AIC DEBE SER INVESTIGADA POR PROBABLE DESTRUCCIÓN DE EVIDENCIA TRAS PRESUNTA DESINSTALACIÓN DE PEGASUS

- *La Agencia de Investigación Criminal (AIC) afirmó al INAI que desinstaló Pegasus de sus equipos; podría constituir delitos por destruir evidencia y entorpecer la investigación penal.*
- *Afirmaciones de que Pegasus nunca fue utilizado son falsas; evidencias en el expediente y declaraciones públicas de altos funcionarios y NSO Group lo refutan.*
- *Celebramos los hallazgos y las expresiones del INAI que reconocen violaciones al derecho de protección de datos personales en la operación del malware Pegasus.*
- *Nueva FGR debe renovar impulso a la investigación y otorgar garantías de independencia y autonomía para combatir la impunidad en el caso.*

Ciudad de México, 20 de febrero de 2019. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha resuelto que la Procuraduría General de la República –ahora Fiscalía General de la República (FGR)– violó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados por utilizar de manera irregular del *malware Pegasus*. No obstante, dentro del proceso de verificación seguido, el INAI dio cuenta de diversas afirmaciones de la Agencia de Investigación Criminal (AIC) que comprometen gravemente la investigación penal abierta en la FGR por el uso de *Pegasus* en contra de periodistas y defensores de derechos humanos.

En particular, la AIC ha afirmado que el *malware Pegasus* habría sido desinstalado de los equipos desde los cuales operó el sistema de vigilancia, lo que pudo haber constituído un acto deliberado de destrucción de evidencia, encaminado a entorpecer la investigación en torno al abuso del sistema que se sigue ante la Fiscalía Especial para la Atención de Delitos contra la Libertad de Expresión (FEADLE) desde 2017.

De comprobarse la desinstalación y la destrucción de información clave relacionada con el uso de dicho *malware*, se habría violado la orden de resguardo que la FEADLE emitió respecto de toda información relacionada con *Pegasus* y se habrían cometido diversos delitos[1] relacionados con la destrucción de evidencia y el entorpecimiento de la investigación penal.

Asimismo, el INAI dio cuenta de las afirmaciones de la AIC de no haber utilizado nunca *Pegasus* –a pesar de haber adquirido el sistema en 2014 por una suma superior a 32 millones de dólares– hasta su supuesta desinstalación. Esta afirmación es abiertamente falsa y podría constituir responsabilidades penales[2] y administrativas.

Existe evidencia fehaciente en el expediente de la investigación penal que demuestra que, al menos hasta el 6 de julio de 2018, *Pegasus* estaba siendo utilizado efectivamente por parte de la AIC. La negativa de uso de la agencia también contradice las declaraciones públicas de altos funcionarios del gobierno federal anterior, como el expresidente Enrique Peña Nieto y la exprocuradora Arely Gómez, quienes aceptaron que *Pegasus* era empleado "de manera legal"[3]; así como declaraciones públicas de NSO Group, empresa fabricante del *malware*.

[1] Por ejemplo el delito de destrucción de información contenida en sistemas y equipos de informática del Estado (Artículo 213 Bis 3 del Código Penal Federal); el delito de ejercicio ilícito del servicio público (Artículo 214, fracciones IV y VI del Código Penal Federal); y delitos contra la administración de justicia (Artículo 225, fracción XXXI) del Código Penal Federal).

[2] Por ejemplo, el delito de ejercicio ilícito del servicio público (Artículo 214, fracción V)

[3] Milenio. Uso de Pegasus fue legal: Arely Gómez *https://www.milenio.com/politica/uso-de-pegasus-fue-legal-arely-gomez y https://www.youtube.com/watch?v=JFhY7FGAJ9E*

De esta manera, a la necesidad de una investigación sobre la adquisición irregular de *Pegasus* por parte de la PGR, así como a la utilización de dicho *malware* en contra de periodistas y defensores de derechos humanos en México, se añade la necesidad de investigar los posibles actos encaminados a entorpecer la investigación penal y encubrir a los perpetradores de estas graves violaciones a la privacidad que permanecen en la impunidad.

Celebramos los hallazgos y lo expresado por el INAI al resolver el proceso de verificación, al tiempo que hacemos un llamado a la nueva Fiscalía General de la República para que, otorgando garantías de independencia y autonomía, reitere el llamado al resguardo de información clave relacionada con la operación de *Pegasus* y brinde un nuevo impulso a la investigación. Es su deber que se avance de manera sustantiva, con profesionalismo y celeridad, para impedir la impunidad por la contratación irregular del *malware*, el espionaje ilegal en contra de periodistas y defensores de derechos humanos y, ahora, los intentos de encubrimiento mediante la posible destrucción de evidencia y la falsedad de declaraciones.

Es importante recordar que, a la fecha, se han documentado 24 casos de intentos de espionaje con el *malware Pegasus*, comercializado por la empresa NSO Group, en contra de activistas, periodistas, opositores políticos y personas defensoras de derechos humanos. Estos ataques, corroborados con apoyo del Citizen Lab de la Universidad de Toronto, se dieron en condiciones de opacidad que sugieren actos graves de corrupción. Aunque los hechos fueron denunciados desde el 19 de junio de 2017 ante la Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión (FEADLE), a más de 20 meses, el caso se mantiene en la impunidad.para construir una Fiscalía que pueda investigar a fondo casos como el arriba mencionado.

CONTACTO PARA PRENSA:

Iván Martínez
Red en Defensa de los Derechos Digitales (R3D)

contacto@r3d.mx
Teléfono móvil: (55) 55041636