HONORABLE ASAMBLEA:

A la Segunda Comisión de Relaciones Exteriores, Defensa Nacional y Educación Pública fueron turnados el Punto de Acuerdo que exhorta a la Secretaría de Relaciones Exteriores a iniciar los trabajos necesarios para la adhesión de México al Convenio de Budapest, a efecto de garantizar mayores instrumentos jurídicos para hacer frente a los delitos cibernéticos y el Punto de Acuerdo por el que exhorta a la Secretaría de Relaciones Exteriores a adherirse al Convenio de Budapest y su protocolo adicional, así como al Convenio 108 en materia de Ciberseguridad.

Con fundamento en el artículo 78 fracción III de la Constitución Política de los Estados Unidos Mexicanos; de los artículos 116, 127 y demás aplicables de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos; así como de los artículos 58, 60, 87, 88, 176 y demás aplicables del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, las y los legisladores integrantes de la Segunda Comisión, emitimos el presente dictamen, el cual se realiza de acuerdo con la siguiente:

METODOLOGÍA

I. En el capítulo **"ANTECEDENTES"** se da constancia del trámite de inicio del proceso legislativo, del recibo de turno de referidas Proposiciones y de los trabajos previos de la Comisión.

II. En el capítulo correspondiente a **"CONTENIDO DE LAS PROPOSICIONES"**, se exponen los motivos y alcance de la propuesta en estudio, asimismo, se hace una breve referencia de los temas que la componen.

III. En el capítulo de **"CONSIDERACIONES"**, la Comisión expresa los argumentos de valoración de la propuesta y los motivos que sustentan el dictamen de las Proposiciones en análisis.

I. ANTECEDENTES

En Sesión celebrada con fecha 30 de mayo del 2017 por la Comisión Permanente del Honorable Congreso de la Unión, se presentó Proposición con Punto de Acuerdo que exhorta a la Secretaría de Relaciones Exteriores a iniciar los trabajos

necesarios para la adhesión de México al Convenio de Budapest, a efecto de garantizar mayores instrumentos jurídicos para hacer frente a los delitos cibernéticos, del Dip. Jesús Valencia Guzmán, del Grupo Parlamentario del Partido de la Revolución Democrática.

Con esa misma fecha, mediante oficio No. CP2R2A.-1105 la Mesa Directiva de la Comisión Permanente, dispuso que la Proposición de referencia se turnara a la Segunda Comisión.

En Sesión celebrada con fecha 7 de junio del 2017 por la Comisión Permanente del Honorable Congreso de la Unión, se presentó Proposición con Punto de Acuerdo por el que exhorta a la Secretaría de Relaciones Exteriores a adherirse al Convenio de Budapest y su protocolo adicional, así como al Convenio 108 en materia de Ciberseguridad, de la Dip. Sofía González Torres e integrantes del Grupo Parlamentario del Partido Verde Ecologista de México.

Con esa misma fecha, mediante oficio No. CP2R2A.-1385 la Mesa Directiva de la Comisión Permanente, dispuso que la Proposición de referencia se turnara a la Segunda Comisión.

II. CONTENIDO DE LA PROPOSICIÓN

El promovente del primer punto precisa que en la sociedad moderna el vertiginoso desarrollo de las Tecnologías de la Información y de la Comunicación (TIC´s) trajo consigo cambios en los hábitos de las personas, generando y aportando grandes beneficios, pero también costos y riesgos como consecuencia del avance informático en la sociedad. A partir del uso masivo de herramientas basadas en las TIC´s como la telefonía celular, el internet y las redes sociales, cada vez es más notoria su influencia en la convivencia entre las personas, el acceso a la información y los vínculos entre ciudadanos. La penetración social que la TIC ha tenido en México alcanza tendencias mundiales, lo cual es innegable.

