Gemeinsamer Offener Brief zivilgesellschaftlicher Organisationen und unabhängiger Experten mit dem Aufruf an Staaten, ein sofortiges Moratorium für den Verkauf, die Weitergabe und den Einsatz von Überwachungstechnologie zu verhängen und umzusetzen.

Wir, die unterzeichnenden zivilgesellschaftlichen Organisationen und unabhängigen Experteninnen und Experten, sind besorgt angesichts der Medienenthüllungen, wonach die Spionagesoftware der NSO Group eingesetzt wurde, um Menschenrechtsverletzungen in massivem Ausmaß auf der ganzen Welt zu ermöglichen.

Diese Enthüllungen sind ein Ergebnis des Pegasus-Projekts und beruhen auf den geleakten 50.000 Telefonnummern potenzieller Überwachungsziele. Die Recherchen sind ein Gemeinschaftsprojekt von über 80 Journalistinnen und Journalisten aus 16 Medienorganisationen in zehn Ländern, koordiniert von Forbidden Stories, einer in Paris ansässigen gemeinnützigen Medienorganisation, mit technischer Unterstützung von Amnesty International, die forensische Tests an Mobiltelefonen durchführten, um Spuren der Pegasus-Überwachungssoftware zu identifizieren.
Diese Enthüllungen widerlegen alle Behauptungen von NSO, solche Angriffe seien selten oder ungewöhnlich oder auf eine böswillige Nutzung ihrer Technologie zurückzuführen. Zwar behauptet das Unternehmen, seine Spyware werde nur für rechtmäßige Ermittlungen zur Kriminalitäts- und Terrorismusbekämpfung verwendet, doch ist klar, dass die Technologie systemischen Missbrauch ermöglicht. So sagte die UN-Hochkommissarin für Menschenrechte: „Wenn die jüngsten Anschuldigungen über den Einsatz von Pegasus auch nur teilweise wahr sind, dann wurde diese rote Linie wieder und wieder völlig straffrei überschritten."

Anhand der geleakten Daten und ihrer Recherchen konnten Forbidden Stories und seine Medienpartner potenzielle NSO-Kunden in elf Ländern identifizieren: Aserbaidschan, Bahrain, Ungarn, Indien, Kasachstan, Mexiko, Marokko, Ruanda, Saudi-Arabien, Togo und die Vereinigten Arabischen Emirate (VAE). NSO behauptet, es verkaufe nur an staatliche Stellen.

Die Untersuchung hat bislang zudem mindestens 180 Medienvertreterinnen und -Vertreter in 20 Ländern identifiziert, die zwischen 2016 und Juni 2021 als potenzielle Ziele für die NSO-Überwachungssoftware ausgewählt wurden. Zu den nun bekannt gewordenen, zutiefst beunruhigenden Details gehören Belege dafür, dass Familienmitglieder des saudischen Journalisten **Jamal Khashoggi** vor und nach seiner Ermordung in Istanbul am 2. Oktober 2018 von saudischen Agenten mit der Pegasus-Software angegriffen wurden, obwohl die NSO Group den Einsatz ihrer Produkte in Zusammenhang mit Khashoggi und seinen Familienmitgliedern wiederholt bestritten hat.

Die Enthüllungen sind nur die Spitze des Eisbergs. Die private Überwachungsindustrie konnte ungehindert schalten und walten. Staaten haben es nicht nur versäumt, ihren Pflichten zum Schutz vor diesen Menschenrechtsverstößen nachzukommen, sondern sie haben auch gegen ihre eigenen Menschenrechtsverpflichtungen verstoßen und diese invasiven Waffen auf Menschen weltweit losgelassen, die nur ihre Menschenrechte ausgeübt haben. Außerdem stellen die gezielten Angriffe möglicherweise nur einen Bruchteil der durch sie erfolgten Menschenrechtsverstöße dar. Denn Verletzungen des Rechts auf Privatsphäre wirken sich

auf zahlreiche andere Menschenrechte aus und zeigen den realen Schaden, der durch eine mit internationalen Normen unvereinbare Überwachung entsteht.

