INICIATIVA QUE REFORMA EL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, A CARGO DEL DIPUTADO JAVIER SALINAS NARVÁEZ, DEL GRUPO PARLAMENTARIO DE MORENA

El suscrito, Javier Salinas Narváez, integrante del Grupo Parlamentario de Morena en la LXIV Legislatura del Congreso de la Unión, con fundamento en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, y 6, numeral 1, fracción I, 77 y 78 del Reglamento de la Cámara de Diputados, somete a la consideración del pleno de la Cámara de Diputados la siguiente iniciativa con proyecto de decreto de reforma constitucional para facultar al congreso de la unión para legislar en materia de ciberseguridad.

Exposición de Motivos

En los últimos años, el número de internautas y el porcentaje de hogares con acceso a Internet en México se ha incrementado rápidamente. La penetración del servicio ha aumentado considerablemente, pasando de 12.8 millones de usuarios en 2004 a 74.3 millones en 2018, lo que significa que el 65.1 por ciento de la población de seis años o más en México es usuaria de Internet, lo que representó un avance de 4.2 puntos porcentuales con respecto a 71.3 millones reportados en 2017, según revelan los datos de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, levantada por el Inegi.

Desafortunadamente, el rápido aumento de la conectividad no ha sido acompañado de una política integral que garantice la protección de los derechos de los usuarios, la protección de la información y la seguridad nacional.

En los últimos años, el dinamismo observado por el desarrollo de las tecnologías de la información ha abierto nuevos frentes para la defensa de los derechos humanos y de los países. Esto es así porque el problema de la seguridad en el ciberespacio (ciberseguridad) es multidimensional. En un primer plano se encuentra la actividad relacionada con el ciberactivismo político, donde la frontera entre la libertad de expresión y lo permisible es muy tenue, pero que requiere un tratamiento distinto porque los daños potenciales son mínimos y meramente políticos. En un segundo plano, ubicamos la ciberactividad relacionada con la comisión de delitos, la cual se encuentra tipificada de manera incipiente en la codificación penal y de seguridad pública. Y en un tercer plano, se haya la ciberactividad que impacta en la seguridad nacional, poniendo en riesgo la información e instalaciones consideradas de seguridad nacional, la cual carece de un marco jurídico adecuado en el país.

El Índice Global de Ciberseguridad 2017 (Global Cybersecurity Index), de la Unión Internacional de Telecomunicaciones, situó a México en el lugar 28 del *ranking* mundial, y en el tercero de América, asignándole 0.660 puntos de 1 000. Empero, en 2018 caímos al lugar 63, el cuarto lugar en el continente, con 0.629 puntos, muy lejos de los estándares de nuestros principales socios comerciales, Estados Unidos, que ocupa el segundo lugar y Canadá que ocupa el noveno lugar.

Garantizar la seguridad de los usuarios y del Estado en el ciberespacio se ha convertido en un objetivo prioritario en las agendas de la mayoría de los gobiernos, ya que puede afectar los derechos de los cibernautas en cuestiones tales como ciberacoso, *ciberbullying,* fraudes cibernéticos, acoso sexual, extorsión a las empresas mediante el secuestro, por ejemplo, de su contabilidad, y afectaciones a la seguridad nacional.

En este sentido, la protección del ciberespacio es un nuevo campo que requiere ser defendido y que incluso ya ha sido área de confrontaciones entre países.

Por tales razones, es indispensable construir una Estrategia Nacional de Ciberseguridad, semejante a la de otros países, que incluya un fuerte marco jurídico; promover buenas prácticas; formar especialistas; colaborar con la iniciativa privada; y vigorizar la ciberdefensa.

Para tal efecto, se requiere legislar en dos frentes:

En primer lugar, se requiere **establecer una legislación nacional en materia de ciberacoso, robo de información personal y espionaje en la Internet.**

Es urgente redefinir el marco jurídico mexicano para asegurar la seguridad de los usuarios de internet. Para nadie es una novedad el que el uso de las tecnologías de la información ha desencadenado graves riesgos para los usuarios de internet.

Los riesgos más comunes son sin duda el ciberacoso *(cyberbullying);* el robo de información personal para fraudes bancarios; y el espionaje.

El ciberacoso afecta en mayor medida a niños y adolescentes. Los resultados psicológicos y emocionales son parecidos a los del acoso escolar tradicional. De acuerdo con estadísticas del Inegi (Módulo sobre Ciberacoso Mociba 2015), más de 25 por ciento de los mexicanos entre 12 y 19 años reportan haber sido víctimas de ciberacoso.

Este fenómeno tiene múltiples formas: llamadas, mensajes, contenido multimedia, robo de identidad y publicación de información personal. El efecto de este delito no debe ser subestimado; cerca del 60 por ciento de suicidios entre adolescentes en México están vinculados con diversos tipos de *bullying*, incluyendo el ciberacoso.

