Carta abierta conjunta de organizaciones de la sociedad civil y expertos/as independientes en la que se insta a los Estados a que apliquen una moratoria inmediata sobre la venta, la transferencia y el uso de tecnología de vigilancia

Las organizaciones de la sociedad civil y los expertos/as independientes abajo firmantes nos sentimos alarmados por las revelaciones aparecidas en los medios de comunicación sobre el uso del software espía de NSO Group para facilitar violaciones de derechos humanos en todo el mundo a gran escala. Estas revelaciones son resultado del Proyecto Pegasus y se basan en la filtración de 50.000 números de teléfono de posibles objetivos de vigilancia. El Proyecto Pegasus es una investigación colaborativa en la que han participado más de 80 periodistas de 16 organizaciones de medios de comunicación de 10 países bajo la coordinación de Forbidden Stories (organización sin ánimo de lucro de medios de comunicación con sede en París), y con el apoyo técnico de Amnistía Internacional, que realizó análisis periciales de teléfonos celulares para identificar rastros del software espía Pegasus.

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. La compañía afirma que su software espía sólo se utiliza en investigaciones penales y de terrorismo legítimas, pero ha quedado claro que su tecnología facilita la comisión de abusos sistémicos. Como dijo la alta comisionada de la ONU para los derechos humanos, "[s]i las recientes alegaciones sobre el uso de Pegasus son incluso parcialmente verdaderas, entonces esa línea roja ha sido traspasada una y otra vez en total impunidad".

A partir de los datos filtrados y sus investigaciones, Forbidden Stories y los medios de comunicación asociados identificaron posibles clientes de NSO en 11 países: Arabia Saudí, Azerbaiyán, Bahréin, Emiratos Árabes Unidos, Hungría, India, Kazajistán, Marruecos, México, Ruanda y Togo. NSO afirma que sólo vende esta tecnología a clientes gubernamentales.

Hasta el momento, la investigación también ha identificado al menos a 180 periodistas en 20 países que fueron seleccionados para un posible ataque con el software espía de NSO entre 2016 y junio de 2021. Entre los datos sumamente preocupantes que han trascendido se incluyen pruebas de que el software Pegasus se utilizó contra familiares del periodista saudí Jamal Khashoggi antes y después de su asesinato en Estambul el 2 de octubre de 2018 a manos de agentes saudíes, pese a que NSO Group ha negado en repetidas ocasiones que sus productos se hayan utilizado contra Khashoggi o sus familiares.

Estas revelaciones son sólo la punta del iceberg. Se ha permitido que la industria de vigilancia privada opere sin control. Los Estados no sólo han incumplido su obligación de proteger a las personas de estas violaciones de los derechos humanos, sino que ellos mismos han incumplido sus obligaciones en materia de derechos humanos al permitir, sin ningún género de dudas, que estas armas invasivas se apliquen libremente sobre personas de todo el mundo sin otra razón que haber ejercido sus derechos humanos. Además, la selección de objetivos puede desvelar sólo parte de la realidad de las violaciones de derechos humanos que denotan, ya que las violaciones del derecho a la privacidad repercuten en otros muchos derechos humanos y muestran el perjuicio real que causa una vigilancia incompatible con las normas internacionales.

En México se seleccionó como objetivo el teléfono del periodista Cecilio Pineda apenas unas semanas antes de su homicidio en 2017. Pegasus se ha utilizado en Azerbaiyán, país en el que sólo quedan unos pocos medios de comunicación independientes. El Laboratorio sobre

Seguridad de Amnistía Internacional concluyó que el teléfono de Sevinc Vaqifqizi, periodista autónoma que colabora con el medio de noticias independiente Meydan TV, estuvo infectado durante un periodo de dos años hasta mayo de 2021. En India, al menos 40 periodistas de los principales medios de comunicación del país fueron seleccionados como posibles objetivos entre 2017 y 2021. Los análisis forenses revelaron que los teléfonos de Siddharth Varadarajan y MK Venu, cofundadores del medio de noticias independiente online The Wire, estaban infectados con el software espía Pegasus en una fecha tan reciente como junio de 2021. Mientras tanto, el periodista y activista de derechos humanos marroquí Omar Radi fue condenado a seis años de prisión. En 2020, Amnistía Internacional ya había realizado un examen forense del teléfono de Radi y determinó que era objeto de vigilancia de Pegasus. En Marruecos, dos de los otros 34 periodistas con teléfonos seleccionados como posibles objetivos de Pegasus están encarcelados. 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. De este grupo, una de las figuras más destacadas es Roula Khalaf, directora del *Financial Times*. Estos objetivos representan tan sólo una pequeña parte de las revelaciones, y el panorama completo aún no ha salido a la luz.

