PRIVACY INTERNATIONAL

Resumen de Privacy International

Las Implicaciones Internacionales de los Derechos Humanos por los Ataques Intrusivos del Gobierno Mexicano Reportados contra Periodistas y Defensores de los Derechos Humanos

28 de junio 2017

A. Introduccion

El 19 de junio de 2017, Citizen Lab de la Escuela Munk de Asuntos Globales de la Universidad de Toronto, Junto con R3D, SocialTIC y el Article 19 de México publicó los resultados de una investigación que indicaba que las autoridades mexicanas habían utilizado el software espía Pegasus del Grupo NSO contra periodistas y defensores de derechos humanos que exponían la corrupción gubernamental y abusos de los derechos humanos. El Grupo NSO es una compañía de tecnología de vigilancia que vende productos y servicios, incluyendo malware, exclusivamente a clientes gubernamentales. Estos ataques fueron diseñados para comprometer los teléfonos móviles estas personas, lo que permite a los atacantes a subrepticiamente encender cámaras y micrófonos, grabar llamadas, leer mensajes y seguir sus movimientos.

Esta investigación se expande en un informe de Citizen Lab de febrero de 2017, que sugirió que las autoridades mexicanas habían utilizado el software espía Pegasus del Grupo NSO para similarmente atacar a personas involucradas en la campaña de alto perfil de ‘’impuestos sobre soda’’ en México. Este informe, a su vez, siguió un informe de Citizen Lab en agosto de 2016, que indicaba que las autoridades de los Emiratos Árabes Unidos (EAU) habían atacado a un defensor de los derechos humanos que también usaba el software espía de Pegasus.

Tras la publicación del informe del 19 de junio de 2017, las víctimas de la campaña de software espía han pedido una investigación independiente por parte de un equipo internacional de expertos. Además, nueve de las víctimas han presentado una denuncia penal ante la Procuraduría General de la Republica. El 22 de junio de 2017, el presidente Enrique Peña Nieto reconoció que el gobierno mexicano había comprado el software espía Pegasus del Grupo NSO, pero negó su participación en los ataques contra periodistas y defensores de los derechos humanos.

Como se explica en el informe adjunto, hacking por el Gobierno mexicano, incluyendo el uso del programa espía del Grupo NSO, plantea graves preocupaciones sobre los derechos humanos y cuestiona si México cumple con sus obligaciones bajo la ley internacional de derechos humanos. Por lo tanto, instamos a las autoridades mexicanas a cesar inmediatamente todas las actividades de hacking. Apoyamos además los llamados de las víctimas para una investigación independiente y pedimos a la Fiscalía General que lleve a cabo una investigación inmediata, exhaustiva e independiente de la denuncia penal.

Además, Privacy International y R3D hacen las siguientes recomendaciones:

Al Presidente de los Estados Unidos Mexicanos:

- Hacer públicas los ataques intrusivos que las autoridades mexicanas han llevado a cabo hasta la fecha y por qué autoridades, incluyendo el uso del programa espía del Grupo NSO contra periodistas, defensores de derechos humanos y activistas;
- Aclarar la comprensión del gobierno mexicano sobre la base legal de sus de ataques intrusivos y qué reglas y salvaguardias, si las hay, regulan sus ataques intrusivos;

- Confirmar qué tipo de herramientas usadas en los ataques intrusivos, incluyendo malware, son empleadas por las autoridades mexicanas y cómo se regula y monitorea la adquisición y uso de estas tecnologías.

A la Procuraduría General de la Nación, al Congreso General de los Estados Unidos Mexicanos, a la Comisión Nacional de Derechos Humanos, al Mecanismo de Protección para Personas Defensoras de Derechos Humanos y Periodistas y al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales:

- Llevar a cabo investigaciones inmediatas, exhaustivas e independientes sobre:
  - La naturaleza y alcance de los ataques intrusivos por del gobierno, incluyendo si tales ataques son conformes con la ley internacional y nacional;
  - El uso del programa espía del Grupo NSO contra organizaciones de la sociedad civil, activistas de derechos humanos y periodistas, con intenciones de llevar ante la justicia a los autores y proporcionar reparación a las víctimas de estos abusos;
  - Los tipos de herramientas usadas en los ataques intrusivos, incluyendo el malware, empleados por agencias gubernamentales mexicanas, incluyendo si su adquisición y uso son conformes con la ley internacional y nacional.
- Hacer públicos todos los hallazgos relacionados con las investigaciones anteriores.

A todas las agencias mexicanas que están realizando o han llevado a cabo ataques intrusivos:

- Notificar a todos las personas que han sido objeto de ataques intrusivos hasta la fecha, incluyendo la base legal y normas pertinentes, si los hubiere, que rigen dichas actividades;
- Destruir todo el material obtenido a través de sus ataques intrusivos;
- Ofrecer a todos los personas que han sido objeto de sus ataques de intrusivos una vía de reparación.

B. Antecedentes

1. Grupo NSO

El Grupo NSO es una de más de 520 compañías de tecnología de vigilancia identificadas por Privacy International que vende productos y servicios exclusivamente a clientes gubernamentales para fines policiales y de recopilación de información.[1] El Grupo NSO fue fundado en 2010 en Israel. Francisco Partners, un fondo de capital privado con sede en los Estados Unidos posee actualmente una participación de control en la compañía después de comprarla por 120 millones de dólares en 2014.[2]

[1] Privacy International, The Global Surveillance Industry, julio de 2016, disponible en https://www.privacyinternational.org/node/911

[2] Joseph Cox y Lorenzo Franchesci-Bicchierai, Meet NSO Group, el nuevo gran jugador en el negocio de spyware del Gobierno, 25 de agosto de 2016, disponible en https://motherboard.vice.com/en_us/article/nso-group-new-big - jugador-en-gobierno-spyware.

Según un folleto promocional, el Grupo NSO se describe a sí mismo como un "líder en el campo de la guerra cibernética. . . trabajando con organizaciones de seguridad militar y de la nación para realzar sus capacidades tecnológicas en los espacios de la guerra cibernética tanto ofensiva como defensiva."[3] El folleto señala además que Pegasus - el conjunto de programa espía utilizado contra periodistas, defensores de los derechos humanos y activistas en México- es "una poderosa y única herramienta de monitoreo. . . que permite la supervisión remota y sigilosa y la extracción completa de datos desde dispositivos remotos a través de comandos no rastreables.''

2. Ataques documentados que implican al software espía del grupo NSO

a. Defensor de los Derechos Humanos de los Emiratos Árabes Unidos Ahmed Mansoor

En agosto de 2016, Citizen Lab publicó los resultados de una investigación que indicaba que las autoridades de los EAU habían atacado a Ahmed Mansoor, un prominente defensor de los derechos humanos, utilizando el software espía Pegasus del Grupo NSO.[4] El Sr. Mansoor había recibido mensajes de texto sospechosos con enlaces que pretendían contener información sobre la tortura de los ciudadanos de los EAU.[5] Al examinarlo, Citizen Lab descubrió que los enlaces pertenecían a "una infraestructura de explotación conectada al Grupo NSO" y "condujo a una cadena de exploits de día cero (" cero días ") que habría remozado remotamente el iPhone 6 de Mansoor e instalado el sofisticado programa espía." [6] Ese programa espía, si hubiera infectado el teléfono del Sr. Mansoor, habría permitido a las autoridades de los Emiratos Árabes Unidos encender secretamente su cámara y micrófono, registrar sus llamadas, registrar mensajes enviados y recibidos en sus aplicaciones de chat y seguir sus movimientos. Citizen Lab notificó a Apple de sus hallazgos, lo que resultó en el lanzamiento de del parche de Apple iOS 9.3.5, que corrige las vulnerabilidades explotadas por el Grupo NSO como parte del ataque contra el Sr. Mansoor.[7]

El 20 de marzo de 2017, el Sr. Mansoor fue arrestado por las autoridades de los Emiratos Árabes Unidos y actualmente permanece en detención frente a cargos relacionados con la expresión que incluyen el uso de sitios web de medios sociales para "publicar información falsa

[3] Folleto promocional del Grupo NSO, disponible en https://sii.transparencytoolkit.org/docs/NSO-Group_Pegasus_Brochuresii_documents.

