NO MÁS VIGILANCIA DIGITAL SELECTIVA CONTRA LAS PERSONAS QUE DEFIENDEN NUESTROS DERECHOS

RESUMEN DEL IMPACTO DEL SECTOR DE LA VIGILANCIA DIGITAL SOBRE LOS DEFENSORES Y DEFENSORAS DE LOS DERECHOS HUMANOS

Amnistía Internacional es un movimiento global de más de

AMNISTÍA INTERNACIONAL

7 millones de personas que trabajan en favor del respeto y la protección de los derechos humanos.

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

Somos independientes de todo gobierno, ideología política, interés económico y credo religioso. Nuestro trabajo se financia principalmente con las contribuciones de nuestra membresía y con donativos.

Publicado por primera vez en 2019
por Amnesty International Ltd.

Peter Benenson House, 1 Easton Street

London WC1X 0DW, Reino Unido

Índice: ACT 30/1385/2019
Idioma original: inglés

amnesty.org

Foto de portada: *© Getty Images*

AMNISTÍA INTERNACIONAL

ÍNDICE

GLOSARIO

PALABRA	DESCRIPCIÓN
VIGILANCIA DIGITAL MASIVA	Práctica que consiste en someter a vigilancia o seguimiento, por medios digitales, a toda una población o a una parte considerable de ésta. Normalmente esto se hace vigilando las comunicaciones electrónicas, instalando cámaras digitales, empleando tecnología de reconocimiento facial, recopilando información con ayuda de bases de datos biométricos o incluso utilizando drones, entre otros muchos métodos. En general, son los gobiernos quienes llevan a cabo esta vigilancia, pero también pueden hacerlo empresas privadas, ya sea por encargo de los gobiernos o por voluntad propia.
VIGILANCIA DIGITAL SELECTIVA	A diferencia de la práctica anterior, ésta consiste en someter a vigilancia o espiar con tecnología digital a determinadas personas u organizaciones que pueden revestir interés para las autoridades. La vigilancia digital selectiva puede llevarse a cabo instalando programas maliciosos o programas espía que afectan a los dispositivos o atacando a las comunicaciones digitales mediante campañas de fraude por Internet (*phishing*), entre otras tácticas.
PHISHING	Forma de ciberataque que consiste en crear y distribuir páginas falsas de conexión a servicios legítimos (como Gmail o Facebook) para obtener los nombres de usuario y contraseñas de las víctimas, con las que, normalmente, se entra en contacto mediante el envío de enlaces falsos.
PROGRAMA MALICIOSO	Los programas maliciosos (*malware*) se diseñan para ser instalados en secreto en el ordenador o el teléfono de la víctima, a fin de acceder a su información privada o perpetrar fraudes de otro tipo, dañar servicios o causar trastornos.
PROGRAMA ESPÍA	Los programas espía (*spyware*) son un tipo concreto de programa malicioso concebido para espiar el ordenador o el teléfono de la víctima, vigilar constantemente sus comunicaciones y robar su información y archivos privados.
DEFENSOR O DEFENSORA DE LOS DERECHOS HUMANOS	Persona que, individual o colectivamente, actúa para defender o promover los derechos humanos a nivel local, nacional, regional o internacional, sin incitar al odio, la discriminación ni la violencia ni emplear ninguna de esas tácticas.

1. RESUMEN DE LA VIGILANCIA DIGITAL SELECTIVA

> **“Los conflictos y el miedo se usan cada vez más en todo el mundo para diseminar la violencia y las divisiones, y silenciar a la sociedad civil. Algunos países le están dando la espalda a la solidaridad y la justicia. Incluso hay líderes que se enorgullecen de las violaciones de los derechos humanos y declaran la guerra abierta a cualquiera que se atreva a defender la justicia. El movimiento de los defensores y defensoras de derechos humanos se enfrenta ahora a un nuevo nivel de persecución y represión.”**
>
> Cumbre Mundial de Defensores y Defensoras de Derechos Humanos , 2018[1].

Entre las tácticas y herramientas represivas que se utilizan contra los defensores y defensoras de derechos humanos, casi con total impunidad, podemos citar las agresiones personales —como las amenazas—, las campañas de desprestigio, la criminalización, las palizas, los homicidios y las desapariciones forzadas. Además, los Estados han aplicado, por ley o en la práctica, toda una batería de restricciones a los derechos de reunión pacífica y asociación, expresión y libertad de circulación.

