Preguntas y respuestas: Campaña contra la vigilancia masiva #DejenDeSeguirme

¿Por qué lanza Amnistía Internacional una campaña global contra la vigilancia masiva?

Internet ha revolucionado la forma en que nos comunicamos. Cada día, tres mil millones de usuarios de Internet se conectan a la web para publicar, compartir, tener acceso a información y comunicarse con otras personas de forma inmediata en todo el mundo. Pero también permite a los Gobiernos registrar y almacenar toda esta información, lo que les da un conocimiento sin precedentes sobre lo que hacemos, pensamos y decimos.

Todas las personas que usan Internet hoy en día corren el riesgo de que su Gobierno y, en algunos casos, Gobiernos de otros países vigilen sus comunicaciones.

Al conectar a Internet aparatos de uso cotidiano, desde televisiones y relojes a frigoríficos y vehículos, los Gobiernos tendrán acceso a datos sobre todo lo que hagamos. Como los ordenadores cada vez son más avanzados y los algoritmos más inteligentes, también aumentará la capacidad de los Gobiernos de hacer suposiciones sobre nosotros basándose en nuestras acciones, desde perfiles a gran escala a análisis predictivos.

Si no actuamos ahora, corremos el riesgo de vivir en sociedades en las que no exista la intimidad.

¿Por qué debe importarme la vigilancia masiva si no tengo nada que ocultar?

La pregunta debería ser: si no he hecho nada malo, ¿por qué se está violando mi intimidad?

Normalmente, los Gobiernos llevan a cabo vigilancia selectiva, el seguimiento de las comunicaciones, acciones o movimientos de una persona. Los Gobiernos solo pueden llevar a cabo ese seguimiento si se dirige a una persona o a un grupo por motivos legítimos concretos. Para ello, las autoridades tendrían que obtener el permiso de un juez, por ejemplo, para el seguimiento del uso del teléfono o de Internet por parte de una persona o un grupo específico del que se sospecha que está implicada en actividades delictivas.

Si el seguimiento se realiza a gran escala y de forma indiscriminada y se vigilan las comunicaciones de las personas sin una sospecha razonable de que estén implicadas en una actividad delictiva, entonces la presunción es que todo el mundo es potencialmente culpable hasta que se demuestre que es inocente.

Una sociedad que respecta la libertad y el Estado de derecho debe respetar la intimidad de las personas. Nunca aceptaríamos que los Gobiernos instalasen grabadoras de voz y cámaras de televisión por circuito cerrado en nuestras casas, abriesen cada carta que enviamos, registrasen cada conversación que tengamos con una persona amiga tomando un café y nos siguiesen a donde quiera que vayamos. Sin embargo, ese es el equivalente en el mundo físico de la vigilancia masiva en Internet.

¿Hasta dónde llega la vigilancia masiva actualmente?

Según datos del Gobierno de los Estados Unidos difundidos por el denunciante estadounidense Edward Snowden en 2013, los Gobiernos recogen, almacenan y analizan millones de comunicaciones privadas de personas en secreto, sin apenas supervisión y rendición de cuentas.

Edward Snowden proporcionó datos que sugieren que el Reino Unido y los Estados Unidos han puesto en marcha programas de vigilancia masiva en alianza con sus socios Canadá, Australia y Nueva Zelanda, la alianza de los Cinco Ojos. Estos programas controlan de forma ilegítima e indiscriminada los correos electrónicos, llamadas de teléfono y el tráfico en Internet de personas corrientes en todo el mundo.

¿Qué deberían hacer los Gobiernos?

Amnistía Internacional pide a los Gobiernos que prohíban los programas de vigilancia masiva. Todos los países deben establecer salvaguardas legales sólidas para proteger a las personas de la interceptación ilegítima de sus comunicaciones y su vida privada.

La vigilancia solo debe tener lugar cuando sea absolutamente necesaria, sobre la base de de indicios suficientes de conducta delictiva, y autorizada por una autoridad estrictamente independiente, como un juez.

¿Cómo viola los derechos humanos la vigilancia masiva?

Todas las personas tienen derecho a la vida privada sin intromisiones del Gobierno. Actualmente, las agencias de seguridad pueden utilizar la vigilancia para inmiscuirse en lo más profundo de nuestra intimidad, haciendo seguimiento de nuestros correos electrónicos, nuestra actividad en Internet y de adonde vamos.

El derecho internacional de los derechos humanos protege los derechos a la intimidad y a la libertad de expresión. Los Estados tiene la obligación legal de protegerlos. Por ejemplo, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos protege a las personas frente a las “injerencias arbitrarias o ilegales en [su] vida privada, su familia, su domicilio o su correspondencia”.

