PRIVACY INTERNATIONAL

No Presten Atención al Hombre Detrás de la Cortina: Exponiendo y Desafiando a los Gobiernos que Recurren al Hackeo para Fines de Vigilancia

Junio 2018

Contenido

Introducción

Tanto la privacidad como la seguridad son esenciales para proteger a los individuos, su autonomía y su dignidad.

El detrimento de la privacidad implica el detrimento de la seguridad de los individuos, sus dispositivos y la infraestructura de la que forman parte. La gente necesita privacidad para sentirse libremente segura y proteger su información, así como para gozar plenamente de otros derechos. A su vez, los sistemas que constituyen nuestra infraestructura moderna, ya sean comerciales o gubernamentales, deben ser seguros y facilitar el derecho a la privacidad.

Garantizar la seguridad de nuestros dispositivos, redes y servicios es un desafío constante. La seguridad requiere de diversos actores –en particular, investigadores en el área de la seguridad, la industria y el Gobierno– que destinen recursos significativos y cooperen entre sí.

Los sistemas tecnológicos deben respaldar y mejorar la privacidad, en lugar de socavarla. La legislación o las prácticas no deben obligar a los individuos o las organizaciones a socavar su seguridad, ni la seguridad que proporcionan a los usuarios que depositan su confianza en ellos.

Desafortunadamente, el compromiso con la seguridad es escaso en todo el mundo. Por el contrario, la legislación en materia de ciberseguridad y ciberdelitos suele estar mal diseñada y se concentra en el monitoreo y la criminalización del comportamiento online, además de aumentar las facultades de vigilancia gubernamental, en lugar de abordar los problemas de seguridad de fondo de los sistemas.

Las organizaciones no suelen elaborar modelos y evaluaciones de riesgos y amenazas antes del desarrollo y la implementación de los sistemas. No se presta la atención suficiente al hecho de que todos los sistemas tienen vulnerabilidades, y no se reconoce que la ética adecuada en materia de seguridad está relacionada con la identificación de dichas vulnerabilidades y la garantía de su divulgación y reparación equitativas.

Esta falta de atención a los problemas centrales de seguridad es particularmente preocupante en relación con las infraestructuras críticas. Estos baches hacen que los países y, a su vez, los datos de las personas, se vuelvan vulnerables a ataques y filtraciones de información, sin que los Gobiernos estén preparados para brindar una respuesta. Este contexto que se está consolidando podría ser catastrófico para la privacidad y la seguridad. Asimismo, genera la pérdida de confianzas y restringe la innovación.[1]

1 En el siguiente enlace podrá consultar el trabajo que Privacy International y los miembros de su red han efectuado sobre seguridad digital: https://www.privacyinternational.org/topics/cyber-security

A lo largo de sus casi tres décadas de trabajo en la materia, Privacy International ha observado que los Gobiernos suponen que la inseguridad es aceptable si les permite cumplir con sus objetivos de vigilancia. Esto es inaceptable.

Los Gobiernos de diversas partes del mundo han justificado el detrimento de tecnologías de cifrado y exigido a las empresas que establezcan mecanismos para poder evadir las protecciones existentes. Incluso han llegado a solicitar la remoción completa de determinados mecanismos de seguridad. Estas demandas ponen en riesgo la seguridad de los dispositivos, las redes y los servicios. Son lo opuesto a la ciberseguridad.

Una cantidad cada vez mayor de Gobiernos en el mundo está recurriendo también al hackeo para facilitar sus actividades de vigilancia. Cuando los Gobiernos emprenden actividades de hackeo para fines de vigilancia, nuevamente buscan priorizar la inseguridad y socavar la protección que tanto necesitamos.

Debido a que las actividades de hackeo que emprende un Gobierno para vigilar interfieren de manera significativa con el derecho a la privacidad y otros derechos, además de generar riesgos importantes para la seguridad de dispositivos y redes, Privacy International pone en duda que dichas prácticas conformen un modo legítimo de vigilancia estatal.

Incluso en los casos en los que los Gobiernos emprenden prácticas de hackeo en conexión con actividades de vigilancia que pueden ser legítimas, como sucede al recoger pruebas en investigaciones penales o actividades de inteligencia, es posible que nunca puedan llegar a demostrar que el hackeo se realiza como una forma de vigilancia compatible con las normas internacionales de derechos humanos. Sin embargo, no se ha debatido públicamente lo suficiente sobre el alcance y la naturaleza de esta facultad y sobre las implicancias que tiene para la privacidad y la seguridad de las personas.

Gobiernos que recurren al hackeo para fines de vigilancia: 10 salvaguardas necesarias

Privacy International ha diseñado un conjunto de 10 salvaguardas necesarias[2], con el fin de ayudar a las partes interesadas a evaluar las actividades de hackeo emprendidas por los Gobiernos, a la luz de las normas internacionales de derechos humanos y las implicancias que dichas actividades de vigilancia tienen para la seguridad. Es nuestro deber priorizar la seguridad de los sistemas y los datos. Esperamos que nuestras salvaguardas contra el hackeo contribuyan a promover el debate público sobre el alcance y la naturaleza de la facultad que tienen los Gobiernos en este ámbito y las implicancias de este tipo de prácticas para la privacidad y la seguridad.

2 Privacy International, Gobiernos que emprenden actividades de hackeo para fines de vigilancia: 10 salvaguardas necesarias, 2017 https://privacyinternational.org/type-resource/hacking-necessary-safeguards

Como parte de una serie publicada por Privacy International[3], la finalidad de este informe es mostrar ejemplos de actividades de hackeo realizadas por Gobiernos para fines de vigilancia, que han sido investigadas por nosotros, organizaciones asociadas a Privacy International, y terceros.

Presentaremos casos de Argentina, Chile, Colombia, Etiopía, México y Uganda, que hemos analizado de acuerdo a las salvaguardas contra el hackeo. Estos ejemplos contextualizan una problemática compleja y demuestran lo alejados que están los Gobiernos de lo que exigen las normas internacionales de derechos humanos respecto a sus actividades de hackeo. También ilustran el desafío que representa para la sociedad civil, porque le exige resaltar la importancia de la seguridad defensiva ante Gobiernos enfocados en actividades ofensivas. Asimismo, intentamos responder algunas preguntas frecuentes sobre el hackeo y sus implicancias para la seguridad.

Alentamos a las partes interesadas a compartir con Privacy International ejemplos de Gobiernos que recurren al hackeo para fines de vigilancia, junto con la legislación correspondiente (si existiera).

Las salvaguardas contra el hackeo forman parte de una estrategia integral emprendida por Privacy International y otras instituciones de la sociedad civil para garantizar que:

- Los Gobiernos y la industria prioricen la seguridad defensiva;
- Nuestros dispositivos, redes y servicios se diseñen de modo tal que garanticen la seguridad y protejan nuestra privacidad, y que dichas protecciones se mantengan y
- Las protecciones legales y tecnológicas se apliquen a todas las personas en todo el mundo.

3 Para obtener más información, consulte las publicaciones del siguiente enlace: https://privacyinternational.org/topics/cyber-security

Preguntas y Respuestas

¿Qué es el hackeo?

El término "hackeo" es difícil de definir. Es esencialmente el intento por comprender un sistema mejor de lo que el sistema se comprende a sí mismo, para luego modificarlo levemente y lograr que haga lo que el hacker desee. En las salvaguardas contra el hackeo, Privacy International propone la siguiente definición:

> El hackeo es un acto o una serie de actos que interfieren con un sistema para lograr que actúe de una manera imprevista o inesperada por el fabricante, usuario o propietario de dicho sistema. "Sistema" se refiere a cualquier tipo de combinación de hardware y software, o a alguno de sus componentes.

Privacy International reconoce que es posible que existan casos de hackeo gubernamental que no respondan a esta definición y que, sin embargo, deban ser investigados. Estamos abiertos a recibir sugerencias sobre cómo modificar esta definición para incluir otras formas de hackeo por parte de Gobiernos.

¿Todas las actividades de hackeo son condenables?

No. El hackeo suele tener una connotación negativa en la esfera pública, donde se lo relaciona frecuentemente con ciberdelitos como el fraude o robo de información personal.

Pero el hackeo puede contribuir a la ciberseguridad. Los sistemas informáticos son complejos y, casi con toda seguridad, tienen vulnerabilidades. El hackeo es esencial para identificar dichas vulnerabilidades, someterlas a pruebas mediante el desarrollo de herramientas especiales para ello, y compartir los resultados obtenidos, lo que es fundamental para mejorar la seguridad y la respuesta ante incidentes. El hackeo, por lo tanto, nos ayuda a mejorar y fortalecer los sistemas que son esenciales para nuestra vida y que la determinan cada vez con mayor frecuencia.

¿Qué capacidades necesitan los Gobiernos para hackear?

La vigilancia se está llevando a cabo en secreto cada vez con mayor frecuencia. Por lo tanto, no debe sorprendernos que muchos Gobiernos encubran sus facultades y capacidades de hackeo.