Los defensores y defensoras de derechos humanos que sufren desigualdad, exclusión y discriminación —como las mujeres, las personas LGBTI, migrantes o de raza negra y las

[1] Véase la página web de la Cumbre Mundial de Defensores y Defensoras de Derechos Humanos 2018 en https://hrdworldsummit.org/la-cumbre/?lang=es/#context.

comunidades indígenas— corren doble peligro, ya que son atacados no sólo por su lucha, sino también por su propia identidad. Los ataques en su contra se llevan a cabo siguiendo métodos concretos, tienen impactos específicos —como la violencia de género— y, con frecuencia, se ven agravados por las desigualdades estructurales y por la exclusión sistemática de las víctimas del poder y del acceso a los recursos.[2]

Estas tácticas inhiben la capacidad de los defensores y defensoras de disentir, denunciar violaciones y hacer campaña en favor de cambios. Cada vez es más frecuente que unos Estados copien las técnicas de otros e importen herramientas y tecnología para poner en marcha estrategias de control y represión.

Una táctica que ocupa un lugar destacado en los manuales de los gobiernos de todo el mundo es la de la vigilancia, ya sea por medios digitales o de otro tipo. A lo largo de los últimos años, la vigilancia digital se ha visto favorecida por el cada vez más frecuente empleo de tecnología para labores policiales y de aplicación de la ley. En nombre de la lucha antiterrorista o del mantenimiento del orden, los gobiernos utilizan diversas tácticas de vigilancia que invaden la intimidad de personas de todo el mundo. Esta vigilancia digital puede ser tanto masiva como selectiva. En el caso de la primera, se suelen controlar las comunicaciones electrónicas, o bien recurrir a circuitos cerrados de televisión, al empleo de tecnología de reconocimiento facial, a la recopilación de información por medio de bases de datos biométricos o incluso a drones, entre otras muchas tácticas. Según informes, la vigilancia digital masiva ha sido practicada por países como **China,**[3] **Estados Unidos**[4] y **Reino Unido**[5].

Por su parte, la vigilancia digital selectiva implica el uso de tecnologías que permiten centrarse en personas concretas, por ejemplo, escuchas telefónicas o tecnología digital. Asimismo, puede llevarse a cabo instalando programas maliciosos y programas espía que afectan a los dispositivos, o interfiriendo en las comunicaciones digitales mediante campañas de *phishing*, entre otras tácticas. Por ejemplo, en **Reino Unido** se tiene constancia de que la policía ha sometido a vigilancia digital a periodistas,[6] mientras que en **Emiratos Árabes Unidos** el gobierno ha utilizado, al parecer, programas espía para vigilar a activistas[7], en **Colombia** la policía nacional ha sometido a periodistas radiofónicos a vigilancia digital (según la información difundida)[8] y en **Etiopía** el gobierno anterior utilizó

---

[2] Véanse los siguientes informes de Amnistía Internacional: *Defensores y defensoras de los derechos humanos bajo amenaza: La reducción del espacio para la sociedad civil* (índice: ACT 30/6011/2017); *Ataques letales pero prevenibles: Asesinatos y desapariciones forzadas de quienes defienden los derechos humanos* (Índice: ACT 30/7270/2019); *Leyes concebidas para silenciar: Ataque mundial a las organizaciones de la sociedad civil* (Índice: ACT 30/9647/2019) y *Desafiar al poder, combatir la discriminación: Llamada a la acción para reconocer y proteger a las defensoras de los derechos humanos* (Índice: ACT 30/1139/2019).

[3] Véase Amnistía Internacional, *Encryption: A Matter of Human Rights* (Índice: POL 40/3682/2016); y Amnistía Internacional Reino Unido, *Campaigners win vital battle against UK mass surveillance at European Court of Human Rights*, www.amnesty.org.uk/press-releases/campaigners-win-vital-battle-against-uk-mass-surveillance-european-court-human y *The UK government has been spying on Amnesty – so we're going to court*, www.amnesty.org.uk/blogs/ether/uk-government-spying-amnesty-mass-surveillance-court.

[4] En esta página web encontrarán información sobre los distintos programas de vigilancia masiva de China: www.hrw.org/tag/mass-surveillance-china

[5] Amnistía Internacional, *Encryption: A Matter of Human Rights* (Índice: POL 40/3682/2016).

[6] Dominic Ponsford, "Surveillance court says Met grabs of Sun reports' call records 'not compatible' with human rights law", 17 de diciembre de 2015, www.pressgazette.co.uk/surveillance-court-says-met-was-right-grab-sun-journalists-call-records-hunt-plebgate-sources/.

