AMNESTY INTERNATIONAL

Dos años después de Snowden: proteger los derechos humanos en una era de vigilancia masiva

Resumen ejecutivo **Índice AI: ACT 30/1795/2015**

"La dura realidad es que el uso de la tecnología de vigilancia masiva realmente suprime por completo el derecho a la privacidad de las comunicaciones en Internet."
Ben Emmerson, consejero de la reina en Reino Unido y **relator especial de la ONU sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo**

El 5 de junio de 2013, un periódico británico, *The Guardian*, publicó la primera de una serie de revelaciones sobre vigilancia masiva e indiscriminada por parte de la Agencia de Seguridad Nacional (NSA) de Estados Unidos y de la Jefatura de Comunicaciones del Gobierno (GCHQ) de Reino Unido. Edward Snowden, denunciante de irregularidades que había trabajado con la NSA, aportó pruebas concretas de programas de vigilancia de las comunicaciones globales que controlan la actividad telefónica y en Internet de cientos de millones de personas en todo el mundo.

Los gobiernos pueden tener razones legítimas para utilizar la vigilancia de las comunicaciones, por ejemplo combatir la delincuencia o proteger la seguridad nacional. Sin embargo, dado que la vigilancia supone una injerencia en el derecho a la privacidad y a la libertad de expresión, debe hacerse de acuerdo con criterios estrictos: la vigilancia debe ser selectiva, basada en sospechas razonables, emprendida conforme a la ley, necesaria para alcanzar un objetivo legítimo y realizada de manera proporcionada a ese objetivo, y no discriminatoria. Esto significa que la vigilancia masiva que recopila de forma indiscriminada las comunicaciones de un gran número de personas no puede justificarse. La vigilancia masiva viola el derecho a la privacidad y a la libertad de expresión.

Este informe presenta un panorama general de la información que ha salido a la luz en los últimos dos años en relación con los programas de vigilancia masiva gestionados por Reino Unido, Estados Unidos y otros gobiernos, así como de los acontecimientos clave que han tenido lugar en este periodo, en los ámbitos jurídico, tecnológico y de políticas, en relación con la vigilancia masiva y el derecho a la privacidad . En este informe, Amnistía Internacional y Privacy International presentan también un plan de acción de siete puntos para garantizar la protección de los derechos humanos en la era digital.

En los últimos dos años hemos conocido la magnitud de los programas de vigilancia masiva gestionados principalmente por la NSA y la GCHQ, con la estrecha cooperación de sus agencias hermanas de Australia, Canadá y Nueva Zelanda, que reciben colectivamente el nombre de Alianza de los Cinco Ojos (o "Cinco Ojos"). Las revelaciones divulgadas por los medios de comunicación a partir de los archivos filtrados por Edward Snowden incluían datos que indicaban que:

- Se obligó a empresas –entre ellas Facebook, Google y Microsoft– a entregar los datos de sus clientes en virtud de órdenes secretas a través del programa Prism de la NSA;
- la NSA grabó, almacenó y analizó los metadatos de cada una de las llamadas telefónicas y de los mensajes de texto transmitidos en México, Kenia y Filipinas;
- la GCHQ y la NSA han requerido a algunas de las mayores empresas de telecomunicaciones del mundo para que intervengan los cables submarinos transatlánticos e intercepten las comunicaciones privadas que transmiten, en virtud de sus respectivos programas TEMPORA y Upstream;
- la GCHQ y la NSA penetraron en la red informática interna de Gemalto, el mayor fabricante de tarjetas SIM del mundo, posiblemente robando miles de millones de claves de encriptado utilizadas para proteger la privacidad de las comunicaciones a través de teléfonos móviles en todo el mundo.

La oposición de la opinión pública ha aumentado en todo el mundo. Una encuesta encargada por Amnistía Internacional, en la que se preguntó a 15.000 personas de 13 países de todos los continentes, reveló que el 71 por ciento de las personas se oponen con firmeza a que sus gobiernos espíen sus comunicaciones telefónicas y a través de Internet.

Instituciones y expertos internacionales y regionales, entre ellos el Alto Comisionado de la ONU para los Derechos Humanos y la Asamblea Parlamentaria del Consejo de Europa, han expresado considerables motivos de preocupación ante los programas de vigilancia masiva y han advertido del peligro que representan para los derechos humanos. En diciembre de 2014, la Asamblea General de la ONU adoptó una segunda resolución sobre el derecho a la privacidad en la era digital, en la que expresó profunda preocupación "por los efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones [...] en particular cuando se llevan a cabo en gran escala". En marzo de 2015, el Consejo de Derechos Humanos de la ONU estableció por primera vez un mandato permanente para un Relator Especial sobre el derecho a la privacidad, una iniciativa histórica que garantizará que los asuntos relativos a la privacidad estarán en primera línea de la agenda de la ONU en los años venideros.