El hackeo se trata fundamentalmente de hacer que las tecnologías actúen de una manera que su fabricante, propietario o usuario no había previsto ni planeado. En el contexto de la vigilancia, es un método para obtener acceso a un sistema y, por lo tanto, a la información de sus usuarios. El hackeo puede incluir interferencias con

los sistemas de la custodia física de los Gobiernos, al igual que interferencias de sistemas a distancia.

Una característica común del hackeo es el aprovechamiento de alguna vulnerabilidad en el software o hardware, que puede ser utilizada por millones de personas.[4] Por ejemplo, es posible que los Gobiernos utilicen estas vulnerabilidades preexistentes para instalar a distancia un malware en un sistema sin la participación del usuario.

Sin embargo, el hackeo también implica aprovecharse de las personas para interferir en sus sistemas. La suplantación de identidad ("phishing"), por ejemplo, es una técnica de ingeniería social común por medio de la que un rival se hace pasar por una persona u organización respetable.

Los ataques de suplantación de identidad suelen adoptar la forma de correos electrónicos o mensajes de texto, que pueden incluir un enlace o archivo adjunto infectado con malware. En ambos ejemplos, las consecuencias de instalar el malware puede dar lugar a que el Gobierno lleve a cabo diferentes actividades de vigilancia: acceder a todos los datos almacenados en el sistema, encender de manera encubierta el micrófono, la cámara o la tecnología de localización GPS de un dispositivo, tomar capturas de pantalla continuamente del dispositivo hackeado u observar toda la información que ingresa a dicho dispositivo o que sale de él (incluidos los detalles y las contraseñas de inicios de sesión, el historial de navegación en Internet y los documentos y las comunicaciones que el usuario no deseaba compartir). El hackeo también permite la manipulación de la información de un sistema, como eliminar, agregar o dañar datos.

Los Gobiernos también pueden desarrollar estas capacidades de manera interna, o adquirir las existentes a través de empresas de tecnología de vigilancia. Las herramientas y los métodos que sabemos que se utilizan en África y en América Latina pertenecen, en su mayoría, al último grupo. Los documentos filtrados de empresas han tenido un papel fundamental en la búsqueda de transparencia para la problemática, particularmente respecto de las empresas que venden *spyware*, un término colectivo que se refiere a capacidades de hackeo que incluyen herramientas y malware de acceso a distancia.[5]

Muchas personas supieron por primera vez que un Gobierno realizaba actividades de hackeo con fines de vigilancia gracias a la filtración o el hallazgo de documentos. Las pruebas de estas herramientas y métodos provienen de fuentes adicionales, como documentos obtenidos mediante el transcurso de nuestras investigaciones, o

4 Para obtener mayor información sobre el hackeo, consulte la presentación que hizo Privacy International sobre el Código de Prácticas para las Interferencias de Equipos el 20 de marzo de 2015. Disponible en: https://www.privacyinternational.org/sites/default/files/PI%20and%20ORG%20Submission%20-%20Draft%20Equipment%20Interference%20Code%2020%20Mar%202015_0.pdf

5 En 2016, Privacy International lanzó el Índice de la Industria de la Vigilancia, el recurso educativo más grande disponible a nivel mundial en su tipo, con datos y documentos sobre la industria de la vigilancia, junto con un informe que registraba el crecimiento de la industria y su alcance en la actualidad https://privacyinternational.org/blog/1236/privacy-international-launches-surveillance-industry-index-and-new-accompanying-report

mediante los informes públicos o de investigación elaborados por periodistas y otras organizaciones de la sociedad civil, incluidos nuestros socios de la red internacional.[6]

Durante la Primavera Árabe de 2011 en Egipto, los activistas recuperaron archivos semitriturados y quemados de la sede abandonada del Servicio de Seguridad egipcio. Entre estos archivos, encontraron documentos y contratos relacionados con la compra de una herramienta de hackeo llamada FinFisher, que permite acceder a dispositivos a distancia. Esta herramienta es desarrollada y vendida por Gamma Internacional, una empresa del Reino Unido.[7] Este descubrimiento provocó que la sociedad civil iniciara diversas investigaciones sobre Gamma International y otras empresas que estaban vendiendo productos de hackeo a regímenes represores y con antecedentes poco satisfactorios en materia de derechos humanos.

En 2013, Privacy International presentó una reclamación ante el Punto Nacional de Contacto de la OECD en relación con la compra de spyware que hicieron funcionarios del Gobierno de Baréin a la empresa Gamma International del Reino Unido y Trovicor, otra empresa de vigilancia[8] con sede en Alemania. Estas compras se descubrieron a través de documentos publicados online en forma anónima.[9] En 2014, Citizen Lab, una organización de la sociedad civil líder en la investigación de estos casos, publicó investigaciones sobre países que habían adquirido FinFisher, y encontró evidencias de spyware en las laptops de activistas.

En 2015, fueron hackeados los sistemas de la empresa de spyware italiana Hacking Team, y se publicaron contratos y correos electrónicos en Internet. En los meses posteriores, la sociedad civil y los periodistas analizaron los documentos y se enteraron de qué Gobiernos habían comprado el spyware y cuánto habían gastado. También, obtuvieron pistas sobre los motivos de la adquisición y contra quién(es) se utilizó la herramienta. Esto dio lugar a diversas acciones y consecuencias que describimos en este informe y que dieron lugar a la elaboración de las salvaguardas contra el hackeo.

¿Cuál es el problema? Los Gobiernos hackean sistemas para atrapar a los delincuentes, ¿no es así?

Los ejemplos que tanto nosotros como terceros hemos recolectado demuestran que el hackeo no suele utilizarse para facilitar actividades legítimas de vigilancia. Se ha comprobado que algunos Estados, con antecedentes nefastos en materia de derechos humanos, han adquirido capacidades de hackeo y las han utilizado

6 Para mayor información sobre la red de Privacy International, consulte: https://privacyinternational.org/partners

7 Karen McVeigh, The Guardian, Empresa británica ofreció software espía a régimen egipcio – documentos, 28 de abril de 2011 https://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finfisher

8 Privacy International et al vs. Gamma International, 1.o de febrero de 2013 https://www.oecdwatch.org/cases/Case_286

9 Adriana Edmeades, Open Democracy, Cómo Baréin espía el suelo británico, 4 de noviembre de 2014 https://www.opendemocracy.net/opensecurity/adriana-edmeades/how-bahrain-spies-on-british-soil

para acceder a los sistemas informáticos de defensores de derechos humanos, periodistas, opositores políticos, manifestantes y disidentes, incluidas personas exiliadas en el extranjero.

En Uganda, el objetivo explícito de la operación de hackeo llamada "Fungua Macho" fue desarticular un movimiento de protestas en contra de una suba de precios.[10] En México, se utilizaron capacidades de hackeo que permitieron espiar a defensores de la salud pública comprometidos con una campaña de alto perfil que promovía "impuestos a refrescos" para combatir la obesidad.[11] En Colombia, las fuerzas militares recurrieron al hackeo para espiar a las personas involucradas en las negociaciones de paz con las FARC, poniendo en peligro todo el proceso.[12]

Incluso en los casos en que los Gobiernos recurren al hackeo para facilitar actividades legítimas de vigilancia, sus implicancias en materia de privacidad y seguridad significan que es posible que los Gobiernos nunca puedan llegar a demostrar que dichas prácticas son una forma de vigilancia compatible con la legislación internacional en materia de derechos humanos.

Cuando los Gobiernos buscan autorizar sus facultades de recurrir al hackeo dentro de ese contexto, deben crear un sólido debate público sobre su necesidad y proporcionalidad, además de evaluar con más detalle esas facultades en vista de las salvaguardas contra el hackeo.

¿Qué es lo preocupante del hackeo desde la perspectiva de la privacidad?

Como mencionábamos, el hackeo permite que los Gobiernos accedan a sistemas a distancia y, por lo tanto, potencialmente a todos los datos almacenados en dichos sistemas. Cada vez con mayor frecuencia, es posible que los Gobiernos dirijan sus facultades para hackear dispositivos nuevos y emergentes, como la Internet de las cosas y los dispositivos corporales e incorporados, como los sensores de salud. Asimismo, el hackeo permite que los Gobiernos practiquen nuevas formas de vigilancia en tiempo real, por ejemplo encendiendo de manera encubierta el micrófono, la cámara o la tecnología de localización GPS de un dispositivo. Finalmente, el hackeo permite a los Gobiernos manipular datos de diversas maneras.

Las intrusiones a la privacidad provocadas por el hackeo se amplifican enormemente cuando un Gobierno interfiere con las redes de comunicación y su infraestructura subyacente. Un único ataque puede afectar a muchas personas, incluidos los individuos que resultan secundarios o no están involucrados en la investigación o la operación gubernamental. Sin embargo, mediante el hackeo a un proveedor

10 Musaazi Namit, Aljazeera Protestas de camino al trabajo en Uganda generan problemas, 18 de abril de 2011 http://www.aljazeera.com/indepth/features/2011/04/201142831330647345.html

11 Azam Ahmed y Nicole Perlroth, El uso de textos como señuelos: spyware del Gobierno espía a periodistas y sus familias, 19 de junio de 2017 https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

12 Associated Press en Bogotá, The Guardian, Ciberespías militares monitorearon a negociadores de la paz colombiana, informa una revista, 4 de febrero de 2014 https://www.theguardian.com/world/2014/feb/04/colombia-farc-peace-talk-negotiators-spied-on-magazine-reports

de Internet, por ejemplo, un Gobierno podría ganar acceso no solo al sistema del proveedor sino también, mediante los datos allí almacenados, a los sistemas de todos sus usuarios.

