

CON PUNTO DE ACUERDO, POR EL QUE SE EXHORTA A LA PGR A DIFUNDIR LA INFORMACIÓN RELATIVA A LAS APLICACIONES DADAS AL EQUIPO ELECTRÓNICO DE ESPIONAJE PEGASUS, Y DETENER EL USO DE TODO PROGRAMA INFORMÁTICO DE ESPIONAJE EN LOS CASOS DONDE NO HAYA MANDAMIENTO JURÍDICO, PUES ATENTAN CONTRA LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, LOS TRATADOS INTERNACIONALES DE QUE EL ESTADO MEXICANO ES PARTE Y LAS NORMAS PROTECTORAS DE LA PRIVACIDAD, A CARGO DE LA DIPUTADA ARACELI DAMIÁN GONZÁLEZ, DEL GRUPO PARLAMENTARIO DE MORENA

Araceli Damián González, en mi calidad de diputada de la LXIII Legislatura, integrante del Grupo Parlamentario de Morena, con fundamento en la fracción I, numeral 1, del artículo 6; y numeral 1, fracción II, del artículo 79 del Reglamento de la Cámara de Diputados, somete a consideración del pleno la presente proposición con punto de acuerdo, bajo las siguientes

Consideraciones

Primera. El 24 de agosto de 2016 el Laboratorio Ciudadano (The Citizen Lab) de la Escuela Munk de Asuntos Globales de la Universidad de Toronto, denunció públicamente el intento de espionaje contra el activista Ahmed Mansoor –originario de los Emiratos Árabes Unidos– mediante el uso del *software* Pegasus, que desarrolla y vende la compañía israelí NSO Group¹. Este programa se infiltra en los teléfonos celulares de los objetivos mediante un mensaje falso que contiene un vínculo a un sitio web apócrifo –la empresa proveedora suplanta la identidad de un sitio de internet válido–, a través del cual se instala un programa que compila toda la información del usuario, interviene llamadas y mensajes, y puede impedir visitar ciertos sitios de internet.

En esta publicación también se denunció que el periodista mexicano Rafael Cabrera, quien formó parte del equipo de investigación que elaboró el reportaje de la “Casa Blanca” de Enrique Peña Nieto, pudo haber sido objeto de reiterados intentos de espionaje a través del mismo *software* en meses pasados.

Segunda. The Citizen Lab desglosó los nombres de los sitios web apócrifos que el proveedor de Pegasus habilita para cumplir con sus labores de espionaje bajo los siguientes criterios: proveedor de servicios de telecomunicaciones, proveedor de servicios de internet, sitios web nacionales, servicios del gobierno, ubicación geográfica, uso de dominios de nivel superior², y nombre del país. Como resultado de este análisis, The Citizen Lab señaló que los sitios web apócrifos relacionados con México para servir como punto de entrada para servicios de espionaje ocupan el primer lugar del total analizado.

Tercera. El 3 de septiembre de este año, el periódico *The New York Times* publicó que el gobierno mexicano ha pagado a NSO Group más de 15 millones de dólares durante tres años por concepto de tres proyectos de espionaje³. La redacción del periódico *Reforma* retomó esta nota y señaló que la adquisición se hizo mediante el único distribuidor autorizado de NSO Group en México, la empresa Balam Seguridad Privada SA de CV⁴. El portal *Wikileaks* divulgó correos electrónicos fechados el 28 de noviembre de 2014 en los que empleados de una subsidiaria de Balam confirman la adquisición del *software* Pegasus por parte de la Procuraduría General de la República, por conducto del entonces director en jefe de la Agencia de Investigación Criminal, Tomás Zerón de Lucio⁵.

