**PROPOSICIÓN CON PUNTO DE ACUERDO, PARA EXHORTAR A LA FGR A HACER PÚBLICOS LOS INFORMES SOBRE LOS CONTRATOS REALIZADOS POR LA APF EN LA ÚLTIMA DÉCADA CON LAS EMPRESAS ENCARGADAS DE LA VENTA DE LA LICENCIA Y USO DEL MALWARE VÍA PEGASUS, A CARGO DE LA DIPUTADA AMALIA DOLORES GARCÍA MEDINA, DEL GRUPO PARLAMENTARIO DE MOVIMIENTO CIUDADANO**

La que suscribe, Amalia Dolores García Medina, diputada federal integrante del Grupo Parlamentario de Movimiento Ciudadano en la LXV Legislatura en la Cámara de Diputados, con fundamento en lo señalado en los artículos 6, numeral 1, fracción I, y 79, numeral 1, fracción II, del Reglamento de la Cámara de Diputados, somete a consideración de esta honorable asamblea la siguiente proposición con punto de acuerdo, con base en la siguiente

**Exposición de Motivos**

Pegasus se ha convertido en el caso de espionaje cibernético más grande y peligroso conocido hasta ahora. El Malware vía Pegasus se instala en el teléfono celular sin que la víctima se dé cuenta, a través de un mensaje invisible, el cual permite que puedan ingresar a todos los datos, desde documentos, fotos, contraseñas, incluso micrófono y cámara sin que la víctima se percate de nada de esto.[1]

La fundadora de la Organización Civil francesa Forbidden Stories, Sandrine Rigaud, explicó cómo es y cómo actúa el programa Pegasus: “Es totalmente invisible, así que no sabes si te atacan o cuándo te atacan”, menciona que, “si tu teléfono está infectado, básicamente, cuando este software espía se instala en tu teléfono, puede extraer cualquier cosa de él: fotos, correos electrónicos, códigos de acceso que hayas instalado. Incluso pueden ver los mensajes que intercambias en aplicaciones encriptadas, como Signal o WhatsApp, así que básicamente toda tu vida está en sus manos.[ii]

En una entrevista el 19 de julio de 2021, Edith Olivares, directora ejecutiva de Amnistía Internacional México, comentó que México es uno de los países más afectados por el uso de este malware; también mencionó que a pesar de que su contratación se llevó a cabo en el año 2017 bajo el gobierno de Enrique Peña Nieto expresidente de México, por la Fiscalía General de la República entonces encabezada por el licenciado Jesús Murillo Karam; la investigación realizada por Amnistía internacional y Forbidden Stories arroja que la actual administración no ha terminado el contrato con la compañía israelí NSO Group, lo que es realmente preocupante, ya que no existe hasta el momento ningún documento que aseguré que no se sigue usando recurso público para mantener el software.[iii] Más aún con las crecientes filtraciones por el hackeo a la Secretaría de la Defensa Nacional.

El 29 de septiembre de 2022, se dio a conocer el ciberataque más grande que del que ha sido protagonista el Gobierno de México. El grupo internacional de hackers denominado “Guacamaya”, conocido por haber burlado la seguridad virtual de otros países en Latinoamérica; envío seis terabytes de información que se compartió el portal de noticias Latinus. El portal reveló parte del contenido que recibieron, dando detalles que incluyen la salud del Presidente de la República, así como datos que van desde el 2016 hasta septiembre de este año; en los que se menciona la versión completa del “Culiacanazo”, la seguridad en las aduanas, así como el poder con el que cuenta el Ejercito en la actual administración, espionaje a colectivos feministas, entre otros.[iv]

Al mismo tiempo el día 4 de octubre del 2022, la empresa R3D: Red en Defensa de los Derechos Digitales, Article 19 México y Centroamérica, y SocialTIC, que contaron con el apoyo del Citizen Lab de la Universidad de Toronto, en colaboración con Animal Político, Aristegui Noticias y la revista Proceso, dieron a conocer la investigación **Ejército Espía** en la que se revelan tres nuevos casos de espionaje en contra de periodistas y personas defensoras de derechos humanos en México, con el uso del malware Pegasus, de la empresa NSO Group entre 2019 y 2021, es decir, durante este sexenio.[v]