Señala que en México, según datos del INEGI, en abril de 2014, se registraron 47.4 millones de personas de seis años o más en el país usuarias de los servicios que ofrece Internet, que representan aproximadamente el 44.4% de esta población, con base en el Módulo sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares 2014 (MODUTIH 2014), mostrando una tasa anual de crecimiento de 12.5%, en el periodo del 2006 al 2014.

Menciona que el acelerado crecimiento en el uso de las tecnologías de la información conlleva también, de manera lamentable un gran riesgo para

quienes navegan en la red. Bajo esa lógica, México ocupa el último lugar en materia de ciberseguridad de la lista de países miembros de la OCDE, el cual según cálculos de la Organización de Estados Americanos (OEA), alcanzó un impacto en México tasado en 3,000 millones de dólares, en el 2014.

En consecuencia, los delitos realizados a través de una computadora o dispositivo informático, conocidos también como delitos informáticos o ciberdelicuencia, han estado en constante crecimiento y transformación. El delito informático se puede definir como toda aquella conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático.

Señala además que los delitos cibernéticos por su misma naturaleza no conocen fronteras físicas ni barreras que impidan su proliferación, la comunidad internacional se ha preocupado para establecer mecanismos de coordinación para hacer frente a éste flagelo, tales como el Convenio de Budapest contra la Ciberdelincuencia, el cual se origina toda vez que "es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos, garantizando la tipificación como delito de dichos actos". Se trata del primer tratado internacional, creado por el Consejo de Europa en 2001, cuyo objetivo es enfrentar los delitos informáticos a través de la "armonización" de leyes y una mayor cooperación entre los países miembro.

Finalmente, propone el siguiente resolutivo:

> **"ÚNICO.** La Comisión Permanente del H. Congreso de la Unión exhorta, respetuosamente, a la Secretaría de Relaciones Exteriores para que, en el ámbito de sus competencias, inicie los trabajos necesarios para la adhesión de México al Convenio de Budapest a efecto de garantizar mayores instrumentos jurídicos para hacer frente a los delitos cibernéticos."

La promovente de la segunda Proposición manifiesta que en México se ha avanzado en la legislación para la protección de datos personales y se trabaja en una estrategia de seguridad de la información con el objeto de asegurar y resguardar la integridad, confidencialidad y privacidad de la información de las personas e instituciones públicas y privadas. Al respecto, el intercambio de información con nuestros socios regionales se debe dar en el marco de acuerdos establecidos y por medio de los canales diplomáticos e institucionales

pertinentes, a fin de garantizar el diálogo, la cooperación y la estabilidad nacional y regional.

Precisa que el aumento de las amenazas vinculadas con la gestión del ciberespacio se ha convertido en una fuente de preocupación para todos los países. El incremento de los ataques en contra de la infraestructura crítica, los intereses económicos, las redes de información y las capacidades de defensa de naciones específicas, demuestra que existen gobiernos, grupos criminales y organizaciones terroristas dispuestas a explotar el ciberespacio con propósitos hostiles.

Menciona que hace unas semanas el mundo fue víctima y testigo de un ciberataque con alcance transcontinental que ha afectado a más de 100 países, mediante un virus llamado Wanna Cry. De acuerdo con lo declarado por el Director de Investigación y Análisis en América Latina de Kaspersky Lab, Dmitry Bestuzhev, al menos 500 organizaciones en nuestro país fueron afectadas por el programa informático nocivo conocido como ransomware. El virus Wanna Cry infectó desde los equipos de 16 hospitales y centros de salud en Reino Unido, hasta los de la empresa de automóviles Renault, en Francia, que se ha visto obligada a parar la producción de varias plantas en el país, pasando por los del Ministerio del Interior ruso. Incluso, una de las oficinas financieras vinculadas a Renault en París ha anunciado inminentes medidas de seguridad tanto en los teléfonos móviles de los empleados como en los ordenadores de mesa.

