Fecha: 24 de enero de 2022 Índice: IOR 40/5179/2022

DERECHO A LA LIBERTAD DE OPINIÓN Y DE EXPRESIÓN: AMENAZAS DE LA VIGILANCIA SELECTIVA ILEGÍTIMA PARA LOS MEDIOS DE COMUNICACIÓN

COMUNICACIÓN PARA EL INFORME DE LA RELATORA ESPECIAL DE LA ONU SOBRE LA PROMOCIÓN Y LA PROTECCIÓN DEL DERECHO A LA LIBERTAD DE OPINIÓN Y DE EXPRESIÓN EN EL 50 PERIODO DE SESIONES DEL CONSEJO DE DERECHOS HUMANOS

Amnistía Internacional presenta este documento en respuesta al llamamiento[1] de la relatora especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión para contribuir al informe que ésta presentará en el 50 periodo de sesiones del Consejo de Derechos Humanos. Aunque los medios de comunicación se enfrentan a numerosas dificultades y amenazas en la era digital, este documento se centra particularmente en la amenaza que supone la vigilancia selectiva ilegítima para periodistas. En él se detallan tendencias globales y se incluyen ejemplos de algunos países. No obstante, no debe considerarse una exposición exhaustiva de la investigación realizada por la organización sobre estos asuntos.

INTRODUCCIÓN

El uso ilegítimo de las tecnologías de vigilancia selectiva contra periodistas y otros miembros de la sociedad civil por parte de los Estados ha provocado una crisis de vigilancia digital. Los Estados utilizan la vigilancia ilegítima en combinación con otras tácticas para silenciar a periodistas y ejercer un efecto disuasorio sobre la sociedad civil, lo que supone una seria amenaza contra la seguridad y la protección de periodistas de todo el mundo. Las consecuencias para las libertades de los medios de comunicación son terribles. Los Estados no sólo han incumplido la obligación de proteger al colectivo periodista frente a estas violaciones de los derechos humanos sino que además han incumplido sus propias obligaciones en esa materia, puesto que claramente han permitido que se utilicen estas armas invasivas contra personas de todo el mundo sin otra razón que haber ejercido sus derechos humanos y trabajar para proteger los derechos de los demás.

El sector de la vigilancia digital privada está facilitando esta tendencia global de utilizar tecnologías de vigilancia selectiva como los programas espía para reprimir los derechos a la libertad de opinión y de expresión. Como ya señalamos en nuestra comunicación previa de febrero de 2019 al anterior relator especial sobre el derecho a la libertad de opinión y de expresión, el sector internacional de vigilancia no está sometido a ningún control. Tanto la normativa actual como los mecanismos de control y supervisión a nivel nacional, regional y global han demostrado ser inadecuados para prevenir las violaciones de derechos humanos e ineficaces para la rendición de cuentas y la reparación de daños.[2]

La vigilancia selectiva ilegítima viola el derecho a la privacidad y los derechos a la libertad de expresión, opinión, asociación y reunión pacífica, que están protegidos tanto por la Declaración Universal de Derechos Humanos (DUDH) como por el Pacto Internacional de Derechos Civiles y Políticos (PIDCP). Este último consagra el derecho de todas las personas a no ser molestadas a causa de sus opiniones y las protege de injerencias arbitrarias o ilegales en su vida privada.[3]

[1] Cuestionario Derecho a la libertad de opinión y expresión: Oportunidades, retos y amenazas para los medios de comunicación en la era digital, https://www.ohchr.org/SP/Issues/FreedomOpinion/Pages/Report-Media-Digital-Age.aspx.
[2] Amnistía Internacional, *The Surveillance Industry and Human Rights: Amnesty International submission to United Nations Special Rapporteur on the Promotion and Protection of The Right to Freedom of Opinion and Expression* (22 de febrero de 2019, Índice: TIGO IOR 40/9868/2019), https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/AMNESTY%20INTERNATIONAL.pdf.
[3] PIDCP, artículos 17 y 19.