Los Gobiernos también pueden interferir con diferentes tipos de redes y su infraestructura. Por ejemplo, en 2013, GCHQ, la agencia de inteligencia de señales del Reino Unido, hackeó a Belgacom, el proveedor de telecomunicaciones más grande de Bélgica.[13] El hackeo de redes podría realizarse para vigilar a individuos, grupos o países específicos, o para abarcar la totalidad de numerosas jurisdicciones.

¿Qué es lo preocupante del hackeo desde la perspectiva de la seguridad?

Los sistemas informáticos son complejos y, casi con toda seguridad, tienen vulnerabilidades. Las personas también tienen su complejidad, y sus interacciones con los sistemas dan lugar a vulnerabilidades que podrían aprovecharse para interferir con sus propios sistemas.

Tanto la identificación de vulnerabilidades, como su sometimiento a pruebas mediante el desarrollo de fallos aprovechables y el intercambio de estos resultados son necesarios para consolidar la seguridad. Pero los Gobiernos que hackean para fines de vigilancia no buscan la seguridad de los sistemas.

En el contexto de la vigilancia estatal, el Gobierno no busca vulnerabilidades para lograr que los sistemas sean seguros mediante la realización de pruebas y una divulgación coordinada, sino para aprovechar dichas vulnerabilidades y facilitar sus actividades de vigilancia. Esta actividad podría socavar la seguridad no solamente de los sistemas vigilados sino también la de otros sistemas no relacionados. Debido a que confiamos cada vez más en Internet y conectamos con mayor frecuencia nuestro mundo físico con ella, este riesgo aumenta.

El derecho a la privacidad no está incluido en la constitución o la legislación de mi país. ¿Siguen siendo aplicables las salvaguardas contra el hackeo?

Sí. Incluso si la privacidad no está contemplada explícitamente en la legislación nacional, la mayoría de los Estados han firmado obligaciones internacionales o regionales que protegen la privacidad. Por ejemplo, el derecho a la privacidad está protegido en el Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por sus siglas en inglés), o instrumentos regionales como el Pacto Estadounidense sobre Derechos Humanos, la Carta Árabe sobre Derechos Humanos o el Consejo del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

13 Ryan Gallagher, The Intercept, How U.K. spies hacked a European ally and got away with it, 17 February 2018 https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/

¿Dónde puedo encontrar leyes sobre el hackeo en mi país?

Muy pocos países han legislado explícitamente el uso que los Gobiernos pueden hacer del hackeo para fines de vigilancia, y los que sí lo han hecho se concentran mayoritariamente en Europa. Derechos Digitales, uno de los socios de Privacy International en Chile, realizó un análisis exhaustivo sobre el uso que hicieron los Gobiernos latinoamericanos del software de Hacking Team y sobre su legalidad. El estudio indica que, en la mayoría de los casos, se lo utilizó sin sustento legal en toda la región.[14]

En algunos casos, los Gobiernos han interpretado que la legislación existente sobre vigilancia autorizaba el uso del hackeo. Pero la facultad de la que disponga el Gobierno para hackear, si obtiene la autorización, debe estar sujeta a un marco regulatorio diseñado para sus exclusivas implicancias en la privacidad y seguridad, algo que todas las salvaguardas contra el hackeo buscan abordar. La interpretación de que un marco existente, que permite otras actividades de vigilancia como las escuchas telefónicas, autoriza también el hackeo se contradice, por lo tanto, con las salvaguardas.

En otros casos, es difícil encontrar disposiciones legales que aborden el uso del hackeo por parte del Gobierno, porque están dispersas en otros instrumentos legislativos como por ejemplo un código penal o la legislación de ciberseguridad. En estas instancias, es posible que estén redactadas de manera tan misteriosa que resulte difícil su interpretación. De hecho, los Gobiernos no suelen utilizar la palabra "hackeo" para describir su facultad de hackear. En los EE. UU., por ejemplo, el Gobierno ha descripto el hackeo como "técnicas investigativas de la red" y "aprovechamiento de las redes informáticas", entre otras frases. En el Reino Unido, la facultad del Gobierno para recurrir al hackeo se menciona como "interferencia de equipos".

Mi Gobierno afirma que el hackeo está legislado en el marco legal existente para la vigilancia de las comunicaciones. ¿Esto es aceptable?

No. Como antes mencionábamos, no es aceptable utilizar el marco legal vigente sobre la vigilancia para justificar la facultad de recurrir al hackeo. Debido a que el hackeo para fines de vigilancia tiene implicancias nuevas y graves para la privacidad y la seguridad, no queda claro que sea compatible con las normas internacionales de derechos humanos.

Si los Gobiernos insisten en autorizar el hackeo para fines de vigilancia, deben aprobar un marco regulatorio con salvaguardas diseñadas para abordar sus exclusivas implicancias. Este es uno de los temas centrales de las salvaguardas contra el hackeo, y se explora en detalle en el presente documento informativo.

14 Lorenzo Franceschi-Bicchierai, Motherboard, El imperio "ilegal" de Hacking Team en América Latina, 18 de abril de 2016 https://motherboard.vice.com/en_us/article/gv5v8q/hacking-team-illegal-latin-american-empire

¿Cuáles son las salvaguardas contra el hackeo de Privacy International? ¿Por qué son necesarias?

Una cantidad cada vez mayor de Gobiernos en el mundo está recurriendo al hackeo para facilitar sus actividades de vigilancia. Sin embargo, muchos implementan esta capacidad de manera secreta y sin una clara justificación legal.

Las salvaguardas contra el hackeo fueron adaptadas, en parte, de los Principios Internacionales sobre la Aplicación de los Derechos Humanos en la Vigilancia de las Comunicaciones (conocidos también como los "Principios Necesarios y Proporcionales" o los "13 Principios") lanzados en 2013. Como iniciativa conjunta de la sociedad civil, la industria y expertos en tecnología, los 13 Principios se desarrollaron para demostrar la manera en que se debe aplicar la legislación existente sobre derechos humanos en los nuevos métodos de vigilancia digital de individuos.[15] Más de 400 organizaciones, expertos y grupos parlamentarios respaldaron los 13 Principios con su firma, además de 300 000 individuos a nivel mundial.[16]

Los 13 Principios describen la manera en que las actividades de vigilancia de las comunicaciones modernas deben estar sujetas a salvaguardas y supervisiones, establecidas por la legislación internacional en materia de derechos humanos.

Si bien los 13 Principios sirven como marco útil para abordar la facultad que puede tener un Gobierno de recurrir al hackeo, las nuevas implicancias que tiene dicha facultad para la privacidad y la seguridad exigían una mayor adaptación de los principios establecidos por la legislación internacional en materia de derechos humanos. Sin embargo, al igual que los 13 Principios, las salvaguardas contra el hackeo hacen hincapié en los principios centrales de legalidad, necesidad y proporcionalidad de cualquier facultad de los Gobiernos que interfiera con el derecho a la privacidad.

En el presente informe, Privacy International se concentró predominantemente en la primera salvaguarda, que aborda la legalidad de la facultad de los Gobiernos de recurrir al hackeo. Como se describe en cada uno de los ejemplos, los Gobiernos están hackeando sistemas de manera secreta y sin un fundamento legal claro.

En el primer ejemplo, el requisito de legalidad garantiza que exista un debate público sobre la necesidad misma de esta facultad. En los casos en que los Gobiernos establecen posteriormente una base legal para dicha facultad, esa base garantizará más sólidamente que la finalidad y el alcance de la facultad son claros y accesibles al público.

De ser relevante, Privacy International también aborda la relevancia de las demás salvaguardas para ejemplos específicos. En particular, los ejemplos a continuación revelan la necesidad de que los Gobiernos lleven a cabo una evaluación de cuáles podrían ser los efectos del hackeo con fines de vigilancia en la seguridad y la

15 https://necessaryandproportionate.org/principles

16 https://necessaryandproportionate.org/sign

integridad de los sistemas y los datos, como parte de un análisis de necesidad y proporcionalidad.

Las diez salvaguardas exploran:[17]

1. Legalidad
2. Seguridad e integridad de sistemas
3. Necesidad y proporcionalidad
4. Autorización judicial
5. Integridad de la información
6. Notificación
7. Destrucción y devolución de datos
8. Supervisión y transparencia
9. Extraterritorialidad
10. Recurso efectivo

17 Privacy International, Gobiernos que emprenden actividades de hackeo con fines de vigilancia: 10 salvaguardas necesarias, 2017 https://privacyinternational.org/type-resource/hacking-necessary-safeguards

Las Salvaguardas Contra el Hackeo en contexto

Argentina

Los correos electrónicos de Hacking Team que se filtraron en julio de 2015 tenían comunicaciones con empresas argentinas que aseguraban tener vínculos con agencias estatales. Sin embargo, no fue posible comprobar ninguna transacción a partir de dichos correos.