[7] Citizen Lab, "The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[8] Comité para la Protección de los Periodistas, "Denuncias sobre espionaje policial a dos periodistas reavivan temores en Colombia", 2016, https://cpj.org/es/2016/02/denuncias-sobre-espionaje-policial-a-dos-periodist.php.

vigilancia electrónica para espiar a activistas de oposición tanto dentro como fuera del país.[9]

Con la llegada y difusión generalizada de tecnología más sofisticada, unida a la aprobación de leyes que restringen la libertad de expresión en Internet e invaden la privacidad online, la amenaza de la vigilancia digital selectiva ha pasado a ser aún más acuciante. Países como **Tailandia**[10] y **Bangladesh**[11] han aprobado leyes que tienen por objeto ampliar el campo de aplicación de la vigilancia electrónica y conceder a los gobiernos facultades para espiar las comunicaciones electrónicas.

Últimamente, los gobiernos han dado un paso de especial trascendencia, al contratar los servicios del sector privado de la vigilancia digital para desarrollar tecnología que les permiten someter a vigilancia digital a personas concretas. Así, están utilizando indebidamente esas herramientas para atacar de manera ilegítima a activistas, a quienes someten a vigilancia. Las empresas activas en este mercado se han convertido en agentes peligrosos, responsables de la creación de herramientas de represión y del agravamiento de las amenazas dirigidas contra las personas que defienden los derechos humanos.

Lo que se sabe de este sector es poco, ya que opera en la sombra, pese a las reiteradas peticiones de transparencia. Al no estar sometidas a una sólida supervisión reguladora y jurídica, estas empresas pueden vender sin problemas su tecnología a países en los que no se protegen ni respetan los derechos humanos, que, a su vez, la utilizan para vigilar y controlar a quienes defienden los derechos humanos.

[9] Amnistía Internacional, *Encryption: A Matter of Human Rights* (Índice: POL 40/3682/2016).
[10] Tech Crunch, "Thailand passes controversial cybersecurity law that could enable government surveillance", 28 de febrero de 2019, https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/ ; y
Reuters, "Thailand defends cybersecurity law amid concerns over rights abuse", 1 de marzo de 2019, **WWW.REUTERS.COM/ARTICLE/US-THAILAND-CYBER/THAILAND-DEFENDS-CYBERSECURITY-LAW-AMID-CONCERNS-OVER-RIGHTS-ABUSE-IDUSKCN1QI4KA**.
[11] Amnistía Internacional Bangladesh: "New Digital Security Act is attack on freedom of expression", noviembre de 2018, www.amnesty.org/en/latest/news/2018/11/bangladesh-muzzling-dissent-online/.

2. LA VIGILANCIA DIGITAL SELECTIVA Y LA REDUCCIÓN DEL ESPACIO PARA LA DISIDENCIA

El hecho de atacar a defensores y defensoras de derechos humanos por su trabajo, utilizando tecnología de vigilancia digital es, sin duda alguna, contrario al derecho internacional de los derechos humanos. Esta vigilancia ilegal viola el derecho a la privacidad y vulnera los derechos a la libertad de expresión, opinión, asociación y reunión, protegidos por la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos. Este último consagra el derecho de todas las personas a no ser molestadas a causa de sus opiniones[12] y las protege de injerencias arbitrarias e ilegítimas en su privacidad.[13] Asimismo, según el derecho y las normas internacionales, toda injerencia del Estado en el derecho a la privacidad debe ajustarse a la ley y ser necesaria, proporcional y legítima. Además, si los derechos de una persona son violados, el Estado debe garantizar a la víctima el acceso a un recurso efectivo.[14]

A menudo, los defensores y defensoras de derechos humanos no tienen ninguna forma de demostrar que están siendo vigilados, ya sea por obstáculos técnicos o porque la vigilancia es encubierta.[15] Sin embargo, aunque no se pueda demostrar un ataque o una infección

[12] Artículo 19, Pacto Internacional de Derechos Civiles y Políticos.
[13] Artículo 17, Pacto Internacional de Derechos Civiles y Políticos.
[14] Artículo 2.3, Pacto Internacional de Derechos Civiles y Políticos.
[15] Amnistía Internacional, *Defensores y defensoras de los derechos humanos bajo amenaza: La reducción del espacio para la sociedad civil (*Índice: ACT 30/6011/2017).

activa,[16] el mero hecho de vivir constantemente con la amenaza de una *posible* vigilancia puede constituir, en sí mismo, una violación de derechos humanos.[17]