[4]Bill Marczak y John Scott-Railton, el Dissidente de Millones de Dólares: Los Días Cero del iPhone del Grupo NSO usados contra un Defensor de los Derechos Humanos de los Emiratos Árabes Unidos, 24 de agosto de 2016, disponible en https://citizenlab.org/2016/08/million-dollar -dissident-iphone-zero-day-nso-group-uae / [en adelante "Million Dollar Disident"]; Vea también Nicole Perlroth, los usuarios del iPhone instados a actualizar el software después de que se detectaron fallas de seguridad, NY Times, 25 de agosto de 2016, disponible en https://www.nytimes.com/2016/08/26/technology/apple-software- Vulnerabilidad-ios-patch.html [en adelante, los usuarios del iPhone instaron]. Citizen Lab fue asistido por un equipo de investigación de Lookout Security.

[5] El Sr. Mansoor ha sido victimar en el pasado con el uso del spyware exclusivo del gobierno. En 2011, fue víctima de FinFisher FinSpy, y en 2012, fue atacado con el sistema de control remoto del equipo de Hacking. Véase Million Dollar Dissident, supra.

[6] *Véase id. Un "día cero" explota una vulnerabilidad desconocida para el fabricante del software o del hardware.*

[7] *Ver Usuarios del iPhone instados, supra.*

que perjudica la unidad nacional".[8] El 28 de marzo de 2017, un grupo de expertos de derechos humanos de las Naciones Unidas pidió al gobierno de los EAU que liberara al Sr. Mansoor inmediatamente, describiendo su detención como "un ataque directo al legítimo trabajo de los defensores de los derechos humanos en los Emiratos Árabes Unidos"[9]. En el 20 de abril de 2017, Una coalición de 20 organizaciones de derechos humanos pidió de manera similar al gobierno de los EAU que liberara a Mansoor inmediatamente, ya que "las acusaciones contra él se relacionan con su trabajo de derechos humanos y sus críticas a las autoridades".[10]

Como parte de su investigación sobre el uso del programa espía del Grupo NSO para atacar al Sr. Mansoor, Citizen Lab también descubrió pruebas de otras personas que pueden haber sido atacadas con el mismo programa espía exclusivo del gobierno. Uno de esos objetivos potenciales fue el periodista mexicano Rafael Cabrera, quien recientemente difundido una historia sobre conflictos de intereses que involucraba al presidente y Primera Dama de México.

b. Investigadores y defensores de la salud pública mexicanas

En febrero de 2017, Citizen Lab publicó los resultados de una investigación que sugirió que las autoridades mexicanas habían utilizado el programa espía Pegasus del Grupo NSO contra las personas involucradas en la campaña de alto perfil sobre "impuesto sobre soda" en México.[11] Estos ataques atacaron al menos a tres individuos: el Dr. Simón Barquera, investigador del Instituto Nacional de Salud Pública (INSP); Alejandro Calvillo, Director de El Poder del Consumidor; y Luis Manuel Encarnación, Coordinador de la Coalición Contra PESO. El Dr. Barquera es un respetado científico que trabaja en política de nutrición y el Sr. Calvillo y el Sr. Encarnación son defensores de la salud pública cuyas respectivas organizaciones se enfocan en la obesidad y consumo de sodas en México. Los tres eran partidarios prominentes del impuesto de soda 2014 de México, que tiene como objetivo reducir el consumo nacional de bebidas que incluyen azúcar añadido.

El informe de Citizen Lab reveló que la infraestructura de explotación de NSO y el software espía descubiertos en su investigación previa de los enlaces enviados al señor Mansoor también se utilizaron para atacar a los señores Barquera, Calvillo y Encarnación. El momento de los enlaces coincidió con el lanzamiento de una campaña de investigadores y organizaciones de

[8] Amnistía Internacional, Emiratos Árabes Unidos: Defensor de los derechos humanos, Ahmed Mansoor, detenido por cargos relacionados con la expresion, 20 de abril de 2017, https://www.amnesty.org/en/documents/mde25/6094/2017/en/.
[9] Office of the U.N. High Commissioner for Human Rights, *UN rights experts urge UAE: "Immediately release Human Rights Defender Ahmed Mansoor*," 28 Mar. 2017, available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21449&LangID=E.
[10] Human Rights Watch, *UAE: Free Prominent Rights Defender*, *Ahmed Mansoor Held on Speech-Related Charges*, 20 Apr. 2017, available at https://www.hrw.org/news/2017/04/20/uae-free-prominent-rights-defender.
[11] John Scott-Railton y otros, Bitter Sweet: Los partidarios del impuesto de soda de México de NSO Exploits, 11 de febrero de 2017, disponible en https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/ [En adelante Sweet amargo]; Vea también Nicole Perlroth, los blancos impares de Spyware: Partidarios del impuesto de la soda de México, NY Times, 11 de febrero de 2017, disponible en https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda- Tax-advocates.html [en adelante Spyware Odd Targets].

salud pública -incluyendo a los doctores Barquera, Calvillo y Encarnación- para duplicar el impuesto a la soda.[12] Al igual que con el ataque anterior al señor Mansoor, estos ataques si tuvieran éxito, habrían comprometido los teléfonos de estos individuos para permitir a los atacantes encender subrepticiamente sus cámaras y micrófonos, registrar sus llamadas, leer sus mensajes y seguir sus movimientos.[13]

c. **Periodistas mexicanos y defensores de los derechos humanos**

El 19 de junio de 2017, Citizen Lab junto con R3D, SocialTIC y Article 19 México publicaron los resultados de una investigación que indicó que las autoridades mexicanas habían utilizado el programa espía Pegasus del Grupo NSO contra periodistas y defensores de derechos humanos. Este informe se amplió en su informe de febrero de 2017 que describe ataques similares dirigidos a los partidarios de la campaña de "impuesto a la gaseosa" de México.

La persona más atacada fue Carmen Aristegui, destacada periodista investigadora y fundadora de Aristegui Noticias, un canal de noticia que ha hecho público numerosas historias importantes sobre escándalos gubernamentales, incluyendo el escándalo de la Casa Blanca en el 2014[14]. La Sra. Aristegui recibió 26 mensajes de texto que contenían enlaces y que aparentemente provenían de diversas fuentes, incluyendo la Embajada de los Estados Unidos en México, AMBER Alerts, su banco y colegas[15]. El hijo de la Sra. Aristegui también recibió por separado más de 21 mensajes, varios también haciéndose pasar por la Embajada de los Estados Unidos o con información relacionada a su madre.

Los ataques atacaron a otros periodistas, entre ellos Sebastián Barragán, periodista que trabaja con Aristegui Noticias; Carlos Loret de Mola, ancla de Televisa; y Salvador Camarena y Daniel Lizárraga, ambos periodistas especializados en investigaciones de anticorrupción (Mexicanos contra la Corrupción y la Impunidad). El Sr. Camarena y el Sr. Lizárraga también han trabajado previamente con Aristegui Noticias[16].
Los ataques también se dirigieron a personas que trabajan en el Centro Miguel Agustín Pro Juárez ("Centro PRODH") e Instituto Mexicano para la Competitividad (IMCO). Centro PRODH es una de las organizaciones de derechos humanos más respetadas de México y representa a las víctimas de abusos de los derechos humanos del gobierno, incluyendo a las familias de 43 estudiantes desaparecidos en la ciudad de Iguala en septiembre de 2014. IMCO es una ONG mexicana cuyo trabajo incluye políticas y promoción de anticorrupción.

---

[12] Vea los objetivos impares de Spyware, supra.
[13] *Véase Bitter Sweet, supra.*
[14] La investigación de Casa Blanca se refería a la construcción de una casa multimillonaria por parte de un contratista gubernamental para la familia del presidente mexicano. Ver Jo Tuckman, el presidente mexicano Enrique Peña Nieto se enfrenta a la protesta sobre la mansión £ 4.4m, The Guardian, 10 Nov. 2014, disponible en https://www.theguardian.com/world/2014/nov/10/mexico-president-enrique -pena-nieto-mansión-explica.
[15] *Véase Reckless Exploit, supra.*
[16] El informe de agosto de 2016 de Citizen Lab sobre el uso del spyware del Grupo NSO para atacar al defensor de los derechos humanos de los Emiratos Árabes Unidos, Ahmed Mansoor, también descubrió evidencia de que Rafael Cabrera, periodista que trabaja con Aristegui Noticias (ahora con BuzzFeed), también pudo ser blanco del spyware. Véase Million Dollar Dissident, supra.