De acuerdo con el actual gobierno, el contrato con la empresa Pegasus venció en 2013, indican que los contratos encontrados son públicos, se tienen contabilizadas 37 solicitudes de información realizadas a través del Instituto Nacional de Transparencia y Acceso a la Información y Protección de Datos Personales; así como de la Comisión Nacional de los Derechos Humanos, esto declaró la Secretaría de la Defensa Nacional a través de un comunicado publicado el día 4 de octubre del presente año.[vi]

Sin embargo, de acuerdo con la investigación de la empresa R3D: Red en Defensa de los Derechos Digitales, NSO Group ha recibido contratos públicos por 681 millones de pesos desde 2008 a la fecha; esto por medio de "30 empresas fachada constituidas en México, Panamá y Estados Unidos, así como una serie de transferencias de dinero entre compañías fachada. En este rubro destacan pagos de las compañías mexicanas a NSO Group y una transferencia adicional a las cuentas bancarias de Shalev Hulio, uno de los creadores del software espía y director ejecutivo de la compañía".[vii]

Este ataque cibernético realizado por los hackers Guacamaya ha proporcionado evidencia de que el gobierno mexicano sigue utilizando el Malware vía Pegasus, para realizar espionaje contra periodistas, activistas de derechos humanos, e incluso políticos.

El 13 de octubre de 2021durante la comparecencia del titular de la Secretaría de la Función Pública, mencioné que la función fundamental de la secretaria es vigilar que los servidores públicos se apeguen a la legalidad durante sus funciones; esto es indispensable para cualquier administración, por lo que se requiere investigar, tener resultados y sancionar, para que no reine la impunidad; y con mayor razón en esta época donde las tecnologías de la información han diseñado mecanismos extraordinariamente patentes e invasivas en la vida de Las personas; en esa ocasión me refería al Malware vía Pegasus; en ese momento requería atención urgente y medidas que ahora son indispensables, para transparentar la información respecto a los contratos, sobre todo los adquiridos en la administración anterior, pero sobre todo en la actual.

El hackeo realizado por el grupo Guacamaya dejó al descubierto que el sistema Pegasus se sigue usando por el actual gobierno, así como por el ejército; y de acuerdo con Citizen Lab ha sido utilizado para el espionaje contra periodistas, activistas y personas defensoras de derechos humanos, políticos, entre otros.

Durante la comparecencia del secretario de la Función Pública realicé unas preguntas que ahora cobran vigencia y cito a continuación:

- ¿Cómo es que se dio esta adquisición, para los organismos de seguridad del Estado?

- ¿Cuáles eran los protocolos que normaban su actuación?

- ¿Quiénes deciden el manejo de este software? ¿Qué no era para la delincuencia y terrorista? sino que afecto a personas en nuestro país con un manejo político.

En octubre del 2021 esto parecía ser una herramienta que solo se había usado en la administración anterior, incluso el secretario Roberto Salcedo Aquino respondió que la investigación estaba abierta, y que sería la Fiscalía General de la República la encargada de dar a conocer los informes. Los informes existieron, sin embargo, no se mostró la finalización de contratos de manera definitiva y en ningún momento se informó que se realizarían nuevos contratos y el uso que se le daría.

La Constitución Política en el artículo 16, establece que nadie puede ser molestado en su persona, excepto con mandamiento judicial, es una garantía extraordinaria. México ha firmado la Alianza de Países Abiertos, para evitar

el espionaje, lo cual es un delito y la opacidad y simulación en el tema, así como la inversión de recursos públicos y poder a las instituciones para la utilización de este malware, debe ser prioridad para el gobierno.

