QUE REFORMA Y ADICIONA LOS ARTÍCULOS 177 Y 211 BIS DEL CÓDIGO PENAL FEDERAL, A CARGO DE LA DIPUTADA BRENDA VELÁZQUEZ VALDEZ, DEL GRUPO PARLAMENTARIO DEL PAN

La que suscribe, Brenda Velázquez Valdez, diputada federal integrante del Grupo Parlamentario del Partido Acción Nacional en la LXIII Legislatura de la Cámara de Diputados, con fundamento en lo dispuesto en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 6, párrafo 1, fracción I, y 77 del Reglamento de la Cámara de Diputados, somete a consideración del pleno de esta honorable asamblea la siguiente iniciativa con proyecto de decreto por el que se reforma y adiciona el Código Penal Federal para aumentar las penas a los servidores públicos que incurran en espionaje ilegal, al tenor de la siguiente

Exposición de Motivos

Con información publicada por Citizen Lab 1 y por las organizaciones Article19 – Oficina para México y Centroamérica–, R3D: Red en Defensa de los Derechos Digitales y Social TIC, una investigación recogida por el diario The New York Times, que demuestra el uso del malware Pegasus altamente sofisticado y comercializado exclusivamente a gobiernos, con el objetivo de espiar los teléfonos móviles de defensores de derechos humanos, periodistas y activistas anticorrupción.

Según reportes de The New York Times (NYT), cada licencia de infección tendría un costo alrededor de 77 mil dólares americanos (o cerca de 1 millón 400 mil pesos provenientes del erario público).

Las nuevas investigaciones surgen después de la publicación de los casos sobre el espionaje ejercido contra los promotores del impuesto a bebidas azucaradas. El doctor Simón Barquera, investigador del Instituto Nacional de Salud Pública (INSP), Alejandro Calvillo, director de la organización El Poder del Consumidor, y Luis Encarnación, coordinador de la coalición Contra Peso, recibieron mensajes de texto SMS en su celular con enlaces aparentemente inofensivos que contenían vínculos infecciosos.

El principal método de infección documentado tanto por Citizen Lab como por las organizaciones consiste en el envío de mensajes SMS con enlaces que, al ser accedidos, provocan la instalación inadvertida del software malicioso.

Otras organizaciones, periodistas y personas críticas al poder también han recibido mensajes de la misma naturaleza y son identificadas como blanco de ataques para tener acceso y control absoluto de sus dispositivos. Los nuevos casos son los siguientes:

1. Centro Miguel Agustín Pro Juárez (Centro Prodh): Entre los meses de abril y junio de 2016, Mario Patrón, director del Centro Prodh, Stephanie Brewer, coordinadora del Área Internacional, y Santiago Aguirre, subdirector de la

organización, recibieron mensajes que se ha confirmado constituyen intentos de infección con el malware de espionaje Pegasus.

Los mensajes fueron recibidos en fechas clave dentro del trabajo de defensa de derechos humanos que el Centro Prodh ha realizado en casos de alto impacto como la desaparición forzada de los 43 estudiantes de Ayotzinapa, la masacre de Tlatlaya y los casos de tortura sexual en Atenco.

2. Aristegui Noticias (Carmen Aristegui, Emilio Aristegui, Rafael Cabrera y Sebastián Barragán): Se han documentado cerca de 50 mensajes recibidos en los años 2015 y 2016 por Carmen Aristegui, por su hijo menor de edad, Emilio Aristegui, y por integrantes de su equipo de investigación, como Sebastián Barragán y Rafael Cabrera.

En los últimos años, la actividad periodística de Aristegui Noticias ha revelado casos de corrupción como el reportaje de la “Casa Blanca” o el plagio de la tesis del presidente Enrique Peña Nieto.

Además, ha hecho reportajes sobre casos de violaciones graves a derechos humanos en México.

Producto del trabajo periodístico de Aristegui Noticias se han documentado diversos actos de hostigamiento, incluido el allanamiento de sus oficinas.

3. Carlos Loret de Mola (Televisa / El Universal / Radio Fórmula): Es periodista de radio, televisión y columnista impreso.