En cambio, se comprobó que figuras políticas como el fallecido fiscal Alberto Nisman y el periodista Jorge Lanata fueron víctimas de espionaje con spyware en 2014. En diciembre de 2015, Citizen Lab documentó una extensa campaña de utilización de malware, suplantación de identidad y desinformación que probablemente había sido patrocinada por el Estado en diversos países latinoamericanos, incluida Argentina.[18]

Existe un debate para determinar si las enmiendas propuestas en 2016 al Código Procesal Penal argentino amplían las facultades de vigilancia del Gobierno para incluir el hackeo.[19] Las enmiendas presentadas para consulta abierta contaban con la introducción de métodos especiales de investigación, incluida la vigilancia a distancia de equipos informáticos, y la vigilancia mediante la captura de imágenes, la localización y el monitoreo. Los propulsores del proyecto de ley argumentaron que las técnicas se justificaban por la necesidad de reaccionar adecuada y flexiblemente a la difícil tarea de combatir la actividad delictiva transnacional.

Los críticos dijeron que el proyecto de ley no incluía la definición de hackeo y que solamente se hacía referencia al uso de "software que permite o facilita el acceso a distancia". También, hicieron hincapié en la falta de información necesaria sobre la autoridad responsable relevante para llevar a cabo dichas actividades.[20]

Finalmente, el proyecto de ley no fue aprobado, pero sin embargo varias de las temáticas abordadas por el mismo fueron tratadas en leyes individuales, con excepción del capítulo sobre vigilancia electrónica.

En abril de 2018, dos senadores presentaron un nuevo proyecto de ley para incorporar al Código Procesal Penal de la Nación todas aquellas leyes que habían sido aprobadas individualmente en años anteriores, pero el proyecto incorporaba

18 Freedom House, Libertad en la red: Argentina, 2017 https://freedomhouse.org/report/freedom-net/2017/argentina ; Citizen Lab, Packrat: siete años de un actor sudamericano amenazante, 2015 https://citizenlab.ca/2015/12/packrat-report/

19 https://www.justicia2020.gob.ar/noticias/proyecto-reforma-al-codigo-procesal-penal-federal-ingreso-al-senado-la-nacion/

20 Consulte, Estado de privacidad, Argentina, 2017 https://privacyinternational.org/state-privacy/57/state-privacy-argentina y Freedom House, Libertad en la red 2017 https://freedomhouse.org/report/freedom-net/2017/argentina

nuevamente disposiciones sobre vigilancia electrónica, como la vigilancia remota sobre equipos informáticos, la vigilancia a través de dispositivos de seguimiento y localización, y técnicas de vigilancia acústica, por nombrar las más preocupantes.

A diferencia de las otras disposiciones contempladas en el proyecto de ley, el capítulo sobre vigilancia nunca fue consagrado por ninguna ley. ADC, una organización de sociedad civil en Argentina, expresó su preocupación por la falta de un debate amplio y público sobre los asuntos tratados en el proyecto, ya que la introducción del hacking estatal y otras técnicas de vigilancia tienen consecuencias claras sobre el derecho a la privacidad de las personas.[21] Cuando el proyecto de ley fue tratado por el pleno de la Cámara de Senadores, varios senadores de la oposición mencionaron la falta de un debate detallado sobre la incorporación de dichas técnicas de vigilancia. Finalmente, durante la sesión, los autores del proyecto de ley presentaron una modificación para eliminar el capítulo completo sobre vigilancia, de esta forma el Senado aprobó el proyecto de ley sin dichas disposiciones. Sin embargo, los autores del proyecto de ley declararon que buscarían incorporar las técnicas de vigilancia en el futuro cercano,[22] haciendo modificaciones al texto original e introduciendo controles y rendición de cuentas.[23]

La inclusión de nuevas facultades de hackeo en el Código Procesal Penal, no cumplen hasta el momento con el principio de legalidad según se describe en la primera salvaguarda, porque dichas facultades no están prescriptas *"explícitamente"* en un marco *"diseñado para las implicancias exclusivas que tiene el hackeo en la privacidad y la seguridad".* Además, debido a la confusión relativa a su significado y alcance, las enmiendas no son *"lo suficientemente claras y precisas para permitir a las personas prever [su] aplicación y la extensión de la interferencia".*[24]

La primera salvaguarda contra el hackeo requiere que las facultades de recurrir al hackeo, como las demás facultades de vigilancia, tengan una clara base legal. En el centro del principio de legalidad se encuentra la premisa importante de que dar "carácter legal a los regímenes intrusivos de vigilancia" los vuelve objeto de "debate público y parlamentario". La legalidad también está estrechamente vinculada con el concepto de "interferencia arbitraria", la idea de que el ejercicio de facultades secretas conlleva el riesgo inherente de ser aplicadas arbitrariamente.[25]

21 ADC, #ReformaEspía: Nuevas técnicas de vigilancia para la investigacíon penal, 2018 https://adcdigital.org.ar/wp-content/uploads/2018/04/AnalisisReformaEspiaCPPF.pdf

22 Página 12, Una media sanción que excluyó la vigilancia electrónica, 2018 https://www.pagina12.com.ar/110681-una-media-sancion-que-excluyo-la-vigilancia-electronica

23 Página 12, "La vigilancia y las escuchas tendrán un plazo de treinta días", 2018 https://www.pagina12.com.ar/109876-la-vigilancia-y-las-escuchas-tendran-un-plazo-de-treinta-dia

24 Primera salvaguarda contra el hackeo: Legalidad https://privacyinternational.org/safeguards/85/hacking-safeguard-1-legality

25 Consulte el comentario sobre legalidad de la primera salvaguarda contra el hackeo https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary#1

Uganda

En 2015, Privacy International publicó una investigación, Para dios y mi presidente: *la vigilancia estatal en Uganda*,[26] en la que se describía una operación gubernamental de vigilancia secreta dirigida a un movimiento de protesta nacional que exponía el aumento del costo de vida. La operación de vigilancia fue posible porque el Gobierno adquirió FinFisher, un malware intrusivo desarrollado y vendido por Gamma, una empresa con base en el Reino Unido.[27] La operación propiamente dicha fue llevada a cabo sin que exista un marco legal riguroso que regule la vigilancia de las comunicaciones en general, y sin ningún marco explícito que regulara el uso del hackeo, en particular.

Según documentos adquiridos por Privacy International, el objetivo explícito de la operación, llamada Fungua Macho ("abre los ojos" en suajili), era desarticular el movimiento de protesta Camino al trabajo[28] mediante la obtención de información personal sobre los manifestantes, que podría utilizarse para silenciarlos y extorsionarlos. La operación también tenía el objetivo de espiar al partido opositor Foro para el Cambio Democrático (FCD), las entidades mediáticas, los parlamentarios y los informantes de inteligencia, infectando los dispositivos de comunicación personal con malware intrusivo.

El Gobierno negó estas acusaciones y Privacy International respondió debidamente exhibiendo la evidencia que había obtenido, compuesta de páginas de documentos oficiales y verificados. En ese momento, agregamos este comentario:

"Asimismo, la Ley de Regulación de las Intercepciones de Comunicaciones (2010) no regula el uso de malware intrusivo como FinFisher. En cambio, únicamente incluye las intercepciones de comunicaciones, en la manera en que se llevan a cabo mediante las redes del proveedor de servicio de Uganda. El uso de FinFisher equivale a "hackear" el dispositivo de un individuo. La operación Fungua Macho, que parecería haber sido finalizada sin ninguna referencia a supervisiones o garantías judiciales, no estaba incluida, entonces, dentro del alcance de la ley".[29]

De esta manera, en la medida en que el Gobierno de Uganda llevó a cabo actividades de hackeo porque confiaba en las facultades otorgadas por la Ley de Regulación de las Intercepciones de Comunicaciones, dichas actividades no

26 Privacy International, Para dios y mi presidente: la vigilancia estatal en Uganda, octubre de 2015 https://privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf

27 La Jefatura de Inteligencia Militar (JIM) adquirió el malware de vigilancia FinFisher en diciembre de 2011 de Gamma International GmbH (Alemania), según documentos obtenidos por Privacy International. Consulte también, Nick Hopkins y Jake Morris, BBC, Kit de vigilancia de empresa del Reino Unido utilizado para desarticular a la oposición en Uganda , 15 de octubre de 2015 http://www.bbc.co.uk/news/uk-34529237

28 Musaazi Namit, Aljazeera Protestas de camino al trabajo en Uganda generan problemas, 18 de abril de 2011 http://www.aljazeera.com/indepth/features/2011/04/201142831330647345.html

29 Privacy International, Documentos revelan que el Gobierno de Uganda implementó el spyware FinFisher para "desarticular" a la oposición y hacer un seguimiento de los funcionarios elegidos y de los medios, en operación secreta durante protestas poselectorales, 15 de octubre de 2015 https://privacyinternational.org/node/694

cumplirían con el principio de legalidad. Este principio, según se articula en la primera salvaguarda contra el hackeo, exige que:

"Las facultades de recurrir al hackeo otorgadas al Gobierno deben estar prescriptas explícitamente en la ley y deben restringirse a las actividades estricta y demostrablemente necesarias para lograr un objetivo legítimo".