Al margen de que la tentativa de vigilancia tenga o no éxito, los ataques contra activistas de derechos humanos tienen un efecto amedrentador e inhibe su capacidad de seguir trabajando sin interferencias indebidas.[18] En muchos casos, hacen que quienes defienden los derechos humanos se autocensuren y se abstengan de ejercer sus derechos a la libertad de expresión, de asociación y de reunión pacífica. A esto se suma la necesidad de hacer frente a insidiosos procesos judiciales —basados en información extraída, indebidamente utilizada y manipulada— en los que los defensores y defensoras se ven obligados a concentrar sus energías y recursos.[19] Además, la amenaza de vigilancia puede ser perjudicial para su salud mental, y la información obtenida puede utilizarse para difundir públicamente datos que los exponen a ataques personales y campañas difamatorias. Todo esto tiene un perverso efecto dominó sobre las comunidades y sociedades por cuyos derechos luchan.

Por ejemplo, en **Azerbaiyán**, los y las activistas de derechos humanos que se ven obligados a dejar sus hogares ante el temor constante de sufrir ataques, tienen dificultades para comunicarse con los seres queridos que quedan allí y, por tanto, viven con la preocupación de que ellos también puedan sufrir ataques.[20] En **Uzbekistán**, las personas que abandonan sus hogares tras haber sufrido ciberataques siguen siendo víctimas de campañas de vigilancia digital.[21] En términos prácticos, esto significa que los defensores y defensoras de derechos humanos viven en un estado de temor y alerta constantes, y con la sensación de peligro inminente dondequiera que vayan. La vigilancia es un medio extremadamente eficaz de disuadir de disentir y denunciar violaciones a quienes defienden los derechos humanos.[22]

[16] Por "ataque" entiéndase el intento de someter a alguien a vigilancia. Puede consistir en el envío, con o sin éxito, de enlaces maliciosos con programas espía, o en cualquier otra acción. Cuando el ataque es efectivo, los dispositivos de la persona en cuestión pueden verse infectados y, por tanto, pasar a ser vulnerables.

[17] Amnistía Internacional, *A Dangerous Alliance: Governments Collaborate with Surveillance Companies to Shrink the Space for Human Rights Work,* (blog, 16 de agosto de 2019).

[18] Centro de Justicia Global de la Facultad de Derechos de la Universidad de Nueva York, *Attempted digital surveillance as a completed human rights violation: Why targeting human rights defenders infringes on rights. Submission to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 1 de marzo de 2019, https://chrgj.org/wp-content/uploads/2019/05/190301-GJC-Submission-on-Surveillance-Software.pdf.

[19] Véase Amnistía Internacional *Leyes concebidas para silenciar: Ataque mundial a las organizaciones de la sociedad civil* (Índice: ACT 30/9647/2019).

[20] Amnistía Internacional, "False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan", (blog, 9 de marzo de 2017).

[21] Amnistía Internacional, "*We Will Find You Anywhere" -The Global Shadow of Uzbekistani Surveillance* (Índice: EUR 62/5974/2017).

[22] Amnistía Internacional, *Defensores y defensoras de los derechos humanos bajo amenaza: La reducción del espacio para la sociedad civil* (Índice: ACT 30/6011/2017).

3. CASO PRÁCTICO: CIBERATAQUES CONTRA LA DEFENSORA PAQUISTANÍ DE DERECHOS HUMANOS DIEP SAEEDA

> **"Ahora, cada vez que abro un correo electrónico tengo miedo. La situación es tan grave que no puedo hacer bien mi trabajo; mi labor social se está resintiendo."**
>
> Diep Saeeda[23]

En 2018, la conocida defensora paquistaní de derechos humanos Diep Saeeda estaba inmersa en una campaña para pedir responsabilidades por la desaparición forzada de otro defensor paquistaní, Raza Khan. En ese momento, fue víctima de una serie de ciberataques concertados: desde una cuenta de Facebook, y utilizando Facebook Messenger, se puso en contacto con ella en repetidas ocasiones una persona que, tras afirmar ser una mujer de nacionalidad afgana, llamada Sana Halimi y residente en Dubái, donde trabajaba para la ONU, le comunicó que tenía información sobre Raza Khan. A continuación, le envió enlaces a archivos que contenían un programa malicioso llamado StealthAgent y que, de haber sido

[23] Amnistía Internacional, *Pakistan: Human Rights Under Surveillance* (Índice: ASA 33/8366/2018).

abiertos, habrían infectado sus dispositivos móviles. Asimismo, usando este perfil —que, a juicio de Amnistía Internacional, era falso— engañaron a Diep para que facilitara su dirección de correo electrónico, donde empezó a recibir mensajes infectados con un programa espía de Windows comúnmente conocido como "Crimson RAT".

