“BASTA CON QUE LA GENTE CREA QUE EXISTE”

SOCIEDAD CIVIL, SECRETISMO Y VIGILANCIA EN BIELORRUSIA

AMNESTY INTERNATIONAL

Amnistía Internacional es un movimiento global de más de 7 millones de personas que trabajan en favor del respeto y la protección de los derechos humanos.

Nuestra visión es la de un mundo en el que todas las personas disfrutan de todos los derechos humanos proclamados en la Declaración Universal de Derechos Humanos y en otras normas internacionales.

Somos independientes de todo gobierno, ideología política, interés económico y credo religioso. Nuestro trabajo se financia principalmente gracias a nuestra membresía y a donaciones públicas.

Publicado por primera vez en 2016
por Amnesty International Ltd.
Peter Benenson House, 1 Easton Street
London WC1X 0DW, Reino Unido

Índice: EUR 49/4306/2016
Idioma original: Inglés

amnesty.org

Foto de portada: *Minsk, Bielorrusia*
© Maxim Sarychau

AMNESTY INTERNATIONAL

1. RESUMEN EJECUTIVO

El marco jurídico que regula la vigilancia secreta en Bielorrusia se caracteriza por no contar con suficientes salvaguardias y permite que las autoridades lleven a cabo una vigilancia amplia con poca o ninguna justificación. Al mismo tiempo que es posible que casi cualquier persona sea sometida a vigilancia, es casi imposible que alguien sepa si está o ha estado vigilado. Esta incertidumbre tiene un efecto inhibitorio en los defensores y defensoras de los derechos humanos, políticos de la oposición, abogados y activistas, y limita su capacidad para ejercer sus derechos humanos, incluidos el derecho a la intimidad y el derecho a la libertad de asociación, de reunión pacífica y de expresión.

Aunque la vigilancia secreta puede ser una herramienta legítima para hacer cumplir la ley, cuando carece de las salvaguardias o la supervisión adecuadas, o no respeta el derecho y las normas internacionales, viola los derechos humanos. Este informe analiza las formas en que la vigilancia secreta ilegítima afecta a los derechos humanos y el efecto que tiene esto en la sociedad civil de Bielorrusia. El informe se basa en entrevistas con más de cincuenta activistas de la sociedad civil, la mayoría en Bielorrusia, aunque también en el exilio. También se basa en un análisis detallado del marco jurídico bielorruso e internacional que regula la vigilancia.

El sistema de vigilancia de Bielorrusia tiene numerosos aspectos problemáticos. Destaca entre ellos el sistema SORM, un conjunto de medios técnicos normalizados para interceptar comunicaciones que permite a las autoridades el acceso directo por control remoto a todas las comunicaciones de usuarios y datos asociados sin notificarlo a los proveedores. Según la legislación bielorrusa, todos los proveedores de telecomunicaciones del país deben usar hardware compatible con el sistema SORM. El sistema facilita la vigilancia en tiempo real de las comunicaciones, así como el acceso a datos que las empresas de telecomunicaciones deben conservar por ley hasta cinco años, y proporciona acceso tanto al contenido de las comunicaciones como a los metadatos asociados (datos como la hora, la clase y la ubicación de la comunicación).

Este problemático sistema de vigilancia es facilitado por actores empresariales, como los proveedores de telefonía móvil o de Internet que —según la legislación bielorrusa— deben permitir a las autoridades el acceso directo a los datos de sus clientes. Estas empresas bielorrusas, y las empresas internacionales que son sus propietarias o accionistas principales, incumplen sus obligaciones al no identificar, prevenir y abordar los abusos derivados de sus operaciones o de sus relaciones empresariales y así, violan normas internacionales sobre empresas y derechos humanos. Las empresas deben tomar medidas positivas para asumir sus responsabilidades en materia de derechos humanos, con independencia del lugar donde decidan operar. Estas medidas deben ser proporcionales al daño que podrían sufrir las personas como consecuencia de sus operaciones.