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. La práctica actual de los Estados, que permite el despliegue sin control de estas herramientas, no cumple con esos criterios. Convertir a periodistas, defensores y defensoras de los derechos humanos en blanco de estas tecnologías por el mero hecho de hacer su trabajo es manifiestamente ilegítimo en virtud del derecho internacional en materia de derechos humanos.[4]

Esta comunicación detalla el uso ilegítimo de la vigilancia selectiva contra periodistas y sugiere vías de actuación para poner fin a esta práctica.

USO DE VIGILANCIA SELECTIVA ILEGÍTIMA CONTRA PERIODISTAS

En los últimos años han empezado a conocerse casos de uso de vigilancia selectiva ilícita contra periodistas, desde las primeras denuncias de escuchas telefónicas pasando por los intentos de *phishing* y mensajes SMS con enlaces maliciosos hasta, en la actualidad, ataques selectivos más sofisticados, como los de programas espía sin necesidad de hacer clic. Así como las tecnologías han ido evolucionando, también lo han hecho las tácticas de represión digital selectiva. Por tanto, el colectivo periodista se enfrenta a nuevas amenazas que son más difíciles de detectar, hacen más difícil protegerse contra ellas y más aún pedir responsabilidades por su uso.

Existen numerosos ejemplos en todo el mundo del uso de tecnologías de vigilancia selectiva contra periodistas. En Reino Unido, informes sugieren que la policía ha sometido a periodistas a vigilancia digital,[5] mientras que en Colombia se ha denunciado esta práctica contra periodistas radiofónicos por parte de la policía nacional.[6] A lo largo de los años, la organización de investigación Citizen Lab ha ido documentando ataques digitales contra periodistas por parte de diversos agentes amenazantes en China, Rusia, Etiopía y México.[7] Amnistía Internacional también ha documentado en el pasado ataques de programas maliciosos contra blogueros y blogueras en Vietnam y un periodista de India.[8] En 2020, Citizen Lab determinó, además, que se había utilizado el programa espía Pegasus del conocido proveedor de cibervigilancia NSO Group para *hackear* los teléfonos personales de 36 miembros del personal de Al Yazira, un periodista de Al Araby TV y otro de *The New York Times*.[9] El Laboratorio sobre Seguridad de Amnistía Internacional identificó pruebas de que tanto Maati Monjib, cofundador de la Asociación Marroquí de Periodismo de Investigación, como Omar Radi, destacado activista y periodista marroquí ahora en prisión, habían sido sometidos a vigilancia utilizando programas espía de NSO Group.[10]

A raíz de estos informes iniciales, en julio de 2021 se hizo público el Proyecto Pegasus. La amplitud y envergadura de los hallazgos del proyecto hicieron patente la gravedad de la amenaza que supone la vigilancia selectiva ilícita para la libertad de prensa. El Proyecto Pegasus fue fruto de la

[4] Comité de Derechos Humanos, Observación general Nº 34, doc. ONU CCPR/C/GC/36, párr. 23.
[5] 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/.
[6] 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.
[7] Véase Marczak et.al., *The Great iPwn*, diciembre de 2020, (https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group- imessage-zero-click-exploit/) y Marczak et.al., *Stopping the Press New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator*, enero de 2020, (https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/).
[8] Véase Amnistía Internacional, Click and Bait: *Vietnamese Human Rights Defenders Targeted with Spyware Attacks*, febrero de 2021 (https://www.amnesty.org/en/latest/research/2021/02/click-and-bait-vietnamese-human-rights-defenders-targeted-with-spyware-attacks/) y Amnistía Internacional, India: *Human Rights Defenders Targeted by a Coordinated Spyware Operation*, junio de 2020, (https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/).
[9] Marczak et al., *The Great iPwn*, diciembre de 2020, https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/.
[10] Véase Amnistía Internacional, "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware", octubre de 2019, (https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/) y Amnistía Internacional, Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools, junio de 2020 (https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/).