Además, Diep Saeeda recibió mensajes de correo electrónico, remitidos supuestamente por personal del Ministro Principal de la provincia de Punyab, que contenían datos falsos sobre una supuesta reunión que iba a celebrarse, a la que asistirían la delegación provincial del Ministerio de Educación y la propia organización de Diep, el Instituto para la Paz y de Estudios Seculares. En otros casos, los atacantes fingieron ser estudiantes que buscaban orientación. Amnistía Internacional pudo también comprobar que otros defensores y defensoras de Pakistán eran víctimas de ataques parecidos.

El ciberataque dificultó la labor de Diep Saeeda, que empezó a vivir con temor y a desconfiar de los mensajes de correo y archivos adjuntos que le enviaban, incluso los de sus familiares, ante la posibilidad de que alguien pudiera haber suplantado su identidad.

4. EL SECTOR DE LA VIGILANCIA DIGITAL PRIVADA

Varios gobiernos compran herramientas de vigilancia digital —y, en particular, programas espías— a empresas privadas de vigilancia. A continuación, estas herramientas se utilizan para seguir, controlar e intimidar a defensores y defensoras de derechos humanos o a otras personas con opiniones divergentes. Tanto los gobiernos como las empresas comercializadoras afirman que esta tecnología se utiliza sólo para fines legítimos, como vigilar y controlar a terroristas y delincuentes. Sin embargo, cada vez más abundantes pruebas de su uso indebido contradicen esa afirmación. Ciertas organizaciones de la sociedad civil, entre las que se cuenta Amnistía Internacional, han sacado a la luz campañas contra defensores y defensoras de derechos humanos en las que se utilizaba tecnología de muchas de estas empresas privadas de vigilancia.

Los propios gobiernos llevan ya tiempo creando programas espía, pero los programas de empresas privadas son relativamente nuevos e igualmente invasivos y sofisticados.[24] Varios son los agentes clave de este opaco y rentabilísimo sector, entre ellos NSO Group (en **Israel** y **Luxemburgo**[25])y Finfisher (en **Reino Unido** y **Alemania**[26]).

Según Citizen Lab, una sola de esas empresas, NSO Group, parece haber estado detrás de los ataques selectivos de vigilancia perpetrados en, al menos, 45 países.[27] En junio de 2018, una persona que trabajaba para Amnistía Internacional recibió un mensaje malicioso por WhatsApp, supuestamente con información sobre **Arabia Saudí**, en el que se incluían unos enlaces que instalaban programas espías fabricados por NSO Group.[28] Muchos de los países

[24] Just Security, "CTRL+HALT+Defeat: State-sponsored Surveillance and the suppression of Dissent", por Julie Bloch, Sukti Dhital, Rashmika Nedungadi y Nikki Reisch, 15 de mayo de 2019, www.justsecurity.org/64095/ctrlhaltdefeat-state-sponsored-surveillance-and-the-suppression-of-dissent/.
[25] Centro de Información sobre Empresas y Derechos Humanos, "Amnesty backs legal action against Israel firm NSO group over spyware used against human rights defenders", mayo de 2019, www.business-humanrights.org/en/amnesty-backs-legal-action-against-israeli-firm-nso-group-over-spyware-use-against-human-rights-defenders.
[26] Amnistía Internacional, "New tool for spy victims to detect government surveillance" (noticia, 20 de noviembre de 2014).
[27] Citizen Lab, "HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries", septiembre de 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.
[28] Amnistía Internacional, "Amnesty International among targets of NSO-powered campaign", 1 de agosto de 2018, www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/.

que han conseguido comprar a estas empresas tecnología de vigilancia tienen pésimos historiales de derechos humanos. Por ejemplo, el software de NSO Group ha sido utilizado para atacar a defensores y defensoras de los derechos humanos en **Arabia Saudí,**[29] **Emiratos Árabes Unidos, Marruecos y México.**[30]

De conformidad con los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos, las empresas —incluida NSO Group— tienen la responsabilidad de garantizar un sólido proceso de diligencia debida a fin de prevenir el empleo de sus productos para cometer cualquier violación de los derechos humanos y mitigar y reparar dichos abusos.[31] Además, los Estados tienen la responsabilidad de proteger a su población frente a entidades privadas que violen los derechos humanos, al margen de que dichas violaciones ocurran dentro o fuera de sus fronteras.