Tribunales de varios países han fallado en contra de la vigilancia masiva y las prácticas de intercambio de información. En Reino Unido, el Tribunal de Facultades de Investigación falló que, con anterioridad a las sentencias dictadas por el Tribunal en diciembre de 2014 y febrero de 2015, el régimen que regulaba la petición, recepción, almacenamiento y transmisión por las autoridades de Reino Unido de comunicaciones privadas de personas ubicadas en Reino Unido, obtenidas por las autoridades de Estados Unidos con arreglo a los programas Prism y Upstream, vulneraba el Convenio Europeo de Derechos Humanos. En Estados Unidos, un tribunal de apelación federal falló en mayo de 2015 que la recopilación masiva de registros telefónicos estadounidenses era ilegal.

Muchas de las mayores empresas de tecnología del mundo también se han pronunciado en contra de la vigilancia masiva. En 2013, 10 empresas –entre ellas Apple, Facebook, Google, Microsoft, Twitter y Yahoo!– lanzaron la Coalición para la Reforma de la Vigilancia Global de los Gobiernos, que propugna el fin de las prácticas de recopilación en bloque en virtud de la Ley Patriótica de Estados Unidos, entre otras reformas legales.

Varias empresas importantes han tomado medidas más tangibles contra la vigilancia, reforzando el encriptado y la seguridad predeterminados que se proporcionan a los usuarios en sus plataformas y servicios, lo que permitirá proteger mejor la privacidad de los usuarios de Internet contra la vigilancia masiva indiscriminada.

También hay indicios de reformas legales limitadas. Por ejemplo, la Ley de Libertad de Estados Unidos, aprobada por la Cámara de Representantes en mayo, intenta poner fin a la recogida en bloque de registros telefónicos de Estados Unidos.[1] Sin embargo, la ley también exigiría a las empresas mantener, buscar y analizar ciertos datos a petición del gobierno, lo que posiblemente ampliaría la base legal para la recopilación de datos en gran escala en vez de poner fin a ella. Además, son muchos los aspectos de la vigilancia de Estados Unidos, como la vigilancia masiva de millones de personas fuera del país, que siguen sin estar suficientemente regulados y de los que no se rinden cuentas en virtud de la nueva ley. Es preciso ejercer presión para garantizar que los gobiernos desmantelan estos sistemas de vigilancia extraordinariamente invasivos tanto en el propio país como en otros países. Un primer paso en este sentido es reconocer que tanto las personas ubicadas en otros países como las que están en el propio país son titulares en igual medida del derecho a la privacidad.

Las empresas tienen la responsabilidad de respetar el derecho a la privacidad en línea. Para cumplir con esta responsabilidad deben adoptar medidas más audaces con el fin de reforzar la seguridad en sus plataformas y servicios, para que los datos de los usuarios privados no sean libremente accesibles para su recolección por los gobiernos.

Es cada vez mayor la corriente de opinión contraria a la vigilancia masiva, pero sigue habiendo mucho en juego. Gobiernos de todo el mundo han promulgado nuevas leyes que les conceden poderes de vigilancia masiva propios. Este año se han introducido nuevos y amplios poderes de vigilancia en Pakistán y Francia, mientras Dinamarca, Suiza, Países Bajos y Reino Unido se disponen a presentar nuevos proyectos de ley sobre información en un futuro próximo.

Para proteger la privacidad, y en última instancia la libertad de expresión, será necesaria una acción concertada de personas a título individual, técnicos, expertos legales, sociedad civil, organizaciones internacionales, empresas y gobiernos. Ninguna solución por sí sola es suficiente; es necesaria una combinación de reformas legales nacionales, normas internacionales fuertes, tecnologías sólidas que protejan la privacidad, compromiso de las empresas con la privacidad del usuario y acciones individuales.

---

[1] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act of 2015), H.R.— 114th Congress (2015-2016).

El camino a seguir

Dos años después de las revelaciones de Edward Snowden, el enorme aparato de vigilancia masiva gestionado por las agencias de inteligencia de Estados Unidos y Reino Unido permanece intacto, y no se vislumbra en perspectiva ningún indicio de que estos países tengan intención de poner fin al despliegue –y de hecho a la ampliación– de sus capacidades.

