Pegasus: El software espía israelí que ya está en Latinoamérica

Por: Rodrigo Bernardo Ortega. 21/11/2024

El 4 de septiembre de 2024 en una alocución presidencial y en medio del paro camionero, el presidente de Colombia Gustavo Petro sorprendió al país con una revelación que confirma la compra del software Pegasus en el gobierno anterior. Ya en febrero de 2024 el periodista de Haaretz, Gur Megiddo, hizo pública una investigación de cómo en el gobierno de Iván Duque, en junio de 2021, habría concretado la compra del software Pegasus en efectivo por 13 millones de dólares, los cuales habrían sido enviados en un jet privado en dos pagos. El diario israelí también informa que los dineros de la transacción provendrían de incautaciones de efectivo producto de operaciones militares contra el narcotráfico, haciéndolo así en un esfuerzo por borrar toda traza de la ilegal operación de compra.

A pesar de estas precauciones, durante la alocución, Petro hizo público un documento de inteligencia clasificado hasta entonces proveniente de la UIAF (Unidad de Inteligencia Financiera) la cual confirmaba el hecho de manera incontrovertible (salvo que el monto mencionado es de 11 millones de dólares en 2 pagos de 5.5 millones cada uno), el dinero pagado en efectivo a NSO Group (NSO significa **Niv, Shalev y Omri**, los nombres de los fundadores de la compañía) fue luego consignado a una cuenta bancaria en Israel.

En revelaciones más recientes se confirmó que los ocupantes de los vuelos que vinieron a Colombia a recoger los dólares eran ciudadanos israelíes, entre quienes estaba Yehuda Lahav, gerente de negocios de NSO Group. El dinero nunca fue declarado en aduana, sobra decir que este monto supera con creces los 10.000 dólares que se pueden llevar consigo en viajes internacionales, por lo cual se configuraría el delito de blanqueo de capitales.

A pesar de lo dificultoso que es avanzar la investigación por el lado israelí en razón a la ruptura de relaciones con dicho país (debido a las fuertes declaraciones de Petro ante, el ya más que probable, genocidio gazatí), NSO Group asevera en una escueta comunicación, que las transacciones “se realizaron de acuerdo con la ley y con la autorización y documentación adecuada en ambos países”, por si quedaban

dudas.

No está claro, por el contrario, qué destino tuvo el software espía adquirido por la anterior administración del expresidente Duque. Todos sus funcionarios aseguran no tener conocimiento de la presencia de Pegasus en Colombia. El mencionado reporte de inteligencia parece dar pistas sobre su destinatario: La DIPOL (Dirección de Inteligencia Policial). La fecha de adquisición tampoco parece aleatoria, para el 2021 en Colombia se estaba desarrollando el *Estallido Social*, una serie de fuertes movilizaciones -brutalmente reprimidas- de la sociedad civil ante las políticas económicas y tributarias del gobierno, en las cuales hubo violaciones a los derechos humanos por parte del aparato policivo. También, por la época, estaban tomando vuelo las campañas presidenciales que llevarían a la casa presidencial a Petro. Cabe recordar que la campaña de Petro estuvo marcada por filtraciones, en el escándalo de los llamados *Petrovideos*. NSO Group, propietaria de Pegasus, afirma que sólo autoriza el uso del software en la lucha contra el crimen organizado y el terrorismo, sin embargo, si tenemos en cuenta: de una parte, la opacidad de la transacción, de otra parte, la forma de actuar del gobierno colombiano de entonces, de otra, la historia de interceptaciones ilegales del país (Chuzadas), así como el escándalo del mal uso del software en otros países, nos queda más que claro que el uso en Colombia de dicho software dista mucho de ser lícito.

¿Pero qué hace tan poderoso a Pegasus con respecto a otros métodos de espionaje? Pegasus puede instalarse sin intervención del usuario, incluso a través de mensajes de texto. Una vez instalado, Pegasus puede acceder a una amplia gama de datos en el dispositivo, incluyendo fotos, videos, ubicación GPS, mensajes de chat (así sean encriptados como Whatsapp, Signal o Telegram), historial de navegación y contactos de redes sociales. También puede activar la cámara y el micrófono del dispositivo. A esto, hemos de sumar, que la detección de Pegasus es casi imposible. Como se puede ver, un uso ilegítimo de Pegasus confirmaría una violación a los derechos fundamentales de privacidad de los ciudadanos.