No es la primera vez que se relaciona el software Pegasus de NSO con violaciones de derechos humanos. Investigadores/as, periodistas, activistas y otras personas han aportado a lo largo de los años pruebas significativas del uso de la tecnología de NSO Group para vigilar a personas. Una investigación anterior de Citizen Lab sacó a la luz cómo Ahmed Mansoor, defensor de los derechos humanos encarcelado en Emiratos Árabes Unidos, fue objetivo de la tecnología de NSO Group en 2016. En México, periodistas, profesionales de la abogacía y de la salud pública también han sido objeto de vigilancia anteriormente.

Cuando la vigilancia se lleva a cabo sin los marcos jurídicos, la supervisión, las salvaguardias y la transparencia adecuados, sus perjuicios tienen un impacto que va mucho más allá de las personas que puedan haber sido seleccionadas como objetivo. Ante la opacidad y unas salvaguardias inadecuadas, especialmente en situaciones en las que se sabe o se sospecha que la vigilancia se lleva a cabo de forma ilegal, tanto defensores/as de los derechos humanos como periodistas se ven obligados a autocensurarse por miedo a ser perseguidos por su trabajo, incluso cuando dicha vigilancia pueda no estar teniendo lugar. De hecho, inmediatamente después de las revelaciones, periodistas y activistas ya perciben un efecto disuasorio en su trabajo.

Cabe destacar que el uso de herramientas de vigilancia digital selectiva como Pegasus infringe el derecho a la privacidad y muchos otros derechos. Pegasus afecta al derecho a la privacidad por su diseño: es subrepticio, se instala sin el conocimiento del titular de los derechos y tiene la capacidad de recopilar y transmitir una selección ilimitada de datos personales y privados (junto con los datos de los contactos con los que interactúa el objetivo). Asimismo, como se ha señalado anteriormente, una violación del derecho a la privacidad puede tener efectos en cascada sobre otros derechos, incluidos los derechos a la libertad de expresión, asociación y reunión pacífica. De estas revelaciones se desprende que estos usos de la herramienta son abusivos y arbitrarios, y no constituyen una injerencia permisible respecto al derecho a la privacidad. Además, el despliegue incontrolado de estas herramientas por parte de los Estados no cumple con los criterios de necesidad, proporcionalidad y objetivo legítimo, tal y como se indica en las normas internacionales.

Ha surgido una cultura de la impunidad específica de la vigilancia digital selectiva que debe contrarrestarse urgentemente. Estas informaciones muestran cómo el uso por parte de los Estados de las herramientas de vigilancia digital selectiva suministradas por uno de los participantes más destacados de la industria está totalmente fuera de control, desestabiliza y

amenaza los derechos humanos de las personas, además de la seguridad física. Las revelaciones arrojan luz sobre una industria y una esfera de prácticas estatales que no rinden cuentas y que no deben seguir operando en sus formas actuales. Nuestros derechos y la seguridad del ecosistema digital en su conjunto dependen de ello.

Apoyamos el llamamiento de la alta comisionada de las Naciones Unidas para que "[l]os gobiernos deberían poner un alto inmediato a su propio uso de las tecnologías de vigilancia que violen derechos humanos y deberían llevar a cabo acciones concretas para proteger la privacidad ante dichas invasiones, regulando la distribución, el uso y la exportación de tecnologías de vigilancia creadas por otros".