A pesar de la información revelada a la opinión pública, los programas de vigilancia masiva de Reino Unido y Estados Unidos continúan envueltos en secreto. Nada ilustra mejor este extremo que la política de "ni confirmar ni desmentir" (NCND) del gobierno de Reino Unido. La política de NCND ha dejado a quienes emprendieron acciones legales contra los programas de vigilancia masiva de Reino Unido sin otra opción que formular argumentos jurídicos sobre situaciones hipotéticas; esto ha significado que programas reales como TEMPORA, cuya existencia está clara de acuerdo con los documentos revelados por Edward Snowden, estén protegidos frente a cualquier clase de escrutinio significativo.

A pesar de la condena generalizada de las prácticas de vigilancia masiva de Estados Unidos y Reino Unido por ser violaciones de derechos humanos, y de los fallos de tribunales en ambos países que confirmaron la ilegalidad de algunas de estas prácticas, no parece que nadie haya rendido cuentas por autorizar estos programas intrusivos.

El mensaje que transmiten los gobiernos de Estados Unidos y Reino Unido –así como sus estrechos aliados Australia, Canadá y Nueva Zelanda– es claro: no renunciarán fácilmente a sus programas de vigilancia masiva. Además, en los dos años transcurridos desde las revelaciones de Snowden, hemos sabido que un número creciente de países, como Egipto,[2] Francia[3] y Pakistán,[4] intentaban aumentar sus capacidades de vigilancia de las comunicaciones.

Las amenazas a la privacidad en Internet están aumentando, y con ellas los riesgos para la libertad de expresión. Sin embargo, tiene lugar un creciente reacción: los periodistas sacan a la luz programas de vigilancia, la sociedad civil cuestiona la vigilancia masiva y las empresas refuerzan las protecciones de la privacidad en sus productos. Pero lo más importante es que, desde las revelaciones de Snowden, cientos de millones de usuarios individuales de Internet han tomado medidas para proteger su privacidad en línea.[5]

Este creciente activismo es lo que se opone a la amenaza de la vigilancia omnipresente en la que los gobiernos espían todo, a todas las personas, en todo momento. Los avances tecnológicos permitirán que las tecnologías de vigilancia sean más baratas y más potentes; muchas de las capacidades a las que hoy sólo tienen acceso la NSA y la GCHQ serán accesibles para la mayoría de los países en cuestión de años. La protección de la privacidad y, en última instancia, de la libertad de expresión en esta era digital exige acciones en varios frentes: el uso generalizado y sin restricciones de herramientas potentes de encriptado y protección del anonimato; la reforma de leyes y políticas nacionales; el respeto de las normas internacionales; y la protección de las personas que denuncien irregularidades que descubran información de interés público como indicios de violaciones de derechos humanos.

El siguiente plan de siete puntos es una llamada a la acción para la sociedad civil, técnicos, expertos, empresas y gobiernos que deseen proteger los ideales que sirvieron de base a Internet: la libertad, el carácter abierto y la accesibilidad. Creemos que estas medidas son imprescindibles para garantizar la protección de los derechos humanos en nuestra era digital.

---

[2] Véase Amnistía Internacional, *Egypt's plan for mass surveillance of social media an attack on internet privacy and freedom of expression*, 4 de junio de 2014, en línea en www.amnesty.org/en/articles/news/2014/06/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression/ y *'You are being watched!' Egypt's mass Internet surveillance*, Mada Masr, 29 de septiembre de 2014, en línea en www.amnesty.org/en/articles/news/2014/06/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression/ (consultados el 28 de mayo de 2015)

[3] Véase Amnistía Internacional, *Francia: Detener la carrera hacia un estado de vigilancia*, 4 de mayo de 2015, en línea en: https://www.amnesty.org/es/articles/news/2015/05/france-surveillance-state/ y Amnistía Internacional, *France: les députés approuvent la surveillance de masse*, 5 de mayo de 2015, en línea en: www.amnesty.fr/Nos-campagnes/Liberte-expression/Actualites/France-les-deputes-approuvent-la-surveillance-de-masse-15061 (consultados el 28 de mayo de 2015)

[4] Véase Privacy International, *International human rights organisations seriously concerned about the prevention of electronic crimes bill 2015 Pakistan*, 20 de abril de 2015, en línea en: www.privacyinternational.org/?q=node/566 (consultado el 28 de mayo de 2015)