Como explica con mayor detalle el comentario legal a esta salvaguarda:

"En términos generales, las leyes que otorgan al Gobierno facultades amplias e imprecisas de vigilancia no pueden autorizar el hackeo, en conformidad con el principio de legalidad. El uso de la palabra "explícitamente" también hace hincapié en que las facultades de recurrir al hackeo otorgadas al Gobierno deben estar sujetas a un marco regulatorio diseñado para sus exclusivas implicancias en la privacidad y seguridad, algo que todas las salvaguardas buscan abordar. La interpretación de que un marco existente, que autoriza otras actividades de vigilancia como las escuchas telefónicas, autoriza el hackeo entra en conflicto, por lo tanto, con las salvaguardas. De igual manera, un marco legal que autoriza un hackeo copiando y pegando literalmente el texto de marcos que se aplican a otras actividades de vigilancia también entrará en conflicto con las salvaguardas".

En el Examen Periódico Universal de Uganda de 2016[30], presentado ante el Consejo sobre Derechos Humanos de las Naciones Unidas, Privacy International recomendaba que el Gobierno:

"Garantizara que el Parlamento condujera una investigación sobre el uso de software intrusivo para evaluar si cumplía con las obligaciones nacionales e internacionales sobre derechos humanos de Uganda, y que pusiera a disposición del público cualquier hallazgo relacionado con dicha investigación";

Y que:

"Detuviera todo proceso de adquisición de malware intrusivo y otras herramientas de hackeo hasta que se conocieran los resultados de la investigación parlamentaria, y que garantizara que existen controles apropiados para evitar el uso de productos de la industria de la vigilancia privada que facilitaran abusos a los derechos humanos".

Desafortunadamente, la respuesta del Gobierno no hizo referencia a ninguna de las recomendaciones, y la ley no ha cambiado.

Chile

En 2015, las filtraciones de Hacking Team revelaron las capacidades de hackeo del Gobierno chileno. Se descubrió que la Policía de Investigaciones de Chile (PDI)

30 Revisión Periódica Universal de Uganda (2016) https://privacyinternational.org/sites/default/files/2017-12/uganda_upr2016.pdf

había adquirido dos sistemas: "Galileo" y "Phantom". Al principio, la PDI negó las compras e hizo hincapié en que, según la legislación chilena, se requería una autorización judicial previa para realizar actividades de hackeo con fines de vigilancia. Sin embargo, posteriormente se confirmaron las compras. Según un análisis de Derechos Digitales:[31]

"…para cumplir con los requisitos del principio de legalidad [en los 13 Principios], es necesario cumplir con el artículo 9 del Código Procesal Penal chileno que exige una autorización judicial para las interferencias de los derechos fundamentales. Sin embargo, el uso de malware no está específicamente autorizado en el texto del código, por lo que su legalidad está condicionada a lo que se persigue con su uso según las regulaciones aplicables como la Ley de Inteligencia, la Ley Antiterrorista y la Ley de Drogas. Las entidades gubernamentales sostuvieron de manera específica que "Phantom" se usaría únicamente para combatir el tráfico de drogas y el delito organizado".

El análisis continúa:

"La PDI defiende su uso de 'Phantom' argumentando una necesidad de modernizar sus capacidades para 'investigar el delito organizado, el terrorismo internacional y el tráfico de drogas a gran escala'. Estas justificaciones están escritas en conformidad con la Ley 19.974 sobre los sistemas de inteligencia [Ley de Inteligencia, 2004]. El artículo 24 consagra "procedimientos especiales para recoger información" a fuentes que están cerradas al público: se limitan exclusivamente a actividades de inteligencia y contrainteligencia que tienen como finalidad salvaguardar la seguridad nacional y proteger a Chile y su pueblo del terrorismo, el delito organizado y el tráfico de drogas, 'e incluyen' la intervención de sistemas y redes informáticas (sección III, párrafo b) y cualquier otro sistema tecnológico de transmisión, almacenamiento o procesamiento de comunicaciones o información (sección III, párrafo d). Dado que dichas operaciones son llevadas a cabo por la policía y con autorización judicial, esta forma de 'intervención' de sistemas informáticos (el uso de malware) se llevaría a cabo en conformidad con esta ley".

Sin embargo, el uso por parte de la PDI de las actividades de hackeo con fines de vigilancia todavía no cumple con el principio de legalidad. Según este principio, de la manera en que está articulado en las salvaguardas contra el hackeo, las facultades para recurrir al hackeo otorgadas al Gobierno deben estar *"prescriptas explícitamente por la ley"* y, de la manera descrita en los ejemplos de Uganda y Argentina antes mencionados, los Gobiernos no pueden sencillamente interpretar que un marco existente, que permite otras actividades de vigilancia, autoriza también el hackeo. Por lo tanto, invocar otras leyes como el Código Procesal Penal resulta insuficiente.

Además, la utilización de una ley anterior, que fue aprobada para investigar el delito organizado, el terrorismo internacional y el tráfico de drogas, con el fin de autorizar el hackeo significa que no se exigió al Gobierno evaluar los riegos y los daños

31 Derechos Digitales, Vigilancia estatal de las comunicaciones y protección de los derechos fundamentales en Chile, julio de 2016. Consulte la sección 2.2.3 Vigilancia focalizada: malware https://necessaryandproportionate.org/country-reports/chile

potenciales para la seguridad e integridad del sistema o los datos que han sido el objetivo (u otros sistemas y datos), según se describe en la segunda salvaguarda contra el hackeo. Este tipo de evaluación es necesario para que los Gobiernos cumplan con los principios de necesidad y proporcionalidad al momento de hackear, según lo descrito en la tercera salvaguarda contra el hackeo.

El Gobierno chileno sostuvo que el uso de hackeo para fines de vigilancia fue legítimo debido a la necesidad de una autorización judicial previa:

"La Comisión de Control de Inteligencia de la Cámara de Diputados citó tanto a los directores de la PDI y la ANI a explicar la compra de este software. Si bien no es posible encontrar registros de dicha sesión, su Presidente, el Diputado Saffirio, afirmó con posterioridad a la misma que "con las explicaciones dadas [en la sesión], quedamos con la certeza de que los controles rigurosos que existen en el interior de la PDI permiten que solo puedan operar estos sistemas (Phantom) previa autorización judicial".

Si bien la autorización judicial previa es una salvaguarda necesaria para autorizar las actividades de vigilancia, incluido el hackeo, según lo descripto en la cuarta salvaguarda contra el hackeo no es suficiente en sí misma para garantizar que las actividades de hackeo cumplan con la legislación internacional en materia de derechos humanos.

Asimismo, el proceso de autorización judicial en sí mismo será diferente en el contexto de hackeo, porque exigirá a la autoridad judicial evaluar las implicancias exclusivas del hackeo para la privacidad y la seguridad. La tercera salvaguarda de hackeo: necesidad y proporcionalidad incluye algunos de los datos exclusivos que deben formar parte de una aplicación para obtener una autorización judicial de hackeo:

"Antes de tomar alguna medida de hackeo, las autoridades gubernamentales deben, como mínimo:

1. *Establecer un alto grado de probabilidad de que:*
    - 1.1 *Haya tenido lugar, o se llevará a cabo, un delito o acto de gravedad, equivalente a una amenaza específica y de gravedad para la seguridad nacional;*
    - 1.2 *El sistema utilizado por la persona que se sospecha cometerá un delito o acto de gravedad, equivalente a una amenaza específica y de gravedad para la seguridad nacional, contiene evidencias relevantes y sustantivas para el presunto delito o acto de amenaza a la seguridad;*
    - 1.3 *Las evidencias relevantes y sustantivas del presunto delito o acto de gravedad, equivalente a una amenaza específica y de gravedad para la seguridad nacional, se obtendrán hackeando el sistema objetivo.*
2. *Establecer, hasta el máximo que fuera posible, la identidad de la persona sospechada de cometer el delito o acto de gravedad equivalente a una amenaza específica y de gravedad para la seguridad nacional, y los detalles de identificación exclusivos del sistema objetivo, incluidas la localización y las configuraciones específicas;*
3. *Determinar que se hayan agotado todos los métodos menos intrusivos, o se haya determinado que serían inútiles, de modo que el hackeo es la opción menos*

intrusiva;

4. *Establecer el método, la extensión y la duración de la medida de hackeo propuesta;*
5. *Garantizar que los datos a los que se acceda y que se recojan se restringirán únicamente a la información relevante y sustantiva en relación con el delito o acto de gravedad, equivalente a la presunta amenaza específica y de gravedad a la seguridad nacional, y las medidas que se tomarán para minimizar el acceso a datos irrelevantes y secundarios, así como su recogida;*
6. *Establecer que únicamente la autoridad especificada accederá a dichos datos y los recogerá, y que dichos datos serán utilizados y compartidos solo a los fines para los que la autorización ha sido otorgada, y durante el tiempo especificado en ella;*
7. *Determinar los riesgos y daños potenciales para la seguridad y la integridad del sistema objetivo y los sistemas en general y de los datos del sistema objetivo y los sistemas en general, y cómo se mitigarán o corregirán dichos riesgos o daños potenciales, para permitir una evaluación de la proporcionalidad de la medida de hackeo propuesta según las implicancias de seguridad".*

Además, el proceso de autorización judicial para hackeo en Chile presenta otros inconvenientes. Por ejemplo, los jueces no tienen acceso a pericia técnica independiente para considerar de manera suficiente la necesidad y la proporcionalidad de una medida de hackeo en particular. Asimismo, Chile carece de un mecanismo de supervisión independiente para este tipo de actividades. Por lo tanto, el proceso de autorización judicial en Chile no puede considerarse una salvaguarda legal adecuada como lo exige la legislación internacional en materia de derechos humanos cuando se realizan interferencias en el derecho a la privacidad.