La vigilancia de las telecomunicaciones no es el único riesgo de vigilancia que afecta a la ciudadanía bielorrusa. El derecho a la intimidad también está en peligro porque la ley prevé amplias facultades de vigilancia física, incluido el monitoreo de audio de personas o recintos, y porque podrían verse comprometidos datos personales cuando las autoridades confiscan ordenadores, teléfonos móviles u otros aparatos. La falta de transparencia sobre la capacidad de vigilancia del Estado hace que, en última instancia, nadie conozca todo el abanico de herramientas y técnicas de que disponen las autoridades.

La vigilancia secreta es realizada por una amplia gama de organismos estatales y es autorizada en virtud de diversos fundamentos legales, generales y poco precisos. Se puede usar, en virtud del derecho interno, para someter a vigilancia a personas que no son sospechosas de delito alguno. La autorización y las

salvaguardias de supervisión son inadecuadas, y normalmente están a cargo de fiscales y no de un órgano judicial independiente.

Cuando la vigilancia desemboca en violaciones de derechos humanos, es muy difícil buscar una reparación en la práctica. Esto es tanto más cierto cuanto que las autoridades no tienen la obligación de notificar a las personas que han sido objeto de vigilancia una vez que ésta ha terminado, ni siquiera si esta notificación podría hacerse sin poner en peligro el propósito de las investigaciones. En consecuencia, las personas afectadas rara vez tienen acceso a pruebas en las que basar una denuncia. Casi ninguno de los activistas que creían que habían sido sometidos a vigilancia ilegal había podido presentar una denuncia y de entre quienes sí pudieron hacerlo, casi ninguno creía que tendría éxito y en su mayoría las habían formulado sólo como protección legal frente a la posibilidad de ser enjuiciados a su vez.

Aunque el marco jurídico bielorruso hace casi imposible que nadie sepa con seguridad si puede estar o haber estado sometido a vigilancia, la historia reciente de Bielorrusia da a muchos activistas razones para creer que lo están.

La represión desatada por las autoridades tras las elecciones presidenciales de 2010 se caracterizó por la detención y el encarcelamiento de miembros de la oposición política por ejercer sus derechos humanos. Muchos de estos difundidos enjuiciamientos se caracterizaron por el uso destacado de comunicaciones personales y datos asociados, y los medios de comunicación informaron ampliamente de que las autoridades habían usado datos de ubicación de telefonía móvil para determinar la identidad de personas que habían asistido a las manifestaciones no autorizadas —aunque en gran medida pacíficas— que se celebraron tras las elecciones.

En parte debido a esto, los activistas que hablaron con Amnistía Internacional expresaron en general la creencia de que estaban sometidos a al menos algún tipo de vigilancia secreta como consecuencia de su activismo. Este miedo a la vigilancia se ve exacerbado por el restrictivo entorno jurídico en el que está inmersa la sociedad civil de Bielorrusia, donde los activistas son castigados a menudo sólo por ejercer sus derechos humanos —como asistir a una protesta pacífica— y los límites al ejercicio de estos derechos en Internet son cada vez más estrictos. Todo esto crea un efecto inhibitorio que hace que muchas personas se autocensuren y eviten ejercer sus derechos en muchos casos.

Los activistas entrevistados por Amnistía Internacional dijeron que, por lo general, no hablan de temas delicados por teléfono: temas como financiar una organización no inscrita legalmente u organizar una protesta pacífica, que pueden desembocar en cargos legales. Incluso tareas organizativas corrientes, como preparar reuniones, conllevan el uso de elaborados sistemas de lenguaje en código y exigen generalmente verse en persona, a menudo al aire libre, sin teléfonos móviles que puedan grabar sus conversaciones o rastrear su ubicación. El miedo a la vigilancia de las comunicaciones digitales también hace que el uso de herramientas de cifrado, como el PGP (sistema para el cifrado del correo electrónico), los programas cifrados de chat y el cifrado de discos sea esencial para el trabajo de los activistas.