colaboración de más de 80 periodistas de 17 medios de comunicación de 10 países bajo la coordinación de Forbidden Stories (organización sin ánimo de lucro con sede en París) y con el apoyo técnico de Amnistía Internacional, que realizó análisis periciales de teléfonos móviles para identificar rastros del programa espía Pegasus. Los investigadores del proyecto pusieron de manifiesto que clientes estatales habían hecho uso de un único proveedor de cibervigilancia, NSO Group, para facilitar violaciones de derechos humanos en todo el mundo a escala masiva. El proyecto identificó posibles clientes de NSO en 11 países: Arabia Saudí, Azerbaiyán, Bahréin, Emiratos Árabes Unidos, Hungría, India, Kazajistán, Marruecos, México, Ruanda y Togo. Las revelaciones del Proyecto Pegasus desmienten las afirmaciones de NSO de que tales ataques son poco frecuentes o anómalos, o que se derivan de un uso indebido de su tecnología. Aunque la empresa afirma que su software espía sólo se utiliza en investigaciones penales y sobre terrorismo legítimas, ha quedado claro que su tecnología facilita la comisión de abusos sistémicos, en los que al parecer ser cómplice.[11]

En el momento de su publicación en julio, los medios de comunicación identificaron al menos a 180 periodistas en 20 países que habían sido blanco de posibles ataque con el software espía de NSO entre 2016 y junio de 2021.[12] Durante un periodo de dos años, al menos 25 periodistas de México fueron blanco de posibles ataques, como el caso de la periodista de investigación Carmen Aristegui, en el que se confirmaron los ataques.[13] Pegasus se ha utilizado en Azerbaiyán, país en el que apenas quedan unos pocos medios de comunicación independientes y donde, según la investigación, se seleccionó como posibles objetivos a más de 40 periodistas. En India, al menos 40 periodistas de casi todos los principales medios de comunicación del país fueron seleccionados como posibles objetivos entre 2017 y 2021. La investigación también identificó como posibles objetivos a periodistas que trabajan para medios de comunicación internacionales de primer orden, entre ellos Associated Press, CNN, *The New York Times* y Reuters.[14]

El Laboratorio sobre Seguridad de Amnistía Internacional confirmó mediante análisis forenses que los dispositivos de gran cantidad de periodistas habían sido blanco de ataques y/o infecciones. En Azerbaiyán, los móviles de las periodistas Sevinc Vaqifqizi y Khadija Ismayilova fueron infectados con el programa espía Pegasus. En India, análisis forenses revelaron que los móviles de los periodistas Siddharth Varadarajan, MK Venu, Paranjoy Guha Thakurta, Sushant Singh y SNM Adbi también habían sido infectados. En Hungría se detectó que los móviles de periodistas como Szabolcs Panyi, Daniel Nemeth, András Szabó y Brigitta Csikász y del propietario de medios de comunicación Zoltán Páva[15] estaban infectados, como también los de Hicham Mansouri, Lénaïg Bredoux y Edwy Plenel, periodistas radicados en Francia.[16]

El informe deja claro que el programa espía Pegasus de NSO Group es el arma preferida de los gobiernos para silenciar a periodistas.[17] El uso de estos programas tiene un efecto disuasorio dirigido a atemorizar a quieres alzan la voz. Incluso en los casos en que no es posible probar la existencia de vigilancia, la mera sospecha de que pueda estar ocurriendo obliga a los periodistas a autocensurarse. La vigilancia ilegítima supone un riesgo enorme para la seguridad física y la salud