In Mexiko wurde das Telefon des Journalisten **Cecilio Pineda** nur wenige Wochen vor seiner Ermordung im Jahr 2017 angegriffen. Auch in Aserbaidschan kam Pegasus zum Einsatz, einem Land, in dem es nur noch wenige unabhängige Medien gibt. Wie das Security Lab von Amnesty International herausfand, war das Telefon von **Sevinc Vaqifqizi**, einer freien Journalistin für das unabhängige Medienunternehmen *Meydan TV*, über einen Zeitraum von zwei Jahren bis Mai 2021 infiziert. In Indien wurden zwischen 2017 und 2021 mindestens 40 Journalistinnen und Journalisten von großen Medienunternehmen des Landes als potenzielle Zielpersonen ausgewählt. Forensische Tests ergaben, dass die Telefone von **Siddharth Varadarajan** und **MK Venu**, Mitbegründer der unabhängigen Nachrichtenwebsite *The Wire*, erst im Juni 2021 mit Pegasus-Spyware infiziert wurden. Inmitten dieser Enthüllungen wurde der marokkanische Journalist und Menschenrechtsaktivist **Omar Radi** am Montag zu sechs Jahren Gefängnis verurteilt. Radis Telefon war zuvor von Amnesty International forensisch untersucht worden; die Organisation hatte dabei die Installation von Pegasus festgestellt. In Marokko sind von den 34 weiteren Journalisten, deren Telefone mit Pegasus infiziert wurden, zwei inhaftiert, andere sind nach Frankreich übersiedelt. Die Untersuchung ergab zudem, dass Journalisten, die für große internationale Medien wie *Associated Press, CNN, The New York Times* und *Reuters* arbeiten, potenzielle Ziele waren. Eine der prominentesten Journalistinnen war **Roula Khalaf**, die Chefredakteurin der *Financial Times*. Diese betroffenen Personen stellen nur einen kleinen Teil der Enthüllungen dar, ein vollständiges Bild des Ausmaßes werden wir uns erst im Laufe der Zeit machen können.

Es ist nicht das erste Mal, dass die Pegasus-Software von NSO mit Menschenrechtsverletzungen in Verbindung gebracht wird. Forscherinnen, Journalisten, Aktivistinnen und andere haben im Laufe der Jahre zahlreiche Beweise für den Einsatz der Technologie der NSO Group zur Überwachung von Personen aufgedeckt. **Ahmed Mansoor**, ein in den Vereinigten Arabischen Emiraten inhaftierter Menschenrechtsverteidiger, wurde 2016 mit Technologie der NSO Group überwacht. Auch in Mexiko gerieten bereits Journalisten, Anwältinnen und Experten des öffentlichen Gesundheitswesens ins Visier.

Wo Überwachung ohne angemessene rechtliche Rahmenbedingungen, Aufsicht, Schutzmaßnahmen und Transparenz betrieben wird, wirkt sich der Schaden weit über die tatsächlich ins Visier genommenen Personen aus. Angesichts von Intransparenz und unzureichenden Schutzmaßnahmen und insbesondere in Situationen, in denen bekannt ist oder vermutet wird, dass die Überwachung auf rechtswidrige Weise erfolgt, sind Menschenrechtsverteidiger und Journalistinnen zur Selbstzensur gezwungen, um nicht für ihre Arbeit verfolgt zu werden, selbst wenn eine solche Überwachung in Wirklichkeit gar nicht stattfindet. Unmittelbar nach den Enthüllungen bemerken Journalistinnen und Aktivisten bereits die lähmende Wirkung auf ihre Arbeit.

Der Einsatz von gezielten digitalen Überwachungsinstrumenten wie Pegasus verletzt das Recht auf Privatsphäre und viele andere Rechte in entscheidender Weise. Pegasus hat schon allein aufgrund seiner Konzeption Auswirkungen auf das Recht auf Privatsphäre: Es wird heimlich eingeschleust, ohne das Wissen des Rechteinhabers eingesetzt und ist in der Lage, eine unbegrenzte Auswahl an persönlichen, privaten Daten zu sammeln und zu übermitteln (zusammen mit den Daten aller Kontakte, mit denen eine Zielperson interagiert). Darüber