Por ello, instamos a todos los Estados a que adopten urgentemente las siguientes medidas:

A todos los Estados:

a. Imponer inmediatamente una moratoria sobre la venta, la transferencia y el uso de tecnología de vigilancia. Dada la amplitud y escala de estos hallazgos, existe una necesidad urgente de detener las actividades de todos los Estados y empresas que emplean la tecnología de vigilancia hasta que la labor de reglamentación de los derechos humanos se ponga al día.
b. Realizar una investigación inmediata, independiente, transparente e imparcial de los casos de vigilancia selectiva. Además, investigar las licencias de exportación concedidas para tecnologías de vigilancia selectiva y revocar todas las licencias de comercialización y exportación en situaciones en las que se pongan en peligro los derechos humanos.
c. Adoptar y aplicar un marco jurídico que exija a las empresas de vigilancia privada y a sus inversores la debida diligencia en materia de derechos humanos en sus operaciones globales, cadenas de suministro y en relación con el uso final de sus productos y servicios. Según esta legislación, las empresas de vigilancia privada deben estar obligadas a identificar, prevenir y mitigar los riesgos relacionados con los derechos humanos en sus actividades y relaciones comerciales.
d. Adoptar y aplicar un marco jurídico que exija transparencia a las empresas de vigilancia privada y que abarque, entre otras cosas, información sobre la autoidentificación/registro, los productos y servicios ofrecidos, los resultados de la diligencia debida periódica, incluidos detalles de cómo abordaron los riesgos y los efectos reales identificados, y las ventas realizadas, así como los clientes potenciales rechazados por no cumplir las normas de derechos humanos o buena gobernanza. Los Estados deben hacer que esta información esté disponible en los registros públicos.
e. Garantizar que todas las empresas de vigilancia domiciliadas en sus países, incluidos los intermediarios comerciales, las filiales, las sociedades de cartera y los propietarios de capital privado, estén obligados a actuar de forma responsable y a responder de las repercusiones negativas sobre los derechos humanos. Debe exigirse por ley que estas empresas ejerzan la diligencia debida en materia de derechos humanos respecto a sus operaciones globales. Esto debe incluir la satisfacción de los daños causados y el acceso de las comunidades afectadas a un recurso efectivo en los Estados de origen de las empresas, para las personas y las comunidades afectadas. Por tanto, los gobiernos deben presentar o apoyar propuestas para adoptar legislación nacional sobre rendición de cuentas de las empresas.
f. Revelar información sobre todos los contratos —pasados, en vigor y futuros— que tengan con empresas de vigilancia privada, ya sea en respuesta a solicitudes de información o tomando ellos mismos la iniciativa de publicarla.
g. Como condición para que las empresas de vigilancia sigan funcionando, exigir la creación inmediata de organismos de supervisión independientes y con múltiples partes

interesadas para NSO Group y todas las demás empresas de vigilancia privada. En esos organismos deberán incluirse a los grupos de derechos humanos y a otros agentes de la sociedad civil.

h. Establecer juntas de supervisión pública comunitarias para supervisar y aprobar la adquisición o el uso de nuevas tecnologías de vigilancia, facultadas para aprobar o rechazar —en función de las obligaciones de los Estados en materia de derechos humanos— las disposiciones relativas a la notificación pública y la presentación de informes.

i. Reformar las leyes existentes que supongan un obstáculo a la reparación para las víctimas de la vigilancia ilegal y garantizar que en la práctica existan vías de recurso, tanto judiciales como no judiciales.

j. Además, los Estados deben aplicar como mínimo las siguientes recomendaciones en el caso de que deba levantarse la moratoria sobre la venta y transferencia de equipos de vigilancia:
   - Aplicar una legislación nacional que imponga salvaguardias contra las violaciones y los abusos de derechos humanos a través de la vigilancia digital y establecer mecanismos de rendición de cuentas que proporcionen a las víctimas de abusos de vigilancia una vía de recurso.
   - Aplicar normas de contratación que restrinjan los contratos públicos de tecnología y servicios de vigilancia únicamente a las empresas que demuestren que respetan los derechos humanos de acuerdo con los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas y que no han prestado servicios a clientes que cometen abusos en materia de vigilancia.
   - Participar en iniciativas multilaterales clave para elaborar normas sólidas en materia de derechos humanos que regulen el desarrollo, la venta y la transferencia de equipos de vigilancia, e identificar los objetivos no permitidos de la vigilancia digital.

k. Informar a las bolsas de valores y a los reguladores financieros acerca de los perjuicios asociados a las empresas de tecnología de vigilancia privada, y exigirles un escrutinio estricto y regular, en conformidad con la legislación y normas nacionales, de las divulgaciones y solicitudes de dichas empresas y sus propietarios, especialmente antes de cualquier acontecimiento importante (salidas a bolsa, fusiones, adquisiciones, etc.).

l. Proteger y promover una encriptación segura, una de las mejores defensas contra la vigilancia invasiva.

