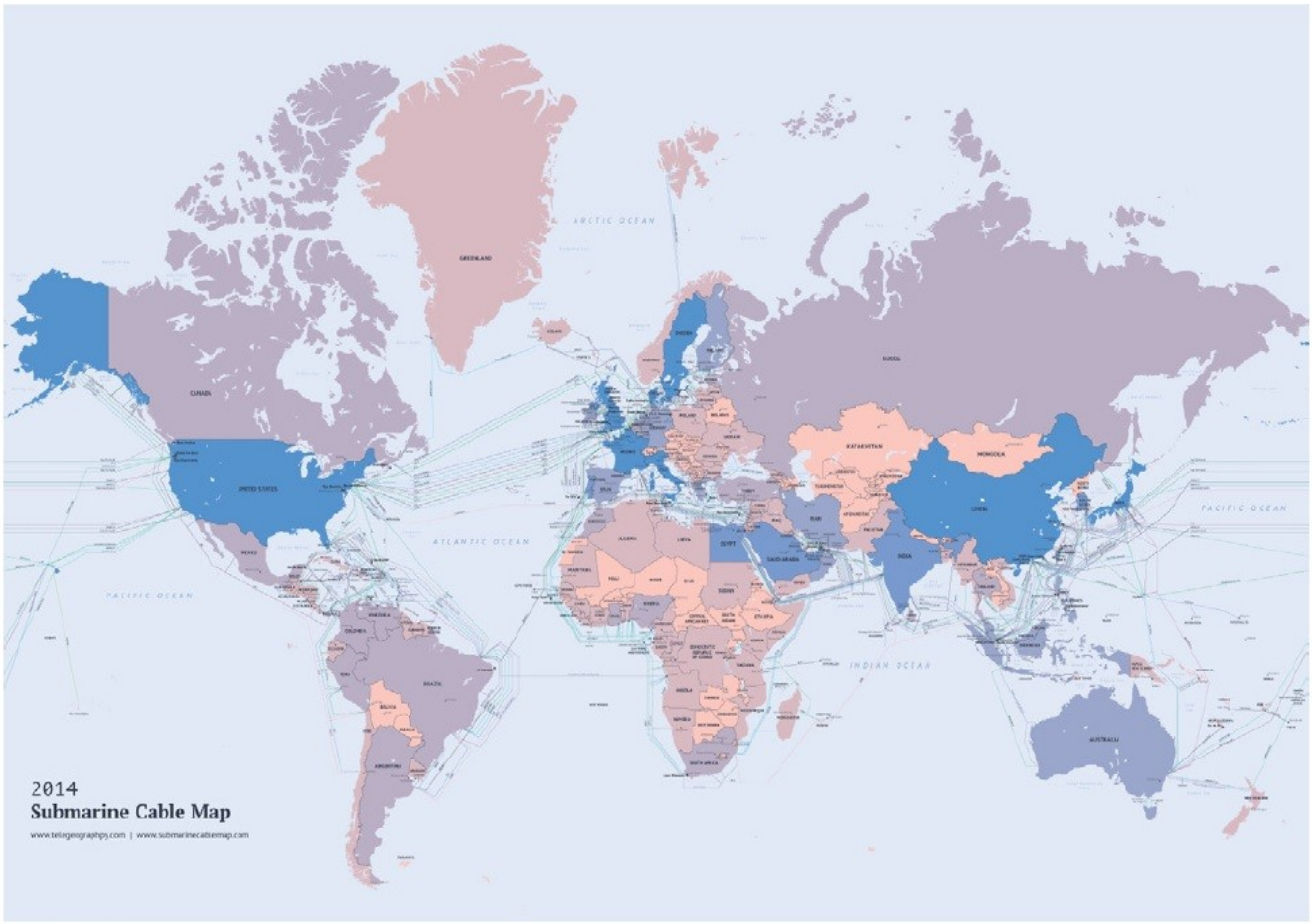
En lo que respecta a EEUU, a pesar de todas las opiniones sobre el terrible estado de la democracia en el país, va muy por delante de los Estados miembros de la UE en lo referente a las reformas internas que pueden ser necesarias para proteger a sus ciudadanos de las extralimitaciones de la inteligencia. Un juez federal ha emitido una norma preliminar en la que señala que la recopilación masiva de registros telefónicos viola probablemente la Constitución de EEUU, calificando la práctica de “indiscriminada”, “arbitraria” y “casi orwelliana”. Este sentimiento tuvo eco en un Informe presidencial del Grupo de Inteligencia y