En el caso de estas empresas, envueltas en secretismo, la rendición de cuentas reviste dificultades especiales. Con mucha frecuencia, se escudan en "razones de seguridad" o "cláusulas de confidencialidad" para impedir que la información sobre sus actividades sea de dominio público. Tampoco se sabe mucho de las empresas en sí y de sus estructuras empresariales. Muchas de ellas no revelan datos sobre licencias de exportación ni tienen ninguna disposición sobre diligencia debida en materia de derechos humanos y reparación de abusos o, si las tienen, son completamente deficientes. Esto, unido a la falta de supervisión reguladora y al escaso rigor de las normas para la concesión de licencias de exportación, tanto nacionales como internacionales, complica la tarea de enfrentarse al sector.

Por ejemplo, ciertos instrumentos, como el Arreglo de Wassenaar —acuerdo multilateral sobre controles de exportación— han sido concebidos para armonizar las normas de exportación de los Estados Partes con respecto a artículos militares y de doble uso y a las tecnologías necesarias para las actividades militares.[32] Sin embargo, aunque el acuerdo pueda ser útil, no ha sido concebido como foro para abordar motivos de preocupación relacionados con los derechos humanos.

Las normas que rigen la concesión de licencias de exportación en algunos países, como Israel[33] y otros, han permitido reiteradamente aprobar licencias, pese a que existían motivos de preocupación con respecto a los derechos humanos, ya que con frecuencia las consideraciones estratégicas han pesado más que las de derechos humanos. Por su parte, la Unión Europea tiene marcos de derechos humanos mejor definidos, pero los distintos Estados miembros siguen concediendo licencias para tecnología de vigilancia, pese a la existencia de motivos de preocupación y de pruebas de anteriores abusos que deberían haber conllevado su denegación.[34] Al mismo tiempo, en algunas jurisdicciones, el

[29] Amnistía Internacional, "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware", 2019 www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/.
[30] Citizen Lab, "HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries", septiembre de 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.
[31] Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos, www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf
[32] https://www.wassenaar.org/es/the-wassenaar-arrangement/.
[33] Amnistía Internacional, *Amnesty International affidavit in support of Israeli petition,* (Índice: ACT 10/0332/2019) e "Israel: Amnistía Internacional participa en acciones judiciales contra web de vigilancia de NSO", (noticia, 13 de mayo de 2019).
[34] Amnistía Internacional, "UE: Varios Estados presionan para flexibilizar el reglamento sobre exportación de tecnología de vigilancia a regímenes que cometen abusos contra los derechos humanos", (noticia, 11 de junio de 2018).

secretismo en torno a la concesión de licencias es tal que socava la capacidad de las propias empresas de cumplir sus obligaciones de derechos humanos.

Todo esto crea un vacío legal y regulador que permite la venta y transferencia de tecnología de vigilancia digital sin las salvaguardias adecuadas. Cuanto más tiempo sigan eludiendo el escrutinio tanto las empresas como los Estados que adquieren tecnología de estas empresas, más peligrosamente irá reduciéndose el espacio para la disidencia y la defensa de los derechos humanos. Necesitamos con urgencia poner fin a estas tentativas de vigilancia de Estados que emplean de manera ilegítima material de vigilancia de fabricación privada para atacar a activistas de derechos humanos.

5. LAS OBLIGACIONES DE DERECHOS HUMANOS DE LOS ESTADOS Y LAS EMPRESAS

A nivel internacional, regional y nacional, varios instrumentos establecen la obligación de respetar y proteger a los defensores y defensoras de los derechos humanos. Los Estados tienen la obligación de hacer valer estas normas para garantizar un entorno seguro y propicio en el que los defensores y defensoras puedan trabajar sin miedo a ataques y continuar con su decisiva labor de protección y promoción de todos los derechos humanos.[35]

La **Declaración de la ONU sobre los Defensores y Defensoras de los Derechos Humanos** (1998)[36] se basa en instrumentos internacionales vinculantes previamente existentes. La Declaración reafirma el derecho a defender los derechos humanos y articula las obligaciones de los Estados con respecto a la función y a la situación de los defensores y defensoras de esos derechos. La Declaración enuncia los deberes y responsabilidades de los Estados a ese respecto y deja claro que son ellos los responsables últimos de proteger a los defensores y las defensoras de los derechos humanos, de impedir que se produzcan abusos y violaciones de los derechos humanos de esas personas, de abordar de manera efectiva las denuncias de violaciones y abusos cometidos contra ellas, y de garantizar que puedan llevar a cabo su labor en un entorno seguro y propicio. Es más, la Declaración resalta el papel fundamental de los defensores y defensoras de los derechos humanos a la hora de hacer realidad los derechos humanos, de desarrollar y debatir nuevas ideas y principios de derechos humanos y de abogar por su aceptación.