[5] Bill Schneier, *Over 700 Million People Taking Steps to Avoid NSA Surveillance*, 15 de diciembre de 2014, en línea en: www.schneier.com/crypto-gram/archives/2014/1215.html#7 (consultado el 28 de mayo de 2015)

Reformas legales y de políticas:

1. Deben reformarse las leyes nacionales para garantizar que se ajustan al derecho y las normas internacionales de los derechos humanos, lo que incluye no permitir la vigilancia masiva indiscriminada. Algunos principios clave que deben respetarse:
    a. Garantizar que la vigilancia de las comunicaciones sólo se lleva a cabo cuando es selectiva, se basa en pruebas suficientes de conducta delictiva y está autorizada por una autoridad estrictamente independiente, como la judicial;
    b. Garantizar que existe una supervisión parlamentaria y judicial transparente e independiente de las facultades de vigilancia;
    c. Poner en conocimiento público las normas y políticas en materia de vigilancia, incluidas las relativas al intercambio de información con otros Estados;
    d. Garantizar que las medidas de protección de la privacidad se aplican por igual a nacionales y no nacionales de los Estados, a quienes viven dentro del territorio del Estado y a quienes viven fuera de él.
    e. El intercambio de información debe estar estrictamente regulado y realizarse de tal manera que se ajuste a las obligaciones de los Estados en materia de derechos humanos;
2. Los gobiernos no deben declarar ilegal la fabricación de tecnologías de encriptado y protección del anonimato ni su uso;
3. Debe concederse a las personas que denuncian irregularidades, y entre ellas a las que trabajan en asuntos de seguridad nacional, una sólida protección jurídica frente a cualquier forma de represalias, incluso a través de enjuiciamiento, por haber revelado información de interés público como violaciones de derechos humanos.[6]

Diligencia debida de las empresas

De acuerdo con la responsabilidad de las empresas de respetar los derechos humanos:

4. Las empresas que poseen y/o gestionan infraestructuras de telecomunicaciones o de Internet, incluidos los cables submarinos de telecomunicaciones, y las empresas de Internet deben garantizar que el acceso a los datos se permite únicamente cuando es ajustado al derecho y las normas internacionales de derechos humanos, lo que incluye emprender acciones legales para cuestionar las peticiones de los gobiernos que intenten el acceso en bloque o en grandes volúmenes al tráfico de comunicaciones;
5. Las grandes empresas de Internet y de telecomunicaciones señalar el camino mediante el uso de tecnologías potentes de encriptado y otras tecnologías para preservar la privacidad, incluso mediante la implementación del encriptado de extremo a extremo por defecto, cuando sea posible;
6. Los proveedores de servicios de Internet, las empresas de telecomunicaciones y las empresas de Internet deben informar claramente a los usuarios sobre los requisitos legales que han de cumplir, especialmente en relación con la entrega de información o contenidos de los usuarios.

Normas internacionales

7. Continuar explorando y desarrollando los medios y medidas necesarios para garantizar la mejora de la implementación de las normas internacionales de derechos humanos aplicables a la vigilancia de las comunicaciones, haciendo uso de las iniciativas para identificar los elementos pertinentes que se han puesto en marcha en los últimos dos años, incluidos los informes del relator especial de la ONU sobre la libertad de expresión,[7] el Alto Comisionado de la ONU para los Derechos Humanos, el relator especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo,[8] así como iniciativas de la sociedad civil como los Principios Necesarios y Proporcionados.[9]

---

[6] Véase *Principios Globales sobre Seguridad Nacional y el Derecho a la Información (Principios de Tshwane)*, en línea en: http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-right-information-tshwane-principles/es. Véase también Asamblea Parlamentaria del Consejo de Europa, *National security and access to information*, Resolución 1954 (2013), en línea en: http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=20190&lang=en (ambos consultados el 28 de mayo de 2015), que celebraba la adopción de los Principios de Tschwane.

[7] Consejo de Derechos Humanos de las Naciones Unidas, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue*, A/HRC/23/40, 17 de abril de 2013, en línea en: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/06/PDF/G1313306.pdf?OpenElement (consultado el 28 de mayo de 2015)

[8] Asamblea General, *Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*, A/69/397, 23 de septiembre de 2014, en línea en: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/22/PDF/N1454522.pdf?OpenElement (consultado el 28 de mayo de 2015)

[9] *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*, mayo de 2014, en línea en: https://en.necessaryandproportionate.org/ (consultado el 28 de mayo de 2015)