[11] Amnistía Internacional, "La magnitud de los sistemas de cibervigilancia opacos, una crisis de derechos humanos internacional en la que NSO Group es cómplice", julio de 2021 https://www.amnesty.org/es/latest/news/2021/07/pegasus-project-spyware-digital-surveillance-nso/ (Comunicado de prensa).
[12] Amnistía Internacional, "Una filtración de datos masiva revela que el software espía de la empresa israelí NSO Group se utiliza para atacar a activistas, periodistas y figuras políticas en todo el mundo", julio de 2021, https://www.amnesty.org/es/latest/news/2021/07/the-pegasus-project/ (Comunicado de Prensa).
[13] Phineas Rueckert, "Pegasus: The new global weapon for silencing journalists", julio de 2021, https://forbiddenstories.org/pegasus-the-new-global-weapon- for-silencing-journalists/.
[14] Amnistía Internacional, "Una filtración de datos masiva revela que el software espía de la empresa israelí NSO Group se utiliza para atacar a activistas, periodistas y figuras políticas en todo el mundo", julio de 2021, https://www.amnesty.org/es/latest/news/2021/07/the-pegasus-project/ (Comunicado de Prensa).
[15] Omer Benjakob, "The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware", enero de 2022, https://www.haaretz.com/israel-news/MAGAZINE-nso-pegasus-spyware-file-complete-list-of-individuals-targeted-1.10549510.
[16] Amnistía Internacional, *Forensic Methodology Report: Pegasus Forensic Traces per Target*, julio de 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/.
[17] Phineas Rueckert, "Pegasus: The new global weapon for silencing journalists", julio 2021, https://forbiddenstories.org/pegasus-the-new-global-weapon- for-silencing-journalists/.

mental de profesionales de la información, también pone en peligro a sus fuentes, colegas, amistades y familiares y puede tener graves consecuencias en la vida cotidiana de quienes son blanco de ataques o infecciones.

En 2017, Amnistía Internacional documentó la vigilancia selectiva ilegítima a la que había sido sometida la periodista uzbeka Galima Bukharbaeva mediante un ataque de *phising* en su correo electrónico. Poco después del ataque, en sitios web que se consideran alineados con el gobierno de Uzbekistán —cuando no controlados por éste— aparecieron noticias que contenían información de los correos privados de Galima. Cuando Gulasal Kamolova y Vasiliy Markov, dos periodistas de Uzbekistán vieron aparecer sus nombres en estos artículos, supieron que podían correr peligro y fueron presa de intenso miedo y ansiedad. Seis meses después del ataque en el correo de Galima, tanto Vasiliy como Gulasal tuvieron que abandonar sus hogares en Uzbekistán y solicitar asilo en otro país.[18]

Familiares y amigos del periodista saudí asesinado Jamal Khashoggi también fueron objeto de ataques con el programa espía Pegasus antes y después del asesinato, a pesar de que el NSO Group negase reiteradamente su implicación. Según los análisis forenses de Amnistía Internacional, el móvil de la ciudadana turca Hatice Cengiz, novia de Khashoggi, había sido blanco de ataques y resultó infectado cuatro días después del asesinato y en múltiples ocasiones durante los días siguientes. Las pruebas forenses también corroboraron que el móvil de Hanan Elatr, esposa de Khashoggi, había sido blanco de ataques con el programa espía, como su amigo Wadah Khanfar, ex director general de Al Yazira, cuyo móvil fue *hackeado*.[19]

Estos casos son ejemplo de cómo grupos enteros de personas pueden ser sometidas a vigilancia y que dicha vigilancia puede estar vinculada a graves abusos contra los derechos humanos. De hecho, gran cantidad de periodistas que han sido objeto de ataques o cuyos móviles se han visto infectados con el programa Pegasus han sufrido represión a manos de los gobiernos, con hostigamiento, campañas difamatorias e incluso prisión. Para las periodistas, en particular, la amenaza de vigilancia es aún más grave.

La información obtenida mediante vigilancia ilegítima puede ser usada como arma contra ellas en campañas difamatorias, de desanonimización y otros ataques digitales. Por eso, la vigilancia es una forma de violencia contra las mujeres.[20] Además, como se ha visto en muchos casos que el Proyecto Pegasus ha sacado a la luz, incluso cuando las personas afectadas deciden abandonar sus países de origen, la vigilancia continúa, lo que convierte la vigilancia selectiva ilícita en una herramienta de represión transnacional y crea el temor de que ningún lugar es seguro.

