

# Proyecto Pegasus: la filtración de software espía sugiere que abogados y activistas están en riesgo en todo el mundo

Los registros filtrados muestran que los disidentes y quienes los ayudan son prominentes entre los amenazados por el software espía NSO

Shaun Walker,  
Stephanie Kirchgaessner,  
Nina Lakhani y  
Michael Safi.

19 de julio de 2021

Una filtración de datos telefónicos sugiere que abogados de derechos humanos, activistas y disidentes de todo el mundo fueron seleccionados como posibles candidatos para una vigilancia invasiva a través de sus teléfonos.

Sus números de teléfono móvil aparecieron en registros filtrados, lo que indica que fueron seleccionados antes de posibles objetivos de vigilancia por parte de clientes gubernamentales de la empresa israelí NSO Group, que desarrolló el software espía Pegasus.

Los registros fueron obtenidos por la organización sin fines de lucro Forbidden Stories y compartidos con un consorcio de medios de comunicación, incluido [The Guardian](#).

NSO ha dicho en repetidas ocasiones que Pegasus, que puede acceder a todos los datos en el dispositivo de un objetivo, así como convertirlos en una grabadora de audio o video, está diseñado para usarse solo contra terroristas y criminales graves.

La selección de activistas, disidentes y periodistas por parte de los clientes de NSO pinta un panorama muy diferente, aunque uno que los activistas dirán que era sombríamente predecible dado que la herramienta se ha vendido a algunos de los regímenes más represivos del mundo.

## Los activistas en riesgo de vigilancia

En Azerbaiyán, donde el antiguo dictador Ilham Aliyev tolera poca disidencia, aparecen numerosos activistas en los datos. Algunos encontraron su

correspondencia personal o fotografías íntimas publicadas en línea o en televisión.

Los números de teléfono de seis disidentes o activistas en el país cuya correspondencia privada se presentó en un programa de televisión de desorden en 2019 se enumeran en los registros filtrados.

Las activistas feministas a menudo son atacadas con kompromat sexual. En un caso particularmente atroz en 2019, fotografías íntimas de la activista de la sociedad civil y periodista Fatima Movlamli, entonces de 18 años, se filtraron a una página falsa de Facebook.

No está claro cómo se obtuvieron las fotografías, y Movlamli cree que se accedió a sus datos privados cuando la policía confiscó su teléfono durante un interrogatorio violento y la obligó a desbloquearlo. Su número también estaba en los registros obtenidos por el consorcio.

“A una edad en la que no me di cuenta del todo de que era mujer, me avergonzaba tener un cuerpo femenino y que la gente lo viera desnudo”, dijo Movlamli. Ella describió la experiencia como "difícil de soportar" y dijo que le había llevado a pensamientos suicidas. “En este país, las mujeres están condenadas a vivir dentro de los límites de lo que quieren los hombres, y pueden linchar a una mujer solo porque ven su cuerpo”.

Sin un análisis forense de un dispositivo, no es posible confirmar un intento exitoso de Pegasus o una infección. Movlamli dijo que reinicia su teléfono o cambia de dispositivo con regularidad, por lo que el análisis no fue posible.

### **En India, se encontraron los números de una variedad de activistas en los datos.**

Umar Khalid, un estudiante activista de la Universidad Jawaharlal Nehru en Delhi y líder de la Unión de Estudiantes Democráticos, fue seleccionado antes de un posible ataque a fines de 2018, poco antes de que se presentaran cargos de sedición en su contra. Fue arrestado en septiembre de 2020 acusado de organizar disturbios, y la policía afirmó que las pruebas en su contra incluían más de 1 millón de páginas de información obtenida de su teléfono móvil, sin dejar en claro cómo se obtuvo la información. Está en la cárcel a la espera de juicio.

Los números de teléfonos móviles de escritores, abogados y artistas que defendían los derechos de las comunidades indígenas y los indios de casta inferior también figuraban en los datos. Los miembros de la red han sido arrestados durante los últimos tres años y acusados de delitos de terrorismo,

incluido el de conspirar para asesinar al primer ministro indio, Narendra Modi. La red incluía a un sacerdote jesuita de 84 años, Stan Swamy, que murió este mes después de contraer Covid-19 en prisión.

Los registros muestran que varias personas acusadas de ser cómplices de Swamy, incluidos Hany Babu, Shoma Sen y Rona Wilson, fueron seleccionadas para posibles objetivos en los meses anteriores y los años posteriores a sus arrestos.

Loujain al-Hathloul , la activista por los derechos de las mujeres más prominente en Arabia Saudita , fue seleccionada para un posible ataque solo unas semanas antes de su secuestro en 2018 en los Emiratos Árabes Unidos y su regreso forzado a Arabia Saudita, donde fue encarcelada durante tres años y presuntamente torturada. Se cree que Hathloul fue seleccionado por la UAE , un cliente conocido de NSO y aliado cercano de Arabia Saudita.

A pesar de su liberación de la cárcel en febrero de 2021, a la activista saudí no se le permite hablar con periodistas ni moverse libremente dentro de Arabia Saudita y todavía está sujeta a una prohibición de viajar. Su teléfono móvil no pudo obtenerse ni probarse en busca de pruebas de que hubiera sido infectado o pirateado.

Hathloul había revelado previamente que sus correos electrónicos habían sido pirateados. "Mi suposición es que la estaban pirateando para conocer las redes de personas con las que se está organizando", dijo Hala al-Dosari, una activista saudí radicada en Estados Unidos que se comunicó con Hathloul antes de su arresto en 2018.