Los activistas denunciaron experiencias —como que los pare la policía, que parecía saber dónde encontrarlos— que atribuían a la vigilancia de los datos de ubicación de su teléfono móvil. Sin embargo, dado el problemático marco jurídico de Bielorrusia, no pueden confirmar estas sospechas, lo que deja a la mayoría de las personas sin más alternativa que suponer que se está rastreando su ubicación.

Algunos activistas temían que sus oficinas o incluso sus domicilios pudieran estar sometidos a monitoreo de audio o vídeo, lo que les impide hacer trabajo delicado en sus propias oficinas, algo que dificulta de forma significativa su capacidad para trabajar.

Amnistía Internacional habló con tres activistas que dijeron que creían que su correo electrónico o sus cuentas en redes sociales habían sido hackeados. y sospechaban que detrás de los ataques podrían estar las autoridades; sospechas que, según dijeron, aumentaron cuando se usaron sus datos personales para amenazarlos o enjuiciarlos. Con más frecuencia, las autoridades habían confiscado ordenadores u otros equipos a los activistas, por lo que éstos no podían seguir trabajando con sus equipos ni siquiera una vez devueltos, por miedo a que hubieran sido infectados con software para monitorear su uso.

El uso de Internet en Bielorrusia ha aumentado rápidamente en los últimos años. En 2014, la penetración de Internet era del 59 por ciento, frente al 39,6 por ciento de 2011.[1] A pesar de esto, el riesgo y la incertidumbre de la vigilancia de las comunicaciones hace que el trabajo de los activistas bielorrusos sea más difícil. Los activistas no pueden beneficiarse del aumento de la conectividad. En cambio, el efecto inhibitorio que crea el miedo a la vigilancia hace que las comunicaciones sean más lentas, el flujo de información esté restringido, la organización se vea obstaculizada y se deteriore la confianza.

Debido al problemático marco jurídico que regula la vigilancia en Bielorrusia, todas las personas se ven obligadas a vivir como si estuvieran sometidas a vigilancia, lo que tiene un impacto perjudicial en los derechos. Aunque no se puede saber la escala actual de la vigilancia, los efectos de su abuso en el pasado son patentes: se siguen citando casos conocidos en los que las autoridades han usado datos de comunicaciones para enjuiciar a políticos de la oposición y defensores de los derechos humanos tras las elecciones de 2010 como razón por la que la gente teme la vigilancia. Los casos descritos por los activistas que hablaron con Amnistía Internacional indican que siguen sometidos a vigilancia secreta.

Las autoridades bielorrusas deben revisar urgentemente las leyes que regulan la vigilancia secreta para que sean compatibles con las normas internacionales. Por ejemplo, deben garantizar que sólo se puede llevar a cabo la vigilancia cuando esté autorizada (y supervisada) por jueces independientes y se base en motivos suficientemente restringidos, teniendo en cuenta la necesidad de una sospecha razonable individualizada de infracción y los requisitos de necesidad y proporcionalidad. El sistema SORM debe ser sustituido por otro que no permita el acceso directo a los datos de las comunicaciones. Los fiscales no deben buscar someter a vigilancia a personas por el ejercicio de sus derechos humanos, como la organización de protestas pacíficas. Los fiscales y las autoridades encargadas de realizar la vigilancia deben ser más transparentes sobre el número de casos en los que se autoriza y se lleva a cabo esta medida. Las personas que son sometidas a vigilancia deben ser notificadas y tener acceso efectivo a remedios para las violaciones de derechos humanos ligadas a esta vigilancia. Las empresas privadas que facilitan la vigilancia en Bielorrusia deben cuestionar las prácticas de vigilancia ilegales del gobierno, presionar a favor de su reforma y ser más transparentes sobre la ley y la práctica que regulan el acceso a los datos de los clientes en Bielorrusia.

Encontrarán más recomendaciones al final de este informe.