En Centro PRODH, los ataques fueron dirigidos al director Mario Patrón, y a dos abogados, Santiago Aguirre y Stephanie Brewer. En IMCO, fueron dirigidos al director, Juan Pardinas, y a una investigadora, Alexandra Zapata.

El informe de Citizen Lab conecta la infraestructura de explotación NSO y el programa espía descubierto en sus investigaciones anteriores con enlaces enviados a los individuos descritos anteriormente[17]. La sincronización de estos enlaces coincidió con investigaciones de alto perfil sobre la corrupción gubernamental o la comisión de abusos contra los derechos humanos entre enero de 2015 y agosto de 2016. Por ejemplo, los ataques hacia los periodistas de Aristegui Noticias fueron durante el período en el que estaban trabajando en escándalo de la Casa Blanca de 2014. Los ataques dirigidos al Sr. Loret corresponde al período en que informó sobre ejecuciones extrajudiciales en una finca conocida como "Rancho El Sol". Los ataques contra el personal del Centro PRODH coincide con el período justo antes de que la organización se dispusiera a hacer público los hallazgos relacionados con los 43 estudiantes desaparecidos. Al igual que con los intentos previos contra el Sr. Mansoor y los defensores mexicanos del impuesto de refresco, estos ataques fueron diseñados para que los atacantes pudieran acceder a una gama de información almacenada en los teléfonos de las víctimas y para facilitar la vigilancia intrusiva en tiempo real.

C. Las implicaciones que los ataques intrusivos del Gobierno tienen sobre la privacidad

Los ataques intrusivos tienen el potencial de ser mucho más intrusivo que cualquier otra técnica de vigilancia existente, incluyendo la interceptación de las comunicaciones. Estos ataques intrusivos permiten a los gobiernos el acceso remoto a dispositivos y por lo tanto a la información almacenada en esos dispositivos. Para un número creciente de personas, los dispositivos digitales personales contienen la información más privada que almacenan en cualquier lugar, reemplazando y consolidando libretas de direcciones, correspondencia, revistas, archivadores, álbumes de fotos y carteras.

Ataques intrusivos también permiten a los gobiernos controlar la funcionalidad de los sistemas, permitiendo formar nuevas y graves formas de vigilancia en tiempo real. A través de ataques intrusivos, un gobierno puede potencialmente ver algo escrito en un dispositivo, incluyendo detalles de inicio de sesión y contraseñas, historial de navegación y borradores de documentos y comunicaciones que el usuario nunca tuvo la intención de difundir. Estos ataques también permiten a los gobiernos encender en secreto el micrófono de un dispositivo, la cámara web y la tecnología de localización basada en GPS.

A través del control sobre la funcionalidad de los sistemas, los ataques intrusivos pueden incluso permitir que los gobiernos corrompan archivos o recuperen archivos que han sido eliminados. También puede permitirles plantar o eliminar documentos o datos, enviar comunicaciones falsas desde el dispositivo o volver a escribir código para agregar nuevas capacidades y borrar cualquier rastro de la intrusión.

[17] *Véase Reckless Exploit, supra.*

Los ataques documentados que implican al programa espía del Grupo NSO ilustran muchas de estas implicaciones de privacidad. Los ataques contra el doctor Barquera, el señor Calvillo y el señor Encarnación buscaron comprometer sus teléfonos móviles personales. Si hubieran tenido éxito, sus teléfonos se habrían convertido en dispositivos de vigilancia total, fotografiando sus alrededores, grabando sus conversaciones y llamadas, accediendo a sus mensajes y correo electrónico, y el seguimiento de sus movimientos. Al acceder a esta información, las autoridades mexicanas podrían haber elaborado un perfil detallado de la vida de cada uno de estos individuos, revelando su identidad, pensamientos, relaciones, intereses y actividades.

D. Las Implicaciones en la Seguridad por los ataques intrusivos del gobierno

Hackeo es un intento de entender un sistema mejor de lo que se entiende el mismo, y luego empujarlo para que haga lo que el hacker quiere. Hackeo puede por lo tanto ayudarnos a entender mejor los sistemas que son esenciales a nuestras vidas, y cada vez más mientras que gobiernan nuestras vidas. Hackeo también puede ayudarnos a entender mejor cómo las personas usan los sistemas y cómo pueden ser manipulados para debilitar o subvertir la seguridad de sus propios sistemas.

Por otro lado, los ataques intrusivos del gobierno para facilitar la vigilancia se basan fundamentalmente en la inseguridad para interferir con el derecho a la privacidad. Tiene el potencial de socavar la seguridad no sólo del dispositivo objetivo sino también de otros sistemas no relacionados, e incluso de Internet en su conjunto. A medida que nos basamos cada vez más en Internet y conectamos más de nuestra infraestructura al Internet, este riesgo aumenta.

Cuando el gobierno explota las vulnerabilidades de seguridad para la vigilancia, esas vulnerabilidades también pueden ser explotadas por otros, en particular si las vulnerabilidades (y exploits) no se informan a los proveedores y no son reparados, y si las vulnerabilidades se conocen. La vulnerabilidad de seguridad utilizada por el gobierno no sólo puede ser posteriormente explotada contra el propio dispositivo, sino también contra otros usuarios del mismo tipo de dispositivo. Por ejemplo, al investigar el ataque contra el Sr. Mansoor, Citizen Lab descubrió que el Grupo NSO utilizaba una cadena de explotaciones de día cero (es decir, hazañas desconocidas para Apple, el fabricante del iPhone del señor Mansoor), lo que ponía en peligro a todos los usuarios de IPhone. Como resultado de la investigación, Apple lanzó un parche para todos los usuarios de iPhone y, de hecho, el informe de Citizen Lab alentó "a los propietarios de iPhone a actualizar a la última versión de iOS (9.3.5) de inmediato."[18]

Los poderes de hackeo por parte del gobierno también suponen riesgos de seguridad de seguimiento: cuando un gobierno implementa malware, no siempre será capaz de controlar completamente su distribución. En un ataque de ingeniería social, como los ataques

[18] Véase Million Dollar Dissident, supra.

documentados contra víctimas mexicanas que usan el programa espía del Grupo NSO, los enlaces infectados con malware se envían directamente a los objetivos. Dichos enlaces pueden, por ejemplo, ser enviados a otros o publicarse en las redes sociales, poniendo en riesgo los dispositivos de aquellos individuos que involuntariamente hacen clic en esos enlaces.

E. Análisis de los Derechos Humanos Internacionales por Ataques Intrusivos del Gobierno Mexicano

Debido a que los ataques intrusivos implican una amplia e intrínseca interferencia con la privacidad y plantea riesgos significativos para la seguridad de dispositivos y redes, Privacy International se pregunta si los ataques intrusivos pueden ser un componente legítimo de la vigilancia estatal. Dada la privacidad y la seguridad de los ataques intrusivos, los gobiernos nunca podrán demostrar su compatibilidad con la ley internacional de los derechos humanos, en particular su necesidad y proporcionalidad como instrumento de vigilancia. Por esa razón, el Relator Especial de la ONU para la Libertad de Expresión ha observado:

> "Los programas de intrusión ofensiva como los troyanos o las capacidades de interceptación masiva constituyen desafíos tan graves a las nociones tradicionales de vigilancia que no pueden conciliarse con las leyes vigentes sobre vigilancia y acceso a la información privada. Estos no solo son nuevos métodos para llevar a cabo vigilancia; Son nuevas formas de vigilancia. Desde el punto de vista de los derechos humanos, el uso de tales tecnologías es extremadamente inquietante."[19]

A continuación, Privacy International aborda con más detalle cómo los ataques intrusivos gubernamentales en México viola específicamente las obligaciones internacionales de México en materia de derechos humanos, en particular el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y el artículo 11 de la Convención Americana sobre Derechos Humanos, que han sido ratificados por México.