Sin embargo, Chile sigue siendo testigo de una inusitada controversia relacionada con el hackeo. En 2017, la policía uniformada chilena (Carabineros) llevó a cabo una operación llamada "Operación Huracán", que tuvo como consecuencia una redada y la consiguiente detención de ocho personas acusadas de violencia y terrorismo rural.[32] Esta operación dependió en gran medida de la intercepción de conversaciones de Whatsapp y Telegram de las personas detenidas,[33] obtenidas aparentemente mediante el uso de hackeo.

La operación fue autorizada supuestamente en conformidad con la Ley de Inteligencia (2004), mediante una orden judicial directamente solicitada por la Unidad de Inteligencia de los carabineros. Sin embargo, en octubre de 2017, el Tribunal Supremo de Chile ordenó la liberación de estas ocho personas, dictaminando que las evidencias no llegaban a demostrar su participación en los presuntos delitos.[34]

En enero de 2018, hubo un giro dramático en la historia: surgió nueva información que demostró que la Unidad de Inteligencia de Carabineros no interceptó las comunicaciones que dijo interceptar, ni hackeó ningún dispositivo con fines de

32 http://www.biobiochile.cl/noticias/nacional/chile/2017/09/25/operacion-huracan-6-meses-de-diligencias-que-terminaron-con-8-detenidos-por-atentados.shtm

33 http://impresa.elmercurio.com/Pages/NewsDetail.aspx?dt=2017-09-26&dtB=26-09-2017%200:00:00&PaginaId=2&bodyid=3

34 http://www2.latercera.com/noticia/suprema-ordena-liberar-detenidos-operacion-huracan/

vigilancia, y la orden judicial de hackeo se utilizó como pretexto para implantar las evidencias en los teléfonos de los detenidos.[35]

Sin embargo, el hecho de que los Carabineros hayan declarado que llevaron a cabo una operación de hackeo indica que creen que gozan de esas facultades, incluso aunque esta vez no las hayan efectuado realmente. Parece además que la base legal de estas facultades vuelve a ser la Ley de Inteligencia, que ya hemos descrito antes como insuficiente para cumplir con el principio de legalidad requerido por la legislación internacional en materia de derechos humanos, y según lo establecido en nuestras salvaguardas contra el hackeo.

Aunque todavía no se conoce todo el desenlace de la historia, como consecuencia de este escándalo renunció el Director General de Carabineros, el General a cargo de la Unidad de Inteligencia y a muchos otros oficiales de policía. La fiscalía presentará además cargos contra diversos oficiales, incluyendo el General a cargo de la Unidad de Inteligencia, por obstrucción a la justicia.[36]

Sin embargo, se le debe al pueblo chileno una explicación pública de cómo tuvo lugar semejante abuso de poder, incluida la base legal por la que se otorgó a la Unidad de Inteligencia la facultad de hackear, y qué reglas, si las hubo, rigen estas facultades. Se deben también explicaciones de cómo se enmendará la legislación vigente para evitar que semejantes abusos de poder se vuelvan a repetir.

Colombia[37]

El conflicto interno de Colombia comenzó en la década de los años cincuenta e impactó al menos a tres generaciones de colombianos, siendo las FARC el grupo guerrillero más antiguo del mundo. El uso que el Gobierno ha hecho de la vigilancia de las comunicaciones contra las FARC fue una parte integral del conflicto, documentado en un informe que Privacy International realizó en 2015.[38]

A partir de las filtraciones de Hacking Team, se supo que la policía colombiana adquirió el sistema de control remoto (SCR) llamado "Galileo", un spyware que la empresa vende exclusivamente a Gobiernos, desde el año 2012.[39] Una investigación realizada por Citizen Lab en 2014 hizo un seguimiento del uso del SCR en Colombia y concluyó que, desde 2012, estuvo asociado con ataques a periodistas, activistas y

35 https://www.derechosdigitales.org/11890/la-mugre-y-la-furia-operacion-huracan-podria-haber-sido-un-montaje/

36 http://www.emol.com/noticias/Nacional/2018/03/22/899703/Fiscalia-formalizara-a-generales-r-Gonzalo-Blu-y-Teuber-por-caso-Huracan.html

37 Material adicional de lectura: https://www.theguardian.com/world/2014/feb/04/colombia-farc-peace-talk-negotiators-spied-on-magazine-reports, https://karisma.org.co/risks-of-an-uncontrolled-state-surveillance-in-colombia/ Departamento de Estado de EE. UU., Colombia 2014, Informe sobre derechos humanos https://www.state.gov/documents/organization/236888.pdf

38 Privacy International, Estado ausente: vigilancia, legislación y orden en Colombia, agosto de 2015 https://privacyinternational.org/sites/default/files/2017-12/ShadowState_English.pdf

39 Privacy International, Fundación Karisma y Dejusticia. Estado de privacidad: Colombia, enero de 2018 https://privacyinternational.org/state-privacy/58/state-privacy-colombia

defensores de derechos humanos.[40]

Cerca de esa fecha, un escándalo relacionado con un hackeo realizado por el Gobierno conmocionó y movilizó a la sociedad civil y todos los habitantes de Colombia. A principios de 2014, a medio camino en el proceso de paz entre el Gobierno de Colombia y las FARC, la revista Semana descubrió[41] una operación militar de hackeo conocida como "Operación Andrómeda", dirigida contra los negociadores del proceso de paz pertenecientes al Gobierno y contra otras figuras.[42] Basado en dicha información, a principios de 2018, el fiscal responsable presentó cargos contra diversos oficiales militares implicados en estas actividades.[43]

El escándalo incluía no solo actividades de hackeo para obtener información sobre la negociación del proceso de paz, sino también actividades de hackeo contra otros objetivos no revelados y la venta de información clasificada. A pesar de los cargos penales, el ministro de Defensa de Colombia sostiene que la operación se llevó a cabo en conformidad con la legislación, aunque con algunas fallas en el protocolo de seguridad.[44] Esto indica que el Gobierno, es decir, el Ministerio de Defensa, había aprobado dicha operación.

En los últimos años, Privacy International, junto a sus socios, han documentado fehacientemente las inquietudes sobre la inadecuación del marco de vigilancia de Colombia, incluida la utilización del hackeo por parte del Gobierno. Como hemos mencionado en la presentación del año 2017 en el Examen Periódico Universal de Colombia ante la ONU:

"Según el artículo 269A del Código Penal de Colombia, el "hackeo" ('el acceso abusivo a un sistema de información') es un delito penal y, por lo tanto, en ausencia de legislación explícita que regule su uso para fines de vigilancia, constituye una forma de vigilancia extralegal que, según la legislación colombiana, es ilegal".[45]

Dado que no existe legislación que regule explícitamente el uso del hackeo para prácticas de vigilancia en Colombia, no queda claro cómo el Ministerio de Defensa colombiano puede afirmar que su operación de hackeo se llevó a cabo en conformidad con la ley. En cualquier caso, Privacy International hace hincapié en que, incluso si tal marco legal existiera, pareciera que el Gobierno colombiano ha

40 The Citizen Lab, Mapeo del "spyware indetectable" de Hacking Team, 17 de febrero de 2014. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

41 Semana, ¿alguien espió a los negociadores de La Habana? 2 de marzo de 2014 http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3

42 https://www.theguardian.com/world/2014/feb/04/colombia-farc-peace-talk-negotiators-spied-on-magazine-reports

43 http://www.eltiempo.com/justicia/investigacion/pliego-de-cargos-a-militares-de-operacion-andromeda-167540 Uno de los hackers implicados que fue acusado, Andrés Sepúlveda, es particularmente famoso y su perfil había sido incluido en Bloomberg en 2006 https://www.bloomberg.com/features/2016-how-to-hack-an-election/

44 http://www.eltiempo.com/archivo/documento/CMS-15141236

45 Informe para interesados de la 30.a sesión de la Revisión Periódica Universal – Colombia: el derecho a la privacidad en Colombia. Presentado por Dejusticia, Fundación Karisma y Privacy International, septiembre de 2017 https://privacyinternational.org/sites/default/files/2018-03/UPR_The%20Right%20to%20Privacy%20in%20Colombia_2017.pdf

hackeado a los negociadores por motivos prohibidos por las normas internacionales de derechos humanos, que disponen que:

"'El silenciamiento de cualquier tipo de adhesión de democracia multipartidista, principios democráticos y derechos humanos' nunca es un objetivo legítimo; de hecho, socava el compromiso público y el debate sobre una temática que contradice el artículo 19 [ICCPR], así como el objeto y los fines del convenio".[46]

El Gobierno colombiano, por lo tanto, no puede afirmar que sus actividades de hackeo se realizan en conformidad con un objetivo legítimo cuando investigan a personas comprometidas con un proceso de paz que tiene como fin terminar con un conflicto de décadas.