[1] http://data.worldbank.org/indicator/IT.NET.USER.P2

2. RECOMENDACIONES

2.1 A LOS PODERES EJECUTIVO Y LEGISLATIVO DEL ESTADO DE BIELORRUSIA:

1. Reformar las leyes que regulan la vigilancia —incluidos la Ley sobre Actividad Operativa de Búsqueda (No. 307-Z de 15 de julio de 2015) y el Código de Procedimiento Penal— para que el régimen jurídico y las prácticas de vigilancia conexas sean compatibles con las leyes y normas internacionales de derechos humanos.
2. Garantizar que la ciudadanía tiene acceso a la información relativa a la ley y la práctica relativas a la vigilancia, como mínimo en la medida prevista en los *Principios Globales sobre Seguridad Nacional y Derecho a la Información (Principios de Tshwane)*.
3. Entre otras cosas, deberán tomarse medidas para garantizar que:

    - Se exige a las autoridades estatales que presenten a los proveedores de telecomunicaciones peticiones de datos autorizadas judicialmente, en lugar de tener acceso directo por control remoto.
    - Los proveedores de telecomunicaciones no tienen la obligación de conservar datos relativos a las comunicaciones fuera del contexto de una investigación criminal en curso y sobre la base de una orden judicial que contenga las debidas individualización y sospecha razonable de infracción.
    - La interceptación y el acceso a las comunicaciones y datos conexos podrá realizarse únicamente cuando sean autorizados —o renovados respectivamente— por un órgano judicial independiente que deberá evaluar la existencia de una sospecha razonable individualizada de infracción por parte del objeto de la vigilancia y tener la seguridad de que se cumplen los requisitos de necesidad y proporcionalidad.
    - Se establecen en la ley razones legales que justifiquen la vigilancia secreta, incluida la definición de "seguridad nacional", y se circunscriben estrictamente a fin de cumplir una norma de claridad y precisión suficiente para garantizar que las personas tienen una indicación adecuada de las circunstancias que pueden llevar a la vigilancia.
    - Las facultades de vigilancia secreta son supervisadas por una autoridad de supervisión auténticamente independiente dotada de recursos adecuados, transparente ante la ciudadanía, con acceso a toda la información y con el poder y el mandato de detectar e investigar los abusos contra los derechos humanos ligados a la vigilancia secreta, y ponerles fin y proporcionar remedios.

- Se modifica la ley para establecer unos límites claros a la duración de la vigilancia secreta en todos los casos.
- La ley establece unos requisitos claros para la destrucción de todos los datos relacionados con la vigilancia.
- Se notifica a las personas objeto de vigilancia secreta que fueron sometidas a vigilancia cuando esto no ponga en peligro, o deje de poner en peligro, el propósito de una investigación en curso.
- Las personas tienen acceso a recursos efectivos y pueden cuestionar las medidas de vigilancia o los abusos contra sus derechos ligados a la vigilancia ante tribunales independientes que ofrecen todas las garantías necesarias de debido proceso.
- Se hace pública suficiente información sobre los detalles técnicos de los sistemas de vigilancia, incluidas las herramientas de espionaje informático.

2.2 A LOS FISCALES:

Hasta que la facultad para autorizar la vigilancia secreta sea transferida a un juez independiente, los fiscales deberán:

1. Garantizar que las peticiones de vigilancia secreta se autorizan sólo cuando se basen en una sospecha razonable individualizada de infracción por parte del objeto de vigilancia, y cuando estas peticiones cumplan los requisitos de necesidad y proporcionalidad.

2. Difundir periódicamente informes públicos en los que se detallen —como mínimo— el número de peticiones de vigilancia secreta presentadas, aprobadas y rechazadas, desglosadas por autoridad solicitante y fundamento jurídico.

3. Garantizar que no se concede ninguna autorización basada en el ejercicio de los derechos humanos, como la participación en grupos no inscritos legalmente o en reuniones pacíficas.

4. Ejercer facultades para supervisar la aplicación de las medidas de vigilancia, y cuando haya pruebas de violaciones de la ley o de los derechos humanos, garantizar que se terminan y que los responsables rinden cuentas de sus actos.

