Paolo Cirio, *Iris*, 2021. Cortesía del artista

TODO PUEDE SER VULNERADO: EL ESPIONAJE A DEFENSORES DE DERECHOS HUMANOS

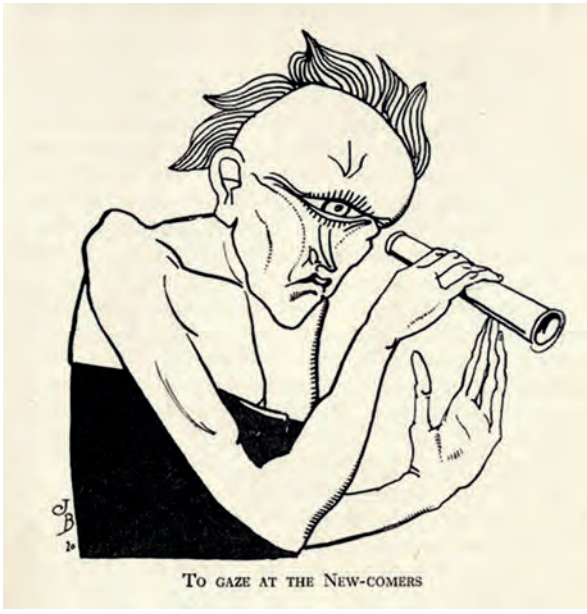
Jair Ortega de la Sancha

El viernes 20 de mayo de 2016, Santiago Aguirre, entonces subdirector del Centro Prodh —asociación civil fundada en 1988 por la Compañía de Jesús, dedicada a la promoción y la defensa de los derechos humanos en México—, recibió el primero de varios mensajes SMS en su teléfono celular: "SrJorge soy Juan Magarino ayuda con mi hermano Heriberto se lo llevo la policia por ser maestro es un delito..." [sic].

Santiago leyó el mensaje y se dio cuenta de que lo acompañaba un *link*. Cinco días antes, el 15 de mayo, el Centro Prodh se había pronunciado en contra de la liberación de tres militares involucrados en la ejecución extrajudicial de veintiún jóvenes en una bodega del municipio mexiquense de Tlatlaya.

***

Meses después, el 10 de agosto de 2016, el defensor de derechos humanos radicado en Emiratos Árabes Unidos, Ahmed Mansoor, abrió su iPhone 6 y leyó dos mensajes de texto que le ofrecían información sobre personas detenidas y torturadas en prisiones de ese país árabe. Ambos mensajes contenían un enlace de donde obtendría la información. En lugar de dar clic, Mansoor solicitó ayuda a investigadores de seguridad cibernética, entre los que se encontraba el Citizen Lab de la Universidad de Toronto, un grupo interdisciplinario que estudia controles de información, vigilancia en la red y filtración de contenido, que impactan la apertura y seguridad de internet.



Jean de Boschère, *Islas extrañas*, 1921.
California Digital Library ©

Gracias a ese acercamiento, los investigadores del laboratorio identificaron el método de infección de Pegasus,[1] el *software* espía (*spyware*) fabricado por la empresa israelí NSO Group. Para acceder a un dispositivo, se enviaba un mensaje SMS con un enlace malicioso a la posible víctima. El contenido del texto era persuasivo: el objetivo era que la persona abriera el enlace adjunto. Al dar clic, el programa redirigía al dispositivo a alguno de los dominios pertenecientes a la infraestructura de la compañía tecnológica, que suplantaba la identidad de sitios web de noticias, redes sociales e incluso páginas gubernamentales.

En ese momento el dispositivo quedaba infectado y se podría extraer todo lo que contenía. Todo. Cualquier mensaje de texto, correo, video o fotografía, así como las búsquedas en internet. La tecnología de Pegasus también puede activar la cámara del teléfono, escuchar a través del micrófono y grabar las pulsaciones del teclado, incluso en aplicaciones cifradas.

***

"Buen día Mtro. trabajo en mi tesis, tome como base su tesina, me interesa su opinion, le mando los adelantos" [sic]. El 28 de junio de 2016, Santiago recibió otro mensaje con un enlace extraño. Era el tercero. Veinte días antes, el 8 de junio, había recibido uno muy parecido: "Mtro, tuve un incidente, le envio nuevamente mi tesis, basada en su tesina para que me de su comentarios..." [sic].