---

2 Glenn Greenwald es un abogado constitucionalista estadounidense, columnista, bloguero y escritor. Desde agosto de 2012 hasta octubre de 2013 fue columnista de la edición estadounidense de The Guardian. Fuente: Wikipedia [N. de la T.].

Tecnologías de Comunicaciones, cuyas 46 recomendaciones, si se implementan al completo, conducirá al menos a frenar los poderes de vigilancia de la NSA. El tiempo dirá si Obama da la batalla; los antecedentes históricos no son muy alentadores.

Mapa de comunicaciones por cable submarino



Telegeography 2014

Legalidad internacional vs. seguridad (trans)nacional

La cuestión es si vivimos en un mundo donde la NSA y sus aliados pueden hacer lo que quieran en internet y los secretos que guarda, o si se trata de respetar el Estado de derecho y los principios universales de derechos humanos, en concreto, el derecho a la privacidad, un derecho del que dependen muchos otros. Como señaló Edward Snowden, «No quiero vivir en un mundo en el que todo lo que diga, lo que haga o todos aquellos a los que hable, cada expresión de creatividad, de amor o de amistad sea grabada».

Los límites a los poderes “internos” de espionaje están recogidos en mayor o menos medida en las constituciones nacionales, que deben garantizar

claramente a los ciudadanos derechos de privacidad y la protección contra interferencias indebidas del Estado.

Mucho más problemático es que las personas originarias de otros países –que habitualmente no disfrutan de los mismos derechos de ciudadanía– pueden convertirse fácilmente en objeto de vigilancia por parte de algún Estado. Se trata de una cuestión crucial por dos razones. Primera, las comunicaciones digitales con frecuencia pasan a través del territorio o jurisdicción de diferentes países, particularmente por EEUU, destino de la mayoría del tráfico mundial de internet. Esto significa que si no eres un ciudadano estadounidense, cualquier derecho constitucional de privacidad que puedas tener en tu país de origen es prácticamente inservible a medida que navegas amplias áreas de internet. Segunda, mientras que el principal protagonista del caso de los archivos de la NSA es, por supuesto, EEUU, esa agencia figura en el centro de una red de inteligencia transnacional de alcance global que aún se guarda en secreto y que opera prácticamente sin regulación. Esta es la razón, según Privacy International, de que abrir *Five Eyes* sea un prerrequisito para restringir sus poderes de forma significativa.

El comité de evaluación de la administración Obama sorprendió a algunos recomendando que la vigilancia a ciudadanos no estadounidenses fuera sometida a controles más estrictos y que su derecho a la privacidad fuera reconocido, pero, de hecho, descartó dar protección judicial a personas objeto de vigilancia extranjera y propuso rebajar el umbral para considerar una “creencia razonable” (más que causa probable) de vigilancia requerida en interés de la seguridad nacional. Tampoco las personas fuera de EEUU se benefician de las obligaciones propuestas por la NSA para minimizar los datos guardados de ciudadanos estadounidenses.

Es improbable que esto satisfaga a los críticos europeos de las prácticas de EEUU o a los del Gobierno brasileño, que demanda que todos los proveedores de servicios de telecomunicaciones extranjeros que operan en Brasil tengan sus servidores en ese país, de modo que los datos de sus ciudadanos estén sujetos exclusivamente a la ley brasileña. Con la amenaza de otros países de actuar en la misma dirección, no son solo las empresas las que previenen para que se evite la “balcanización” de internet, a medida que las normas actuales y los estándares técnicos quedan pulverizados.