México

En 2015, se descubrió que el Gobierno mexicano también era cliente de Hacking Team.[47] En febrero de 2017, una investigación llevada a cabo por Citizen Lab[48] reveló que se utilizó el spyware de la firma israelí NSO Group en una operación que tenía como objetivo a científicos de alimentos del Gobierno mexicano y a dos defensores de la salud pública, comprometidos en una campaña de alto nivel para promover "impuestos a refrescos" y combatir la obesidad. Rafael Cabrera, un periodista que investiga la corrupción oficial, también había sido víctima del spyware.[49] En junio de 2017, Citizen Lab[50] y el grupo de sociedad civil mexicana R3D[51], junto con SocialTIC y Article 19 México revelaron más detalles sobre las personas que habían sido víctimas del hackeo.

Entre ellas se incluían los abogados que investigaban la desaparición en masa de 43

46 Informe de Amici Curiae, ONU Expertos en derechos humanos, en respaldo del demandante-apelado y la sentencia revocatoria, John Doe (Kidane) vs. la República Democrática Federal de Etiopía, D.C. Ct. Ap., n.o 16-7081, p. 15 (1 de nov. de 2016), disponible en https://www.eff.org/files/2016/11/01/11.1.16_unitednations_human_rights_experts_amicus_brief.pdf (cita del comentario general n.o 34, supra, en 35) [de aquí en adelante, Informe de los expertos en derechos humanos de la ONU]. Los expertos en derechos humanos de la ONU que elaboraron el informe eran relatores especiales sobre la libertad de expresión, la libertad de reunión pacífica y los defensores de la situación de derechos humanos.

47 Consulte el Estado de privacidad en México, 2017 https://www.privacyinternational.org/state-privacy/1006/state-privacy-mexico Entre las tecnologías adquiridas se encontraba el sistema de control remoto de Hacking Team, "Da Vinci", y otras herramientas de malware utilizadas para espiar las redes sociales y los servicios de correo, incluidos Facebook, Twitter y Gmail.

48 Citizen Lab, Agridulce. Defensores de impuestos a refrescos en México son víctimas de vínculos de aprovechamiento de NSO, 11 de febrero de 2017 https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/

49 Nicole Perlroth, New York Times, Usuarios de IPhone deben actualizar software después de encontrarse fallas de seguridad, 25 de agosto de 2016 https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html

50 Citizen Lab, Imprudencia de Redux: legisladores y políticos mexicanos de alto rango víctimas de spyware de NSO, 29 de junio de 2019 https://citizenlab.org/2017/06/more-mexican-nso-targets/

51 R3D, #GobiernoEspía: vigilancia sistemática a periodistas y defensores de derechos humanos en México, 19 de junio de 2017. https://r3d.mx/2017/06/19/gobierno-espia/

estudiantes en Ayotzinapa, un académico que trabajaba contra la corrupción, dos periodistas influyentes y un estadounidense que representaba a víctimas de abuso sexual por parte de la policía.[52]

En el primer caso, estas personas no podrían considerarse objetivos legítimos de vigilancia. Por lo tanto, el Gobierno mexicano que recurrió al hackeo no respetó la legislación internacional en materia de derechos humanos.

Privacy International y R3D publicaron un análisis completo en 2017[53] y destacaron que no parece existir una base legal adecuada para que el Gobierno mexicano realizara actividades de hackeo, incluso para fines legítimos de vigilancia.

En junio de 2017, Privacy International y R3D escribieron al presidente de México para solicitarle transparencia en la problemática y para que clarificara la base legal de las actividades de hackeo. La carta también solicitaba a la procuraduría general que se investigara el alcance de las actividades de hackeo y la investigación con spyware de periodistas, defensores de derechos humanos y activistas.[54]

En diciembre de 2017, la ONU y los Relatores Especiales de la CIDH sobre libertad de expresión solicitaron en conjunto al Gobierno mexicano que llevara a cabo una investigación independiente sobre el uso del spyware y que estableciera un marco legal para proteger a los individuos de la interferencia arbitraria y clandestina en su privacidad.[55] Hasta la fecha, el Gobierno no ha informado en qué condiciones se utilizarían estas técnicas, con qué finalidad, qué entidad las usarían y cuál es la base legal de su implementación.

El análisis adicional de Privacy International y R3D se focalizó en el marco de vigilancia existente y determinó que *"no queda claro si estas actividades incluso respetan los procedimientos y las salvaguardas establecidas en el marco de vigilancia mexicano".*[56] Como hemos visto en ejemplos anteriores, justificar el hackeo para fines de vigilancia mediante marcos de vigilancia existentes no respeta la legislación internacional en materia de derechos humanos porque quebranta el principio de legalidad.

En 2017, la Secretaría del Interior mexicana (SEGOB) respondió a la carta enviada,

52 Azam Ahmed y Nicole Perlroth, El uso de textos como señuelos: spyware del Gobierno espía a periodistas y sus familias, 19 de junio de 2017 https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

53 Informe de Privacy International, Implicancias para los derechos humanos internacionales de las actividades de hackeo por parte del Gobierno mexicano para investigar a periodistas y defensores de derechos humanos, 28 de junio de 2017 https://privacyinternational.org/sites/default/files/2017-12/Briefing%20on%20the%20International%20Human%20Rights%20Implications%20of%20Reported%20Mexican%20Government%20Hacking%20Targeting%20Journalists%20and%20Human%20Rights%20Defenders.pdf

54 https://www.privacyinternational.org/sites/default/files/2017-12/PI-R3D%20Joint%20Letter.pdf

55 Observaciones preliminares del Relator Especial de la ONU sobre la libertad de expresión y el Relator Especial sobre libertad de expresión de la CIDH después de su visita conjunta en México, 27 de noviembre – 4 de diciembre de 2017

56 Informe de Privacy International, Implicancias para los derechos humanos internacionales de las actividades de hackeo por parte del Gobierno mexicano para investigar a periodistas y defensores de derechos humanos, 28 de junio de 2017, página 12.

señalando que que habían organizado encuentros para determinar algunos puntos de acción en respuesta a los diversos informes y análisis. En conformidad con la legislación internacional sobre derechos humanos, las autoridades gubernamentales deben someter sus facultades y actividades de vigilancia a una supervisión independiente. Un cuerpo de supervisión con sede en el Ministerio del Interior no sería un órgano independiente. La octava salvaguarda contra el hackeo aborda la supervisión y la transparencia:

"Las autoridades gubernamentales deben ser transparentes en cuanto al alcance y el uso de sus facultades y actividades de hackeo, y deben someter dichas facultades y actividades a una supervisión independiente. Deben publicar periódicamente, como mínimo, información sobre el número de aplicaciones para autorizar hackeos que hayan sido aprobadas y rechazadas, la identidad de las autoridades gubernamentales que aplicaron, los delitos especificados en las aplicaciones y el método, la extensión y la duración de las medidas de hackeo autorizadas, incluidas las configuraciones específicas de los sistemas objetivo".

Otros organismos han hecho el intento de realizar una supervisión del Gobierno mexicano. El INAI (Instituto Nacional de Transparencia, Acceso a Información y Datos Personales), inició una investigación y, en octubre de 2017, ordenó al Gobierno que presentara los contratos de adquisición de capacidades de hackeo. Sin embargo, el Gobierno ha estado bloqueando y retrasando estos esfuerzos.

Etiopía

El Gobierno de Etiopía tiene un extenso historial en la adquisición de spyware y en su aplicación contra la sociedad civil, tanto en Etiopía como en el extranjero. Citizen Lab ha publicado cinco conjuntos de evidencias desde 2013, que vinculan al Gobierno de Etiopía con el uso indebido de spyware contra actores de la sociedad civil. Las personas investigadas se encontraban en Canadá, EE. UU., Europa y otros países,[57] lo que demuestra tanto el alcance extraterritorial del spyware comercial como la evasión de mecanismos legales, un claro ejemplo de quebrantamiento de las obligaciones legales internacionales.