---

[35] Amnistía Internacional, *Amnesty International Comments on the European Commission Dual-Use Export Proposal* (Índice: POL 10/1558/2017).

[36] Declaración sobre el Derecho y el Deber de los Individuos, los Grupos y las Instituciones de Promover y Proteger los Derechos Humanos y las Libertades Fundamentales Universalmente Reconocidos, 1998, doc. ONU A/RES/53/144.

En virtud del derecho internacional de los derechos humanos, los Estados están obligados a proteger los derechos humanos de abusos perpetrados por terceros. Esto incluye la obligación de regular la conducta de los agentes no estatales que estén bajo su control para impedir que cometan o contribuyan a cometer violaciones de derechos humanos, incluso en el caso de que éstos se produzcan en otros países.

Tal como se establece en los **Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos**[37], las empresas tienen también la responsabilidad de respetar los derechos humanos con independencia del lugar del mundo en el que operen. Los Principios exigen a las empresas tomar medidas, por iniciativa propia, para garantizar que sus operaciones internacionales no causan ni contribuyen a causar abusos contra los derechos humanos, y responder a los abusos contra los derechos humanos que se pudieran producir. Para ajustarse a esa responsabilidad, las empresas deben ejercer la diligencia debida en materia de derechos humanos para "identificar, prevenir, mitigar y rendir cuentas de cómo abordan su impacto sobre los derechos humanos". La responsabilidad de las empresas de respetar los derechos humanos existe con independencia de la capacidad o voluntad de los Estados de cumplir sus propias obligaciones de derechos humanos y está por encima del cumplimiento o no de las leyes y normas nacionales de derechos humanos. Por ejemplo, la guía para la interpretación de los Principios Rectores especifica que una empresa puede contribuir a una violación de derechos humanos si proporciona "datos sobre los usuarios del servicio de Internet a un gobierno que los utiliza para rastrear y hostigar a disidentes políticos vulnerando los derechos humanos".[38]

Es más, una empresa que venda material de vigilancia puede ser cómplice de las violaciones de derechos humanos que se cometan más adelante utilizando ese material. Un grupo de expertos de la Comisión Internacional de Juristas ha examinado en cierta profundidad la cuestión de la complicidad de las empresas en las violaciones de derechos humanos y aclarado cuándo podría entrañar responsabilidades jurídicas, tanto civiles como penales. Así, el grupo de expertos de la Comisión consideró que, legalmente, se puede establecer un vínculo de responsabilidad suficiente entre la conducta de una empresa y la comisión de abusos graves contra los derechos humanos cuando dicha conducta ha permitido, agravado o facilitado los abusos y la empresa sabía, o hubiera debido saber, que los abusos ocurrirían, así como que —muy importante— una empresa puede permitir, agravar o facilitar dichos abusos mediante, entre otras cosas, el suministro de sus artículos o servicios.[39]

[37] Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos, www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf

[38] OACNUDH, *La responsabilidad de las empresas de respetar los derechos humanos: Guía para la interpretación*, 2012, p. 26, https://www.ohchr.org/Documents/Publications/HR.PUB.12.2_SP.pdf.

[39] CIJ, *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 2008, www.icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes/.

6. RECOMENDACIONES

> **"Los Estados deben imponer una moratoria inmediata a la exportación, venta, transferencia, uso o prestación de servicios de asistencia para instrumentos de vigilancia desarrollados por empresas privadas hasta que se establezca un régimen de salvaguardias que respete los derechos humanos."**
>
> Relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye[40]

Los Estados son los responsables últimos de proteger a los defensores y defensoras de los derechos humanos, impedir que se produzcan abusos y violaciones de sus derechos humanos, abordar de manera efectiva las denuncias de violaciones y abusos cometidos en su contra o contra su labor de derechos humanos, y garantizar que pueden llevar a cabo su trabajo en un entorno seguro y propicio. Queda mucho por hacer para reconocer y proteger a todas las personas que alzan la voz y luchan contra la injusticia y para protegerlas, en concreto, de la vigilancia digital.