Mientras que “el verano de Snowden” demostró el poder de la NSA y de las grandes compañías tecnológicas, también ha mostrado la debilidad de la normativa internacional y del actual sistema de gobernanza. La legalidad y jurisprudencia de derechos humanos deja poco margen de duda de que lo que *Five Eyes* y otras estructuras han estado haciendo contraviene tanto la letra como

el espíritu de la legalidad internacional. No se trata solo de que han sido ignorados los estándares de derechos humanos; la cuidadosa elaboración de marcos de asistencia legal mutuos (que permiten a los Estados solicitar y acceder a información o evidencia mutuamente sobre sus respectivos ciudadanos) durante décadas se han adelgazado desde el 11-S.

Los defensores de la gobernanza global deberían estar reclamando acuerdo internacionales que limiten la vigilancia al tiempo que consagren los derechos individuales de privacidad y el proceso debido, pero actualmente es inconcebible que los Estados acepten cualquier tratado internacional que pretenda limitar sus estructuras de seguridad. Es fácil de anticipar que las corporaciones que manejan estas enormes cantidades de información se resistirán a cualquier intento de regular el derecho a la privacidad o la protección de datos en la legalidad internacional. A pesar de todo el debate en torno a la reforma sobre la vigilancia, es significativo que los principios de Silicon Valley no hagan mención en absoluto a ningún derecho individual, digital o de otro tipo. Sin embargo, existe un apoyo tangible y creciente hacia tales medidas.

La Asamblea General de la ONU ha aprobado recientemente una Resolución pionera (propuesta por Alemania y Brasil) sobre “El derecho a la privacidad en la era digital”, aunque solo vinculante para el Alto Comisionado para los Derechos Humanos de la ONU, que recibirá el encargo de preparar un informe sobre el asunto. También se ha sugerido un nuevo protocolo opcional de la Convención Internacional de Derechos Civiles y Políticos, pero incluso si logra congregar a la clase política, en el mejor de los casos, llevará años alcanzar un acuerdo, y mucho más ratificarlo. En el corto plazo, las medidas nacionales que limitan la vigilancia por parte de agencias de inteligencia son la única vía significativa de reforma.

Agujas vs pajares

Las revelaciones de Edward Snowden ya han inspirado una serie creciente de retos legales y los tribunales en Europa y EEUU se encuentran ante la petición de sopesar la legalidad de lo revelado, que contravienen las leyes de respeto a los derechos humanos y al proceso debido. Se trata de la encarnación más reciente del debate, ya con una década de antigüedad, sobre la necesidad de equilibrar libertad y seguridad y las nuevas prácticas introducidas bajo la guerra contra el terror. La libertad ha estado mucho tiempo en la parte perdedora; es de esperar que Snowden haya revertido esta tendencia. En la arena política este debate ha tomado la forma de lucha contra la vigilancia masiva e indiscriminada y a favor de leyes que limiten la vigilancia solo a los casos estrictamente necesarios, una vigilancia enfocada y proporcionada.

Lo que a menudo ignoran estos debates es el cambio fundamental de lo que hoy implica la seguridad nacional, desde la recopilación de datos intensiva en empleo de la era Hoover y MacCarthy a los grandes bancos de datos y procesamiento intensivo de información de la NSA que dirige actualmente Keith Alexander. En este sentido, la lucha de poder se establece actualmente entre el sistema de controles y contrapesos de la democracia liberal del siglo XX, enraizados en los Estados-nación y la regulación de poderes investigativos, y un nuevo modelo basado en la vigilancia masiva transnacional y "preventivo" desarrollado en el siglo XXI. La dificultad de tratar de hacer que este nuevo modelo respete las tradicionales nociones de causa probable y proceso debido surge del hecho de que muchos de los métodos que utiliza son antitéticos a tales nociones.