En 2014, después de leer los informes de Citizen Lab sobre las actividades de espionaje por motivos políticos que el Gobierno de Etiopía había llevado a cabo, Tadesse Kersmo, un activista de Etiopía exiliado en el Reino Unido pensó que su laptop podría haber sido infectada con malware. Tadesse se acercó a Privacy International y junto con investigadores de Citizen Lab, se examinó su laptop. Estaba

57 http://hchr.org.mx/images/doc_pub/ES-final-version-preliminary-observations.pdf
Citizen Lab, Spyware comercial, la industria multimillonaria construida sobre un atolladero ético y legal, 6 de diciembre de 2017 https://citizenlab.ca/2017/12/legal-overview-ethiopian-dissidents-targeted-spyware/; Citizen Lab, Impaciencia cibernética: disidentes de Etiopía víctimas de nuevo spyware comercial, 6 de diciembre de 2017 https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

infectada con el software intrusivo FinSpy,[58] que había estado activo desde junio de 2012, después de que el activista hubiera llegado al Reino Unido.[59]

A nivel nacional, el régimen de vigilancia de Etiopía es amplio e impreciso. Un informe que realizó Human Rights Watch en 2014 sobre la vigilancia en Etiopía descubrió que *"las autoridades encuentran muy pocas barreras, en las leyes y en la práctica, para hacer uso de sus facultades de vigilancia, dada la falta de salvaguardas de privacidad y de supervisión independiente para evitar abusos. A diferencia de las formas tradicionales de vigilancia, la naturaleza a distancia de estas tácticas también permite al Gobierno extender estas actividades perjudiciales más allá de sus límites".*[60]

Si bien Etiopía no ha adecuado a ningún nivel su régimen de vigilancia, y hay mucho por decir al respecto en las salvaguardas contra el hackeo, debido a los casos extraordinarios de hackeo internacional, esta sección se concentra en las implicancias extraterritoriales del hackeo de Etiopía. Como se articula en la novena salvaguarda contra el hackeo:

"Al poner en práctica una medida de hackeo extraterritorial, las autoridades gubernamentales deben cumplir en todo momento con las obligaciones legales internacionales, incluidos los principios de soberanía y no intervención, que expresan restricciones al ejercicio de la jurisdicción extraterritorial. Las autoridades gubernamentales no deben utilizar el hackeo para evadir otros mecanismos legales (como tratados de asistencia legal mutua u otros mecanismos consensuados) con el fin de obtener datos localizados fuera de su territorio. Estos mecanismos deben documentarse claramente, ponerse a disposición del público y estar sujetos a garantías de equidad procedimental y sustantiva".

Los Estados confían tradicionalmente en mecanismos consensuados cuando es necesario ejercer acciones de cumplimiento de leyes en jurisdicciones extraterritoriales. El mecanismo principal es un Tratado de Asistencia Legal Mutua (TALM), un acuerdo bilateral que incluye procedimientos para obtener y proporcionar asistencia en cuestiones penales. Esta salvaguarda se aplica a las medidas de hackeo con consecuencias extraterritoriales, incluidas las medidas que interfieren intencionalmente con un sistema objetivo localizado extraterritorialmente.

En conformidad con lo anterior, Ron Deibert, director de Citizen Lab, como consecuencia de la publicación más reciente de las evidencias, escribió:

58 Una vez descargado en un sistema informático, FinSpy permite al operador del troyano tener acceso total a la computadora. Esto significa que era posible leer los correos electrónicos de Tadesse, incluso los cifrados, buscar documentos en su laptop, monitorear su navegación en Internet, escuchar sus llamadas de Skype con otros miembros del comité ejecutivo de Ginbot 7, seguir sus conversaciones de chat e incluso encender a distancia la cámara web y el micrófono de su computadora para extender la vigilancia más allá del dispositivo e investigar lo que estaba sucediendo en el entorno en la privacidad de la casa de Tadesse.

59 Privacy International, La vigilancia sigue a un refugiado político de Etiopía hasta el Reino Unido, 16 de febrero de 2014 https://privacyinternational.org/blog/1199/surveillance-follows-ethiopian-political-refugee-uk

60 Human Rights Watch (2014) They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia

"Si un Gobierno desea recoger evidencias sobre una persona en otro país, la costumbre es que debe realizar un pedido formal y legal a otros Gobiernos mediante un proceso como el de los Tratados de Asistencia Legal Mutua. Parecería que Etiopía ha omitido todo ese procedimiento. Las normas internacionales sugerirían que los Gobiernos cuyos ciudadanos han sido monitoreados sin autorización realicen una gestión diplomática o "démarche" ante Etiopía, pero eso sucederá de manera imperceptible, si es que sucede".

En 2014, la Electronic Frontier Foundation (EFF) presentó acciones legales en los EE. UU. en representación de un ciudadano estadounidense nacido en Etiopía, conocido como Kidane, cuya laptop también fue infectada con FinSpy. La acusación consistió en que el Gobierno de Etiopía violó la Ley sobre Espionaje Telefónico de EE. UU. La corte desestimó el caso en 2016, lo que, como explica Deibert, *"estableció un precedente problemático".*

Todo esto se suma a una falta de acceso a recursos efectivos, según lo requiere la legislación internacional en materia de derechos humanos y según se articula en la décima salvaguarda de hackeo:

"Las personas que han sido víctimas de actividades de hackeo ilícitas por parte del Gobierno, independientemente de dónde residan, deben tener acceso a recursos efectivos".

El comentario legal continúa diciendo:

"…existen circunstancias en las que una medida de hackeo puede interferir con sistemas que se encuentran fuera de la jurisdicción del Gobierno que implementa la medida. En dichas circunstancias, todas las personas víctimas del hackeo ilícito por parte del Gobierno deben tener acceso a recursos efectivos, independientemente de su localización".

Conclusión

Como lo demuestran muchos de los ejemplos antes mencionados, los Estados de África y América Latina implementan cada vez con mayor frecuencia actividades de hackeo con fines de vigilancia.

No queda claro si estas actividades pueden en alguna instancia realizarse en conformidad con las normas internacionales de derechos humanos. Si los Gobiernos insisten, a pesar de lo anterior, en poner en práctica estas facultades, deben cumplir con una serie de salvaguardas necesarias mínimas (según lo establece la legislación internacional en materia de derechos humanos) que aborden las implicancias que tiene el hackeo en la seguridad.

Los ejemplos citados demuestran, asimismo, que en la mayoría de los casos los Gobiernos no han articulado una base legal clara para sus actividades de hackeo, según lo requiere la normativa internacional de derechos humanos. La aplicación de nuestras salvaguardas contra el hackeo significa, entonces, que los Gobiernos no logran siquiera superar el primer paso porque no cumplen con el principio de legalidad.

Como se afirmó al inicio, esto resulta de máxima importancia porque en el centro del principio de legalidad se encuentra la premisa de que dar "carácter legal a los regímenes intrusivos de vigilancia" los vuelve objeto de "debate público y parlamentario". La legalidad también está estrechamente vinculada con el concepto de "interferencia arbitraria", la idea de que el ejercicio de facultades secretas conlleva el riesgo inherente de ser aplicadas arbitrariamente.[61]

Sin un marco legal claro que rija las actividades de hackeo, todas las actividades de hackeo llevadas a cabo por los Gobiernos violarán normas internacionales de derechos humanos, incluso si existiesen otras salvaguardas, como la de contar con una autorización judicial previamente. Sin embargo, con fines ilustrativos, también hemos citado ejemplos para debatir sobre la aplicación de principios adicionales consagrados en las salvaguardas contra el hackeo.

El presente informe ha demostrado las dificultades relacionadas con el descubrimiento y el cuestionamiento de las actividades de hackeo ilegales que llevan a cabo los Gobiernos. Las salvaguardas contra el hackeo se diseñaron como herramienta para asistir a las organizaciones de la sociedad civil: proporcionan un marco que puede utilizarse como fundamento para los cuestionamientos, además de pasos claros para que los Gobiernos justifiquen sus actividades.

Después de estas revelaciones, todavía no han/hahabido investigaciones o

61 See the legal commentary to the first hacking safeguard on legality https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary#1

revisiones judiciales oficiales, ni tampoco cambios en las leyes de ninguno de estos países. Esperamos que el trabajo continuo de las organizaciones de la sociedad civil cambie el statu quo, y que las salvaguardas contra el hackeo se conviertan en una herramienta que las partes interesadas puedan utilizar al momento de cuestionar el hackeo como método de vigilancia gubernamental.

Privacy International está trabajando para lograr transparencia en las actividades de hackeo de los Gobiernos y para cuestionar su uso mediante investigaciones, la defensa de políticas y litigios. Esto implica:

- Comprender a través de los hechos cómo hackean los Gobiernos y
- Comprender legalmente cómo deberían aplicarse los marcos internacionales de derechos humanos en las actividades de hackeo de los Gobiernos, ejemplificado por las salvaguardas contra el hackeo.

Confiamos en que nuestros socios, los periodistas y otras organizaciones de la sociedad civil denuncien e investiguen los casos de hackeo. También insistimos en que los Gobiernos deben transparentar sus acciones en la materia.

Otras herramientas a nuestra disposición son el uso de solicitudes de acceso a información pública y la presión sobre los organismos de supervisión. Nos entusiasma la idea de asociarnos con otras organizaciones para lograr estos objetivos, y nos complacería trabajar en conjunto en estas solicitudes de acceso, o para pedir respuestas a los organismos de supervisión. También esperamos ayudar a las organizaciones a utilizar y aplicar estas salvaguardas en sus jurisdicciones.

Si desea trabajar con nosotros en este tema, póngase en contacto con la responsable de políticas públicas de Privacy International, Lucy Purdon (lucyp@privacyinternational.org), o la asesora jurídica de Privacy International, Scarlet Kim (scarlet@privacyinternational.org).

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471