Cuarta. En la misma nota del periódico estadounidense, el vocero de NSO Group informó que la empresa israelí tiene por política sólo vender su producto para investigaciones criminales y terroristas; no obstante, declinó comentar si dejará de proveer sus servicios de espionaje a los gobiernos de Emiratos Árabes Unidos y México tras la revelación que hizo The Citizen Lab el 25 de agosto. Mientras tanto, funcionarios de la embajada de México en Estados Unidos afirmaron al *New York Times* que los sistemas de espionaje del gobierno están sujetos a la ley y que hay autorización para emplearlos; además, afirmaron que estas herramientas de espionaje no se emplean contra periodistas ni contra activistas⁶. No obstante, ante los señalamientos hechos por los investigadores canadienses, es de relevancia nacional e interés público tanto que se haya ocultado la adquisición del equipo de espionaje cuanto que se haya hecho mal uso del mismo.

Quinta. Ante los señalamientos hechos en el reporte antes mencionado, cabe recordar que tanto los tratados internacionales que ha suscrito el Estado mexicano cuanto nuestras normas jurídicas nacionales fijan límites estrictos a la intromisión en la vida privada de las personas. El artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos se expresan en idénticos términos: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”. De igual forma, el artículo 16 de nuestra Carta Magna acota el margen de acción de las instituciones del estado en este asunto al señalar, además de la prohibición a la autoridad para molestar a persona alguna sin orden judicial, el carácter inviolable de las comunicaciones privadas. El párrafo 13 de tal artículo establece que:

“Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración (...).”

Las leyes mexicanas, aun las recientemente reformadas, marcan límites claros a la forma, medios y tiempo de los trabajos de investigación, y todas señalan que cualquier forma de intervención deberá hacerse con una adecuada fundamentación y motivación. El artículo 292 del Código Nacional de Procedimientos Penales fija claramente que:

“La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos y, en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención.

El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.”

En idénticos términos se expresa el artículo 17 de la Ley Federal contra la Delincuencia Organizada. Además, también la agencia de inteligencia del Estado mexicano cuenta con controles similares; en los artículos 34, 38, 40 y 43 de la Ley de Seguridad Nacional se define, con limitantes similares a las ya señaladas, la manera en que el Centro de Investigación y Seguridad Nacional puede actuar al intervenir comunicaciones.

Además, el párrafo segundo del artículo 294 del Código Nacional de Procedimientos Penales y el párrafo tercero del artículo 18 de la Ley Federal contra la Delincuencia Organizada marcan ciertos límites sobre los asuntos en los que no pueden hacerse intervenciones:

“En ningún caso se podrán autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.”

No obstante, hay límites adicionales que derivan de las interpretaciones que ha hecho la Suprema Corte de Justicia de la Nación sobre el carácter inviolable de la vida privada de las personas. En tesis aislada, la Segunda Sala ha señalado que:

Derecho a la privacidad o intimidad. Está protegido por el artículo 16, primer párrafo de la Constitución Política de los Estados Unidos Mexicanos. Dicho numeral establece, en general, la garantía de seguridad jurídica de todo gobernado a no ser molestado en su persona, familia, papeles o posesiones, sino cuando medie mandato de autoridad competente debidamente fundado y motivado, de lo que deriva la inviolabilidad del domicilio, cuya finalidad primordial es el respeto a un ámbito de la vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, con la limitante que la Constitución Política de los Estados Unidos Mexicanos establece para las autoridades. **En un sentido amplio, la referida garantía puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente la privacidad o la intimidad, de lo cual deriva el reconocimiento en el artículo 16, primer párrafo, constitucional, de un derecho a la intimidad o vida privada de los gobernados que abarca las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de la vida.**

Amparo en revisión 134/2008. Marco Antonio Pérez Escalera. 30 de abril de 2008. Cinco votos. Ponente: Genaro David Góngora Pimentel. Secretario: Rolando Javier García Martínez.

Novena Época. Registro: 169700. Instancia: Segunda Sala de la Suprema Corte de Justicia de la Nación. Tesis aislada. Fuente: Semanario Judicial de la Federación y su Gaceta. XXVII, mayo de 2008. Materia(s): constitucional. Tesis: 2a. LXIII/2008. Página: 229.