Las revelaciones del Proyecto Pegasus iniciaron un proceso que, durante un año y gracias a investigaciones de la sociedad civil y de grandes empresas tecnológicas, ha sacado a la luz numerosas irregularidades del sector de la vigilancia digital. A raíz de estas nuevas revelaciones, la lista de clientes potenciales de NSO Group ahora incluye a El Salvador, Ghana, Polonia, Tailandia y Uganda.[21] En fecha tan reciente como enero de 2022, Citizen Lab y Access Now, en colaboración con Front Line Defenders, SocialTIC y Fundación Acceso, investigaron el uso del programa espía Pegasus para *hackear* comunicaciones en El Salvador. Estas investigaciones confirmaron 35 casos de periodistas y personas de la sociedad civil cuyos móviles habían sido infectados con el programa espía de NSO entre julio de 2020 y noviembre de 2021. Entre las personas afectadas había

[18] Amnistía Internacional, "We will find you, anywhere: The global shadow of Uzbekistani surveillance", marzo de 2017, (EUR 62/5974/2017), https://www.amnesty.org/en/documents/eur62/5974/2017/en/.
[19] Amnistía Internacional, *Forensic Methodology Report: Pegasus Forensic Traces per Target*, julio de 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/.
[20] Access Now y Frontline Defenders, "Unsafe anywhere: women human rights defenders speak out about Pegasus attacks", enero de 2022 https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/.
[21] Véase: https://www.amnesty.org/es/latest/news/2022/01/poland-use-of-pegasus-spyware-to-hack-politicians-highlights-threat-to-civil-society/ , https://techcrunch.com/2021/11/24/apple-nso-hacking-notify/ y https://www.primenewsghana.com/politics/stan-dogbe-alleges-state-sponsored- attack-on-his-phone.html.

periodistas de *El Faro*, *GatoEncerrado*, *La Prensa Gráfica*, *Revista Digital Disruptiva*, *Diario El Mundo*, *El Diario de Hoy* y dos periodistas independientes.[22]

Es importante señalar que, a medida que se descubren nuevos casos, NSO Group no es la única empresa que comercializa estas herramientas. Citizen Lab descubrió que un periodista egipcio en el exilio había sido objeto de ataques con programas espía de la empresa Cytrox.[23] Preocupa que la falta de transparencia de un sector que sigue operando en la sombra signifique que, posiblemente, los casos identificados en el informe no sean más que la punta del iceberg y, por tanto, este documento no pretende ser exhaustivo.

VÍAS DE ACTUACIÓN

Como señalamos en nuestra comunicación de 2019 para el anterior relator especial, los marcos reguladores y mecanismos de reparación actuales siguen siendo ineficaces e inadecuados.[24] Hasta la fecha, la situación no ha cambiado. Ya hemos analizado con anterioridad que, en muchas jurisdicciones, la legislación nacional relativa a la vigilancia, sistemas nacionales y regionales de control de las exportaciones y otros mecanismos como el Acuerdo de Wassenaar en su forma actual no cumplen su cometido de combatir la amenaza de la vigilancia selectiva ilegítima.[25] Incluso cuando se han actualizado los mecanismos de regulación, como en el caso de la normativa europea sobre tecnologías de doble uso, la regulación es insuficiente[26] y sólo será efectiva si se aplica con la debida transparencia.[27] De hecho, el anterior relator especial de las Naciones Unidas sobre la libertad de opinión y de expresión indicó en su informe: "Decir que todo un sistema completo de control y utilización de tecnologías de vigilancia selectiva ha dejado de funcionar ni siquiera se acerca a la realidad. La realidad es que apenas existe."[28]