La prevención ha estado durante mucho tiempo en el núcleo de la misión de seguridad nacional del Estado. Mientras que la vigilancia policial en una investigación por actividades criminales debe iniciarse sobre la base de que existe una "causa probable" que un sospechoso merece atención, seguido de autorización judicial para evitar medidas intrusivas, las agencias de seguridad nacional se ocupan básicamente de identificar amenazas y mitigar riesgos antes de que se materialicen. Después del 11-S este paradigma de gestión del riesgo se ha extendido por todo el aparato de la seguridad nacional hasta englobarlo todo, desde la detención preventiva a las listas negras secretas y los asesinatos extrajudiciales por ataques de *drones*, atizando la represión estatal en todo el mundo y promoviendo el cerco a cualquiera que desafíe al *statu quo*.

Forzados por primera vez a defender sus programas de recopilación masiva de datos, los jefes de inteligencia han repetido el mismo mantra una y otra vez: «necesitamos el pajar para encontrar la aguja». En consecuencia, se argumenta que cualquier freno a la vigilancia compromete la seguridad nacional. Mientras que esta afirmación puede resultar una defensa conveniente de la vigilancia masiva, la realidad es que la policía y los servicios de inteligencia han accedido por igual desde hace mucho a los "pajares" en una lógica de caso por caso, o incluso de forma amplia; lo que Snowden ha revelado es la construcción de un pajar masivo compuesto por tantos datos históricos como sea posible que permitan a la NSA y sus aliados rebobinar literalmente lo que sus ciudadanos han estado haciendo en momentos concretos.

La primera prueba para una reforma significativa de la vigilancia se concreta en que las agencias de inteligencia den por terminada la recogida masiva de datos. Dada la cultura de la vigilancia entre cientos de miles de agentes estatales y contratistas y la infraestructura en la que ha invertido la NSA para facilitar esta vigilancia masiva (acaba de construir uno de los centros de almacenamiento de datos más grandes del mundo en Utah), no debemos

subestimar la magnitud de esta tarea. La segunda es evitar que las agencias estatales accedan a grandes bolsas de datos −no solo metadata de comunicaciones, sino datos financieros, de viajes, de salud, etc.− en ausencia de una razón legítima para hacerlo y una vigilancia efectiva de esas peticiones. Si vamos a proteger la presunción de inocencia y el derecho a la privacidad en un entorno de grandes cantidades de datos, entonces en último término necesitamos cortafuegos que limiten tanto la evaluación por perfil como que eviten las "expediciones de pesca" diseñadas para obtener motivos de sospecha entre los inocentes.

La tercera prueba apunta a circunscribir las condiciones bajo las que las agencias de seguridad e inteligencia pueden acceder a estos datos para satisfacer su cometido. Este desafío necesita tanto más transparencia por parte de aquellos que realizan la vigilancia (necesitamos saber quién y cómo se utilizan los "pajares" en la práctica) como una distinción mucho más clara entre los asuntos de seguridad nacional, por una parte, y la recogida de datos de inteligencia criminal por otra. Se trata realmente de determinar qué grado de la "guerra contra el terror" debe ser gestionada por agencias secretas de inteligencia y militares y qué grado debe ser procesada dentro de un marco del Estado de derecho. El cuarto reto es reemplazar los acogedores comités parlamentarios favorables al *establishment* que actualmente tienen la tarea de vigilar a estas agencias a través de sensatos mecanismos de control democrático.

En última instancia, el actual debate sobre la aguja y el pajar gira en torno a cuántos datos (si es que alguno) deberían ser retenidos por las compañías que los almacenan o transportan con propósitos legales o de seguridad y las circunstancias bajo las cuales puede accederse a ellos. El peligro reside en los pretextos y trucos que pueden normalizar la situación existente en lugar de examinar lo que se ha revelado. El panel de valoración de la NSA de Obama propuso poner fin a la recogida masiva de metadatos por la NSA, pero a cambio los proveedores de servicios los pueden conservar 30 meses y tener acceso a los datos controlados por los (tradicionalmente permisivos) tribunales de vigilancia.

Como se señaló anteriormente, la UE puede estar avanzando en la dirección opuesta: la recomendación de su Tribunal de Justicia ha visto con malos ojos su Directiva de Retención de Datos y el principio de conservar los datos mucho tiempo solo por si pueden resultar de utilidad a la policía y a agencias de seguridad.