6.1 ESTADOS

Amnistía Internacional pide a todos los Estados que:

- Suspendan la venta y la transferencia de instrumentos de vigilancia hasta que se instaure un marco regulador adecuado y respetuoso con los derechos humanos.
- Revelen información sobre todos los contratos —pasados, en vigor o futuros— que tengan con empresas privadas de vigilancia, respondiendo a las solicitudes de información o tomando ellos mismos la iniciativa de publicarla.
- Denieguen autorización para la exportación cuando exista un peligro considerable de que la exportación en cuestión pueda ser utilizada para violar los derechos humanos, bien sea mediante actividades ilegítimas de vigilancia o porque el país de destino no tenga las salvaguardias jurídicas, procedimentales y técnicas adecuadas para impedir esos abusos.

[40] OACNUDH, *La vigilancia y los derechos humanos*, informe del relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, doc. ONU A/HRC/41/35, 28 de mayo de 2019.

- Garanticen que todas las tecnologías pertinentes sean sometidas a examen antes de su transferencia.
- Garanticen transparencia con respecto al volumen, la naturaleza, el valor y el destino de las transferencias de tecnologías de vigilancia.
- Garanticen que las herramientas de codificación y las herramientas legítimas de seguridad digital no estén sujetas a controles de exportación.
- Implanten instrumentos legislativos dentro de sus territorios que limiten la vigilancia digital, garantizando lo siguiente:
    - que la vigilancia se rija por leyes precisas y de acceso público;
    - que sólo se someta a vigilancia a personas concretas, previa autorización de un cuerpo judicial competente, independiente e imparcial y con las limitaciones correspondientes de tiempo, manera, lugar y finalidad de la vigilancia;
    - que se guarden registros detallados de la vigilancia digital autorizada, de conformidad con los procedimientos legales pertinentes para las órdenes judiciales, y que se informe a las personas vigiladas lo antes que sea posible hacerlo sin poner en peligro el propósito de la vigilancia.
- Garanticen que toda vigilancia digital sea sujeta a mecanismos públicos de supervisión, que incluyan:
    - un proceso de aprobación;
    - notificación y consulta públicas sobre las nuevas adquisiciones de vigilancia;
    - publicación periódica de información.
- Garanticen la existencia de mecanismos adecuados para solicitar reparaciones legales en los casos de vigilancia digital selectiva ilegítima o abusiva.

6.2 EMPRESAS

Amnistía Internacional insta a las empresas a:

- Comprometerse públicamente a respetar los derechos humanos y el trabajo y la seguridad de los defensores y defensoras de esos derechos.
- Implementar procesos de diligencia debida adecuados en materia de derechos humanos, tal y como establecen los instrumentos internacionales sobre empresas y derechos humanos (entre los que figuran los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos y las Líneas Directrices de la OCDE para Empresas Multinacionales), a fin de garantizar que sus actividades y las de sus filiales, subcontratistas y proveedores respeten los derechos de los defensores y defensoras y no obstaculicen su legítima labor.
- En el marco de su responsabilidad de ejercer la diligencia debida en materia de derechos humanos, las empresas deben llevar a cabo una detallada evaluación de los riesgos de derechos humanos que supone cada transferencia propuesta. Dicha evaluación deberá ser examinada, a su vez, por las autoridades de exportación, y hecha pública;
- Garantizar transparencia con respecto a las ventas y los contratos;
- Llevar a cabo consultas con los y las titulares de derechos antes de firmar contratos en los distintos países en los que éstos/as viven;
- Incluir en los contratos salvaguardias para prevenir abusos contra los derechos humanos;
- Optar por formas de diseño e ingeniería que incorporen salvaguardias de derechos humanos;
- Garantizar que sus procesos de verificación sean sometidos periódicamente a auditorías y que los resultados de éstas sean públicos;
- Contar con procesos de notificación adecuados para informar sobre el uso indebido de su tecnología y con mecanismos para la presentación de quejas;

- Implantar mecanismos sólidos de indemnización para las víctimas de vigilancia ilegítima u otras formas de reparación.

6.3 INVERSIONISTAS

Amnistía Internacional insta a todos los inversionistas a:

- Asegurarse de que con su participación en las empresas de vigilancia no contribuyen a violaciones de derechos humanos. Para ello, deberán exigir a las empresas de vigilancia en cuestión amplia transparencia y diligencia debida en materia de derechos humanos.
- Comunicar a las empresas de vigilancia en las que tengan participación las recomendaciones pertinentes de entre las expuestas, y pedir que las apliquen.

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

CONTÁCTANOS


info@amnesty.org


+44 (0)20 7413 5500

ÚNETE A LA CONVERSACIÓN


www.facebook.com/AmnestyGlobal


@AmnistiaOnline