INICIATIVA QUE REFORMA Y ADICIONA LOS ARTÍCULOS 14, 18 Y 20 DE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA, A CARGO DE LA DIPUTADA ADRIANA GABRIELA MEDINA ORTIZ, DEL GRUPO PARLAMENTARIO DE MOVIMIENTO CIUDADANO

La suscrita, diputada Adriana Gabriela Medina Ortiz, integrante del Grupo Parlamentario de Movimiento Ciudadano en la LXIV Legislatura de la Cámara de Diputados, con fundamento en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, 6, numeral 1, fracción I, y 77 y 78 del Reglamento de la Cámara de Diputados del honorable Congreso de la Unión, somete a consideración de esta asamblea la siguiente **iniciativa con proyecto de decreto que reforma la fracción XIX, recorriéndose y modificándose las subsecuentes al artículo 14; se reforma la fracción XXV, recorriéndose y modificándose las subsecuentes al artículo 18, y se adiciona un inciso e) a la fracción III del artículo 20 de la Ley del Sistema Nacional de Seguridad Pública, para impulsar una cultura de seguridad cibernética orientada a la transparencia, rendición de cuentas, prevención, resiliencia y estricto apego a los derechos humanos en nuestro país, con base en la siguiente**

Exposición de Motivos

En las últimas décadas hemos sido testigos de un crecimiento exponencial en las posibilidades del mundo digital y su impacto cultural, político, económico y social tanto a nivel personal como a nivel global. Por ejemplo, de existir 4 mil 300 millones de conexiones a internet en 2011, al día de hoy se proyectan "340 mil millones de millones de millones de direcciones IP únicas".[1]

En consecuencia, se puede apreciar que el desarrollo de las tecnologías de la información y la socialización del mundo digital representa una de las oportunidades más grandes que ha tenido la humanidad para comunicarse, crear y reforzar los lazos de unidad, mejorar la calidad de vida, conocer y aprovechar las diferencias para construir sociedades más prósperas y libres. Sin embargo, en ese abanico de posibilidades existen también espacios de conflicto que han derivado en diversas acciones y eventos en los que por incentivos económicos, políticos o bélicos, personales o comunitarios, se han vulnerado derechos humanos, estabilidad económica y financiera, confianza institucional, de individuos en lo particular, organizaciones públicas y privadas y naciones enteras en lo general.

Ante dicha realidad creada a partir del ciberespacio, definido como "el conjunto de dispositivos conectados a través de redes basadas en IP, no solo internet", surge la necesidad de protección, individual y colectiva, de derechos, propiedades, recursos, capacidades, bienes y servicios vinculados a la seguridad de personas y la estabilidad de naciones. En consecuencia de manera transversal se plantea el ámbito de la seguridad cibernética o ciberseguridad, que recorre necesidades en planos personales a internacionales y de las materias de la seguridad individual hasta la seguridad nacional e internacional. Ello exige "la creación de estrategias, normas e instituciones para hacer del ciberespacio un espacio más estable y seguro, y busca proteger la información y los datos (información personal, de propiedad intelectual y de comunicaciones) y reducir el riesgo de perturbaciones en el entorno cibernético y en las infraestructuras y los servicios críticos que dependen de él".[2]

A partir de esta realidad, generada en lo que probablemente es el ámbito de mayor libertad que tiene el ser humano dentro de las estructuras que ha creado, se plantean divergencias axiológicas que impactan en las políticas públicas a partir de dicotomías como libertad individual contra "seguridad colectiva"; interés colectivo contra "seguridad nacional"; libre expresión contra censura; "certidumbre comercial" contra "libre comercio", etcétera.

Derivado de lo anterior, en el marco internacional se han definido una serie de lineamientos y consensos sobre la ruta deseable para que los marcos legales nacionales e internacionales respeten las libertades y los derechos humanos por sobre todos los aspectos regulatorios y policiales que se desee o se requieran aplicar. Ello, ha

derivado en la construcción de instituciones cuya velocidad y efectividad se ha definido con mayor énfasis en tres factores, la organicidad de las sociedades, las condiciones geopolíticas de los países y el alcance de las perspectivas que los grupos de poder al interior de cada país tengan.