hinaus kann, wie oben erwähnt, eine Verletzung des Rechts auf Privatsphäre Kaskadeneffekte auf andere Rechte haben, darunter das Recht auf freie Meinungsäußerung, das Recht auf Vereinigungsfreiheit und das Recht auf friedliche Versammlung. Die Enthüllungen haben gezeigt, dass die Verwendung der Software missbräuchlich und willkürlich ist und keinen zulässigen Eingriff in das Recht auf Privatsphäre darstellt. Darüber hinaus erfüllt der unkontrollierte Einsatz dieser Werkzeuge durch Staaten nicht die Kriterien der Notwendigkeit, der Verhältnismäßigkeit und des legitimen Ziels, wie sie in den internationalen Standards dargelegt sind.

Speziell bei der gezielten digitalen Überwachung hat sich eine Kultur der Straflosigkeit entwickelt, der dringend entgegengewirkt werden muss. Wie die Enthüllungen zeigen, ist der staatliche Einsatz gezielter digitaler Überwachungsinstrumente, die von einem der prominentesten Branchenteilnehmer bereitgestellt werden, völlig außer Kontrolle geraten, wirkt destabilisierend und bedroht die Menschenrechte des und der Einzelnen, einschließlich des Rechts auf körperliche Unversehrtheit. Die Enthüllungen werfen ein Licht auf eine niemandem Rechenschaft schuldige Industrie und eine niemandem Rechenschaft schuldige Sphäre staatlicher Praxis, die in ihrer jetzigen Form nicht weiter betrieben werden darf. Unsere Rechte und die Sicherheit des digitalen Ökosystems als Ganzes hängen davon ab.

Wir unterstützen die Forderung der UN-Hochkommissarin, dass „Regierungen ihren Einsatz von Überwachungstechnologien in menschenrechtsverletzender Weise sofort einstellen und konkrete Maßnahmen zum Schutz vor solchen Eingriffen in die Privatsphäre ergreifen sollten, indem sie die Verbreitung, den Einsatz und den Export von Überwachungstechnologien, die von anderen geschaffen wurden, regulieren."

Wir fordern daher alle Staaten auf, dringend die folgenden Schritte zu unternehmen:

An alle Staaten:
a. unverzüglich ein Moratorium für den Verkauf, die Weitergabe und den Einsatz von Überwachungstechnologie in Kraft zu setzen. Angesichts des Umfangs und des Ausmaßes der gewonnenen Erkenntnisse ist es dringend notwendig, die von Überwachungstechnologie gestützten Aktivitäten aller Staaten und Unternehmen zu stoppen, bis die Bemühungen zur Regulierung der Menschenrechte aufgeholt haben.

b. eine sofortige, unabhängige, transparente und unparteiische Untersuchung von Fällen gezielter Überwachung durchzuführen. Zu überprüfen sind außerdem die für gezielte Überwachungstechnologie erteilten Exportlizenzen. Alle Vermarktungs- und Exportlizenzen in Situationen, in denen die Menschenrechte gefährdet sind, müssen widerrufen werden.

c. einen gesetzlichen Rahmen zu verabschieden und durchzusetzen, der private Überwachungsunternehmen und ihre Investoren dazu verpflichtet, bei ihren globalen Aktivitäten, Lieferketten und in Bezug auf die Endnutzung ihrer Produkte und Dienstleistungen menschenrechtliche Sorgfaltsprüfungen durchzuführen. Im Rahmen dieser Gesetzgebung sollten private Überwachungsunternehmen dazu verpflichtet werden, die menschenrechtsbezogenen Risiken ihrer Aktivitäten und Geschäftsbeziehungen zu identifizieren, ihnen vorzubeugen und sie zu mindern.

d. einen Rechtsrahmen zu verabschieden und durchzusetzen, der private Überwachungsunternehmen zu Transparenz verpflichtet. Unter anderem sollten sie Informationen über die Selbstidentifizierung/Registrierung, die angebotenen Produkte und Dienstleistungen und die Ergebnisse regelmäßiger Sorgfaltsprüfungen liefern, darunter auch detaillierte Informationen darüber, wie sie den identifizierten Risiken und tatsächlichen Auswirkungen begegnen, Informationen über getätigte Verkäufe sowie über potenzielle Kunden, die aufgrund fehlender Einhaltung von Menschenrechtsstandards oder fehlender Einhaltung der Standards guter Unternehmensführung abgelehnt wurden. Staaten sollten diese Informationen in öffentlichen Registern zur Verfügung stellen.

