

## **PROPOSICIÓN CON PUNTO DE ACUERDO DE URGENTE U OBVIA RESOLUCIÓN POR EL QUE SE SOLICITA LA CREACIÓN DE UNA COMISIÓN ESPECIAL PARA EL CASO DE ESPIONAJE MEDIANTE EL MALWARE PEGASUS.**

La que suscribe, Diputada federal **Laura Imelda Pérez Segura**, integrante de la LXIV Legislatura del Congreso de la Unión y del Grupo Parlamentario de MORENA, y con fundamento en lo dispuesto por los artículos 58, 59 y 60 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, someto a la consideración de la Comisión Permanente del Congreso de la Unión la presente proposición con Punto de Acuerdo con el tenor de las siguientes:

### **ANTECEDENTES**

El 24 de agosto de 2016, es la fecha en que se da el primer caso de espionaje reportado mediante el uso del software Pegasus, que desarrolla y vende la compañía israelí NSO Group

Pegasus es una herramienta de acceso remoto (RAT por sus siglas en inglés) con capacidades de software espía para dispositivos Android y iOS y es capaz de extraer datos de aplicaciones de mensajería digital como WhatsApp, Facebook y Viber, así como de correo electrónico y navegadores. Este malware espía puede vigilar a distancia a las víctimas a través del micrófono y la cámara del celular infectado, así como realizar capturas de pantalla y registrar las entradas<sup>1</sup> del usuario.

En México, durante el gobierno del presidente Enrique Peña Nieto el Software diseñado como herramienta para perseguir

---

<sup>1</sup> Así logró el software Pegasus espiar a 25 periodistas mexicanos, disponible en: <https://www.forbes.com.mx/tecnologia-asi-software-pegasus-espiar-25-periodistas-mexicanos/>

criminales y terroristas, se convirtió en un instrumento de persecución política.

De acuerdo con una investigación de Amnistía Internacional y Forbidden Stories, alrededor de 15,000 personas entre los que se encuentran políticos, periodistas, abogados, activistas, fiscales, diplomáticos, jueces, médicos y académicos, han sido víctimas de espionaje por el software Pegasus, convirtiendo a México es uno de los países con más casos.

Dentro de los anteriormente mencionados se encuentran al menos 50 personas cercanas al presidente Andrés Manuel López Obrador, entre los que destacan su familia (esposa, hijos y hermanos); su actual equipo de presidencia (Julio Scherer Ibarra, Jesús Ramírez, Gabriel García Hernández y Alfonso Romo); su gabinete (Rocío Nahle, Delfina Gómez, Zoe Robledo, Manuel Barlett y Octavio Romero); y, otros políticos como Claudia Sheinbaum, Ricardo Monreal y Bertha Lujan, entre otros.

NSO Group, empresa israelí y creadora de Pegasus, ha asegurado que solo vende el software a autoridades de países que tienen el fin de perseguir a criminales y terroristas, no obstante, en el caso de México se utilizó para fines políticos.

Ante esta situación la organización Amnistía Internacional (AI) señaló que Pegasus ha sido utilizado para facilitar la comisión de violaciones de derechos humanos a gran escala en todo el mundo.

A su vez, la Secretaria General de AI declaró que la evidencia pone al descubierto que Pegasus es “el arma preferida” de los gobiernos represivos que intentan silenciar periodistas y atacar activistas.

El primer caso de contratación de un malware en México, de acuerdo con información de la Unidad de Inteligencia

Financiera de la Secretaría de Hacienda y Crédito Público, se dio durante el gobierno de Felipe Calderón y fue instrumentado por el entonces Secretario de Seguridad, Genaro García Luna que contrató el software NiceTrack.

A su vez, Santiago Neto, titular de la Unidad de Inteligencia Financiera (UIF) declaró durante la conferencia matutina del presidente Andrés Manuel López Obrador, del pasado 22 de julio del año en curso, que el software Pegasus costó al erario 5 mil 914 millones de pesos, monto que se deriva de la adquisición del software, mantenimiento, ventas a sobre precio y una red de corrupción orquestada desde el gobierno federal.

Detalló, además, que fue durante el sexenio de Enrique Peña Nieto que se adquirió el servicio por 32 millones de dólares, esto mediante la adjudicación de un contrato a favor de Grupo Tech Bull SA de CV, empresa fachada y constituida por Balam Seguridad Privada.

En este sentido y atentos a lo que establecen los tratados internacionales en la materia que ha suscrito el Estado mexicano, podemos citar que el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos establecen que: *“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”*.

Asimismo, el artículo 16 de nuestra Constitución Política establece la prohibición a la autoridad para molestar a persona alguna sin orden judicial y le da carácter de inviolables a las comunicaciones privadas.