Precisa que la Seguridad Cibernética resulta un tema complejo debido a que converge en un asunto híbrido, es decir, conlleva un aspecto de Seguridad Nacional y a su vez, constituye un asunto de Seguridad Interior. En primer término, es un asunto de Seguridad Nacional toda vez que los ataques en el ciberespacio pueden originarse desde el sitio más lejano, como puede ser otro país o continente, con la intención de desestabilizar la soberanía nacional y atentar contra el Estado Mexicano.

En un segundo plano, compete a la Seguridad Interior cuando estos ataques provienen desde el interior de nuestro país, ya sea por una o varias personas pertenecientes a miembros de la delincuencia organizada que buscan desestabilizar o atentar contra nuestras instituciones o una industria específica, creando así una amenaza contra el orden interno del Estado Mexicano.

El resolutivo que propone es el siguiente:

"ÚNICO. La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente exhorta a la Secretaría de Relaciones Exteriores para que, a través de la Dirección General para Europa, realice las acciones necesarias para la adhesión de México al Convenio de Budapest y su protocolo adicional, así como al Convenio 108 del Consejo de Europa, con el objetivo de enriquecer el marco jurídico en materia de Ciberseguridad."

III. CONSIDERACIONES

1. Las y los legisladores integrantes de la Segunda Comisión de Relaciones Exteriores, Defensa Nacional y Educación Pública coinciden en la necesidad de contar con marcos normativos que garanticen la seguridad de las personas ante los riesgos exponenciales del uso de las tecnologías de la información y comunicación.

2. En ese sentido, la dictaminadora coincide en que el Estado Mexicano cuente con herramientas para la prevención y sanción de los denominados ciberdelitos que, como los define la Organización para la Cooperación y Desarrollo Económico son cualquier conducta, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos; ejemplo de ellos son distribución de códigos maliciosos, robo de información, distribución y almacenamiento de pornografía infantil, acoso, extorsión, estafas comerciales y bancarias.

3. Reportes de la Organización de Estados Americanos y de la Policía Cibernética de nuestro país mencionan que, las pérdidas anuales por los ciberdelitos en México ascienden a 3 mil millones de dólares. En 2015, la ciberdelincuencia tuvo un costo de 101 mil 400 millones de pesos, de acuerdo con Symantec, lo que representa 13 veces más de lo obtenido por fraudes bancarios el año previo. Además, se considera el segundo delito más importante en México después del narcotráfico que afecta al menos a cinco de cada seis empresas con 22 millones de personas que han sido víctimas de esas conductas delictivas.

4. A esos datos se suma el hecho que México, según datos del INEGI, en abril de 2014, se registraron 47.4 millones de personas de seis años o más en el país usuarias de los servicios que ofrece Internet, que representan aproximadamente el 44.4% de esta población, con base en el Módulo sobre Disponibilidad y Uso de las Tecnologías de la Información en los

Hogares 2014 (MODUTIH 2014), mostrando una tasa anual de crecimiento de 12.5%, en el periodo del 2006 al 2014. Para el segundo trimestre de 2015, el 57.4 por ciento de la población de seis años o más en México, se declaró usuaria de Internet, equivalente a 62.4 millones de personas. Éste acelerado crecimiento en el uso de las tecnologías de la información conlleva también, de manera lamentable un gran riesgo para quienes navegan en la red.

5. En nuestro país se tipifican algunas conductas en el Código penal Federal y en algunas entidades federativas; sin embargo, lo vertiginoso de las tecnologías de la información y las nuevas modalidades en las que se configuran esos ilícitos, hacen indispensable adoptar un marco de referencia con mayores estándares de protección, además de cooperación internacional, dado que no se reconocen fronteras territoriales en los delitos cibernéticos.