El abogado y especialista en derechos humanos Santiago Aguirre trabajaba también como profesor en la Universidad Iberoamericana y cada tanto los alumnos le pedían que leyera sus trabajos. "Eso me llevó a dar clic en el mensaje, que me dirigió a una infraestructura de internet que estaba caída. No tenía más elementos para pensar que fuera algún tipo de ataque digital", dice, casi ocho años después, una tarde de mayo de 2024.

Este ataque no fue casual, el espionaje nunca es azaroso; lo demuestran investigaciones como *Gobierno espía*, realizada por la R3D (Red en Defensa de los Derechos Digitales), Artículo 19 y SocialTIC, donde se menciona que el caso de Santiago sucedió dos días antes del segundo aniversario de la masacre de Tlatlaya. Leopoldo Maldonado, director regional para México y Centroamérica de Artículo 19, me explica que estos ataques "surgen en contextos específicos, donde se involucra a las Fuerzas Armadas o se trastocan sus intereses". Me cita un ejemplo: "El activista Raymundo Ramos fue espiado mientras estaba investigando sobre unas ejecuciones extrajudiciales cometidas contra unos jóvenes en 2020, en Tamaulipas".

[1] Bill Marczak y John Scott-Railton, "The Million Dollar Dissident", Citizen Lab, 24 de agosto de 2016. Disponible en acortar.link/q3Z9HG.

Cuando Israel le vende cibervigilancia a un país africano, se aseguran su voto en Naciones Unidas.

Poco después de la infección, le avisaron a Santiago que una de sus llamadas con un padre de los estudiantes desaparecidos de Ayotzinapa se había publicado a través de un perfil falso de Facebook. Dentro del Centro Prodh comenzaron las sospechas de un posible espionaje: "En ese momento a mí me parecía difícil pensar que alguna instancia el Estado se hubiese tomado la molestia de mandar un mensaje de texto con información personalizada que te iba a hacer *clickear* para después vulnerar el teléfono. La primera reacción fue esa: incredulidad", recuerda Aguirre, quien ahora es director del Centro Prodh.

Pero luego del peritaje de Citizen Lab, Santiago comprendió cómo ocurría la infección y cuáles eran sus consecuencias: "Simplemente el hecho de pensar que fotografías del ámbito familiar no estén bajo tu control, y estén en manos de personas con quién sabe qué intención, te hace sentir muy vulnerable".

Otra preocupación que surge entre quienes descubren que el Estado los espía es que sus agentes tomen información personal para sacarla de contexto y atacar en público a sus blancos. "Todos tenemos nuestras vidas, intentamos que la brecha entre lo que hacemos y lo que decimos sea corta, pero somos personas con zonas de claroscuros, hemos cometido errores, nos hemos equivocado. Y pensar que esas cosas de las que te sientes menos orgulloso puedan ser expuestas para deslegitimar el trabajo que hace tu organización, para deslegitimar lo que en público defiendes, hace sentir temor, mucho temor", dice Santiago.

***

Shalev Hulio y Omri Lavie fundaron NSO Group en 2010. En su libro *El laboratorio palestino: cómo Israel exporta la tecnología de la ocupación* (2024), el periodista Antony Loewenstein describe a estos dos emprendedores israelíes como "amigos del colegio que habían entrado en el mundo de las *startups* tecnológicas en la década del 2000 y que no tardaron en darse cuenta del potencial de desarrollar una herramienta que pudiera penetrar un móvil sin ser detectada". Poco después de la fundación de la compañía, se les unió Niv Karmi, antiguo miembro del Mossad y agente de inteligencia militar. No era el único con ese pasado. A inicios del siglo XXI, Hulio dirigió operaciones de las Fuerzas de Defensa de Israel en Cisjordania. Lavie también fue agente del cuerpo de inteligencia del ejército de su país.

En el capítulo del libro titulado "Vigilancia masiva israelí en el cerebro de tu teléfono", Loewenstein explica que desde hace más de una década el gobierno del primer ministro Benjamín Netanyahu y la empresa tecnológica NSO Group han impulsado la venta de su tecnología de vigilancia como parte de su estrategia de política exterior: "Amitai Ziv, periodista especializado en tecnología que escribía en *Haaretz* [periódico israelí] y responsable de parte de la investigación más esclarecedora para destapar a NSO Group, me contó que el poder de [esta compañía] no reside en el dinero, sino en la diplomacia: 'Cuando Israel le vende cibervigilancia a un país africano, se aseguran su voto en Naciones Unidas. Desde que existe la ocupación, necesitamos los votos'".