Los ciudadanos también pueden enfrentar el robo de su información personal, tales como las contraseñas de las cuentas bancarias para la comisión de fraudes. De acuerdo con un estudio de *Mckinsey and Compañy* (Perspectiva de Ciberseguridad en México, 2018)), en 2017 *Facebook* estimó que existían 270 millones de perfiles falsos o duplicados en su plataforma. Empero, también somos responsables de cuidar la información de nuestros contactos. En el 2015, un asociado de *Cambridge Analytica* lanzó una aplicación que encuestaba a usuarios de Facebook para uso presuntamente académico. Aunque menos de 300 mil personas bajaron la aplicación se recopilaron los datos de 87 millones de usuarios.

También podemos ser víctimas de amenazas o espionaje por nuestro trabajo o afiliación política. Éstas pueden llegar a incluir amenazas de muerte. Como todos recordamos, en 2017, 21 personas –entre políticos, periodistas y activistas– fueron víctimas de ciberespionaje por el gobierno a través del spyware Pegasus, según una investigación del Citizen Lab de la Universidad de Toronto y del *New York Times.*

De ahí la necesidad de redefinir el marco jurídico nacional para la ciberseguridad de los usuarios de los servicios digitales, armonizando las legislaciones federales y estatales, garantizando la protección de nuestros datos personales y dotar a los cuerpos der seguridad de las herramientas adecuadas para la prevención e investigación de las conductas delictivas en el ciberespacio que afectan a las personas y su patrimonio.

En segundo lugar, se requiere **establecer un marco legal en materia de ciberseguridad nacional.**

Una cuestión que se encuentra poco desarrollada en nuestro país, es la relativa a la ciberseguridad en las instituciones del Estado, a pesar de tratarse de un claro asunto de seguridad nacional.

El gobierno almacena y administra importantes volúmenes de información nuestra, de los ciudadanos, tales como datos de identificación, información electoral, tributaria, sobre educación y salud, domicilio, teléfono, y familiares, entre otras. Consecuentemente, es obligación del Estado protegernos frente a riesgos cibernéticos. En México, se han presentado casos de vulnerabilidad a los sistemas del sector público, como el que afectó al INE, cuando una base de datos del listado nominal de electores se alojaba en la nube de la empresa Amazon

Web Services sin contraseña alguna, y se expusieron nombres, apellidos, direcciones y números de identidad de más de 93 millones de mexicanos.

Por otra parte, los gobiernos poseen y operan infraestructura pública para proveer servicios a los ciudadanos, como electricidad, agua, manejo de desechos, telecomunicaciones, servicios de salud, educación y asistencia social. Estos activos pueden sufrir ciberataques que afectan la prestación de servicios a millones de personas. Por ejemplo, en 2017, un ataque a la red eléctrica de Ucrania provocó fallas en el servicio.

De acuerdo con el Índice Global de Ciberseguridad (Unión Internacional de Comunicaciones, ITU), de Naciones Unidas, México figura entre los países con nivel medio en cuanto a capacidad para enfrentar el problema.

Muchos gobiernos han desarrollado estrategias nacionales para alcanzar la ciberresiliencia y ya están en su segunda o tercera versión de la misma. Sin embargo, en nuestro país, recién iniciamos en 2017 con la Estrategia Nacional en la materia, con magros resultados, dado el cierre de la administración de Peña Nieto. Empero, en lo fundamental, sólo se han adoptado estrategias para el sector financiero.

En México tenemos un marco legal para la protección de datos personales cubierto principalmente por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (para organismos no gubernamentales) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (para organismos gubernamentales). Sin embargo, la complejidad tecnológica del problema y su diversidad son factores que dificultan también su combate.

Por ello se requiere establecer mecanismos de defensa activa, de respuesta y de mitigación del impacto de ciberataques dentro de los organismos de gobierno, de recopilación y difusión de inteligencia, y de combate al cibercrimen. Dichos mecanismos deben incluir planes de contingencia de operación, comunicaciones, y manejo de reputación de las instituciones afectadas.

En este tenor, se requiere un marco legal habilitador de la ciberseguridad nacional del país, enfocado en fortalecer la prevención de ciberataques y responder de manera correcta ante los incidentes.

Fundamento legal

Por lo expuesto, con fundamento en lo dispuesto en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, y 77, 78 y demás relativos y aplicables del Reglamento de la Cámara de Diputados, se somete a consideración del pleno de la Cámara de Diputados la siguiente iniciativa con proyecto de

Decreto de reforma constitucional para facultar al Congreso de la Unión para legislar en materia de ciberseguridad

Único. Se **modifica** la fracción XXIX-M del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Artículo 73. ...

I. a XXIX-L. ...

XXIX-M. Para expedir leyes en materia de seguridad nacional, estableciendo los requisitos y límites a las investigaciones **de seguridad cibernética y proteger los derechos humanos en el ciberespacio.**

XXIX-N. a XXXI. ...

Transitorio

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

Palacio Legislativo de San Lázaro, a 24 de septiembre de 2019.

Diputado Javier Salinas Narváez (rúbrica)