Dentro del programa anual de trabajo correspondiente al primer año de ejercicio de la LXV Legislatura, de la Comisión de Transparencia y Anticorrupción (octubre 2021-agosto2022); propuse con fundamento en el artículo 152 del Reglamento Interior de la honorable Cámara de Diputados, poner a consideración de los integrantes de la Comisión, la creación de una subcomisión que dé seguimiento al caso del programa informático Pegasus. Sin embargo, al día de la presentación de este punto de acuerdo, no se ha llevado a cabo.[viii]

De acuerdo con el informe de transparencia y responsabilidad de NSO Group, publicado en junio de 2021, la compañía tiene 60 clientes en 40 países. En dicho informe la empresa creadora de Pegasus menciona que la finalidad de este programa es rastrear terroristas y criminales, la cuestión es que cada cliente define sus categorías como y contra quien usarlo. En nuestro país por ejemplo se demostró que se usó para vigilar Periodistas, activistas pro-Derechos Humanos, empresarios y políticos.[ix]

Las investigaciones realizadas por Amnistía Internacional y Forbidden Stories indican que tuvieron acceso a una lista de hasta 50 mil números seleccionados para ser infiltrados con este sistema de espionaje, de los cuales por lo menos 15mil de estos números corresponden a México.[x]

El 29 de julio de 2021 en un documento emitido por Amnistía Internacional le hace un llamado al gobierno mexicano en el cual "solicita a la Presidencia de la República revelar información sobre todos los contratos –pasados, vigentes o futuros- con NSO Group o con otras empresas privadas de vigilancia".[xi] Al mismo tiempo menciona que los objetivos de esta vigilancia y hostigamiento pone en peligro su seguridad, libertad e incluso su vida. Existen casos como el del periodista independiente Marroquí Omar Radi o el defensor de los derechos humanos Anand Teltumbde que han sido encarcelados por la información recopilada de sus intervenciones telefónicas. En México en 2016 se descubrió que se investigaba a la periodista Carmen Aristegui, su equipo e incluso su familia incluyendo a su hijo menor de edad en ese momento; o el caso Jorge Carrasco, el director del semanario mexicano Proceso, quien de acuerdo con el Security Lab de Amnistía Internacional se descubrió que fue víctima en 2016 de un intento de infección por el software Pegasus, entre muchos otros defensores, activistas, periodistas, empresarios y políticos.

Forbidden Stories menciona que las autoridades estadounidenses indican que los cárteles del narcotráfico han tenido acceso a este programa con ayuda de funcionarios corruptos. John Scott-Railton funcionario de la DEA, Agencia Antidroga Estadounidense, menciona que varias empresas privadas de software han vendido sus programas a varios servicios de Policías Federales y de Estados mexicanos.[xii]

El uso y compra de instrumentos de vigilancia debe parar hasta que se cree un marco que lo regule en total apego a los Derechos Humanos. La información sobre este tipo de contratos, vigencia y terminación debe ser pública y en total apego a la ley, la cual deberá prevenir, delimitar y sancionar el abuso de este tipo de herramientas.

Por lo anteriormente expuesto, se somete a consideración de la Cámara de Diputados del honorable Congreso de la Unión la siguiente proposición con

**Punto de Acuerdo**

**Primero. -** La Cámara de Diputados del honorable Congreso de la Unión exhorta al Fiscal General de la República para que haga públicos los informes sobre los contratos realizados por la administración pública federal en la última década hasta la actual administración con la empresa o empresas, encargadas de la venta de la licencia y uso del malware vía Pegasus u otros con la misma finalidad.

**Segundo. -** La Cámara de Diputados del Honorable Congreso de la Unión exhorta a Secretaría de la Función Pública del gobierno federal, para que haga pública la documentación que compruebe que las dependencias públicas cancelaron y/o suspendieron el uso del malware de espionaje como Pegasus y demás, así como las fechas de terminación de la vigencia contratada.

**Tercero. -** La Cámara de Diputados del honorable Congreso de la Unión exhorta a la Fiscalía General de la República para que investigue, compruebe y sancione a servidores públicos, instituciones o quien resulte responsable, por los probables delitos de espionaje contra periodistas, personas activistas de derechos humanos y políticos por el uso del Malware Pegasus; desde el inicio del programa en 2016 a la fecha 2022.