1. Ataques intrusivos del Gobierno Mexicano No Están De Conformidad Con la Ley

a. El Principio de Legalidad

[19] Informe de la Relatora Especial de la ONU para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, Doc. U.N. A / HRC / 23/40, párr. 62, 17 de abril de 2013, disponible en http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf [en adelante Informe 2013 del Relator Especial de las Naciones Unidas sobre la Libertad de Expresión]. Informe del Relator Especial de la ONU sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, UN Doc. A / HRC / 23/40, párr. 62, 17 de abril de 2013, disponible en http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf [en adelante Informe 2013 del Relator Especial de las Naciones Unidas sobre la Libertad de Expresión].

La ley internacional de los derechos humanos dispone que cualquier interferencia con en el derecho a la intimidad debe ser conforme a la ley.[20] En el centro del principio de legalidad se encuentra la importante premisa que establece que el uso de "regímenes de vigilancia intrusivos sobre una base estatutaria" los somete al "debate público y parlamentario."[21]. La legalidad también está estrechamente vinculado al concepto de "interferencia arbitraria", la idea es que el ejercicio de un poder secreto conlleva el riesgo inherente de su aplicación arbitraria. [22]

El significado de la "ley" implica ciertos requisitos cualitativos mínimos de accesibilidad y previsibilidad. El Comité de Derechos Humanos de la ONU ha elaborado el significado de la "ley" por los propósitos del artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, que protege el derecho a la libertad de opinión y de expresión de la siguiente manera:

> "La norma, que debe caracterizarse como una" ley ", debe ser formulada con suficiente precisión para permitir a una persona regular su conducta en consecuencia y debe ser accesible al público. . . . Las leyes deben proporcionar suficiente orientación a los encargados de su ejecución para que puedan determinar qué tipos de expresión están debidamente restringidas y cuales no lo están."[23]

---

[20]Véase el Artículo 17 (1), PIDCP ("Nadie será objeto de interferencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ..."); Artículo 11, CEDH ("2. Nadie podrá ser objeto de una injerencia arbitraria o abusiva en su vida privada, en su familia, en su domicilio o en su correspondencia ... 3. Toda persona tiene derecho a la protección de la ley contra Tal interferencia ... "); Artículo 8, apartado 2, del Convenio Europeo para la Protección de los Derechos Humanos ("CEDH") ("No habrá injerencia de una autoridad pública en el ejercicio del [derecho al respeto de la vida privada y familiar] la Ley . . . ."); Véase también el Comité de Derechos Humanos de la ONU, Observación general Nº 16 (Artículo 17 PIDCP), 8 de abril de 1988, párr. 3, disponible en http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1_Global/INT_CCPR_GEC_6624_E.doc [en adelante, Observación general Nº 16] (observando que "el término" ilícito "significa que no La injerencia puede tener lugar salvo en los casos previstos por la ley "y que" [e] nterferencia autorizada por los Estados sólo puede tener lugar sobre la base de la ley, que debe cumplir las disposiciones, objetivos y objetivos del Pacto "); Principio 1, Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones ("Principios Necesarios y Proporcionados"), disponible en https://necessaryandproportionate.org/principles. Los Principios Necesarios y Proporcionados aplican el derecho internacional de los derechos humanos a la vigilancia digital moderna. Fueron redactados en 2013 por una coalición internacional de expertos de la sociedad civil, privacidad y tecnología y han sido respaldados por más de 600 organizaciones de todo el mundo.

[21]Informe del Relator Especial sobre la Promoción y Protección de los Derechos Humanos y de las Libertades Fundamentales de la Organización de las Naciones Unidas para la Lucha contra el Terrorismo (U.N. Doc. A / HRC / 34/61, párr. 36 (21 de febrero de 2017), disponible en http://www.ohchr.org/Documents/Issues/Terrorism/A-HRC-34-61.pdf [en adelante 2017 Informe del Relator Especial sobre la Lucha contra el Terrorismo].

[22] Malone c. Reino Unido, Tribunal Europeo de Derechos Humanos, App. Nº 8691/79, 2 de agosto de 1984, párr. 67 ("Especialmente cuando un poder del ejecutivo se ejerce en secreto, los riesgos de la arbitrariedad son evidentes."); Véase también la Observación general Nº 16, supra, párr. 4 (observando que "la expresión" interferencia arbitraria "puede extenderse también a la interferencia prevista por la ley" y que "la introducción del concepto de arbitrariedad tiene por objeto garantizar que incluso la interferencia prevista por la ley debe ser conforme Con las disposiciones, los objetivos y los objetivos del Pacto y debería ser, en cualquier caso, razonable en las circunstancias particulares ").

[23] Comité de Derechos Humanos de los Estados Unidos, Observación general Nº 34 (Artículo 19 PIDCP), 12 de septiembre de 2011, párr. 25, disponible en http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf [en adelante, Observación General No. 34].

> La Comisión Interamericana de Derechos Humanos ("CIDH") ha determinado de manera similar, en su interpretación del artículo 11 de la CADH:
>
> "El párrafo 2 del artículo 11 prohíbe específicamente la interferencia 'arbitraria o abusiva' con el derecho [a la intimidad]. Esta disposición indica que, además de la condición de legalidad, que siempre debe observarse cuando se impone una restricción a los derechos de la Convención, el Estado tiene una obligación especial de prevenir las interferencias "arbitrarias o abusivas". La noción de "interferencia arbitraria" se refiere a elementos de injusticia, imprevisibilidad e irracionabilidad. . . ."[24]

Los requisitos de accesibilidad y previsibilidad también se reflejan en la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH):

> "En primer lugar, la ley debe ser adecuadamente accesible: el ciudadano debe poder tener una indicación adecuada en las circunstancias de las normas jurídicas aplicables a un caso determinado. En segundo lugar, una norma no puede considerarse una ley a menos que se formule con suficiente precisión para que el ciudadano pueda regular su conducta; Debe poder -si es necesario con un asesoramiento adecuado- prever, en un grado que sea razonable en las circunstancias, las consecuencias que una acción determinada puede acarrear."[25]

La Asamblea General de las Naciones Unidas ha reconocido la aplicación del principio de legalidad al contexto de vigilancia, resolviendo que la "vigilancia de las comunicaciones digitales debe ser consistente con las obligaciones internacionales de derechos humanos y debe llevarse a cabo sobre la base de un marco legal que debe ser públicamente accesible, claro, preciso, amplio y no discriminatorio."[26]

Tanto la Corte Interamericana de Derechos Humanos (TIDH) como el TEDH han aplicado explícitamente el principio de legalidad al contexto de la vigilancia. En Escher et al. V. Brasil, la Corte IDH sostuvo que las medidas de vigilancia "deben basarse en una ley que debe ser precisa."[27]La Corte observó además que la ley debe "indicar las normas claras y correspondientes, tales como las circunstancias en que se puede adoptar esta medida de [vigilancia], las personas autorizadas a solicitarla, ordenarla y llevarla a cabo,". Del mismo modo, en el caso Weber & Saravia c. Alemania, el TEDH se refirió a las "salvaguardias

[24] Sra. X y Y c. Argentina, Comisión Interamericana de Derechos Humanos, Caso 10.506, Informe No. 38/96, 15 de octubre de 1996.
[25] Sunday Times contra Reino Unido, Tribunal Europeo de Derechos Humanos, App. Nº 6538/74, 26 de abril de 1979, párr. 49.
[26]Resolución de la Asamblea General de las Naciones Unidas sobre el derecho a la intimidad en la era digital, U.N.Doc.A/RES/71/199,25deenerode2017,disponibleenhttp://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199 [en adelante Resolución de la Asamblea General de las Naciones Unidas] .
[27]Escher et al. Brasil, Corte Interamericana de Derechos Humanos, Caso 12.353, 2 de marzo de 2006, párr. 131.

mínimas que deberían establecerse en el derecho estatutario para evitar abusos de poder" cuando el Estado lleva a cabo la vigilancia:

> "[1] la naturaleza de los delitos que pueden dar lugar a una orden de [] [vigilancia]; [2] una definición de las categorías de personas sujetas a [vigilancia]; [3] un límite en la duración de la [vigilancia]; [4] el procedimiento a seguir para examinar, utilizar y almacenar los datos obtenidos; [5] las precauciones que deben tomarse al comunicar los datos a otras partes; Y [6] las circunstancias en las que las grabaciones pueden o deben ser borradas o las cintas destruidas."[28]

