

# Spyware Pegasus: Israel y sus exportaciones para delinquir

**Por: Pablo Jofré Leal. 03/08/2021**

La entidad sionista ha vendido al mundo una imagen de régimen innovador, tecnológicamente avanzado, desarrollado en aspectos relacionados con el uso del agua, la agricultura, pero su esencia no puede ocultar sus acciones en campos claramente violatorios del derecho internacional y que se expresa en las denuncias por el uso de programas informáticos de espionaje.

Efectivamente, esta entidad que gasta cientos de millones de dólares anualmente para limpiar su imagen de un régimen que ocupa y coloniza Palestina, denunciado por crímenes de guerra y lesa humanidad, no ha podido esconder una cuestionable área de exportación. Me refiero a aquella, donde las revelaciones que han salido a la luz pública muestran su labor en el espionaje mundial, en el robo de información y el uso de datos para la vigilancia llevada a cabo por los servicios de inteligencia de países, que adquieren dichos programas o software espías llamados también spyware maliciosos (1) para acciones claramente ilegales. Utilizados por gobiernos de países con antecedentes de vigilar a sus ciudadanos y a gobiernos y sociedades fuera de sus fronteras, mediante hackeos y ataques cibernéticos. Una querella que ya se había hecho pública en febrero del año 2019, pero que en este mes de julio del 2021 estalló en toda su magnitud (2)

Es el Ministerio de guerra israelí quien ha concedido a NSO Group la licencia para exportar el software Pegasus, como también a otras empresas dedicadas a este negocio calificado como un área opaca, donde se genera una enorme magnitud de violaciones de derechos humanos perpetradas a través de sistemas de cibervigilancia, que ha desatado, según señala Amnistía Internacional (AI) crisis global en materia de derechos humanos. Mediante un documento titulado “Descubriendo el Iceberg: La crisis de la vigilancia digital provocada por los Estados y el sector privado” (Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector) este organismo internacional revela el devastador impacto que la industria del software espía, que está apenas regulada, tiene en los derechos humanos a escala global.

La secretaria general de AI, Agnès Callarmard señaló frente a lo denunciado respecto a NSO Group que “en los últimos días, el mundo se ha sentido indignado, con razón, por los ataques sistemáticos a activistas de derechos humanos, profesionales del derecho y periodistas que el Proyecto Pegasus ha puesto al descubierto. El Proyecto no sólo denuncia el riesgo y el daño a las personas atacadas ilegítimamente, sino también las consecuencias extremadamente desestabilizadoras en los derechos humanos a nivel mundial y en la seguridad del entorno digital en general”

La acusación, entregada por diversos medios de comunicación y entidades defensoras de los derechos humanos, coordinados por Forbidden Stories (organización periodística radicada en París) junto a Amnistía Internacional y una veintena de medios, que denominaron a este sistema de espionaje como Proyecto Pegasus) develando la existencia de una lista de teléfonos vigilados, superior a los 50 mil números enfocados en políticos, empresarios, periodistas, diplomáticos, militares, incluyendo a jefes de estado, ministros y casas monárquicas, altos ejecutivos de empresas transnacionales, activistas de derechos humanos, entre otros, sujetos a vigilancia y el robo de la información en materia de correos electrónicos, whatsapp y otros archivos de los teléfonos intervenidos. Fue el laboratorio de seguridad de la organización Amnistía Internacional, quien realizó el análisis de los aparatos telefónicos, para así identificar a las víctimas de este proceso de espionaje.