Se ha documentado que en los años 2015 y 2016 recibió al menos 7 mensajes que pretendían infectar su dispositivo con el malware Pegasus. La mayoría de los mensajes fueron recibidos alrededor del extenso trabajo periodístico que Carlos Loret de Mola llevó a cabo durante los meses de agosto y septiembre de 2015 respecto de las ejecuciones extrajudiciales en Tanhuato, Michoacán, por parte de la Policía Federal.

4. Mexicanos Contra la Corrupción y la Impunidad (MCCI): Se ha documentado que los periodistas Salvador Camarena y Daniel Lizárraga, director general de Investigación Periodística y jefe de Información de la organización respectivamente, recibieron al menos 3 mensajes intentando infectar sus teléfonos con malware de NSO en el mes de mayo de 2016, justo cuando se hizo público el nacimiento del proyecto y se publicaron investigaciones sobre actos de corrupción por parte del exgobernador de Veracruz Javier Duarte y el exdirector de la Conagua.

Salvador Camarena y Daniel Lizárraga en el pasado también fueron parte de Aristegui Noticias y participaron en investigaciones, como la publicación de los “Papeles de Panamá”.

5. Instituto Mexicano por la Competitividad (Imco): Se ha documentado que el director de la organización, Juan Pardinas y Alexandra Zapata, investigadora en dicha organización, han recibido al menos 4 mensajes intentando infectar su dispositivo a finales de 2015 y en el mes de mayo de 2016.

Imco ha sido una de las organizaciones que ha liderado esfuerzos de incidencia para la reforma legal anticorrupción, en particular, fue impulsor de la ley conocida como “Ley 3 de 3”, la cual generó gran resistencia y ataques por parte de fuerzas políticas asociadas al gobierno federal durante el primer semestre de 2016, justo en el momento en que fueron recibidos los mensajes.

De igual manera el dirigente del Partido Acción Nacional, Ricardo Anaya, denunció que junto a otros cuatro integrantes del blanquiazul, lo intentaron espiar por medio del malware Pegasus, el cual habría sido obtenido por el gobierno mexicano y fue usado para espiar a defensores de derechos humanos y periodistas.

Cuando un dispositivo es infectado con el malware instalado al dar ‘clic’ a los enlaces enviados por SMS, el atacante adquiere acceso a toda la información almacenada como mensajes, correos y contactos, registro de cada tecla oprimida, monitoreo remoto de datos de localización e incluso a la información obtenida a través de la activación inadvertida del micrófono y la cámara de los dispositivos.

Según la investigación de Citizen Lab, la mayoría de los nombres de dominio de la infraestructura de NSO se encuentran vinculados a México, lo cual, en conjunto con otras evidencias presentadas en esta nueva investigación, reafirma que autoridades mexicanas, como la Secretaría de la Defensa Nacional (Sedena), la Procuraduría General de la República (PGR), y el Centro de Investigación y Seguridad Nacional (Cisen), son clientes de NSO y que personas en México han sido objetivos de esta forma de vigilancia.

Consideramos de la mayor importancia que se aumenten las penas a los servidores públicos que resulten responsables de utilizar las herramientas de intervención de comunicaciones de particulares de forma ilegal, para evitar que se utilice el espionaje en contra de los ciudadanos ya que esta práctica constituye violaciones al derecho a la privacidad de las personas y a la libertad de expresión en México

Por lo anteriormente expuesto, someto a consideración del pleno de la honorable Cámara de Diputados la siguiente iniciativa con proyecto de

Decreto

Artículo Primero. Se reforma el artículo 177 del Código Penal Federal, para quedar como sigue:

...

Artículo 177. A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de doce a veinticuatro años de prisión y de seiscientos a mil doscientos días multa.

...

Artículo Segundo. Se reforma el artículo 211 Bis del Código Penal Federal, para quedar como sigue:

...

Artículo 211 Bis. A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de doce a veinticuatro años de prisión y de seiscientos a mil doscientos días multa.

...

Transitorio

Único. El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Dado en el Palacio Legislativo de San Lázaro, a 12 de septiembre de 2017.

Diputada Brenda Velázquez Valdez (rúbrica)