Sucede con países como Hungría, India, Polonia, Arabia Saudita y, por supuesto, México, el primer y más exitoso campo de prueba internacional. Según los investigadores de Citizen Lab, México es el país al que más dominios falsos dedicó la infraestructura de NSO

Stanisław Ignacy Witkiewicz, *Múltiples autorretratos en espejo*, *ca*. 1917 ©

Group. Este dato se corroboró en abril de 2023, con una investigación de *The New York Times* que reveló que el Ejército mexicano es el cliente más antiguo de Pegasus y el que "ha atacado más teléfonos móviles con ese programa malicioso que cualquier otra agencia gubernamental del mundo".[2] La Secretaría de Defensa Nacional (Sedena) adquirió el programa espía durante el sexenio de Felipe Calderón, también lo hicieron la Procuraduría General de la República y el Centro de Investigación y Seguridad Nacional, hoy Centro Nacional de Inteligencia. A partir de documentos filtrados, se sabe que las licencias de la Sedena se han renovado en las administraciones de Enrique Peña Nieto y Andrés Manuel López Obrador.

[2] Natalie Kitroeff y Ronen Bergman, "Cómo México se convirtió en el mayor usuario del programa de espionaje más conocido del mundo", *The New York Times*, 18 de abril de 2023. Disponible en acortar.link/q41J9I.

Luego de haber comprobado su efectividad, el uso de Pegasus se extendió a gobiernos de todo el mundo. La tecnología de vigilancia israelí dio y continúa dando poder a Estados autoritarios para que espíen a reporteros y activistas mientras garantiza el silencio internacional ante la masacre palestina. Uno de los teléfonos de Jamal Khashoggi, periodista asesinado en noviembre de 2018 por el gobierno de Arabia Saudita en el consulado saudí en Estambul, estaba infectado con Pegasus. Tres años después se descubrió que también lo estaban dos dispositivos de la defensora saharaui de derechos humanos Aminatou Haidar. El teléfono del periodista mexicano Cecilio Pineda fue infectado con el programa israelí semanas antes de su asesinato, en marzo 2017 en el estado de Guerrero. Son algunos de los casos conocidos, algunos de los más terribles; no los únicos.

Con el paso de los años, esta clase de espionaje se ha refinado y es difícil identificar víctimas sin un peritaje realizado por especialistas. Pepe Flores, integrante de R3D, me explica en entrevista que "el método de infección de Pegasus ha evolucionado. Hace ocho, nueve años [se limitaba a] enviar un mensaje SMS para dar un clic y que en ese momento se activara el *malware*. Ya es más sofisticado, tienen una tecnología que se llama *cero clics*, es decir, entra directo". Esta evolución convierte a la tecnología de NSO Group en imperceptible porque "solo se puede identificar una vez ocurrida la infección. Antes, más o menos se podía prevenir si tú no habías dado clic al *link* malicioso", dice Flores.

siguiente declaración suya se encuentra en *El laboratorio palestino*: "gracias a la tecnología de vigilancia [...], hoy en día puedes identificar y vigilar al próximo Nelson Mandela incluso antes de que él mismo sepa que es Nelson Mandela".

***

El 15 de diciembre de 2022, Santiago Aguirre y María Luisa Aguilar, coordinadora del Área Internacional del Centro Prodh, estaban trabajando en las oficinas de su organización, en la Ciudad de México, cuando recibieron mensajes en sus teléfonos celulares. En la pantalla se leía: "Apple cree que estás siendo objetivo de atacantes patrocinados por el Estado

El poder que tienen las tecnologías de espionaje y sus consecuencias nocivas para las democracias del mundo son innegables.

NSO Group se ha negado a cooperar en investigaciones judiciales sobre el uso ilegal de su *software* con el argumento de que la información de sus clientes es confidencial. Algunos ejemplos de estas negativas a entregar información son el caso mexicano y el del político Pedro Sánchez, presidente del Gobierno de España.[3]