En 2013, los Relatores Especiales de la ONU y de la Organización de Estados Americanos sobre Libertad de Expresión emitieron una Declaración Conjunta sobre Vigilancia en la que destacaron la aplicación del principio de legalidad en el contexto de la vigilancia:

> "Los Estados deben garantizar que la intercepción, recopilación y uso de la información personal, incluidas todas las limitaciones del derecho de la persona afectada a acceder a esta información, estén claramente autorizadas por la ley a fin de protegerlos de la interferencia arbitraria o abusiva con sus intereses privados. La ley debe establecer límites con respecto a la naturaleza, alcance y duración de este tipo de medidas; Las razones para ordenarlas; Las autoridades con facultades para autorizarlas, ejecutarlas y supervisarlas; Y los mecanismos legales por los cuales pueden ser impugnados."[29]

b. Ataques Intrusivos del Gobierno Mexicano no Están de Conformidad con La Ley

Los ataques intrusivos llevadas a cabo por las autoridades mexicanas, incluido el uso de programa espía del Grupo NSO, violan el principio de legalidad. Los ataques intrusivos del gobierno mexicano carecen de base legal bajo el marco de vigilancia vigente en México. Además, no está claro si estas actividades se ajustan a los procedimientos y salvaguardas establecidos en el marco mexicano de vigilancia.

El marco mexicano de vigilancia consiste en una serie de leyes constitucionales y estatutarias. De conformidad con el artículo 16 de la Constitución mexicana:

---

[28] Weber & Saravia c. Alemania, Tribunal Europeo de Derechos Humanos, App. Nº 54934/00, de 29 de junio de 2006, párr. 95; Véase también Malone, supra, párr. 67 (señalando que "la ley debe ser suficientemente clara en sus términos para dar a los ciudadanos una indicación adecuada de las circunstancias y condiciones en que las autoridades públicas están facultadas para recurrir a esta secreta y potencialmente peligrosa interferencia con el derecho al respeto de Vida privada y correspondencia ").

[29] Relator Especial de las Naciones Unidas para la Protección y Promoción del Derecho a la Libertad de Opinión y Expresión y Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión 2013, párr. 8, disponible en http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

"Las comunicaciones privadas no serán violadas. La ley sancionará cualquier acción contra la libertad y privacidad de tales comunicaciones, excepto cuando sean voluntariamente dadas por uno de los individuos involucrados en ellas. Un juez evaluará las implicaciones de tales comunicaciones, siempre que contengan información relacionada con la perpetración de un delito. Las comunicaciones que violen la confidencialidad establecida por la ley no serán admitidas en ningún caso.

Sólo la autoridad judicial federal podrá autorizar la interceptación de comunicaciones privadas a solicitud de la autoridad federal competente o del Ministerio Público del Estado. La autoridad que la solicite deberá presentar por escrito las causas legales de la solicitud, describiendo en ella el tipo de interceptación requerida, los individuos sujetos a intercepción y el término de los mismos. La autoridad judicial federal no puede autorizar el uso telefónico ni la interceptación de comunicaciones en los siguientes casos: a) cuando los casos sean de carácter electoral, fiscal, comercial, civil, laboral o administrativo; b) comunicaciones entre el acusado y su abogado.

. . .

El acceso telefónico autorizado y la interceptación de comunicaciones estarán sujetos a los requisitos y limitaciones establecidos en la ley. Los resultados de la escucha telefónica y la interceptación de comunicaciones que no cumplan con los requisitos antes mencionados no serán admitidos como evidencia ".

Por lo tanto, la Constitución establece ciertas salvaguardias antes de la interceptación de comunicaciones, incluyendo la limitación de dicha vigilancia a ciertas autoridades federales; exigiendo a dichas autoridades que establezcan el fundamento jurídico de la solicitud y articulen el tipo de intercepción, los temas y la duración de la vigilancia; Y la autorización judicial federal.

Además de la Constitución, diversas leyes federales mexicanas rigen las actividades de vigilancia del gobierno.[30] En virtud de estos estatutos, se permite a tres autoridades interceptar comunicaciones: 1) la Fiscalía General de la República ("PGR"), encargada de investigar los delitos y supervisar los fiscales de cada una de las 32 entidades federales; (2) la Policía Federal; Y (3) el Centro de Investigaciones y Seguridad Nacional ("CISEN"). De conformidad con el Código de Procedimiento Penal Federal, se puede conceder a la PGR

[30] Para una discusión detallada de los estatutos aplicables, vea Luis Fernando García, Vigilancia de las Comunicaciones del Estado y la Protección de los Derechos Fundamentales en México, disponible en https://necessaryandproportionate.org/country-reports/mexico#footnote3_1906uo2 [en adelante, Vigilancia Estatal de las Comunicaciones en México] Y Privacy International & R3D, Estado de Privacidad México, 14 de marzo de 2017, disponible en https://www.privacyinternational.org/node/972 [en adelante, Estado de Privacidad México] .Para un análisis detallado de los estatutos aplicables, Luis Fernando García, Vigilancia de las Comunicaciones Estatales y Protección de los Derechos Fundamentales en México, disponible en https://necessaryandproportionate.org/country-reports/mexico#footnote3_1906uo2 [en adelante, Vigilancia de las Comunicaciones Estatales en México] y Privacy International & R3D, Estado de Privacidad México, 14 de marzo de 2017, disponible en https://www.privacyinternational.org/node/972 [en adelante, Estado de Privacidad México].

autorización judicial para interceptar comunicaciones "cuando haya pruebas suficientes que confirmen la probable responsabilidad en la comisión de un delito grave."[31] La Ley de la Policía Federal dispone que la Policía Federal podrá recibir autorización judicial para interceptar comunicaciones "cuando haya pruebas suficientes que demuestren la organización de" una lista específica de delitos.[32] Por último, la Ley de Seguridad Nacional dispone que la CISEN podrá recibir autorización judicial para interceptar comunicaciones en casos de "amenaza inminente a la seguridad nacional", que se define como una serie de categorías de actos.[33] Los ataques intrusivos del gobierno mexicano carece de base legal bajo el marco vigente de vigilancia mexicana, lo que viola el principio de legalidad. El marco mexicano de vigilancia rige la interceptación de las comunicaciones. Como se mencionó anteriormente, Los ataques intrusivos tiene el potencial de ser mucho más intrusivo que la interceptación de las comunicaciones y también plantea problemas de seguridad únicos y convincentes. Por lo tanto, un marco que rija la interceptación de las comunicaciones no puede abordar la naturaleza de la interferencia con la privacidad planteada por ataques intrusivos. Por lo tanto, cualquier interferencia con la privacidad a través de los ataques intrusivos debe, por sí mismo, cumplir con el principio de legalidad.[34]

Además, no está claro si los ataques intrusivos del gobierno mexicano aún se ajustan a los procedimientos y salvaguardas establecidos en el marco mexicano de vigilancia. Primero, como se discutió anteriormente, sólo se permite a tres autoridades gubernamentales interceptar comunicaciones bajo el marco mexicano de vigilancia. Sin embargo, en julio de 2015, la divulgación de documentos internos de otra empresa de vigilancia, la empresa italiana Hacking Team, reveló la venta de programas espías a por lo menos 14 estados mexicanos y agencias gubernamentales, incluidas las no autorizadas para realizar interceptaciones de comunicaciones conforme al Marco mexicano de vigilancia.[35] Al igual que Grupo NSO, Hacking Team es una empresa de tecnología de vigilancia que pretende vender su tecnología de vigilancia exclusivamente a clientes del gobierno. En respuesta a las revelaciones sobre Hacking Team, el Relator Especial para la Libertad de Expresión de la CIDH señaló explícitamente:

---

[31] *Véase Vigilancia de las comunicaciones estatales en México, supra; Estado de Privacidad, supra.*
[32] *Véase Vigilancia de las comunicaciones estatales en México, supra; Estado de Privacidad, supra..*
[33] *Véase Vigilancia de las comunicaciones estatales en México, supra; Estado de Privacidad, supra.*
[34]El principio de legalidad exige que cualquier interferencia con la privacidad "tenga lugar sobre la base de la ley, la cual debe cumplir con las disposiciones, objetivos y objetivos del PIDCP". Comentario General Nº 16, supra, párr. 3; Véase también 2017 Informe del Relator Especial sobre la Lucha contra el Terrorismo, supra, párr. 36 ("La legislación primaria disponible públicamente no basta, por sí sola, para garantizar la compatibilidad de esos regímenes con el derecho internacional de los derechos humanos. Debe tenerse también en cuenta la necesidad, la proporcionalidad y la no discriminación, así como el establecimiento de salvaguardias Contra la arbitrariedad, la supervisión independiente y las vías de reparación ")..
[35]Ver Mattathias Schwartz, Cyberware para la venta, N.Y. Times, 4 de enero de 2017, disponible en https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html; Arturo Ángel, Sedena negoció compra de software a Hacking Team en 2015 para espiar a 600 personas, Animal Político, 21 de julio de 2015, disponible en http://www.animalpolitico.com/2015/07/sedena-negocio-compra-de- Software-a-hacking-equipo-en-2015-para-espiar-a-600-personas /; Arturo Ángel, México, el principal cliente de una empresa que vende software para espiar, Animal Político, 7 de julio de 2015, disponible en http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por- Venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente /. Estas revelaciones también revelaron que México era el cliente más grande del equipo de Hacking.

> "El programa de vigilancia comercializado por [Hacking Team] está diseñado para. . . Permitir [] la recolección de información, mensajes, llamadas y correos electrónicos, voz sobre IP y comunicación de chat desde dispositivos cotidianos. Este software también puede activar de forma remota micrófonos y cámaras. . .. [Esta] Oficina ha declarado que la vigilancia de las comunicaciones y la injerencia en la intimidad que excede lo estipulado por la ley, orientadas a fines distintos de los que la ley permite o se llevan a cabo clandestinamente, deben ser severamente castigados. Tales interferencias ilegítimas incluyen acciones tomadas por razones políticas contra periodistas y medios independientes."[36]

Dadas las similitudes entre el Grupo NSO y Hacking Team, así como entre sus productos espías, parece razonable cuestionar si las entidades gubernamentales mexicanas no autorizadas para llevar a cabo actividades de vigilancia estaban detrás de la compra y uso del programa espía del Grupo NSO en cuestión en los recientes ataques contra periodistas, defensores de los derechos humanos y activistas.

Además, el marco mexicano de vigilancia requiere que la interceptación de comunicaciones sea autorizada por una autoridad judicial federal. La sociedad civil mexicana ha expresado escepticismo de que los ataques anteriores contra los defensores mexicanos del "impuesto al refresco" fueron autorizados judicialmente [37]. Ex funcionarios de inteligencia mexicanos también han expresado dudas de que las autoridades del gobierno mexicano solicitaron autorización judicial para los más recientes ataques contra periodistas y defensores de derechos humanos[38]. (Y, en cualquier caso, el marco mexicano de vigilancia no provee base legal para los ataques intrusivos que pudiera ser autorizada judicialmente). Ese escepticismo debe trasladarse a los ataques más recientemente reportados, los cuales comparten muchas de las mismas características de los ataques contra los defensores del "impuesto al refresco". Este escepticismo se justifica teniendo en cuenta los perfiles de las víctimas de estos ataques. El marco mexicano de vigilancia limita la interceptación de comunicaciones a circunstancias que involucran delincuencia y seguridad nacional. Ninguna de las víctimas parece haber sido atacada para tales fines.

2. Ataques intrusivos por el gobierno mexicano no son ni necesarios ni proporcionales

[36]Oficina del Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Preocupación por la Adquisición y Ejecución de Programas de Vigilancia por los Estados del Hemisferio, Comunicado de Prensa R80 / 15, 21 de julio de 2015.

[37] Vea Spyware's odd targets, supra.

[38] "Las agencias de seguridad mexicanas no pedirían una orden judicial, porque saben que no conseguirían una", dijo Eduardo Guerrero, ex analista del Centro de Investigación y Seguridad Nacional, agencia de inteligencia de México Y una de las agencias gubernamentales que usan el spyware de Pegasus "Quiero decir, ¿cómo podría un juez autorizar la vigilancia de alguien dedicado a la protección de los derechos humanos?" Allí, por supuesto, no hay base para esa intervención, pero eso es además El punto ", agregó." Nadie en México nunca pide permiso para hacerlo ".

a. Necesidad y Proporcionalidad

La ley internacional de los derechos humanos exige que toda injerencia en el derecho a la intimidad no sólo sea conforme con la ley, sino que también sea necesaria y proporcionada[39]. El principio de necesidad "implica que las restricciones no deben ser simplemente útiles, razonables o deseables para lograr un objeto gubernamental legítimo", sino que "un Estado debe demostrar de manera" específica e individualizada la naturaleza precisa de la amenaza que pretender abordar y "una conexión directa e inmediata entre la expresión y la amenaza"[40]. Este concepto de necesidad también se expresa a veces como exigiendo que cualquier interferencia con el derecho a la privacidad sea "necesaria para alcanzar un objetivo legítimo."[41]

El Relator Especial de la CIDH para la Libertad de Expresión ha aplicado el principio de necesidad al contexto de la vigilancia, señalando que "para que un programa de vigilancia de comunicaciones en línea sea apropiado, los Estados deben demostrar que las limitaciones al derecho a la privacidad y a la libertad de expresión de esos programas son estrictamente

[39] Véase Comité de Derechos Humanos de la Unión de Estados Unidos, Toonen c. Australia, Comm. Nº 488/1992, Doc. U.N.
CCPR / C / 50 / D / 488/1992 (31 de marzo de 1994), párr. 8.3 ("Toda interferencia con la privacidad debe ser proporcional al fin buscado y ser necesaria en las circunstancias de cualquier caso"); Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El Derecho a la Privacidad en la Era Digital, Documento de la U.N. A / HRC / 27/37 (30 de junio de 2014), párr. 23, disponible en https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/088/54/PDF/G1408854.pdf?OpenElement [en adelante, Informe 2014 del ACNUDH] ("Estas fuentes autorizadas [HRC Los comentarios generales 16, 27, 29, 31 y 34 y los Principios de Siracusa] señalan los principios generales de legalidad, necesidad y proporcionalidad ... "); Resolución del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital U.N.
Doc. A / HRC / 34/7, 23 de marzo de 2017, párr. 2 disponible en https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement ("Recordando que los Estados deben asegurar que cualquier interferencia con El derecho a la intimidad es compatible con los principios de legalidad, necesidad y proporcionalidad ").

[40] Breve de Amici Curiae, U.N. Expertos en Derechos Humanos en Apoyo al Demandante-Apelante y Reversión, John Doe (Kidane) v. La República Democrática Federal de Etiopía, D.C. Ct. App., No. 16 - 7081, pág. 14 (1 de noviembre de 2016), disponible en https://www.eff.org/files/2016/11/01/11.1.16_united_nations_human_rights_experts_amicus_brief.pdf (citando la Observación general Nº 34, supra, pág. Expertos en Derechos Humanos de la ONU]. Los expertos en derechos humanos de la ONU que redactaron el informe fueron los Relatores Especiales de la ONU para la Libertad de Expresión, la Libertad de Asamblea Pacífica y la Situación de los Defensores de Derechos Humanos

[41] El artículo 30 de la CADH prevé que las restricciones de los derechos reconocidos por la Convención "no pueden aplicarse salvo con arreglo a las leyes promulgadas por razones de interés general y de conformidad con el fin para el que se han establecido esas restricciones". En el sentido de que "no debe haber injerencia de una autoridad pública en el ejercicio del derecho a la intimidad", salvo en los casos en que sea conforme a la ley y sea necesaria en una sociedad democrática en interés de la seguridad nacional, La seguridad pública o el bienestar económico del país, la prevención del desorden o la delincuencia, la protección de la salud o la moral o la protección de los derechos y libertades de terceros ". Véase también 2014 Informe del ACNUDH, supra, párr.. 23 ("La limitación debe ser necesaria para alcanzar un objetivo legítimo ... La responsabilidad recae sobre las autoridades que pretenden limitar el derecho a demostrar que la limitación está relacionada con un objetivo legítimo"); Principio 2, Necesidad y Principios Proporcionados ("Las Leyes sólo deben permitir la Vigilancia de las Comunicaciones por parte de las autoridades estatales especificadas para alcanzar un objetivo legítimo que corresponda a un interés legal predominantemente importante que es necesario en una sociedad democrática.").