**Notas**

i Amnistía Internacional. (2021). *Proyecto Pegasus: Una filtración de datos masiva revela que el software espía de la empresa israelí NSO Group se utiliza para atacar a activistas, periodistas y figuras políticas en todo el mundo.* Recuperado en*:*

https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/proyecto-pegasus-una-filtracion-de-datos-masiva-revela-que-el-software-espia-de-la-empresa-israeli-nso-group-se-utiliza-para-atacar-a-activistas-periodistas-y-figuras-politicas-en-todo-el-mundo/

iii Forbidden Stories. (2021). *Espionaje en periodistas mexicanos: Una investigación sobre el rentable negocio del ciberespionaje* . Recuperado de: https://forbiddenstories.org/es/espionaje-de-periodistas-mexicanos-una-investigacion-sobre-el-rentable-negocio-del-ciberespionaje/

iv Latinus. (2022) Loret capítulo 96.

https://latinus.us/2022/09/29/loret-capitulo-96/

v Amnistía Internacional (2022, 4 de octubre). Nuevos casos de espionaje con Pegasus en México no deben quedar en la impunidad https://amnistia.org.mx/contenido/index.php/nuevos-casos-de-espionaje-con-pegasus-en-mexico-no-deben-quedar-en-la-impunidad/

vi Latinus. (2022, 4 de octubre). Sedena niega que se espíe a periodistas y activistas en el actual gobierno: "El contrato de Pegasus venció en 2013" https://latinus.us/2022/10/04/sedena-niega-espie-periodistas-activistas-actual-gobierno-contrato-pegasus-vencio-2013/

vii Aristegui Noticias. (2021). Pegasus Project: la red de empresas que vendió Pegasus al gobierno de Peña Nieto https://aristeguinoticias.com/2107/mexico/pegasus-project-la-red-de-empresas-que-vendio-pegasus-al-gobierno-de-pena-nieto/

viii Programa anual de trabajo correspondiente al primer año de ejercicio de la LXV Legislatura. (2021) página 42 https://portalhcd.diputados.gob.mx/PortalWeb/Comision/5dd9143b-3d39-4483-8818-deb1314a8282/ProgramaTrabajo/284d4f94-0aff-4adf-b762-0b63641dfb0 4.pdf

ix Forbidden Stories. (2021). *Pegasus: La nueva arma mundial para silenciar a los periodistas* . Recuperado de: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

x Amnistía Internacional (2021, 29 de julio). *Amnistía Internacional hace un llamado al gobierno mexicano a publicar el contrato con Pegasus y a legislar para proteger a la población de la cibervigilancia.* Recuperado de:

https://amnistia.org.mx/contenido/index.php/amnistia-internacional-hace -un-llamado-al-gobierno-mexicano-a-publicar-el-contrato-con-pegasus-y-a -legislar-para-proteger-a-la-poblacion-de-la-cibervigilancia/

xi Amnistía Internacional (2021, 29 de julio). Amnistía Internacional hace un llamado al gobierno mexicano a publicar el contrato con Pegasus y a legislar para proteger a la población de la cibervigilancia. Recuperado de: https://amnistia.org.mx/contenido/index.php/amnistia-internacional-hace -un-llamado-al-gobierno-mexicano-a-publicar-el-contrato-con-pegasus-y-a -legislar-para-proteger-a-la-poblacion-de-la-cibervigilancia/

xii Forbidden Stories. (2021). *El Proyecto Pegasus.* Recuperado de: https://forbiddenstories.org/es/espionaje-de-periodistas-mexicanos-una- investigacion-sobre-el-rentable-negocio-del-ciberespionaje/

Dado en el Palacio Legislativo de San Lázaro, a 11 de octubre de 2020.

Diputada Amalia Dolores García Medina (rúbrica)

Sistema de Información Legislativa de la Secretaría de Gobernación http://sil.gobernacion.gob.mx/portal
Fuente: "http://www.diputados.gob.mx/"