e. sicherzustellen, dass alle in ihnen ansässigen Überwachungsunternehmen, einschließlich Verkaufsvermittler, Tochterunternehmen, Holdinggesellschaften und Private-Equity-Eigentümer, zu verantwortungsvollem Handeln verpflichtet und für ihre negativen Auswirkungen auf die Menschenrechte haftbar gemacht werden. Diese Unternehmen müssen gesetzlich dazu verpflichtet werden, Maßnahmen zur menschenrechtlichen Sorgfaltspflicht in Bezug auf ihre weltweiten Aktivitäten zu ergreifen. Dies sollte die Haftung für verursachte Schäden und den Zugang zu Rechtsmitteln für betroffene Personen und Gemeinschaften in den Heimatländern der Unternehmen beinhalten. Regierungen sollten daher innerstaatliche Vorschläge für Gesetze zur Rechenschaftspflicht von Unternehmen initiieren oder unterstützen.

f. Informationen über alle früheren, aktuellen und zukünftigen Verträge mit privaten Überwachungsfirmen durch die Beantwortung von Informationsanfragen oder durch proaktive Auskünfte offenzulegen.

g. als Bedingung für den fortgesetzten Betrieb von Überwachungsfirmen die sofortige Einrichtung unabhängiger Multi-Stakeholder-Aufsichtsgremien für die NSO Group und alle anderen privaten Überwachungsfirmen zu fordern. Menschenrechtsgruppen und andere Akteurinnen und Akteure der Zivilgesellschaft sollten Teil dieser Gremien sein.

h. gemeinschaftliche öffentliche Aufsichtsgremien zur Überwachung und Genehmigung des Erwerbs oder der Nutzung neuer Überwachungstechnologien einzurichten, die befugt sind, auf der Grundlage der Menschenrechtsverpflichtungen von Staaten Bestimmungen zur öffentlichen Bekanntmachung und Berichterstattung zu genehmigen oder abzulehnen.

i. die bestehenden Gesetze, die Rechtsmittel für die Opfer rechtswidriger Überwachung behindern, zu reformieren; außerdem muss sichergestellt werden, dass in der Praxis sowohl gerichtliche als auch außergerichtliche Wege der Abhilfe zur Verfügung stehen.

j. Darüber hinaus müssen Staaten mindestens die folgenden Empfehlungen umsetzen, wenn das Moratorium für den Verkauf und die Weitergabe von Überwachungsausrüstung aufgehoben werden soll:

- Umsetzung nationaler Gesetze, die Schutzmaßnahmen gegen Menschenrechtsverletzungen und Fälle von Missbrauch durch digitale Überwachung und Rechenschaftsmechanismen vorsehen, welche Opfern von Überwachungsmissbrauch einen Weg der Abhilfe bieten.
- Umsetzung von Beschaffungsstandards, die staatliche Aufträge für Überwachungstechnologie und -dienstleistungen nur an solche Unternehmen

vergeben, die nachweislich die Menschenrechte im Einklang mit den UN-Leitprinzipien respektieren und keine Dienstleistungen für Kunden erbracht haben, die an Überwachungsmissbrauch beteiligt waren.
- Beteiligung an wichtigen multilateralen Bemühungen zur Entwicklung robuster Menschenrechtsstandards, die die Entwicklung, den Verkauf und die Weitergabe von Überwachungstechnik regeln und unzulässige Ziele der digitalen Überwachung identifizieren.

k. Wertpapierbörsen und Finanzaufsichtsbehörden über die mit privaten Überwachungstechnologieunternehmen verbundenen Schäden zu informieren. Eine strenge, regelmäßige Prüfung der Offenlegungen und Anwendungen dieser Unternehmen und ihrer Eigentümer ist gesetzlich und regulatorisch vorzuschreiben, unter anderem vor allen größeren Ereignissen (Börsengänge, Fusionen, Übernahmen usw.).

l. eine starke Verschlüsselung, eine der besten Verteidigungsmaßnahmen gegen invasive Überwachung, zu schützen und zu fördern.