Al final, ambas partes tendrán que resolver al menos algunas de sus diferencias en relación a los poderes de vigilancia y protección de la intimidad/privacidad si se ha de mantener o profundizar la cooperación UE/EEUU.

Esto puede incluso mejorar las perspectivas para el desarrollo de un acuerdo internacional sustantivo a largo plazo.

El Estado dentro del Estado en el que estamos

En la mayoría de demandas por la reforma en la vigilancia post-Snowden aparece casi en la cima de la lista más transparencia y control de los servicios de inteligencia. Sin embargo, se constata la falta de voluntad política a la hora de examinar cómo las democracias liberales han permitido a sus aparatos de inteligencia hacerse tan extraordinariamente poderosos y sin controles. Como escribió un ex juez británico después de las filtraciones de Snowden, «los aparatos de seguridad en muchas democracias son hoy capaces de imponer su poder sobre otros órganos del Estado que precisan de autonomía: promoviendo legislación que prioriza sus propios intereses sobre los derechos de los individuos, dominando el proceso de toma de decisiones al máximo nivel, excluyendo a sus antagonistas fuera de los procesos judiciales y operando prácticamente sin escrutinio público».

Esto es lo que combaten las campañas para la reforma de la vigilancia; es ingenuo pensar que las demandas de un mayor control a los poderes de vigilancia tendrán éxito fácilmente después de una década de intentos para que EEUU y sus aliados respondan por su papel en las “entregas extraordinarias”, tortura, detenciones ilegales secretas, internamiento y crímenes de guerra bajo la guerra contra el terror se han encontrado con tal resistencia (por no mencionar la conducta criminal que se remonta a mucho antes del 11-S). A lo largo de Europa y América del Norte, interrogatorio tras interrogatorio, juicio tras juicio, la ley ha dictaminado en la mayoría de los casos que se rectificara, mientras los Estados han cerrado filas y los gobiernos han adoptado una posición defensiva, ignorando o exonerando las acciones de sus agencias de inteligencia y seguridad. ¿Por qué? Porque los aparatos de seguridad nacional y de inteligencia internacional están íntimamente implicados en todo lo que los Estados hagan militarmente y en muchas de sus intereses y políticas económicas e internacionales. En geopolítica, las estructuras de vigilancia, o “conocimiento situacional”, está en el corazón de la proyección del poder duro y blando.

Otro tema fundamental en relación a muchos de los actuales llamamientos a la reforma en la vigilancia es que tratar de introducir de algún modo los mecanismos de control y contrapesos dentro de las agencias de vigilancia, que operan en secreto para adelantarse a las “amenazas” de enemigos conocidos y desconocidos, inevitablemente se convierte en un ejercicio contradictorio: llevado a su conclusión lógica, el argumento de que toda vigilancia debe ser necesaria, proporcionada y bajo un adecuado control democrático y judicial es realmente una razón para restringir de forma radical el mandato y poderes de los servicios de inteligencia y asignar en su lugar a la policía y a los servicios de investigación

criminal problemas como el del terrorismo. Gracias a la obsesión cercana al culto con la (in)seguridad en los medios de comunicación tal pretensión se equipara con la blasfemia.

Quizá esta es la razón por la que tantos activistas hablan de la vigilancia como si ocurriera en un vacío, ignorando el asombroso desarrollo de los aparatos de seguridad nacional, en particular desde el 11-S, su impacto sobre "comunidades sospechosas" y su relación con estrategias para luchar contra la "radicalización" y el "extremismo interno". El moreno es el nuevo negro, y el verde es el nuevo rojo.[3] En todo el mundo, la protesta pacífica y desobediencia civil que los demócratas afirman respetar es atacada como nunca por aquellos que (lógicamente) los partidarios de una acción directa más pacífica califican como "extremistas", o incluso "terroristas". La lucha contra la vigilancia sin control debe estar en el núcleo de las luchas por la justicia social.