Así, por ejemplo, desde hace años el Reino Unido ha planteado una estrategia de ciberseguridad que se actualiza cada cinco años y desde 2011 a la fecha ha invertido alrededor de 860 millones de libras; Canadá tiene estrategias de seguridad cibernética desde la década del 2000; Jamaica tiene estrategias en esta materia desde 2013; Colombia desde 2011; Panamá desde 2013; Estonia desde 2008; Israel, Estados Unidos y la mayoría de los Estados europeos entre 1997 y 2010, y Corea del Sur desde 2014. Todo ello, desarrollando presupuestos, políticas públicas, proyectos de generación de capacidades en sus sociedades e información pública que les permite ir modulando sus estrategias y replanteando sus objetivos y alcances.

En nuestro país se decidió generar la Estrategia de Seguridad Cibernética hasta 2017, para ser observada a mediados de 2018, en consecuencia el rezago es evidente y se refleja en actividades antisociales y probables delitos que van desde intrusión en equipos hasta la parálisis de áreas de instituciones, pasando por fraudes a usuarios de banca electrónica o robo de identidad.

Por ejemplo, de acuerdo con la justificación de la presentación de la Estratega Nacional de Seguridad Cibernética, "la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) señala que durante el primer trimestre de 2011, el fraude cibernético pasó del 7 por ciento (38 mil 539 quejas) de las reclamaciones por posible fraude, al 42 por ciento (639 mil 857 quejas) en el mismo periodo del 2017. El monto reclamado en el primer trimestre de 2017 asciende a mil 167 millones de pesos, del cual se abonó el 53 por ciento del total; y el 90 por ciento de los asuntos se resolvieron a favor del usuario. En cuanto al canal por donde más se presenta el fraude cibernético, el 91 por ciento es por comercio electrónico y llama la atención el incremento de las operaciones por internet para personas físicas y de banca móvil (167 por ciento y 74 por ciento respectivamente) en comparación al año anterior.

Por su parte, en 2017 el promedio mensual de fraudes cibernéticos en comercio electrónico fue de 193 mil casos, cuando el año anterior era de solo 131 mil. En cuanto a fraudes cibernéticos en banca móvil, en el mes de marzo de 2017 se presentó una cifra histórica con 3 mil 682 casos". Es decir no somos inmunes y se afecta a un espectro importante de la sociedad, tal vez lo pasamos desapercibidos porque no tenemos información pública estandarizada, ni transparencia y rendición de cuentas en lo que hace o deja de hacer el Estado mexicano, dejando dispersos los esfuerzos particulares y gubernamentales en materia de seguridad cibernética.

En este contexto, a pesar de la publicación de la estrategia, la creación de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico y la intención de crear un Catálogo Nacional de las Infraestructuras Críticas de la Información (CNICI), hoy no hay ni información ni certidumbre para valorar el alcance de esos esfuerzos.

Asimismo, al revisar la información en materia de seguridad cibernética lo que se encuentra es una dispersión de esfuerzos de generación de información, no estandarizados, ni validados que como consecuencia impiden articular políticas públicas, los procesos de toma de decisiones al respecto y la participación de la sociedad. Todos estos elementos indispensables para lograr la preservación de nuestras libertades y el despliegue de la seguridad, misma que dentro de las circunstancias particulares del ciberespacio, obligan a cualquier gobierno a apoyarse en los individuos y las empresas para asegurar su infraestructura estratégica, prevenir ataques, disminuir la incidencia de delitos cibernéticos.