necesarios en una sociedad democrática para lograr los objetivos que persiguen."[42] Además, el Relator Especial observó que "es insuficiente para que la medida sea" útil "," razonable "o" oportuna "." El Estado debe establecer claramente "la verdadera y convincente necesidad de imponer la limitación. "

El TEDH también ha tenido ocasión de aplicar el principio de necesidad a las interferencias con el artículo 8 en el contexto de la vigilancia. En el caso Szabó & Vissy c. Hungría, el Tribunal Europeo de Derechos Humanos indicó que, dado el "potencial de las tecnologías de vigilancia de vanguardia para invadir la privacidad de los ciudadanos", el requisito del "objetivo legítimo" debía interpretarse estrictamente de la siguiente manera:

"Una medida de vigilancia secreta sólo puede considerarse conforme a la Convención si es estrictamente necesario, como consideración general, para la salvaguardia de las instituciones democráticas y, además, si es estrictamente necesario, como una consideración particular, para la obtención de inteligencia vital en una operación individual. En opinión del Tribunal, cualquier medida de vigilancia secreta que no responda a estos criterios será propensa a abusos por parte de las autoridades con tecnologías formidables a su disposición. La Corte observa que tanto el Tribunal de Justicia de la Unión Europea como el Relator Especial de las Naciones Unidas requieren medidas secretas de vigilancia para responder a la estricta necesidad, un enfoque que considera conveniente aprobar."[43]

El principio de proporcionalidad exige que la injerencia en la privacidad sea "proporcional al objetivo, y la opción menos intrusiva disponible."[44] El Relator Especial de la ONU para la Lucha contra el Terrorismo ha proporcionado orientación adicional a los Estados para demostrar la proporcionalidad en el contexto de la vigilancia. Sostuvo que "la proporcionalidad implica equilibrar el alcance de la intrusión en los derechos de privacidad de Internet contra el beneficio específico que se deriva de las investigaciones emprendidas por una autoridad pública de interés público."[45] También ha indicado que "en el contexto de la vigilancia encubierta. . . [L] a proporcionalidad de cualquier interferencia con el derecho a

[42]Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Libertad de Expresión e Internet, 31 de diciembre de 2013, párr.. 159-60, disponible en http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf [en adelante Informe 2013 del Relator Especial de la CIDH].
[43]Szabó & Vissy c. Hungría, App. Nº 37138/14, 12 de enero de 2016, párr. 73.
[44]2014 Informe del ACNUDH, supra, párr. 23; Véase también el Comité de Derechos Humanos de la ONU, Toonen c. Australia, supra, párr. 8.3 .; Informe del Relator Especial de la ONU sobre la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, A / HRC / 13/37, 28 de diciembre de 2009, párr. 49, disponible en http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf ("[P] rotecciones [del derecho a la privacidad] requieren que los Estados tengan Agotar las técnicas menos intrusivas antes de recurrir a otros ... Los Estados deben incorporar este principio en las políticas existentes y futuras, ya que presentan cómo sus políticas son necesarias y, a su vez, proporcionadas "); (Señalando que la proporcionalidad requiere que "las restricciones sean [...] las menos intrusivas entre aquellas que podrían lograr su función protectora [...] [y] proporcionadas al interés que se debe tener" protegido"); Principio 5, Necesidad y Principios Proporcionados.
[45]Informe del Relator Especial sobre la Promoción y Protección de los Derechos Humanos y de las Libertades Fundamentales de la Organización de las Naciones Unidas para la Lucha contra el Terrorismo (U.N. Doc. A / 69/397, párr. 51 (23 de septiembre de 2014).

la intimidad. . . Ser juzgados en las circunstancias particulares del caso individual ". Sin embargo, enfatizó que" en ningún caso las restricciones pueden ser aplicadas o invocadas de manera que perjudiquen la esencia de un derecho del Pacto ". La Oficina del Alto Comisionado de las Naciones Unidas para Derechos Humanos ha observado de manera similar que "toda limitación al derecho a la intimidad no debe hacer que la esencia del derecho carezca de sentido y debe ser compatible con otros derechos humanos."[46]

El Relator Especial de la CIDH para la Libertad de Expresión también ha influido en el análisis de proporcionalidad en el contexto de la vigilancia, indicando que "para definir si una medida es proporcional, su impacto en la capacidad de Internet para garantizar y promover la libertad de expresión debe ser evaluado."[47] El Relator Especial también instó a que "[l] a importancia del ejercicio de estos derechos en un sistema democrático, la ley autorice el acceso a los datos personales y las comunicaciones únicamente en las circunstancias más excepcionales definidas por la ley". El Relator Especial observo:

> "Cuando se invocan motivos razonablemente abiertos como la seguridad nacional como motivo para controlar los datos personales y la correspondencia. . . [Su] solicitud debe ser autorizada únicamente cuando exista un riesgo definido para los intereses protegidos y cuando ese daño sea mayor que el interés general de la sociedad en mantener el derecho a la intimidad y la libre expresión del pensamiento y la circulación de la información."

b. Ataques intrusivos por el gobierno mexicano no son ni necesarios ni proporcionales

Los ataques intrusivos por parte de las autoridades mexicanas no son ni necesarios ni proporcionales. Los ataques documentados contra los periodistas, defensores de los derechos humanos y activistas, no son necesarios porque no persiguen un objetivo legítimo.

Como medida crucial, las autoridades mexicanas no han hecho ninguna justificación pública sobre la vigilancia hacia estos defensores. Ninguna de estas personas parece ser objetivos legítimos conforme al marco mexicano de vigilancia, que limita la interceptación de comunicaciones a circunstancias que involucran delincuencia y seguridad nacional. De hecho, las autoridades mexicanas parecen haber atacado a estas víctimas por razones prohibidas por la ley internacional de los derechos humanos. Bajo la ley internacional de los derechos humanos, "el amordazamiento de cualquier defensa de la democracia multipartidista, los principios democráticos y los derechos humanos" nunca es un objetivo legítimo; De hecho, socava la participación y el debate públicos en una cuestión que va en

[46]2014 informe del ACNUDH, supra, párr. 23; Véase también Zakharov c. Rusia, Tribunal Europeo de Derechos Humanos, App. Nº 47143/06, 4 de diciembre de 2015, párr. (Observando que existía "el riesgo de que un sistema de vigilancia secreta creado para proteger la seguridad nacional pueda socavar o incluso destruir la democracia bajo el manto de defenderla".).
[47] 2013 Informe del Relator Especial de la CIDH, supra, párrs. 161-62.

contra del artículo 19 (ACNUDH) y del objeto y los propósitos del Pacto."[48] Por lo tanto, las autoridades mexicanas no pueden justificar los ataques intrusivos como necesario en busca de un objetivo legítimo cuando atacan a periodistas, defensores de los derechos humanos y activistas por su labor de promoción pública y derechos humanos.

Dado que las autoridades mexicanas no pueden justificar sus actividades de hacking como necesario, el análisis de su proporcionalidad es discutible. La evaluación de la proporcionalidad equilibra el alcance de la injerencia en la intimidad contra el objetivo legítimo buscado por el Estado. Por lo tanto, un requisito previo para la evaluación de la proporcionalidad es un objetivo legítimo, que aquí carece.

Sin embargo, Privacy International aprovecha esta oportunidad para enfatizar que la extensa interferencia con la privacidad planteada por ataques intrusivos, así como los riesgos que estos representan para la seguridad de nuestros dispositivos, sugiere que esta actividad puede ser inherentemente desproporcionada. Si las autoridades mexicanas continúan insistiendo en ataques intrusivos para fines de vigilancia, tiene la difícil carga de demostrar cómo estas actividades pueden conciliarse con la ley internacional de los derechos humanos y, en particular, con el requisito de proporcionalidad.