Dosari dijo que las autoridades sauditas habían obtenido información no pública sobre pagos diarios de alrededor de € 50 (£ 43) por día que se le habían hecho a Hathloul en relación con su defensa, posiblemente a través de su teléfono móvil.

En México, los datos muestran una amplia selección de activistas, abogados y defensores de los derechos para posibles ataques, incluido Eduardo Ferrer Mac-Gregor Poisot, un juez que fue presidente de la Corte Interamericana de Derechos Humanos y Alejandro Solalinde, un sacerdote católico y campeón de los derechos de los migrantes.

Solalinde dijo que creía que el gobierno mexicano anterior estaba "buscando algo para dañar mi reputación y usarlo como chantaje" debido a su apoyo a un rival político, y dijo que un ex agente de la Agencia Nacional de Inteligencia (Cisen) le había advertido que era bajo vigilancia.

John Scott-Railton de Citizen Lab, que publicó un informe sobre los ataques contra el activista emiratí Ahmed Mansoor con Pegasus en 2016, dijo: “Los ataques contra los disidentes [deberían] estar en la misma caja mental que los ataques contra los jefes de estado, el objetivo de embajadores, como el objetivo de grandes corporaciones y contratistas de defensa ”.

## **Los abogados en riesgo de vigilancia**

Los abogados también figuran en gran medida en los datos filtrados.

Rodney Dixon, un destacado abogado con sede en Londres, que ha asumido numerosos casos de derechos humanos de alto perfil, fue seleccionado para atacar en 2019. El análisis forense de su dispositivo mostró actividad relacionada con Pegasus, pero sin infección exitosa.

Entre sus clientes se encuentran Matthew Hedges, un estudiante de doctorado británico encarcelado en los Emiratos Árabes Unidos, y Hatice Cengiz, la prometida del periodista saudí asesinado Jamal Khashoggi. Ella también fue atacada con Pegasus, y los forenses mostraron evidencia de una infección exitosa.

Dixon dijo: “Nadie debería ser un objetivo de esta manera. Para los abogados es particularmente preocupante, ya que viola los principios fundamentales del privilegio y la confidencialidad abogado-cliente, que son fundamentales para los procedimientos legales justos y equitativos”.

El análisis forense en el teléfono del abogado francés de derechos humanos Joseph Breham muestra que se vio comprometido varias veces con Pegasus en 2019, y los registros filtrados sugieren que anteriormente había sido seleccionado para posibles objetivos de Marruecos.

“No hay justificación posible para que un estado extranjero escuche a un abogado francés. No hay justificación a nivel legal, ético o moral ”, dijo.

Dos abogados que están entablando una demanda contra NSO en nombre de Omar Abdulaziz, un saudí que vive exiliado en Canadá, también vieron sus números en los datos filtrados. Abdulaziz fue un colaborador cercano y amigo de Khashoggi.

El análisis de los teléfonos móviles de ambos abogados no encontró pruebas de ningún intento de utilizar el software Pegasus en su contra.

“No solo piratean a la gente por sus actividades políticas, sino que si estas [víctimas] buscan algún tipo de rendición de cuentas, irán tras las personas que las ayudan”, dijo uno de los abogados, que pidió no ser identificado.

Un portavoz del gobierno indio dijo: "Las acusaciones sobre la vigilancia gubernamental de personas específicas no tienen ninguna base concreta o verdad asociada". Los gobiernos de Marruecos, Azerbaiyán y México no respondieron a las solicitudes de comentarios en el momento de la publicación.

NSO Group ha afirmado que cortará a los clientes si hacen un mal uso de Pegasus. En respuesta al consorcio , negó que los registros filtrados fueran evidencia de un ataque con Pegasus y dijo que "continuará investigando todas las denuncias creíbles de uso indebido y tomará las medidas adecuadas en función del resultado de estas investigaciones".

El uso de software espía y piratería en un país como Azerbaiyán, donde los activistas comprometidos parece ser una política del gobierno, puede tener un efecto paralizante no solo en los destinatarios, sino en toda la sociedad civil.

Samed Rahimli, un abogado de derechos humanos de Azerbaiyán, cuyo propio número figuraba en los datos, dijo que el uso de kompromat les había dificultado la vida a los activistas del país, especialmente a las activistas. “Mucha gente tiene miedo de vivir su vida personal de forma normal. Muchos también enfrentan problemas psicológicos y han buscado apoyo profesional ”.

... tenemos un pequeño favor que pedir. Millones de personas recurren a The Guardian en busca de noticias abiertas, independientes y de calidad todos los días, y los lectores de 180 países de todo el mundo ahora nos apoyan económicamente.

Creemos que todos merecen acceso a información basada en la ciencia y la verdad, y un análisis basado en la autoridad y la integridad. Es por eso que tomamos una decisión diferente: mantener nuestros informes abiertos para todos los lectores, independientemente de dónde vivan o cuánto puedan pagar. Esto significa que más personas pueden estar mejor informadas, unidas e inspiradas para emprender acciones significativas.

En estos tiempos peligrosos, una organización mundial de noticias que busque la verdad como The Guardian es esencial. No tenemos accionistas ni propietarios multimillonarios, lo que significa que nuestro periodismo está libre de influencias comerciales y políticas, esto nos hace diferentes. Cuando nunca ha sido más importante, nuestra independencia nos permite investigar, desafiar y exponer sin miedo a los que están en el poder.