PROPOSICIÓN CON PUNTO DE ACUERDO, A FIN DE EXHORTAR A LA SRE A REALIZAR GESTIONES DIPLOMÁTICAS PARA IMPULSAR LA ADHESIÓN DE MÉXICO AL CONVENIO DE BUDAPEST, SOBRE CIBERDELINCUENCIA, A CARGO DE LA DIPUTADA MARÍA EUGENIA HERNÁNDEZ PÉREZ, DEL GRUPO PARLAMENTARIO DE MORENA

La que suscribe, María Eugenia Hernández Pérez, diputada federal de la LXIV Legislatura del honorable Congreso de la Unión, e integrante del Grupo Parlamentario de Morena, con fundamento en lo dispuesto en los artículos 6, numeral 1, fracción I, y 79, numeral 1, fracción II, del Reglamento de la Cámara de Diputados del honorable Congreso de la Unión, somete a consideración de esta asamblea la presente proposición con punto de acuerdo, al tenor de las siguientes

Consideraciones

Los grandes avances en las últimas décadas en torno a las nuevas tecnologías, nuevos esquemas de negocio y la interconectividad global han traído múltiples beneficios en torno a las capacidades humanas de interacción y comunicación de distintos tipos de información. Estos beneficios crecen exponencialmente y se reflejan en un aumento del PIB a nivel mundial, no obstante, con el crecimiento del ciberespacio también se incrementaron el número de cibercrímenes, ya que la delincuencia sigue evolucionando con el tiempo y la rápida disminución en la brecha digital en América Latina se ha ido reduciendo en los últimos años, lo cual ha dado paso nuevos tipos de crímenes y delitos cibernéticos.

Para enfrentar esta creciente amenaza, la vinculación y cooperación entre sector público, privado, sociedad y academia debe ser eje vital, con una agenda coordinada de acciones y líneas de trabajo. Si bien la ciberseguridad en sí misma debería ser el objetivo central de esta agenda, otro factor de alta relevancia sería mejorar la resiliencia de los activos informáticos de los mismos sectores, con el motivo de incrementar su habilidad de enfrentar los ciberataques a largo plazo evitando así impacto en la continuidad de sus actividades diarias. Cada sector enfrenta diferentes riesgos, la coordinación y comunicación entre ellos fortalece sus capacidades y mejora sus probabilidades de éxito a través de un dialogo constante concebido más bien como un acompañamiento mutuo donde juntos vayan avanzando y las experiencias de uno sean de provecho para todos los sectores.

Es importante en este punto describir a grandes rasgos las características y naturaleza del problema al que nos enfrentamos. La ciberseguridad es el conjunto de acciones tomadas por las organizaciones e individuos para mitigar los riesgos que enfrentan en el ciberespacio, con el propósito de disminuir las posibilidades de recibir un ciberataque, esto a través de soluciones tecnológicas, campañas de cultura de ciberseguridad y estrategias cibernéticas de respuesta a incidentes y gestión de riesgos.[1]

De acuerdo con la Encuesta de Delitos Económicos[2] se han reportado pérdidas económicas bastante considerables derivadas de estos delitos, al solicitar a los encuestados que se cuantificara el impacto monetario más significativo en los últimos 2 años, se estimó una cantidad de entre 100 mil y un millón de dólares en el 18 por ciento de los encuestados. En el año 2004, los estados miembros de la Organización de Estados Americanos (OEA) reconocieron formalmente que combatir los delitos cibernéticos y fortalecer la resiliencia cibernética eran cuestiones imperativas para el desarrollo económico y social, la gobernanza democrática, la seguridad nacional y la de los ciudadanos, según un informe[3] realizado por la OEA y Symantec titulado "Tendencias de seguridad informática en América Latina y el Caribe".

En este sentido la iniciativa más importante de la comunidad internacional en torno a la ciberseguridad, fue creada en noviembre del 2001 a través del **Convenio sobre la Ciberdelincuencia,** [4] mejor conocido como el **Convenio de Budapest** debido a la ciudad donde fue desarrollado. El Convenio fue ratificado por los Estados miembros del

Consejo de Europa, por los Estados no miembros que participaron en su elaboración, y quedó abierto para la adhesión de otros Estados no miembros.