3. El Marco de Vigilancia Mexicano Existente carece de Salvaguardias Adecuadas

Privacidad Internacional también aprovecha esta oportunidad para observar con preocupación que el actual marco de vigilancia de México -incluso cuando se aplica a la interceptación de comunicaciones- carece de ciertas salvaguardas importantes para asegurar su cumplimiento con la legislación internacional de derechos humanos [49]. Si bien está fuera del alcance de esta

[48]Resumen de los Expertos en Derechos Humanos de la U.N., supra, p. 15 (citando la Observación general Nº 34, supra, párrafo 23).

[49] Observación general Nº 16, supra, párr. 10; Véase también Uzun contra Alemania, Tribunal Europeo de Derechos Humanos, App. Nº 35623/05, 2 de septiembre de 2010, párr. 63 ("En el contexto de medidas secretas de vigilancia por parte de las autoridades públicas, debido a la falta de control público y al riesgo de abuso de poder, la compatibilidad con el estado de derecho exige que el derecho interno proteja adecuadamente la injerencia arbitraria Derechos del artículo 8. La Corte debe estar convencida de que existen garantías adecuadas y efectivas contra los abusos, que dependen de todas las circunstancias del caso, como la naturaleza, el alcance y la duración de las posibles medidas, los motivos necesarios para ordenarlas, Las autoridades competentes para permitirlas, llevarlas a cabo y supervisarlas, así como el tipo de recurso previsto por la legislación nacional. ").

carta para elaborar cada una de estas salvaguardias, éstas incluyen, entre otras cosas, la notificación a objetivos de vigilancia [50], supervisión efectiva[51] y requisitos de transparencia.[52]

El actual marco mexicano de vigilancia carece de cada una de estas importantes salvaguardias. No requiere que las autoridades mexicanas notifiquen a los sujetos a los que se dirige la vigilancia. No prevé mecanismos de supervisión independientes que permitan un examen después de la vigilancia. Tampoco establece requisitos de información sobre transparencia. Privacy International por lo tanto insta a México a establecer estas salvaguardias para que su actual marco de vigilancia sea compatible con la ley internacional de los derechos humanos.

F. Conclusion

Por las razones expuestas anteriormente, ataques intrusivos por parte del gobierno mexicano, incluyendo el uso del programa espía del Grupo NSO, plantea graves preocupaciones sobre los derechos humanos y cuestiona si México cumple con sus obligaciones bajo la ley internacional de derechos humanos. Privacy International, por lo tanto, insta a las autoridades mexicanas a cesar inmediatamente todos los ataques intrusivos. Apoyamos además los

[50] Véase la Observación general Nº 16, supra, párr. 10 ("Para tener la protección más eficaz de su vida privada, cada individuo debe tener el derecho de averiguar de forma inteligible si, y en caso afirmativo, qué datos personales se almacenan en los archivos de datos automáticos y con qué fines. Cada individuo también debe poder determinar qué autoridades públicas o particulares controlan o pueden controlar sus archivos. "); U.N. Comité de Derechos Humanos, Observaciones finales sobre el tercer informe periódico de la ex República Yugoslava de Macedonia, Doc. CCPR / C / MKD / CO / 3, 17 de agosto de 2015, párr. 23 ("[El Estado Parte debería] velar por que las personas que sean objeto de un control ilícito estén sistemáticamente informadas y tengan acceso a recursos adecuados"); 2013 Informe de la Relatora Especial de la ONU sobre Libertad de Expresión, supra, párr. 82 ("Los individuos deben tener el derecho legal de ser notificados de que han sido sometidos a vigilancia de comunicaciones o de que sus datos de comunicaciones han sido alcanzados por el Estado." Reconociendo que la notificación anticipada o simultánea podría poner en peligro la efectividad de la vigilancia, Notificado una vez que se haya completado la vigilancia. ").

[51] Véase Resolución de la Asamblea General de las Naciones Unidas, supra, párr. D) Establecer o mantener mecanismos de supervisión interna independientes, eficaces, dotados de recursos adecuados e imparciales, judiciales, administrativos y / o parlamentarios, capaces de asegurar la transparencia, según proceda, y la rendición de cuentas por parte de los Estados
Vigilancia estatal de las comunicaciones, su interceptación y la recogida de datos personales. . . . "); Comité de Derechos Humanos, Observaciones Finales sobre el Sexto Informe Periódico del Canadá, Doc. UIT-R CCPR / C / CAN / CO / 6, 13 de agosto de 2015, párr. (El Comité también está preocupado por la falta de mecanismos de supervisión adecuados y eficaces para examinar las actividades de los organismos de seguridad y de inteligencia y la falta de recursos y poder de los mecanismos existentes para vigilar esas actividades ... El Estado Parte debería [...] D) Establecer mecanismos de supervisión de los organismos de seguridad y de inteligencia que sean eficaces y adecuados y dotarles de los poderes apropiados y de los recursos suficientes para cumplir su mandato. "); 2013 Informe de la Relatora Especial de la ONU sobre Libertad de Expresión, supra, párr. 93 ("Los Estados deben establecer mecanismos independientes de supervisión capaces de garantizar la transparencia y la rendición de cuentas de la vigilancia estatal de las comunicaciones").

[52] Véase Informe de 2013 de la Relatora Especial de la ONU sobre Libertad de Expresión, supra, párr. 91 ("Los Estados deben ser totalmente transparentes sobre el uso y el alcance de las técnicas y facultades de vigilancia de las comunicaciones, deberían publicar, como mínimo, información sobre el número de solicitudes aprobadas y rechazadas, una desagregación de las solicitudes por propósito."); 2013 Informe del Relator Especial de la CIDH, supra, párrs. 168 ("Los Estados deben divulgar información general sobre el número de solicitudes de interceptación y vigilancia que hayan sido aprobadas y rechazadas y que incluyan tanta información como sea posible, por ejemplo, un desglose de las solicitudes por parte del proveedor de servicios, el tipo de investigación, Período cubierto por las investigaciones, etc. ").

llamados de las víctimas para una investigación independiente y pedimos a la Fiscalía General de la Nación que lleve a cabo una investigación rápida, completa y creíble de la denuncia penal.

Además, Privacy International y R3D hacen las siguientes recomendaciones:

Al presidente de los Estados Unidos Mexicanos:

- Hacer públicas los ataques intrusivos que las autoridades mexicanas han llevado a cabo hasta la fecha y por qué autoridades, incluyendo el uso del programa espía del Grupo NSO contra periodistas, defensores de derechos humanos y activistas;
- Aclarar la comprensión del gobierno mexicano sobre la base legal de sus de ataques intrusivos y qué reglas y salvaguardias, si las hay, regulan sus ataques intrusivos;
- Confirmar qué tipo de herramientas usadas en los ataques intrusivos, incluyendo malware, son empleadas por las autoridades mexicanas y cómo se regula y monitorea la adquisición y uso de estas tecnologías.

A la Procuraduría General de la Nación, al Congreso General de los Estados Unidos Mexicanos, a la Comisión Nacional de Derechos Humanos, al Mecanismo de Protección para Personas Defensoras de Derechos Humanos y Periodistas y al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales:

- Llevar a cabo investigaciones inmediatas, exhaustivas e independientes sobre:
    - La naturaleza y alcance de los ataques intrusivos por del gobierno, incluyendo si tales ataques son conformes con la ley internacional y nacional;
    - El uso del programa espía del Grupo NSO contra organizaciones de la sociedad civil, activistas de derechos humanos y periodistas, con intenciones de llevar ante la justicia a los autores y proporcionar reparación a las víctimas de estos abusos;
    - Los tipos de herramientas usadas en los ataques intrusivos, incluyendo el malware, empleados por agencias gubernamentales mexicanas, incluyendo si su adquisición y uso son conformes con la ley internacional y nacional.
- Hacer públicos todos los hallazgos relacionados con las investigaciones anteriores.

A todas las agencias mexicanas que están realizando o han llevado a cabo ataques intrusivos:

- Notificar a todos las personas que han sido objeto de ataques intrusivos hasta la fecha, incluyendo la base legal y normas pertinentes, si los hubiere, que rigen dichas actividades;
- Destruir todo el material obtenido a través de sus ataques intrusivos;
- Ofrecer a todos los personas que han sido objeto de sus ataques de intrusivos una vía de reparación.

Le agradecemos su atención en este asunto y esperamos una pronta respuesta.