Dichos usos ilegítimos han sido más que probados.

https://www.eltiempo.com/opinion/caricaturas/rodrigo-guerreros/caricatura-de-rodrigo-guerreros-3393525

En el 2021, un equipo de 80 periodistas de 14 periódicos en todo el mundo, analizaron una filtración que contenía más de 50.000 números de teléfonos infectados. De manera probada establecieron que periodistas, políticos, activistas de al menos los siguientes países: México, Arabia Saudita, España, Reino Unido, Francia, Hungría, Turquía, India, Azerbaiyán, Kazajstán, Egipto, Argelia, Marruecos, Togo, Ruanda, RD Congo, Uganda, Qatar, Bahréin y Emiratos Árabes Unidos fueron el objetivo de este software espía. Se confirmó por ejemplo que personas cercanas al periodista Jamal Khasshoggi, fueron infectadas por el malware antes que éste fuera asesinado y descuartizado en un consulado saudí en Estambul.

En Latinoamérica, se siguen revelando casos de vigilancia ilegal en la región con Pegasus. En El Salvador, se ha conocido el caso de infección a una magistrada de

la Corte Suprema, así como al menos 35 periodistas de un diario opositor al presidente Bukele. En México, diferentes organizaciones estatales de manera independiente adquirieron el software en el sexenio de Enrique Peña Nieto como arma contra el narcotráfico. Pero se reveló que políticos opositores (entre ellos el hoy presidente AMLO), así como periodistas (entre ellas la afamada Carmen Aristegui de CNN) fueron también objetivos ilegítimos. En República Dominicana, la periodista Nuria Piera fue identificada como víctima de Pegasus, lo que llevó a la CIDH y a la RELE a pedir una investigación al Estado.

Ahora hemos de adicionar a Colombia en esta triste lista.

De otra parte, la revelación de Petro también ha tenido graves consecuencias para el Colombia, pues el país pertenece al grupo EGMONT, una organización internacional que promueve la cooperación y el intercambio de inteligencia entre 177 países para combatir el lavado de activos y la financiación del terrorismo, pero después de la filtración, decidió suspender el acceso de Colombia a su plataforma de intercambio de información confidencial.

Según INFOBAE: “El comunicado emitido por la organización destaca la importancia de la “cooperación internacional” en la lucha contra el blanqueo de capitales y los delitos asociados. En él se enfatiza que “el compromiso del Grupo Egmont con la cooperación internacional es fundamental” y que este se basa en “una sólida base de confianza mutua que garantiza que las Unidades de Inteligencia Financiera (UIF) **miembros cumplan con altos estándares de responsabilidad en lo que respecta a la protección y confidencialidad de la inteligencia financiera que se intercambia”.**

Lo anterior significa que Colombia pierde acceso a importante información financiera sobre lavado de activos, por tanto, la lucha contra el narcotráfico se verá seriamente comprometida.

Volviendo a Pegasus, están ampliamente documentados los excesos y usos ilegales del software, sin embargo, NSO Group no revela la lista de clientes ni las acciones que ha tomado para prevenir el abuso de su producto. Esta compañía, además, actúa sin escrutinio parlamentario o judicial: Israel apenas ha adelantado investigaciones que desestima, y no ha tomado medidas contra la compañía cuya residencia fiscal está en su territorio. Después de todo, NSO Group es una empresa privada, pero no puede vender su tecnología sin la aprobación del Gobierno israelí.

Este gobierno emite las licencias de mercado, necesarias antes de iniciar negociaciones con un cliente, y las licencias de exportación, que autorizan cada venta, regulando así la industria de defensa.

La alineación del Estado con la empresa NSO Group en estos procesos ha sido total.

Lo cierto es que Pegasus se ha convertido en una herramienta clave para la industria de ciberseguridad de Israel. El programa ha sido utilizado por agencias de inteligencia como el Mossad y el Shin Bet para operaciones de espionaje sin dejar rastros. Esta es sin más la razón que Hezbollah, en el Líbano, dejara de utilizar celulares para la comunicación entre sus miembros a favor de *Beepers* (buscapersonas, localizadores), circunstancia que facilitó la infiltración en la cadena de producción de los aparatos por parte de Israel, y que resultó en la explosión de miles de estos aparatos en septiembre del 2024.

Pero quizá el activo más importante para el gobierno hebreo que le trae Pegasus es la diplomacia. La exportación de programas como Pegasus fue una parte integral de la estrategia de los gobiernos del primer ministro Benjamín Netanyahu entre 1999 y 2021 para mejorar la imagen internacional de Israel, afectada por el conflicto palestino. Al ofrecer estos programas de ciberespionaje, Israel buscaba ganar aliados en Naciones Unidas, donde se cuestiona regularmente la ocupación de Cisjordania y Jerusalén Este, así como el bloqueo de la franja de Gaza. Extrabajadores de NSO revelaron a Haaretz que responsables del Mossad solían visitar la sede central de la empresa en Herzliya, junto con delegaciones de países árabes y africanos interesados en adquirir Pegasus.