6. El Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como el "Convenio de Budapest", constituye el primer tratado internacional sobre delitos cometidos a través de internet y de otros sistemas informáticos. Fue elaborado por expertos del Consejo de Europa, con ayuda de especialistas de otros países ajenos a la Organización, como Estados Unidos, Canadá y Japón. Entró en vigor el 1° de julio de 2004 y, a la fecha, ha sido ratificado por cuarenta y siete Estados. Además, cabe señalar que han sido invitados a hacerse Parte del referido Convenio otros Estados no miembros del Consejo de Europa, entre ellos, Argentina, Chile, Costa Rica, Colombia, México y Perú.

7. El Convenio se encuentra estructurado sobre la base de un Preámbulo, en donde se consignan los motivos que tuvieron a las Partes para adoptarlo; y de cuarenta y ocho artículos, donde se despliegan las normas que conforman su cuerpo dispositivo. El principal objetivo es el desarrollo de una política criminal común frente al ciberdelito, mediante la homologación de la legislación penal, sustantiva y procesal, y el establecimiento de un sistema rápido y eficaz de cooperación internacional. Parte de reconocer que existen diversos ilícitos asociados al uso de plataformas tecnológicas. Algunos de ellos son exclusivamente del ámbito del ciberespacio, como el sabotaje informático o el acceso indebido a sistemas de información, en tanto otros pueden ser facilitados

o tener un alcance mayor gracias a internet, como la estafa, la adquisición o almacenamiento de material pornográfico infantil y la comercialización y producción de éste.

8. Por lo que hace al Protocolo Adicional, como se manifiesta en las propuestas de estudio, su propósito es complementar las disposiciones del Convenio de Budapest con respecto a la penalización de actos y conductas de naturaleza racista y xenofóbica cometidas a través del uso de sistemas de cómputo y representa una extensión adicional del alcance del Convenio, incluyendo sus disposiciones sustantivas, procedimentales y de cooperación internacional que prevé la inclusión de delitos tales como la propaganda racista y xenofóbica a través de Internet, así como procurar la posibilidad de que los países firmantes utilicen los medios y canales de cooperación internacional establecidos en el marco del propio Convenio de Budapest para el combate a ese tipo de delitos que son cada vez más comunes particularmente en la lucha contra grupos terroristas que utilizan el Internet para fomentar y propagar sus ideales y creencias.

9. Este órgano legislativo destaca que es el primer tratado internacional que, junto con su protocolo y el Convenio 108 del Consejo de Europa, buscan hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. El objetivo principal de esos instrumentos es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional. Por lo que se busca armonizar los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico y el establecimiento de un régimen rápido y eficaz de la cooperación internacional.

10. Esta dictaminadora, por la importancia que reviste la problemática manifestada considera oportuno exhortar exhorta a las dependencias competentes del Gobierno Federal para que realicen las acciones necesarias a efecto de que el Estado Mexicano se adhiera y aplique las disposiciones del Convenio sobre Ciberdelincuencia conocido como Convenio de Budapest, su protocolo adicional, así como al Convenio 108

del Consejo de Europa, con objeto de fortalecer el marco jurídico en materia de ciberseguridad y reforzar la cooperación internacional para prevenir estos delitos.

Por las consideraciones antes expuestas, la Segunda Comisión de Relaciones Exteriores, Defensa Nacional y Educación Pública, somete a consideración de la Comisión Permanente del H. Congreso de la Unión el siguiente:

ACUERDO

Único. La Comisión Permanente del H. Congreso de la Unión, con pleno respeto a la división de poderes, exhorta a las dependencias competentes del Gobierno Federal para que realicen las acciones necesarias a efecto de que el Estado Mexicano se adhiera y aplique las disposiciones del Convenio sobre Ciberdelincuencia conocido como Convenio de Budapest, su protocolo adicional, así como al Convenio 108 del Consejo de Europa, con objeto de fortalecer el marco jurídico en materia de ciberseguridad y reforzar la cooperación internacional para prevenir estos delitos.

Dado en la Sala de Juntas de la Segunda Comisión,
a los 13 días del mes de junio del 2017.