2.3 A LAS AUTORIDADES QUE REALIZAN 2.4 ACTIVIDADES OPERATIVAS DE BÚSQUEDA:

Hasta que se adopten las reformas recomendadas, deberán:

1. Difundir periódicamente informes públicos en los que se detallen —como mínimo— el número de peticiones de vigilancia secreta presentadas, aprobadas y rechazadas, desglosadas por fundamento jurídico.

2. Publicar información sobre el número de veces que se ha usado la tecnología SORM para acceder a datos, y el fundamento jurídico de dichos usos.

3. Abstenerse de pedir autorización para realizar vigilancia basada en el ejercicio de los derechos humanos, como la participación en grupos no inscritos legalmente o en reuniones pacíficas.

2.5 A LAS EMPRESAS DE TELECOMUNICACIONES:

1. Deberán ejercer la diligencia debida en materia de derechos humanos para identificar, prevenir, mitigar y responder del impacto sobre los derechos humanos de sus operaciones o de las operaciones de sus filiales, en Bielorrusia y otros países, lo que incluye como mínimo:

    - Cuestionar los requisitos legales que sean contrarios a las leyes y normas internacionales de derechos humanos.
    - Publicar periódicamente datos sobre el número de solicitudes y casos de acceso a las comunicaciones y datos conexos de los clientes. Cuando esto no sea posible, publicar información detallada y accesible sobre el marco jurídico y las prácticas que regulan la revelación de datos de clientes a las autoridades del Estado.
    - Presionar por la renegociación de los requisitos para la aplicación del SORM y por la revisión de las obligaciones legales o de otra índole de revelar datos de clientes de un modo incompatible con las leyes y normas internacionales de derechos humanos.

AMNISTÍA INTERNACIONAL ES UN MOVIMIENTO GLOBAL DE DERECHOS HUMANOS. LAS INJUSTICIAS QUE AFECTAN A UNA SOLA PERSONA NOS AFECTAN A TODAS Y A TODOS.

CONTÁCTANOS

info@amnesty.org

+44 (0)20 7413 5500

ÚNETE A LA CONVERSACIÓN

www.facebook.com/AmnestyGlobal

@AmnestyOnline

“BASTA CON QUE LA GENTE CREA QUE EXISTE”

SOCIEDAD CIVIL, SECRETISMO Y VIGILANCIA EN BIELORRUSIA

La legislación de Bielorrusia permite a las autoridades llevar a cabo una vigilancia de amplio alcance por casi cualquier motivo y sin supervisión independiente. Este sistema de vigilancia secreta tiene un efecto debilitador en la sociedad civil de Bielorrusia, cuyo trabajo ya se ve gravemente menoscabado por la amenaza de castigos penales o administrativos sólo por ejercer sus derechos humanos, como asistir a protestas.

En este entorno, el temor a la vigilancia crea un efecto inhibitorio que hace que incluso tareas cotidianas básicas —como hacer llamadas telefónicas, concertar reuniones y planificar eventos públicos— sean más difíciles y peligrosas. Los teléfonos móviles pueden servir para escuchar conversaciones privadas, rastrear la ubicación del usuario y revelar con quién se ha reunido una persona. El acceso ilegal a la información privada de las cuentas de correo electrónico o de redes sociales de los activistas puede causarles serios problemas legales.

El sistema en Bielorrusia permite pocos recursos en la práctica para las personas cuyos derechos han sido violados por la vigilancia. Este sistema es facilitado por la colaboración de las empresas de telecomunicaciones bielorrusas y extranjeras, que dan al gobierno acceso directo a las comunicaciones y datos de los clientes a través del sistema SORM.

Este informe contiene recomendaciones al gobierno bielorruso, así como a las empresas de telecomunicaciones bielorrusas e internacionales, para que pongan fin a los abusos contra los derechos humanos relacionados con la vigilancia en Bielorrusia.

ÍNDICE: EUR **49/4306/2016**
JULIO DE 2016
IDIOMA: INGLÉS

amnesty.org

AMNESTY INTERNATIONAL