Instamos a Israel, Bulgaria, Chipre y a cualquier otro estado en el que NSO tenga presencia empresarial a lo siguiente:

a. Los Estados exportadores, incluidos Israel, Bulgaria y Chipre, deben revocar inmediatamente todas las licencias de comercialización y exportación concedidas a NSO Group y sus entidades, y llevar a cabo una investigación independiente, imparcial y transparente para determinar el alcance de los objetivos ilegales, que culmine con una declaración pública sobre los resultados de los esfuerzos y las medidas para evitar futuros daños.

Firmantes

Organizaciones de la sociedad civil
#SeguridadDigital
Access Now
Advocacy for Principled Action in Government
Africa Open Data and Internet Research Foundation (AODIRF)
African Freedom of Expression Exchange (AFEX)
Al-Haq
ALQST for Human Rights
Amman Center for Human Rights Studies (ACHRS)
Amnesty International
ARTICLE 19: Global Campaign for Free Expression
Asian Forum for Human Rights and Development (FORUM-ASIA)
Asociación por los Derechos Civiles (ADC)
Association for Progressive Communications (APC)
Barracón Digital
Bits of Freedom
Bloggers of Zambia
BlueLink Foundation
Body & Data, Nepal
Brazilian Association of Investigative Journalism (Abraji)
Brazilian Institute of Consumer Protection (Idec)
Breakpointing Bad
Business & Human Rights Resource Centre
Center for Democracy & Technology
Center for Civil Liberties (Ukraine)
Centro de Análisis Forense y Ciencia Aplicadas -CAFCA-
Centro de Documentación en Derechos Humanos "Segundo Montes Mozo S. J." (CSMM)
Citizen D | Državljan D
Civic Assistance Committee, Russia
CIVICUS: World Alliance for Citizen Participation
Civil Rights Defenders
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Comisión Ecuménica de Derechos Humanos, Ecuador
Comisión Intereclesial de Justicia y Paz
Comisión Intereclesial de Justicia y Paz
Comisión Mexicana de Defensa y Promoción de los Derechos Humanos
Committee to Protect Journalists (CPJ)
Conectas Direitos Humanos
Conectas Human Rights
Conexo
Cooperativa Tierra Común - México
CyberPeace Institute
Data Privacy Brasil Research Association
Datysoc
Deache
Defend the Defenders
Defense for Children International - Palestine
Derechos Digitales · América Latina
Digitalcourage

Digital Defenders Partnership
Digital Empowerment Foundation
Digital Rights Foundation
Digital Rights Kashmir
Digital Security Lab Ukraine
DPLF - Due Process of Law Foundation/Fundación para el Debido Proceso
Egyptian Initiative for Personal Rights (EIPR)
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)
ELSAM epicenter.works
Equipo de Reflexión, Investigación y Comunicación de la Compañía de Jesús en Honduras
Equipo Jurídico por los Derechos Humanos (Honduras)
Ethics in Technology a 501c3
European Center for Not-for-Profit Law (ECNL)
European Digital Rights (EDRi)
FIDH - International Federation for Human Rights
Fitug e. V.
Franciscans International
Free Expression Myanmar (FEM)
Fundació. Cat
Fundación Acceso (Central America)
Fundación Datos Protegidos
Fundación InternetBolivia.org
Fundación Karisma (Colombia)
Global Partners Digital
Global Voices
Global Witness
GlobaLeaks
Guardian Project
Gulf Centre for Human Rights (GCHR)
Health, Ethics and Law Institute of Forum for Medical Ethics Society, India
Heartland Initiative
Hermes Center
Hiperderecho (Perú)
Hivos
Homo Digitalis
Horizontal
Human Rights Commission of Pakistan
Human Rights First
Human Rights House Foundation (HRHF)
IFEX
IFEX-ALC
Iniciativa Mesoamericana de Mujeres Defensoras de Derechos Humanos (IM-Defensoras)
INSM Network (Iraq)
Institute for Policy Research and Advocacy (ELSAM), Indonesia
Instituto para la Sociedad de la Información y 4ta Revolución Industrial (ISICRI) de Perú
International Commission of Jurists (ICJ)
International Corporate Accountability Roundtable
International Legal Initiative