The Washington Post, uno de los medios que ha dado a conocer los delitos cometidos por el uso de este spyware señaló que “La asociación de medios de comunicación, que adoptó el nombre de Proyecto Pegasus, analizó la lista de los teléfonos intervenidos, mediante entrevistas y análisis forenses de los teléfonos, y a través de la comparación de detalles de información previamente proporcionada sobre NSO. El Laboratorio sobre seguridad de Amnistía Internacional examinó a 67 teléfonos sospechosos de haber recibido ataques cibernéticos. De ellos, 23 habían sido infectados con éxito y 14 mostraron señales de intento de intrusión” Tras la denuncia de este medio estadounidense, el director ejecutivo de NSO, Shalev Hulio, expresó hipócritamente su preocupación sobre algunos de los detalles que había leído en las historias del Proyecto Pegasus, cuestionando que la lista de más de 50,000 números telefónicos tuviera algo que ver con NSO o Pegasus. Una disculpa tan ilusa como plagada de falsedad pues su responsabilidad ha quedado más que demostrada (3)

NSO Group es la empresa israelí que reconoció la venta de este software de espionaje, considerado de grado militar, pero negándose a dar los datos de sus clientes alegando acuerdos de confidencialidad. Negativa que debería contrarrestada con exigencias internacionales, para develar estas acciones delictivas. Las investigaciones llevadas a cabo por los medios de información involucrados en dar luz sobre estos hechos relatan que hasta ahora se conocen algunos de los países involucrados con esta empresa: Azerbaiyán, Baréin, Hungría, India, Kazajistán, México, Marruecos, Ruanda, Arabia Saudita y los Emiratos Árabes Unidos. La asociación de medios encontró muchos de los números de teléfono en este grupo de países, los cuales fueron sometidos a un análisis más profundo por parte de la organización Citizen Lab.

NSO Group ha estado estrechamente vinculada a empresas como Novalpina Capital, Francisco Partners, vinculadas a su vez a empresas de fondos de pensiones de Gran Bretaña y Estados Unidos, relacionadas con grupos proionistas y financistas de la política de ocupación y colonización de Palestina. NSO Group describió a sus clientes como 60 agencias de inteligencia, militares y policiales en 40 países, negándose dar nombres citando acuerdos de confidencialidad con los clientes, afirmando que su venta tenía el objeto de rastrear terroristas y delincuentes. Información que de inmediato fue contrarrestada con el hecho que el programa Pegasus se utilizó para vigilar a activistas de derechos humanos, periodistas de diversos medios, incluyendo aquellos vinculados a gobiernos aliados

de Israel, tales como: CNN, The Associated Press, Voice of America, The New York Times, The Wall Street Journal, Bloomberg News, Le Monde en Francia, The Financial Times. Se dio a conocer también que familiares y amigos cercanos al asesinado periodista saudí Jamal Kashoggi en Turquía, a manos de agentes de la inteligencia de la monarquía saudí, fueron intervenidos.

Agnés Callamard, manifestó: “La revelación sin precedente de que los teléfonos de al menos 14 jefes de Estado pueden haber sido hackeados con el software espía Pegasus de NSO Group debería provocar escalofríos a los dirigentes mundiales...Sabemos desde hace mucho tiempo que se hackean subrepticamente teléfonos de activistas y periodistas, pero está claro que incluso quienes se sitúan en las más altas esferas del poder tampoco escapan a la tenebrosa expansión del software espía de NSO. Una empresa que no puede seguir escudándose en la afirmación de que su software espía sólo se utiliza para combatir la delincuencia; parece que Pegasus es también el software espía preferido de quienes tienen entre sus planes el espionaje de gobiernos extranjeros...Las contundentes revelaciones del Proyecto Pegasus subrayan la necesidad urgente de una reglamentación estricta que ponga orden en el “salvaje oeste” que es la industria de la vigilancia. Los Estados deben suspender en todo el mundo la exportación, venta, transferencia y uso de tecnología de vigilancia hasta que se establezca un marco regulador sólido que respete los derechos humanos.” (4)

Entre los políticos que han sido espiados se menciona al rey Mohammed VI, de Marruecos y el primer ministro de este país Saad-Eddine El Ohtmani. Emmanuel Macron, de Francia (espiado por los servicios secretos de marruecos). Barham Salih, de Irak. Cyril Ramaphosa, de Sudáfrica; Mostafa Madbouly, de Egipto; Imran Khan, de Pakistán. Saad Hariri, del Líbano; Ruhakana Rugunda, de Uganda, y Charles Michel, de Bélgica. Como hecho anecdótico se menciona que el Dalai Lama no había sido espiado por autoridades de la India, simplemente porque no usa teléfono celular. Entre los años 2016 y 2017 el actual presidente de México Andrés Manuel López Obrador, bajo la presidencia del ex mandatario Enrique Peña Nieto fue objeto de vigilancia.