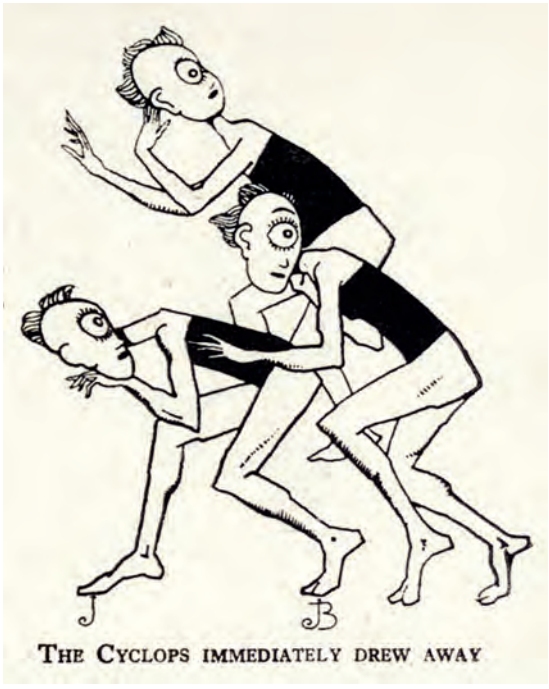
El poder que tienen las tecnologías de espionaje y sus consecuencias nocivas para las democracias del mundo son innegables. Quizá nadie lo ha expresado mejor que Eitay Mack, abogado y activista israelí por los derechos humanos, que desde hace años busca que se cancele la licencia de exportación de NSO. La

que están intentando comprometer remotamente el iPhone asociado a tu Apple ID".

Su reacción inmediata fue de angustia y preocupación; pero también sentían decepción, molestia: "Fue una expresión más de que no estaban ocurriendo en este sexenio los cambios que creíamos que podrían ser posibles", dice Santiago. Dos meses antes del mensaje que recibieron él y María Luisa, el presidente López Obrador negó que en su gobierno existieran labores de espionaje: "no es cierto que se espíe a periodistas o a opositores. No somos iguales a los anteriores [...]. Yo hice el compromiso de que nadie iba a ser espiado, ningún opositor. Si tienen pruebas que las presenten", dijo en la mañanera del 4 de octubre de 2022.

Las pruebas se presentaron. Organizaciones como R3D y Artículo 19 publicaron investigaciones sobre casos como el del activista

[3] "Spain's High Court shelves Israeli spyware probe on lack of cooperation", *Reuters*, 10 de julio de 2023. Disponible en acortar.link/Se6lo9.



Jean de Boschère, *Islas extrañas*, 1921.
California Digital Library ©

Raymundo Ramos; y el nuevo análisis forense que Citizen Lab realizó en los equipos de Santiago y María Luisa demostró que las infecciones ocurrieron entre junio y septiembre de 2022. El primer ataque contra Santiago ocurrió el miércoles 22 de junio, la fecha en que víctimas y familiares de víctimas de violaciones a derechos humanos cometidas por el ejército en la Guerra Sucia (varios de ellos reciben acompañamiento del Centro Prodh) realizaron una protesta durante un evento de la Comisión para la Verdad y Justicia por los Hechos 1965-1990 en el Campo Militar Número Uno, en la Ciudad de México. Al día siguiente también se infectó el dispositivo de María Luisa Aguilar.

Pese al temor de saber que tienen acceso a sus archivos personales, María Luisa me explica, en entrevista en las oficinas del Centro Prodh, que como defensores de derechos humanos también sienten una fuerte preocupación porque se vulnera nuevamente a las víctimas: "Obviamente está la parte de la vida privada, pero hay otra igual de importante: la información que tenemos sobre nuestro trabajo, sobre las personas a las que acompañamos. Nuestros acompañamientos se hacen desde la Ciudad de México a personas que están en condiciones muy remotas. Pienso, por ejemplo, en las propias familias de los estudiantes de Ayotzinapa. Es muy difícil encontrar otras vías de comunicación que no sean la llamada por teléfono o el mensajito de WhatsApp cuando tienen acceso a internet satelital".

***

Centro Militar de Inteligencia (CMI). Se sabe que existe por la filtración de documentos del colectivo Guacamaya. Opera en un búnker en el Campo Militar Número Uno. En entrevista, Leopoldo Maldonado me dice quiénes operan actualmente Pegasus dentro de las Fuerzas Armadas de México: "Esta entidad incluso tiene un reglamento, un logo. Fue visitada por generales del Comando Norte, por parte de generales estadounidenses". Un documento lo comprueba: "El 24 de septiembre de 2019, el general secretario de la Defensa Nacional, acompañado del almirante secretario de Marina, participaron en la reunión de alto nivel con los comandantes del Comando Norte y Sur de los E.U.A., en las instalaciones del Centro Militar de Inteligencia (C.M.I.)".