Las empresas que operan en este ámbito lo hacen con opacidad e impunidad. Hemos señalado repetidamente que las alegaciones de NSO Group sobre su respeto de los derechos humanos carecen de sentido y que sus políticas y prácticas son ineficaces. Nuestra larga relación con la empresa demuestra que no podemos confiar en que los proveedores de cibervigilancia se autorregulen. Además, los inversores tienen la responsabilidad de asegurarse de que sus inversiones en estas empresas no están contribuyendo o están directamente vinculadas a abusos contra los derechos humanos.[29]

Amnistía Internacional reitera su petición de que los Estados impongan una moratoria inmediata a la venta, transferencia y uso de las tecnologías de vigilancia hasta que se establezcan marcos normativos que respeten los derechos humanos. También hemos instado a la Unión Europea, entre

---

[22] Railton et. al, *Proyecto Torogoz Hackeo extensivo de los medios de comunicación y la sociedad civil en El Salvador con el programa espía Pegasus*, enero de 2022. https://citizenlab.ca/2022/01/proyecto-torogoz-hackeo-extensivo-de-los-medios-de-comunicacion-y-la-sociedad-civil-en-el-salvador-con-el-programa-espia-pegasus/.

[23] Marczak, et. al, *Pegasus vs. Predator Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, diciembre de 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

[24] Amnistía Internacional, *The Surveillance Industry and Human Rights: Amnesty International submission to United Nations Special Rapporteur on the Promotion and Protection of The Right to Freedom of Opinion and Expression* (22 de febrero de 2019, Índice: TIGO IOR 40/9868/2019) https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/AMNESTY%20INTERNATIONAL.pdf.

[25] Amnistía Internacional, "Operating from the Shadows: Inside NSO Group's Corporate Structure", mayo de 2021, DOC 10/4182/2021, https://www.amnesty.org/en/documents/doc10/4182/2021/en/.

[26] Amnistía Internacional, "New EU Dual Use Regulation agreement 'a missed opportunity' to stop exports of surveillance tools to repressive regimes", marzo de 2021, https://www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of- surveillance-tools-to-repressive-regimes/ (Comunicado de prensa).

[27] Access Now et.al, *Human Rights Organizations Call for Robust Implementation of New EU Export Control Rules and Investigation of EU member states' role in Pegasus affair*, septiembre de 2021, https://www.accessnow.org/cms/assets/uploads/2021/09/Pegasus_Export_Control_Rules_Statement.pdf.

[28] Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión, doc. ONU A/HCR/41/35, párr. 46, https://undocs.org/A/HRC/41/35.

[29] Amnistía Internacional, "Operating in the shadows: Investor risk from the private surveillance industry", octubre de 2021, https://www.amnesty.org/en/documents/doc10/4359/2021/en/ (DOC 10/4359/2021).

otras entidades, a imponer sanciones específicas a NSO Group.[30] Para combatir esta crisis es necesaria una acción múltiple en diversos niveles. Por tanto, recordamos las recomendaciones que hacemos a diversos actores en nuestro informe titulado *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector*.[31]

Ha surgido una cultura de impunidad específica de la vigilancia digital selectiva que debe contrarrestarse urgentemente. La información presentada en esta comunicación evidencia que el uso de las herramientas de vigilancia digital selectiva por parte de los Estados está totalmente fuera de control, desestabiliza y amenaza los derechos humanos de las personas, además de su seguridad física. Estas revelaciones arrojan luz sobre un sector y un ámbito de prácticas estatales que no rinden cuentas y que no deben seguir operando en sus formas actuales. Los derechos de periodistas a expresarse con libertad y realizar su trabajo sin miedo y de forma segura, así como la seguridad del ecosistema digital en su totalidad, dependen de ello.

[30] Véase https://www.hrw.org/news/2021/12/03/joint-letter-urging-eu-targeted-sanctions-against-nso-group.
[31] Amnistía Internacional, *Uncovering the Iceberg:" "The Digital Surveillance Crisis Wrought by States and the Private Sector*, julio de 2021, https://www.amnesty.org/en/documents/doc10/4491/2021/en/ (DOC 10/4491/2021).