Por su parte los párrafos 12 y 13 del artículo citado establecen, respectivamente, que:

**Párrafo 12.- Las comunicaciones privadas son inviolables.** La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

**Párrafo 13.- 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. La autoridad judicial federal no podrá otorgar estas autorizaciones 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.

Por su parte, el **artículo 292 del Código Nacional de Procedimientos Penales** establece 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 concesionaria 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, solo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.*

Además, el artículo 167 del Código Nacional de Procedimientos Penales, considera el espionaje como delito grave y a su vez, el artículo 177 del Código Penal Federal señala que:

*A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.*

Sumado a ello, la ONG Amnistía Internacional ha urgido al gobierno israelí a revocar las licencias de exportación que ha concedido a NSO Group, debido a el riesgo que los softwares de espionaje representan para los derechos humanos.

Paralelo a ello, llamó a NSO Group a cerrar inmediatamente los sistemas de clientes donde haya claros indicios de mal uso del malware. y a su vez emita un informe de transparencia en el que se detalle los casos de mal uso de sus productos, países a los que van destinados, contratos y toda la información necesaria para investigar posibles violaciones de derechos.

Es por lo anterior que se solicita respetuosamente expedir el acuerdo para que se cree una comisión especial que dé seguimiento a las investigaciones de la FGR relativas a los casos de espionaje a través del software Pegasus durante la administración anterior, cuyo objeto resulta violatorio y sancionado por nuestro marco jurídico.

Además, es preciso que la sociedad mexicana conozca a fondo todo lo relacionado con el proceso de compra del software multicitado, el mantenimiento y también los fines que se le dio a dicha información.

Por ello, es necesario que exista información objetiva y pueda ser dada a conocer a la opinión pública y sobre todo se sancione ejemplarmente a quienes hayan realizado esta adquisición, hasta quiénes y cómo se utilizó esta información y con qué fin.

Por lo anteriormente expuesto y con fundamento en lo dispuesto por párrafo primero del artículo 207 del Reglamento de la Cámara de Diputados es que pongo a consideración del pleno la siguiente proposición con:

## **Punto de Acuerdo**

**PRIMERO.** - La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente a la Junta de Coordinación Política de la Cámara de Diputados a expedir el acuerdo para integrar una Comisión Especial con el objetivo coadyuvar y dar seguimiento a las investigaciones de la FGR relativas con el sistema de espionaje **PEGASUS**, contratado durante la administración del expresidente Enrique Peña Nieto, así como promover cualquier acción penal y fincar responsabilidades administrativas a quienes resulten responsables de las conductas presuntamente constitutivas de delito.

**SEGUNDO.** – Con fundamento en el numeral 2 del artículo 207 del Reglamento de la Cámara de Diputados, la comisión se extinguirá una vez cumplido o agotado su objetivo, por lo que habrá un proceso de transición entre las y los legisladores que la integren durante la LXIV Legislatura y quienes la integrarán durante la LXV Legislatura.

**A T E N T A M E N T E**

**DIP. LAURA IMELDA PÉREZ SEGURA**

Palacio Legislativo a 27 de Julio del 2021

## REFERENCIAS:

1. 50 cercanos a AMLO, entre los posibles espiados con el software Pegasus:  
<https://www.forbes.com.mx/50-cercanos-amlo-posibles-espiados-software-pegasus/>
2. Gobierno de Peña pagó 32 mdp por software espía Pegasus: UIF, confirma entramado empresarial:  
<https://www.proceso.com.mx/nacional/2021/7/21/gobierno-de-pena-pago-32-mdd-por-software-espia-pegasus-uif-confirma-entramado-empresarial-268241.html>
3. Estima UIF que Pegasus costó al erario casi 6,000 millones de pesos :  
<https://www.eleconomista.com.mx/politica/Estima-UIF-que-Pegasus-costo-al-erario-casi-6000-millones-de-pesos-20210722-0009.html>
4. Amnistía Internacional pide a Israel frenar la exportación de Pegasus:  
<https://www.forbes.com.mx/amnistia-internacional-israel-freno-exportacion-pegasus/>
5. El 'caso Pegasus': así evolucionó la amplísima red de vigilancia sostenida desde el Gobierno de México:  
<https://elpais.com/mexico/2021-07-25/el-caso-pegasus-asi-evoluciono-la-amplisima-red-de-vigilancia-sostenida-desde-el-gobierno-de-mexico.html>

6. The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. Disponible en <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>
  
7. Así logró el software Pegasus espiar a 25 periodistas mexicanos, disponible en: <https://www.forbes.com.mx/tecnologia-asi-software-pegasus-espiar-25-periodistas-mexicanos/>