También podemos preguntar cómo es que el neoliberalismo ha logrado capturar tantos servicios públicos bajo la retórica del despilfarro y ineficiencia, mientras que los "Altos Sacerdotes de los Estados Securitarios" pueden gastar a su antojo incontables billones en ejércitos de contratistas e instalaciones ideadas por diseñadores de los decorados de Hollywood. Después de asistir a MILIPOL, la XVIII edición de la exposición mundial de "seguridad interna para los Estados" en París, encuentro más difícil que nunca evitar la simple conclusión de que la razón es que lo que es bueno para la seguridad del Estado es bueno para los negocios, y viceversa.

La seguridad nacional, centrada en su mayor parte de una u otra forma en técnicas de vigilancia masiva, ya es un negocio multimillonario. Con él llega la difuminación creciente de los límites entre el ejército, la seguridad nacional y el orden público, y la manía por todo tipo de cachivaches, desde *drones* a armas "menos letales", tecnologías de control de masas, aplicaciones de vigilancia masiva, controles fronterizos militarizados y todo lo demás en el escaparate de MILIPOL.[4] Me pregunto cuántos de los grandes actores estarán ahora en Davos esgrimiendo el miedo y la inseguridad para vender lo que en la feria se parece bastante a los poderosos tratando de protegerse a sí mismos de los débiles.

---

3 La frase alude al hecho de que las personas de tez morena, en especial asiáticas y latinas, son las principales víctimas del racismo en Estados Unidos actualmente; por su parte el ecologismo y sus activistas han pasado a heredar el estigma que tuvo el comunismo en su día. Ver, por ejemplo: http://bgpappa.hubpages.com/hub/Racism-In-America-Brown-is-the-new-Black y http://www.motherjones.com/mojo/2011/05/green-new-red-crackdown-environmental-activists .

4 Véase además B. Hayes, *NeoConOpticon,* TNI y Statewatch, 2009. Disponible en: http://www.tni.org/report/neoconopticon

El emperador lleva ropa de diseño y armadura de diseño. Debe suponerse que una ya poderosa industria de la vigilancia querrá llenar cualquier hueco de "seguridad" dejado por el control democrático en el Estado de la vigilancia. Si somos serios en nuestro propósito de limitar la vigilancia, necesitamos restricciones serias tanto del Estado como del sector privado.

Poder y autonomía bajo el capitalismo digital: ¿la mercantilización de los derechos?

La vigilancia masiva y globalizada ha emergido porque los acuerdos internacionales diseñados para prevenir la aparición en Europa de Estados autoritarios en los albores de la segunda guerra mundial no han logrado, precisamente, controlar la consolidación de esta clase de poder ilegítimo, en particular desde el final de la guerra fría. Entidades como la UE y la ONU, capturadas por corporaciones o pequeños grupos de países poderosos, han acelerado estos procesos sin proponérselo. Los que controlan los grandes bancos de datos han garantizado todos los derechos y toda la información. La privacidad se ha convertido en algo a lo que optas: evitando algunos servicios y haciendo uso de otros. También hay un mercado para esta clase de "seguridad"; simplemente todavía no goza del apoyo gubernamental y las subvenciones públicas que disfruta la industria de la seguridad.

En un artículo en *The Financial Times*, el astuto inconformista Evgeny Morenov criticaba la estrecha visión de los debates sobre el "alcance de la inteligencia" argumentando que todos, incluido el mismo Snowden, se han equivocado en el punto clave sobre el mundo de la vigilancia masiva que él denunció: «la tendencia mucho más preocupante por la cual la información personal sobre nosotros, más que nuestro dinero, se convierte en la principal forma de pagar por nuestros servicios, y ¿quizá pronto por los objetos cotidianos que utilizamos?».

Durante mucho tiempo se ha entendido que si un servicio es gratuito, *tú eres el producto*, pero a medida que los consumidores proporcionan más y más datos personales en retribución por capital social y ganancia material, mayor es el potencial para aquellos que controlan las grandes bases de datos para influir en el destino de estos de maneras que aún desconocemos, una premisa que, en sí misma, es profundamente antidemocrática. Para Morenov, esto constituye una «nueva tensión en los cimientos mismos del capitalismo actual y de la vida democrática». Tiene razón en que hace falta «un poco más de imaginación» para resolverlo.