Wir fordern Israel, Bulgarien und Zypern und alle anderen Staaten, in denen NSO eine Firmenpräsenz hat, auf:
a. Exportierende Staaten, darunter Israel, Zypern und Bulgarien, müssen sofort alle Marketing- und Exportlizenzen widerrufen, die der NSO Group und ihren Unternehmen erteilt wurden, und eine unabhängige, unparteiische, transparente Untersuchung durchführen, um das Ausmaß der unrechtmäßigen Überwachung festzustellen. Am Ende dieser Untersuchung muss eine öffentliche Erklärung über die Ergebnisse der Bemühungen und Schritte zur Verhinderung zukünftigen Schadens stehen.

Unterzeichnende

Zivilgesellschaftliche Organisationen

#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)
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, Russland
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 Mexicana de Defensa y Promoción de los Derechos Humanos
Committee to Protect Journalists (CPJ)
Conectas Direitos Humanos
Conectas Human Rights
Conexo
Cooperativa Tierra Común, Mexiko
CyberPeace Institute
Data Privacy Brasil Research Association
Deache
Defense for Children International, Palästina
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
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, Kolumbien
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, Indien
Heartland Initiative
Hermes Center
Hiperderecho, Peru
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, Irak
Institute for Policy Research and Advocacy (ELSAM), Indonesien
Instituto para la Sociedad de la Información y 4ta Revolución Industrial (ISICRI) de Perú
International Corporate Accountability Roundtable
International Legal Initiative
International Service for Human Rights
Internet Freedom Foundation, Indien
Internet Protection Society, Russland
IPANDETEC Centroamérica
Jordan Open Source Association (JOSA)
Justice for Iran
Kijiji Yeetu, Kenia
Liga voor de Rechten van de Mens (LvRM), Niederlande
Ligue des droits humains, Belgien
Masaar – Technology and Law Community
Media Foundation for West Africa (MFWA)
MediaNama, India
Meedan
Nothing2Hide
ONG Acción Constitucional
OpenArchive
Paradigm Initiative (PIN)
PDX Privacy
PEN America
PEN International
Pen Iraq
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, Russland
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

Unabhängige Expertinnen und Experten

Alex Orué, LGBTQ- und Digital-Aktivist, Mexiko
Alex Raufoglu, Washington D.C, USA
Alexandra Argüelles (Mozilla-Mitarbeiterin)
Arzu Geybulla (Azerbaijan Internet Watch)
Chip Pitts, unabhängiger Experte
David Kaye, Rechtswissenschaftler an der UC Irvine School of Law und ehemaliger Sonderberichterstatter der Vereinten Nationen für die Förderung und den Schutz des Rechts auf Meinungsfreiheit
Douwe Korff, emeritierter Professor für internationales Recht, London Metropolitan University
Dr. Courtney Radsch
Dr. Koldo Casla, Dozent, University of Essex School of Law and Human Rights Centre
Dr. Tara Van Ho, Dozentin, University of Essex School of Law and Human Rights Centre

Elies Campo, Telegram Messenger
Elio Qoshi (Ura Design)
Arbeitsgruppe für Reflexion, Forschung und Kommunikation der Compañía de Jesús in Honduras
Juristisches Büro für Menschenrechte (Honduras)
Giorgio Maone (NoScript)
Hannah R. Garry, Rechtswissenschaftlerin, Direktorin, USC International Human Rights Clinic
Jennifer Green, Klinische Professorin für Jura, University of Minnesota Law School
John Scott-Railton, Leitender Wissenschaftler, Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy
Kenneth Harrow, Ruanda-Experte, Amnesty International USA
Kiran Jonnalagadda, Hasgeek
Kushal Das, Technologie-Experte, Freedom of the Press Foundation, Direktor der Python Software Foundation
Marietje Schaake, Präsidentin CyberPeace Institute
Nikhil Pahwa, MediaNama
Rebecca MacKinnon, Mitbegründer Global Voices
Ritumbra Manuvie, University of Groningen
Ron Deibert, Professor für Politikwissenschaften und Direktor des Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy
Susan Farrell (OTF AC)
Tarcizio Silva (Mozilla-Mitarbeiter)