Este convenio entró en vigor en el año 2004 y tiene por objetivo combatir la ejecución de delitos cometidos a través de internet y otras redes informáticas, constituyendo hasta ahora el único instrumento internacional que aborda de manera directa el tema del cibercrimen. Este convenio enuncia y describe distintos tipos de actividades criminales que se podrían realizar en el ciberespacio y que deberían ser considerados para hacerse acreedores a alguna sanción, dependiendo de la legislación y las condiciones del país donde se considere su implementación. Los cibercrímenes, plantea el Convenio de Budapest, deben enfrentarse con acciones a nivel nacional y en algunos casos más críticos aprovechar la colaboración internacional derivada del mismo convenio.

A lo largo de sus 48 artículos, el Convenio sobre la Ciberdelincuencia describe las diversas modalidades de delitos que se pueden perpetrar en el ciberespacio y al mismo tiempo emite una seria de medidas y recomendaciones para acompañar las sanciones jurídicas, tales como asistencia los 365 días del año, asistencia mutua para la obtención de datos en tiempo real, consultas entre miembros del Convenio, etcétera. Si bien en su mayoría el Convenio de Budapest es un marco de referencia para tipificar los delitos cibernéticos y proponer sanciones a los mismos, podemos notar que también busca acciones internacionales que sumen esfuerzos para combatir la amenaza de los ciberdelitos, que por su misma naturaleza es un fenómeno de interés internacional. Asimismo es importante tomar en cuenta algunas cuestiones sensibles en temas de soberanía nacional y en términos de protección a los derechos humanos, ya que las cláusulas de cooperación internacional pueden implicar la obligación para los estados de entregar información de sus ciudadanos a terceros países, en dicho escenario, no se debe considerar a la seguridad y la defensa de los derechos como ideas contrapuestas al convenio si no como aliadas en la generación de un marco jurídico útil y que respete la privacidad y derechos humanos de los ciudadanos de los países que se adhieren al tratado.

Por ello, sería de gran provecho para México adherirse al Convenio de Budapest, ya que constituye un instrumento que nos ofrece un adecuado marco normativo en torno a los ciberdelitos, que podría servir de guía para que nuestro país pueda empezar a transitar a un marco jurídico que le permita abordar el cibercrimen en condiciones razonables. Con la adhesión al Convenio de Budapest, México fortalecería su Estado de Derecho en materia de prevención, investigación, persecución y castigo a la amplia gama de delitos cibernéticos que causan tanto daño a la sociedad y la economía nacionales.

Cabe señalar que México puede adherirse al Convenio de Budapest, a pesar de no ser miembro del Consejo de Europa, como lo ha hecho en el caso del Convenio Europeo de Información sobre Derecho Extranjero, y el Convenio de Derecho Penal sobre la Corrupción. En este orden de ideas, puede asentarse que han firmado el Convenio los 47 países miembros del Consejo de Europa, con la única excepción de Rusia, y 43 lo han ratificado. Para efectos de contextualizar la eventual adhesión de México, hay que considerar que se han adherido 18 países no miembros del Consejo Europeo, incluyendo países de América Latina como Chile, Argentina, Costa Rica, República Dominicana, Panamá y Paraguay.

Con base en las consideraciones expuestas, se somete a consideración de esta soberanía el siguiente

Punto de Acuerdo

Único. La Cámara de Diputados exhorta de manera respetuosa al titular de la Secretaría de Relaciones Exteriores, a que realice todas las gestiones diplomáticas necesarias para impulsar la adhesión de México al Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest.

Notas

1 https://consejomexicano.org/multimedia/1528987628-817.pdf

2 https://www.pwc.com/mx/es/publicaciones/c2g/2018-04-13-encuesta-delitos-economicos-2018-

mexicov4.pdf?utm_source=Website&utm_medium=Consult a%20%20https://pwc.to/2HariCi

3 https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20

Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Ca ribe.pdf

4 https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Palacio Legislativo de San Lázaro, a 29 de octubre de 2019.

Diputada María Eugenia Hernández Pérez (rúbrica)