COMUNICADO
DGDDH/154/2022

Ciudad de México a 26 de mayo de 2022

CNDH emite Recomendación General a autoridades del Estado mexicano por el caso de espionaje y su impacto en la libertad de expresión relacionado con el software Pegasus

<< La CNDH identificó que existe un riesgo grave de un posible ejercicio abusivo de las facultades previstas en la Ley de Seguridad Nacional, el Código Nacional de Procedimientos Penales y el Código Militar de Procedimientos Penales, ya que la redacción actual de estas normas facilita a las autoridades el uso de tecnologías de espionaje tan avanzadas como Pegasus

La Comisión Nacional de los Derechos Humanos (CNDH) emitió la Recomendación General 47/2022 a la presidenta de la Mesa Directiva de la Cámara de Senadores, Olga María del Carmen Sánchez Cordero Dávila; al presidente de la Mesa Directiva de la Cámara de Diputados, Sergio Carlos Gutiérrez Luna; a la presidenta de la Comisión Bicamaral de Seguridad Nacional del Poder Legislativo, Imelda Castro Castro; a la titular de la Secretaría de Seguridad y Protección Ciudadana (SSPC), Rosa Icela Rodríguez Velázquez, y al titular de la Fiscalía General de la República (FGR), Alejandro Gertz Manero por la ausencia de regulación jurídica para la adquisición y uso de tecnologías para la vigilancia, intervención y recolección de datos de personas en territorio nacional: su impacto en la libertad de expresión, el derecho a defender los derechos humanos y su vinculación al deber de cuidado a cargo del Estado mexicano.

La CNDH integró el expediente en atención a la queja presentada por personas defensoras de derechos humanos y periodistas, en la que argumentaron que, entre los años 2015 y 2016, fueron objeto de intentos de ataques informáticos de vigilancia vía teléfonos celulares, a través de mensajes de texto "maliciosos" que incitaban a presionar dominios que fueron identificados por una organización como causantes de la *infección* por el sistema Pegasus, sospechando que tales intentos de actos de espionaje provenían de autoridades del Gobierno mexicano, pues existe información pública que acredita que el Estado mexicano adquirió dicho sistema.

En la queja presentada se añade que el programa Pegasus funciona explotando una vulnerabilidad de seguridad inédita del sistema operativo; que, a través de la *infección* se hace un desbloqueo al dispositivo en cuestión y se instala un sofisticado *spyware* que permite al interceptor tomar control de diferentes funciones del aparato, así como acceder a sus

contenidos, tales como: archivos, datos del calendario, listas de contactos, contraseñas, mensajes de texto, datos de otras aplicaciones, como: Gmail, WhatsApp, Skype, Facebook y Telegram, entre otros. Además, permite escuchar llamadas realizadas por teléfono o vía WhatsApp o Viber, así como grabar activa o pasivamente, utilizando el micrófono y la cámara del dispositivo.

Con el objetivo de allegarse mayores datos relacionados con los hechos, este Organismo Nacional solicitó información al ex inspector general de la Comisión Nacional de Seguridad; al director jurídico de Petróleos Mexicanos; al secretario técnico del Consejo Nacional de Seguridad Pública; al comisionado presidente del Instituto Federal de Telecomunicaciones; a la coordinadora nacional Antisecuestros; al titular de la Unidad de Asuntos Jurídicos de la Auditoría Superior de la Federación; al secretario de la Defensa Nacional; al secretario de Marina; al titular del entonces Centro de Investigación y Seguridad Nacional, así como a los fiscales generales y secretarios generales de Gobierno de las 32 entidades federativas.

La CNDH analizó la investigación relativa a la presunta intervención de las comunicaciones privadas referidas, así como las normas legales que facultan a las autoridades para utilizar sistemas como Pegasus para intervenir teléfonos y otros dispositivos electrónicos, de lo que advirtió la existencia de normas que facilitan que las autoridades, valiéndose del argumento de investigar amenazas a la seguridad nacional o delitos graves, empleen sistemas como Pegasus para intervenir comunicaciones privadas de manera inmediata y sin controles legales claros.

La Comisión Nacional cuenta con información de la que se advierte que, entre 2011 y 2017, el entonces Gobierno Federal adquirió el programa Pegasus; que, a pesar de la potencialidad lesiva de dicho sistema, no tomaron medidas para contener el riesgo y prevenir las posibles violaciones a derechos humanos que la posesión y uso del mencionado sistema implica. Además, se advierte que las personas periodistas y personas defensoras de derechos humanos, al ejercer tales actividades, se encuentran en una situación especial que actualiza el riesgo del posible uso de tecnologías para el espionaje, intervención y recolección ilegal de datos en su agravio.

En consecuencia, la CNDH identificó que existe un riesgo grave de un posible ejercicio abusivo de las facultades previstas en la Ley de Seguridad Nacional, el Código Nacional de Procedimientos Penales y el Código Militar de Procedimientos Penales, ya que la redacción actual de estas normas facilita a las autoridades el uso de tecnologías de espionaje tan avanzadas como Pegasus, al ser susceptible de una interpretación subjetiva para justificar, con el discurso de seguridad nacional o investigación de delitos graves, el uso irrestricto de este tipo de tecnología.

Ante tales hechos, la CNDH solicita a la Cámara de Senadores y Cámara de Diputados del Congreso de la Unión, así como a la Comisión Bicamaral de Seguridad Nacional del Poder

Legislativo que se realicen las adiciones o modificaciones del marco jurídico actual sobre intervención de comunicaciones privadas, considerando que se evite el uso de términos generales, abiertos y ambiguos, respecto a los actos que pueden ser considerados amenazas a la seguridad nacional. Se establezcan procedimientos que incorporen criterios claros e inequívocos sobre la elección, adquisición y uso de tecnologías para la vigilancia, intervención y recolección de datos. Y se precise el perfil de las personas servidoras públicas responsables del uso de tecnologías para la vigilancia, intervención y recolección de datos, así como de las personas servidoras públicas responsables del manejo de la información obtenida mediante tales tecnologías.

De igual forma, solicita que se prevea la responsabilidad de las empresas que desarrollen y comercialicen tales tecnologías en aquellos casos en que sus actividades puedan ocasionar violaciones a derechos humanos como consecuencia de las operaciones, productos o servicios que realicen. Se establezcan prohibiciones claras y específicas sobre la modificación personalizada de los productos, la selección de objetivos y la prestación de servicios de mantenimiento o asistencia que supongan una infracción al derecho nacional o internacional de los derechos humanos. Y se realicen las adiciones o modificaciones al marco jurídico actual para que se establezca como una obligación a cargo de las autoridades que realicen intervenciones a comunicaciones privadas, el rendir un informe al Poder Judicial de la Federación, con una periodicidad específica, sobre el uso y destino de los datos e información obtenidos, como estadístico.

A la SSPC le solicita impulsar ante el Consejo de Seguridad Nacional la emisión de un instrumento administrativo mediante el cual se regule el uso de aparatos y/o sistemas útiles en la intervención de comunicaciones privadas. Mientras que, a la FGR le exhorta a que continúe con la investigación del caso en el ámbito de su competencia.

La Recomendación General 47/2022 ya fue debidamente notificada a sus destinatarios y puede ser consultada en la página web cndh.org.mx.

¡Defendemos al pueblo!

***