Durante años se ha denunciado el papel violador que cumple la entidad sionista en amplias áreas del derecho internacional. Entre ellos, los crímenes de guerra y lesa humanidad que se perpetran contra Palestina desde el año 1948 a la fecha y que implican asesinato de su población, detenciones arbitrarias, el expolio de sus tierras, demolición de viviendas, destrucción de cultivos, creación de un sistema de

segregación. A esto se une la exportación de una industria de armas ofrecidas en el mercado como “aprobadas en terreno” lo que es lisa y llanamente, experimentarlas en los cuerpos de decenas de miles de palestinos detenidos, torturados, heridos y asesinados en los últimos 73 años.

Hoy, las denuncias del Proyecto Pegasus muestran esa cara sucia que se quiere esconder del régimen israelí y que es hora de denunciar con fuerza y sobre todo detener: la violación de la privacidad de miles de personas, gobiernos, entidades públicas y privadas y el uso de esa información, cuyo objetivo es seguir fortaleciendo una política donde se benefician gobiernos aliados del sionismo y aquellos grupos empresariales, que ligados a esta ideología criminal suelen financiar la investigación y comercio de estos sistemas de espionaje. Si algo positivo arroja el develar las acciones del Spyware Pegasus es que permite dejar de lado la hipocresía respecto a este régimen y reconocerlo como lo que es: Un violador del derecho internacional y una entidad, que ha basado su breve historia en el despojo y el crimen.

## Notas:

1. Spyware, o software espía, es un término general para denominar a una categoría de software malicioso, o programa maligno, que busca recopilar información de la computadora, teléfono u otro dispositivo de otra persona. El software espía más avanzado permite espiar y sacar información de los teléfonos incluso aquellos dotados de extremas medidas de seguridad. El spyware más avanzado es utilizado por agencias de inteligencia, con un mercado dominado por Estados Unidos y el régimen sionista. A las denuncias contra NSO Group se suma las efectuadas contra la también empresa israelí Candiru, había sido utilizado para infectar las computadoras y teléfonos de activistas, políticos y otras víctimas por medio de sitios web falsos que se hacían pasar por páginas de Black Lives Matter o grupos de salud según señalaron los propios medios estadounidenses entre ellos el participante del consorcio internacional denunciante de NSO Group, The Washington Post.

<https://www.washingtonpost.com/es/technology/2021/07/19/malware-pegasus-espionaje-como-detectar-preguntas-spyware/>

El software espía puede determinar la ubicación de un usuario, además de si la persona está detenida o en movimiento —y hacia qué dirección lo hace—. Puede recolectar contactos, nombres de usuario, contraseñas, notas y documentos. Eso incluye fotografías, videos y grabaciones de sonido. El spyware más avanzado puede incluso activar micrófonos y cámaras, sin encender luces o cualquier otro

indicador que informe que hay una grabación en curso.

2. <https://r3d.mx/2019/02/14/francisco-partners-vende-nso-group-en-medio-del-escandalo-por-operacion-encubierta/>
3. <https://www.washingtonpost.com/es/world/2021/07/21/proyecto-pegasus-malware-espia-periodistas-activistas-mexico-spyware/>
4. <https://www.amnesty.org/es/latest/news/2021/07/world-leaders-potential-targets-of-nso-group-pegasus-spyware/>

[LEER EL ARTICULO ORIGINAL PULSANDO AQUÍ](#)

Fotografía: Rebelión

**Fecha de creación**

2021/08/03