En consecuencia, como un primer paso para transformar esta riesgosa e irresponsable realidad en la que se haya nuestro país, presento ante esta soberanía, una propuesta para que a través del Sistema Nacional de Seguridad Pública, las mexicanas y mexicanos tengamos acceso a una fuente de información confiable que nos permita

valorar las acciones en la materia, sus impactos y generar una perspectiva más realista sobre los retos que enfrenta nuestra nación en materia de seguridad cibernética. Ello, a partir de tres modificaciones a la Ley del Sistema Nacional de Seguridad Pública para que el Consejo Nacional pueda promover entre los distintos actores sociales la cooperación en materia de seguridad cibernética con estricto respeto a los derechos humanos, para que el Secretariado Ejecutivo pueda generar información en materia de seguridad cibernética, integrando la información que genera el resto de los actores sociales, y para que el Centro Nacional de Prevención del Delito y Participación Ciudadana promueva una cultura de seguridad cibernética respetuosa de los derechos humanos en gobierno y sociedad.

Por lo anteriormente expuesto y fundado, me sirvo someter a consideración de esta soberanía, la siguiente iniciativa con proyecto de

Decreto que reforma la fracción XIX, recorriéndose y modificándose las subsecuentes al artículo 14; se reforma la fracción XXV, recorriéndose y modificándose las subsecuentes al artículo 18, y se adiciona un inciso e) a la fracción III del artículo 20 de la Ley del Sistema Nacional de Seguridad Pública para impulsar una cultura de seguridad cibernética orientada a la transparencia, rendición de cuentas, prevención, resiliencia y estricto apego a los derechos humanos en nuestro país.

Artículo Único. Se reforma la fracción XIX, recorriéndose y modificándose las subsecuentes al artículo 14; se reforma la fracción XXV, recorriéndose y modificándose las subsecuentes al artículo 18, y se adiciona un inciso e) a la fracción III del artículo 20 de la Ley del Sistema Nacional de Seguridad Pública para quedar como sigue:

Artículo 14. El Consejo Nacional tendrá las siguientes atribuciones:

I. a **XVII.** ...

XVIII. Crear grupos de trabajo para el apoyo de sus funcion***es;***

XIX. Promover la cooperación entre instancias de los tres niveles de gobierno, instituciones académicas, organizaciones empresariales y sociedad civil organizada para el intercambio de información, mejores prácticas y tecnologías en materia de seguridad cibernética con estricto respeto a los derechos humanos, y

XX. Las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento del Sistema.

Artículo 18. Corresponde al secretario ejecutivo del Sistema:

I. a **XXIII. ...**

XXIV. Coordinar la homologación de la carrera policial, la profesionalización y el régimen disciplinario en las instituciones de seguridad pública;

XXV. Generar información estadística de carácter público sobre seguridad cibernética integrando la información que generen las instituciones de seguridad pública de los tres niveles de gobierno, organizaciones de la sociedad civil, organismos empresariales e instituciones académicas, y

XXVI. Las demás que le otorga esta ley y demás disposiciones aplicables, así como las que le encomiende el Consejo Nacional o su presidente.

Artículo 20. El Centro Nacional de Prevención del Delito y Participación Ciudadana tendrá como principales atribuciones:

I. ...

II. ...

III. ...

a) ....

b) ....

c) Prevenir la violencia generada por el uso de armas, el abuso de drogas y ***alcohol;***

d) Garantizar la atención integral a las víctimas, y

e) Promover prácticas orientadas a la construcción de una cultura preventiva y resiliente de seguridad cibernética cuyo eje central sea el respeto a los derechos humanos.

IV. a **VI. ...**

VII. Organizar seminarios, conferencias y ponencias sobre prevención social del delito **y seguridad cibernética** ;

VIII. a **X.** ....

Transitorios

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

Segundo. A partir de la entrada en vigor del presente decreto, el Ejecutivo federal tendrá hasta 180 días para realizar las adecuaciones a que haya lugar en reglamentos, normas y acuerdos que correspondan.

Notas

1 Semar, Seguridad y Defensa en el Ciberespacio, Cesnav, México, 2015.

2 James Andrew Lewis, *Experiencias avanzadas en políticas y prácticas de ciberseguridad,* Banco Interamericano de Desarrollo-Porrúa, 2016.

Dado en el Palacio Legislativo de San Lázaro, a 9 de abril de 2019.

Diputada Adriana Gabriela Medina Ortiz (rúbrica)