Además, también destaca la Suprema Corte que:

Derecho a la vida privada. Su contenido general y la importancia de no descontextualizar las referencias a la misma. [...] las personas tienen derecho a gozar

de un ámbito de proyección de su existencia que quede reservado de la invasión y la mirada de los demás, que les concierna sólo a ellos y les provea de condiciones adecuadas para el despliegue de su individualidad –para el desarrollo de su autonomía y su libertad– . A un nivel más concreto, la misma idea puede describirse apelando al derecho de las personas a mantener fuera del conocimiento de los demás (o, a veces, dentro del círculo de sus personas más próximas) ciertas manifestaciones o dimensiones de su existencia (conducta, datos, información, objetos) y al correspondiente derecho a que los demás no las invadan sin su consentimiento. En un sentido amplio, entonces, **la protección constitucional de la vida privada implica poder conducir parte de la vida de uno protegido de la mirada y las injerencias de los demás, y guarda conexiones de variado tipo con pretensiones más concretas que los textos constitucionales actuales reconocen a veces como derechos conexos** : el derecho de poder tomar libremente ciertas decisiones atinentes al propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, **la protección contra el espionaje, la protección contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular.**

Amparo directo en revisión 2044/2008. 17 de junio de 2009. Cinco votos. Ponente: José Ramón Cossío Díaz. Secretarios: Francisca María Pou Giménez y Roberto Lara Chagoyán.

Novena Época. Registro: 165823. 1a. CCXIV/2009. Instancia: Primera Sala. Semanario Judicial de la Federación y su Gaceta. Tomo XXX, Diciembre de 2009, Pág. 277.

La información divulgada el mes pasado sobre la posibilidad de haber intentado violar las comunicaciones privadas de al menos un periodista mexicano, sin que haya indicio alguno de la comisión de un delito, lleva a pensar que las instituciones del estado gastan recursos públicos para acosar periodistas y personas que “incomodan” al gobierno. Si es así, resulta totalmente inaceptable que los derechos a la vida privada y la intimidad de una persona se vulneren por causas políticas, completamente opuestas a los ordenamientos jurídicos en la materia.

Por lo anteriormente expuesto, pongo a consideración del pleno la siguiente proposición con

Puntos de Acuerdo

Primero. La Cámara de Diputados solicita a la titular de la Procuraduría General de la República, Arely Gómez González, haga pública la información relativa a las aplicaciones que se han dado al equipo electrónico de espionaje Pegasus.

Segundo. La Cámara de Diputados solicita a la titular de la Procuraduría General de la República detener el uso de todo programa informático de espionaje en los casos en que no exista mandamiento jurídico, por atentar contra la Constitución Política de los Estados

Unidos Mexicanos, los tratados internacionales de los que el Estado mexicano es parte y las normas mexicanas que protegen la vida privada

Notas

1 Bill Marczak y John Scott-Railton, “The Million Dollar Dissident: NSO Group’s iPhone Zero-Days used against a UAE Human Rights Defender”, <https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>

2 El dominio de nivel superior asignado a México es “.mx”.

3 Nicole Perlroth “Phone Spying Is Made Easy. Choose a Plan.”, *The New York Times* , 3 de septiembre de 2106, p. A1.

4 “Adquiere la PGR equipo para espiar”, *Reforma* , 12 de septiembre de 2016, p. 1.

5 <https://wikileaks.org/hackingteam/emails/emailid/5391>. La conversación completa de la subsidiaria de Balam Seguridad Privada SA de CV con una compañía italiana de servicios de seguridad llamada Hacking Team se encuentra en: <https://wikileaks.org/hackingteam/emails/emailid/5455>

6 N. Perlroth, *op.cit.* , p. A1.

Palacio Legislativo de San Lázaro, a 27 de septiembre de 2016.

Diputada Araceli Damián González (rúbrica)