Estos encuentros se dieron en el marco de los llamados Acuerdos de Abraham, dichos acuerdos, firmados en 2020, buscaban normalizar las relaciones diplomáticas y comerciales entre Israel y cuatro países árabes: Emiratos Árabes Unidos, Bahréin, Sudán y Marruecos. Mediados por Estados Unidos, estos acuerdos representaban un cambio significativo en la política de la región, ya que excluían a Palestina, lo que ha generado críticas al interior de los países mencionados por lo que consideran un pacto “envenenado”.

No es casualidad que los países árabes que firmaron los Acuerdos de Abraham sean clientes de NSO, al igual que Arabia Saudí. El Ministerio de Defensa y el Mossad han incentivado a NSO y otras empresas similares a vender sus tecnologías a estos países. Benjamín Netanyahu, por ejemplo, ordenó reanudar la venta de

Pegasus a Arabia Saudí tras una solicitud de Mohamed Bin Salman (príncipe coronado Saudí), a pesar del veto impuesto por el antes mencionado caso Khashoggi.

NSO tiene un comité ético que evalúa los contratos, pero este es criticado por ser una fachada, ya que los contratos son considerados secretos de Estado y pocas personas tienen acceso a la lista de clientes. Además, si la empresa descubre que su tecnología se está utilizando para espiar a periodistas, no puede cancelar el contrato sin causar una crisis diplomática. La empresa, además, tiene órdenes de no cuestionar a las organizaciones o personas que otros países consideran terroristas o criminales.

Israel, ha liberado en el mundo un poderoso virus, y lo ha puesto en las manos de gobiernos inescrupulosos adrede, para ganar influencia y comprar aliados.

Latinoamérica, en medio de un proceso de cambios políticos que cada vez más lo alejan del polo EE.UU., puede ser terreno fértil para comprar conciencias con esta poderosa tecnología, y que ésta, sea utilizada en contra de quienes se atrevan a ejercer una política no alineada.

POST SCRIPTUM:

https://www.wradio.com.co/2024/11/08/caso-pegasus-sera-abordado-en-reunion-diplomatica-entre-colombia-y-estados-unidos

Para acabar de enredar este nudo de informaciones contradictorias, dando un giro totalmente inesperado, a comienzos del mes de noviembre 2024, el periódico El Tiempo emite la siguiente información: “funcionarios americanos consultados aseguraron que **Estados Unidos no solo estuvo pendiente de la compra, sino que la financió con recursos lícitos con el fin de perseguir a narcotraficantes y también hizo control para que el software se usara de manera legal.** Agregaron que el presidente Iván Duque no fue informado porque se trataba de la cooperación rutinaria con la que han trabajado ambos países durante décadas en contra de amenazas comunes. “Solo sabía un grupo pequeño de personas en los organismos de seguridad del país”, le dijeron al periódico en Bogotá.”

Fuentes:

- $13m Cash on a Private Jet: How Colombia Paid for Israeli Spyware – Israel News – Haaretz.com
- Israel confirma compra de software espía Pegasus por parte de Colombia bajo el mandato de Duque (cambiocolombia.com)
- Pegasus: Lo que descubrimos del cracker de teléfonos inteligentes – The New York Times
- Pegasus, la cara oculta del poder al servicio de los intereses de Israel | España | EL PAÍS
- Pegasus, el fantasma de los “falsos positivos”
- Fiscal general dice que sí existió pago para comprar Pegasus – La Silla Vacía
- La plataforma mundial de inteligencia financiera suspende a Colombia por la revelación de Petro sobre Pegasus | EL PAÍS América Colombia
- NSO Group confirma compra de ‘Pegasus’ y dijo que fue una transacción legal | El Nuevo Siglo
- ¿Qué es la Dipol y cómo adquirió el software Pegasus?
- La viuda de Jamal Khashoggi denuncia al programa de software Pegasus por espiarla a través de su teléfono
- La viuda de Jamal Khashoggi denuncia al programa de software Pegasus por espiarla a través de su teléfono
- The Washington Post: investigación descubre que se usó software espía Pegasus, diseñado por Israel, para hackear a periodistas y activistas de todo el mundo | CNN
- Hezbolá: Qué son los “beepers” y por qué esta tecnología de hace décadas sigue siendo utilizada por la organización islamista – BBC News Mundo
- Pegasus, el caballo desbocado de Israel
- Esto debes saber sobre los “Acuerdos de Abraham”, el último plan de paz en Medio Oriente | CNN
- Qué son los Acuerdos de Abraham entre Israel y otros países

Fotografía: El pitazo

Fecha de creación
2024/11/21