El derecho internacional permite a los Gobiernos llevar a cabo acciones que interfieren con esos derechos en determinadas circunstancias, y la vigilancia legítima de las comunicaciones es una de ellas. Cualquier injerencia que no sea acorde con las obligaciones de los Estados es una violación de derechos humanos.

También sabemos que algunos Gobiernos han empezado a importar la tecnología de vigilancia más reciente y la utilizan para reprimir a la oposición política y a las personas que luchan por los derechos humanos. La tecnología para llevar a cabo esa vigilancia es cada vez más barata y muy fácil de conseguir para cualquier Gobierno que desee adquirirla.

En algunos países, los datos privados se utilizan para perseguir a periodistas, activistas, hacer perfiles de las minorías y discriminarlas, y tomar medidas enérgicas contra la libertad de expresión. Por ejemplo, en Bahréin, la vigilancia electrónica se ha utilizado para perseguir a activistas de derechos humanos y Etiopía ha perseguido a activistas y periodistas en Etiopía y en el extranjero.

¿Estoy bajo vigilancia?

Si utilizas Internet o un teléfono móvil, la respuesta probablemente es que sí.

Al parecer, programas secretos gubernamentales de vigilancia como Prism y Upstream (de la estadounidense Agencia de Seguridad Nacional, NSA) y Tempora (de la británica Jefatura de Comunicaciones del Gobierno, GCHQ) te espían al obtener datos de Google, Microsoft, Facebook y otras empresas importantes de Internet y al acceder a cables de fibra óptica que llevan comunicaciones globales por Internet. El espectacular ámbito de aplicación de estos programas y el modo en que se realizan las comunicaciones electrónicas globales supone que se puede espiar a la gente en casi todos los países de la Tierra.

Para estos programas tú solo eres un número de teléfono, correo electrónico, ordenador o una dirección IP más que es dirigido a sus centros de datos.

Al parecer, muchos otros países del mundo tienen programas de vigilancia masiva más modestos que controlan las comunicaciones en el ámbito nacional.

¿Qué hacen con mis datos?

Tus datos pueden interceptarse a través de tu red de telefonía móvil, tu proveedor de servicio de Internet, los cables de datos de Internet en tu país, o incluso los cables submarinos de fibra óptica que canalizan el tráfico global de Internet. Posteriormente se guardan en grandes centros de datos.

Al parecer, las agencias de seguridad estadounidense NSA y la británica GCHQ tienen algunos de los centros de datos más grandes del mundo. Posteriormente, los datos pueden buscarse y analizarse por medios de algoritmos informáticos y se ponen a disposición de agencias de seguridad de Australia, Canadá y Nueva Zelanda por medio de X-Keyscore, una potente base de datos de millones de registros privados.

Además de los Cinco Ojos, la NSA tiene otros socios con los que intercambia información de forma más limitada. Algunas de las coaliciones son:

Los Nueve Ojos: además de los Cinco Ojos, Dinamarca, Francia, Países Bajos y Noruega

Los 14 Ojos: que incluye a Bélgica, Alemania, Italia, España y Suecia

Los 41 Ojos: que incluye los 14 Ojos y la coalición aliada en Afganistán

Para más información, véase Privacy International https://www.privacyinternational.org/?q=node/51

¿La vigilancia masiva no es necesaria para parar a los terroristas?

No hay pruebas de que la vigilancia masiva ayude a evitar el terrorismo. De hecho, puede obstaculizar los esfuerzos por identificar actividades terroristas al sobrecargar a agentes de seguridad con un montón de datos no procesados.

La vigilancia masiva aumenta el riesgo de que las agencias de inteligencia y encargadas de hacer cumplir la ley pasen por alto amenazas reales, creíbles, al distraerse con falsos positivos. La inteligencia sale de los programas de vigilancia masiva como una manguera contra incendios - y no se puede tomar un trago de una manguera contra incendios.

Los Gobiernos ya tenían medios más que adecuados a fin de hacer cumplir la ley, y para obtener información. La cuestión es que están recabando información que hace una década no podían haber imaginado y siempre nos dirán que necesitan más. Es necesario que se establezcan limitaciones para garantizar que la vigilancia solo se lleva a cabo cuando haya una base legal legítima para hacerlo y se utilicen los medios menos intrusivos posible.

¿Cuándo es legal la vigilancia?