Maldonado, abogado y maestro en derechos humanos por la Universidad Iberoamericana, me explica que el CMI opera de manera ilegal porque las Fuerzas Armadas de México no cuentan con las facultades para espiar civiles. La Sedena niega la existencia de esta entidad, como se ha negado a entregar los contratos de adquisición de Pegasus y cualquier otro tipo de información sobre el tema a la Fiscalía Ge-

neral de la República, que en 2017 inició una investigación judicial sobre el espionaje a periodistas y activistas mexicanos.

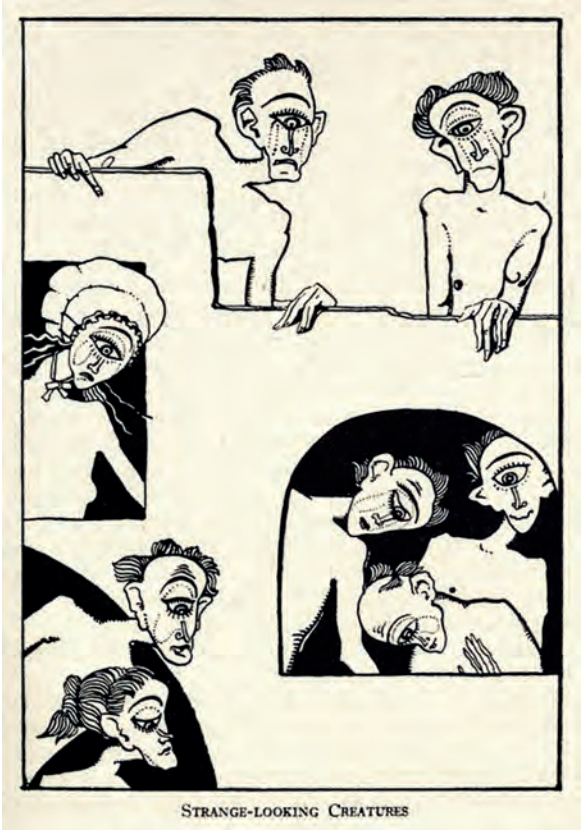
El periodista Mathieu Tourliere, en su reportaje "Centro Militar de Inteligencia, el búnker de la 4T para espiar" publicado por *Proceso* en marzo de 2023, informa que este centro es parte del Estado Mayor de la Defensa Nacional y "responde directamente al general Luis Cresencio Sandoval González, titular de la Sedena. Al igual que el resto del aparato militar, el CMI ha crecido mucho durante el gobierno de Andrés Manuel López Obrador: entre 2018 y 2021, su plantilla de agentes pasó de 293 a 619".[4]

***

Ha pasado más de un año desde el segundo ataque al teléfono de Santiago Aguirre, y casi ocho del primero. En ambas ocasiones, Santiago y el Centro Prodh presentaron denuncias: no ha habido avances en ninguna; es complicado que las entidades del Estado se investiguen a sí mismas. A eso hay que agregar que, según informes internos de la Sedena, hackeados por Guacamaya, en 2022 esta dependencia catalogó al Centro Prodh como "grupo de presión".

Sin embargo, a pesar del espionaje y el acoso del Ejército, el Centro Prodh no ha detenido su labor. Tras dos ataques, estos defensores de derechos humanos actúan con precaución ante el hecho de que cualquiera de sus actividades pueda ser monitoreada: "Lo que hemos hecho es no compartir información delicada por correo", confiesa Santiago, "andamos cargando siempre nuestros pequeños USB; así vamos moviendo documentos. Cada que alguien se incorpora al Centro intentamos hacer conciencia de que tenemos que dar por sentado que hoy todo lo que conversemos en los teléfonos es objeto de vulneración. Trabajamos asumiendo que esa es la realidad".

El panorama es desolador. "Pero eso no puede traducirse en inmovilidad y resignación", me dice Santiago. Ante esto solo queda, enfatiza, organizarse, crear propuestas de contrapeso, exigir rendición de cuentas, denunciar y acompañar a víctimas cuyos derechos fueron vulnerados por el Estado. En este momento solo se puede hacer eso. Resistir.



Jean de Boschère, *Islas extrañas*, 1921.
California Digital Library ©

[4] Mathieu Tourliere, "Centro Militar de Inteligencia, el búnker de la 4T para espiar", *Proceso*, 11 de marzo de 2023. Disponible en acortar.link/JV0DF7.