International Service for Human Rights
Internet Freedom Foundation, India
Internet Protection Society (Russia)
IPANDETEC Centroamérica
Jordan Open Source Association (JOSA)
Justice for Iran
Kijiji Yeetu, Kenya
Liga voor de Rechten van de Mens (LvRM), The Netherlands
Ligue des droits humains, Belgium
Masaar -Technology and Law Community
Media Foundation for West Africa (MFWA)
MediaNama, India
Meedan
Mnemonic
Nothing2Hide
ONG Acción Constitucional
OpenArchive
Ordem dos Advogados do Brasil (OAB)
Panoptikon Foundation
Paradigm Initiative (PIN)
PDX Privacy
PEN America
PEN International
PEN Iraq
Planet Ally
Privacy International (PI)
Protection International (PI)
Punjab Women Collective
Ranking Digital Rights (RDR)
Red de Desarrollo Sostenible Honduras
Red en Defensa de los Derechos Digitales (R3D)
Reporters Sans Frontières / Reporters Without Borders (RSF)
Rethink Aadhaar
Robert F. Kennedy Human Rights
Roskomsvoboda (Russia)
S. T. O. P. - The Surveillance Technology Oversight Project
Security First
Seguridad en Democracia (SEDEM)
Sin Olvido
Sin Olvido Verde
SMEX
Southeast Asia Freedom of Expression Network (SAFENet)
Statewatch
Sursiendo, Comunicación y Cultura Digital
TEDIC NGO
Tejiendo Redes Infancia en América Latina y el Caribe
Terra-1530
The Bachchao Project (TBP)
The Humanism Project
The London Story, The Netherlands
Ubunteam
Universidad de Paz

Ura Design
Urgent Action Fund for Women's Human Rights (UAF)
Wikimedia France
Women's International League for Peace and Freedom (WILPF)
World Organisation Against Torture (OMCT)
Xnet

Expertos/as independientes

Alex Orué, activista LGBTQ+ y digital, México
Alex Raufoglu, Washington D. C., EE. UU.
Alexandra Argüelles (beneficiaria del programa de becas de Mozilla)
Arzu Geybulla (Azerbaijan Internet Watch)
Chip Pitts, experto independiente
David Kaye, profesor clínico de derecho de la Facultad de Derecho de la Universidad de California en Irvine y antiguo relator especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión
Douwe Korff, profesor emérito de derecho internacional de la Universidad Metropolitana de Londres
Dra. Courtney Radsch
Dr. Koldo Casla, profesor de la Facultad de Derecho y del Centro de Derechos Humanos de la Universidad de Essex
Dra. Tara Van Ho, profesora de la Facultad de Derecho y del Centro de Derechos Humanos de la Universidad de Essex
Elies Campo, Telegram Messenger
Elio Qoshi (Ura Design)
Giorgio Maone (NoScript)
Hannah R. Garry, profesora clínica de derecho y directora del Consultorio Internacional de Derechos Humanos de la Universidad de Carolina del Sur
Jennifer Green, profesora clínica de derecho de la Facultad de Derecho de la Universidad de Minnesota
John Scott-Railton, investigador principal del Citizen Lab de la escuela Munk de relaciones internacionales y política pública de la Universidad de Toronto
Kenneth Harrow, especialista de país (Ruanda), Amnistía Internacional EE. UU.
Kiran Jonnalagadda, Hasgeek
Kushal Das, especialista en tecnología de interés público, Freedom of the Press Foundation, director de Python Software Foundation
Marietje Schaake, presidenta del CyberPeace Institute
Nikhil Pahwa, MediaNama
Rebecca MacKinnon, cofundadora de Global Voices
Ritumbra Manuvie, Universidad de Groningen
Ron Deibert, profesor de ciencias políticas y director del Citizen Lab de la escuela Munk de relaciones internacionales y política pública de la Universidad de Toronto
Susan Farrell (OTF AC)
Tarcizio Silva (beneficiario del programa de becas de Mozilla)