Algunos programas de vigilancia son obviamente ilegítimos incluso de conformidad con la legislación nacional, por ejemplo cuando ocurre sin autorización legal. El marco jurídico nacional puede autorizar la vigilancia de las comunicaciones. Sin embargo, la vigilancia que tiene apariencia legal no es necesariamente legal según el derecho internacional. Los Estados tienen obligaciones en materia de derechos humanos en virtud del derecho internacional y conforme a sus ordenamientos jurídicos internos. La vigilancia que no es compatible con los derechos humanos es ilegítima en virtud del derecho internacional y conforme a la mayoría de los ordenamientos jurídicos internos.

La vigilancia de las comunicaciones afecta a la intimidad y a la libertad de expresión, derechos incluidos en la Declaración Universal de Derechos Humanos y garantizados por el derecho internacional de los derechos humanos. La vigilancia solo es legítima en las siguientes circunstancias:

- Está **autorizada por la legislación**; es decir, se hace según leyes y normas claras que son de acceso público;

- Está **autorizada por una orden** emitida por una autoridad independiente, como un juez;

- Se utiliza para conseguir un **fin legítimo**, por ejemplo, en el contexto de una investigación penal o para fines de seguridad nacional;

- **Está dirigida** a una persona, un grupo de individuos definido o un lugar concreto que es directamente pertinente para el logro de un fin legítimo;

- Es **necesaria**, es decir, la vigilancia es necesaria para lograr una finalidad legítima como la investigación y prevención de un delito;

- Es **proporcionada**; es decir, el alcance de la vigilancia es proporcional a la finalidad (legítima) para la que se lleva a cabo y se equilibra con cómo afecta a los derechos humanos. Para lograr este fin deben utilizarse los medios menos intrusivos posible.

Por ejemplo, la vigilancia de las comunicaciones de los teléfonos e Internet de una presunta red de blanqueo de capitales con el fin de presentar una causa judicial penal puede ser legítimo si se

hace según estas normas.

No obstante, la vigilancia masiva de las comunicaciones de países enteros como la llevada a cabo por la estadounidense Agencia de Seguridad Nacional (NSA) y la británica Jefatura de Comunicaciones del Gobierno (GCHQ) es ilegítima. Es desproporcionada y los Gobiernos no han presentado pruebas convincentes de su necesidad. Además, muchos de estos programas de vigilancia (y programas similares que puede que tengan otros países) están autorizados por leyes imprecisas que incluso los legisladores y los jueces tendrían dificultades en interpretar. En numerosos casos, el proceso para autorizar la vigilancia se hace sin la supervisión adecuada.

Por ejemplo, en Estados Unidos, un programa que recoge registros telefónicos tiene que ser renovado cada 90 días. El Tribunal estadounidense de la Ley de Vigilancia de la Inteligencia Exterior (Foreign Intelligence Surveillance Act, FISA), conocido como el Tribunal FISA, decide sobre estas solicitudes así como sobre otras solicitudes de vigilancia electrónica, registros físicos y otras acciones de investigación con fines de información exterior. La mayoría de las actuaciones de este tribunal son secretas, la mayoría de sus procedimientos judiciales son no contenciosos, los registros de las vistas no se hacen públicos y queda a criterio del tribunal publicar o no sus fallos.

En Reino Unido el Secretario de Estado del Ministerio del Interior pueden emitir –y renovar- órdenes que autoricen la vigilancia masiva indiscriminada y que no necesitan autorización judicial.

¿Existe la vigilancia masiva legal?

No. Amnistía Internacional considera que la vigilancia masiva indiscriminada no supera la prueba de constituir una injerencia necesaria y proporcionada en los derechos humanos.

En algunos casos, un Estado puede realizar tareas de vigilancia sobre un gran número de personas de forma legítima, por ejemplo cuando se sospecha que son miembros de un grupo delictivo, o sobre todas las personas que visitan una página web ilegal (por ejemplo, una página web utilizada para vender armas ilícitas o con pornografía infantil). En estos casos se considera que la vigilancia es selectiva.

¿Cómo puedo protegerme frente a la vigilancia en Internet?

Hay muchas cosas prácticas que puedes hacer. Por ejemplo, la Fundación Frontera Electrónica (Electronic Frontier Foundation, EFF) tiene consejos, herramientas y procedimientos muy útiles para llevar a cabo comunicaciones más seguras por Internet https://ssd.eff.org/ así como un marcador útil para aplicaciones de mensajería https://www.eff.org/secure-messaging-scorecard

También puedes visitar security-in-a-box https://securityinabox.org/ y las guías de Access https://www.accessnow.org/pages/tech

Pero incluso si tomas precauciones para protegerte, puede que los Estados estén un paso o dos por delante.