PROPOSICIÓN CON PUNTO DE ACUERDO QUE EXHORTA AL EJECUTIVO FEDERAL A LOS TRABAJOS NECESARIOS PARA LA ADHESIÓN DE MÉXICO AL CONVENIO SOBRE LA CIBERDELINCUENCIA, O CONVENIO DE BUDAPEST.

SENADO DE LA REPÚBLICA
LXIV LEGISLATURA

La suscrita, **Senadora Alejandra Lagunes Soto Ruiz**, integrante del Grupo Parlamentario del Partido Verde Ecologista de México en la LXIV Legislatura de la Cámara de Senadores, de conformidad con lo establecido en los artículos 8, numeral 1, fracción II y 276 del Reglamento del Senado de la República, someto a consideración de esta Honorable Asamblea la siguiente **PROPOSICIÓN CON PUNTO DE ACUERDO QUE EXHORTA AL EJECUTIVO FEDERAL A INICIAR, A TRAVÉS DE UN PROCESO DE MÚLTIPLES PARTES INTERESADAS, LOS TRABAJOS NECESARIOS PARA LA ADHESIÓN DE MÉXICO AL CONVENIO SOBRE LA CIBERDELINCUENCIA, O CONVENIO DE BUDAPEST**, con base en las siguientes:

CONSIDERACIONES

En la década de los 80s las tecnologías de comunicaciones como televisores, radios y teléfonos se encontraban claramente diferenciadas de las tecnologías de la información, consistentes, básicamente, en equipos de cómputo. Con el avance de la digitalización, la frontera entre ambas tecnologías fue desapareciendo. Hoy, resulta casi imposible separar unas de otras.

La rápida evolución de Internet y de las tecnologías de la información ha favorecido el crecimiento económico y social en todo el mundo. Sin embargo, la mayor dependencia de Internet en casi todas nuestras actividades ha generado también mayores riesgos y vulnerabilidades, abriendo paso a nuevas posibilidades para las actividades delictivas.

La Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC) en su *"Estudio Exhaustivo Sobre el Delito Cibernético, 2013"* [*] señala que las definiciones de delito cibernético dependen en gran medida del propósito para el que se use el término. Un número limitado de actos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos representan el núcleo del delito cibernético; los actos informáticos realizados por beneficio o daño personal o financiero, que incluyen formas delincuenciales relacionadas con la identidad y actos relacionados con contenidos informáticos no se prestan fácilmente para los esfuerzos de acuñar definiciones legales del término compuesto. Asimismo, el término delito cibernético debe ser considerado como un conjunto de actos o conductas que pueden organizarse en categorías basadas en el objeto del delito material y el modus operandi.

La National Crime Agency (NCA) divide al delito cibernético en dos categorías amplias:

- Los delitos cibernéticos (o crímenes cibernéticos "puros") son delitos que solo pueden cometerse con una computadora, redes de computadoras u otras formas de tecnología de comunicación de la información (TIC). Un ejemplo de un delito cibernético depende de obtener acceso no autorizado a la red de computadoras de alguien, esto también puede denominarse "piratería informática".
- Los delitos cibernéticos (como el fraude, la compra de drogas ilegales y la explotación sexual infantil) pueden llevarse a cabo en línea o fuera de línea, pero en línea pueden tener lugar a una escala y velocidad sin precedentes. [*]

A nivel mundial, la ciberdelincuencia se distribuye ampliamente entre actos impulsados financieramente, actos relacionados con el contenido informático y actúa contra la confidencialidad, integridad y accesibilidad de los sistemas informáticos. Sin embargo, las percepciones de riesgo y amenaza relativas varían entre los gobiernos y las empresas del sector privado. Actualmente, las estadísticas de delincuencia pueden no representar una base sólida para las comparaciones entre países, aunque dichas estadísticas a menudo son importantes para la formulación de

políticas a nivel nacional. Las medidas legales desempeñan un papel clave en la prevención y la lucha contra el delito cibernético. Estos se requieren en todas las áreas, incluida la penalización, los poderes de procedimiento, jurisdicción, autoridades en general, cooperación internacional y responsabilidad de todos los sectores.

De acuerdo con las definiciones antes valoradas se puede definir el delito electrónico, en un sentido amplio, como las conductas criminales que se cometen con el empleo de la tecnología, como medio o fin. Mientras que un delito informático, que tiene como común denominador la protección de los activos de información, es decir proteger la disponibilidad, confidencialidad e integridad de la información en ellos contenidos.

Haciendo énfasis en las consecuencias que podrían tener los delitos informáticos, repercusiones en el mundo real, la delincuencia organizada ha aprovechado rápidamente las oportunidades que ofrece Internet, en particular el crecimiento del comercio electrónico y la banca en línea.

Los grupos delictivos especializados se dirigen a individuos, pequeñas empresas y grandes redes corporativas para robar información personal de forma masiva a fin de aprovechar los datos comprometidos que tienen a su disposición.

La ciberdelincuencia es una de las prácticas criminales transnacionales de más rápido crecimiento a los que se enfrentan tanto Estados como actores privados. La naturaleza sin fronteras de los ciberdelitos, así como la asimetría entre países en términos de capacidades técnicas y humanas para prevenirlos, perseguirlos y sancionarlos, han representado serios obstáculos para responder eficazmente a estas amenazas.

El estudio *Tendencias de Seguridad Cibernética* 2014, de la Organización de Estados Americanos, estimó que los costos de los delitos cibernéticos en dicho año ascendieron a 113,000 millones de dólares en América Latina y el Caribe. Tan solo en México, los costos ascendieron a 3,000 millones de dólares, lo cual nos ubicó como el tercer país con mayores costos inherentes a los crímenes cibernéticos, solo por debajo de Brasil y Colombia [*] . Además, de acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), en el primer trimestre de 2018, los fraudes cibernéticos crecieron 63% respecto del mismo periodo de 2017. [*]

Las cifras revelan que los ciberdelitos se encuentran en constante y exponencial crecimiento, por lo que se requieren mayores y mejores esfuerzos para combatirlos efectivamente. Por este motivo, en noviembre 2017 el Gobierno Federal presentó la Estrategia Nacional de Ciberseguridad, que definió 5 objetivos estratégicos: [*]

- Sociedad y derechos
- Economía e innovación
- Instituciones públicas
- Seguridad pública
- Seguridad Nacional

Estos objetivos se acompañaron de tres principios rectores (i) Perspectiva de derechos humanos (ii) Enfoque basado en gestión de riesgos y (iii) Colaboración multidisciplinaria y de múltiples actores.

Sin embargo, una estrategia nacional no es suficiente, el carácter transfronterizo de estos delitos ha requerido la cooperación y la coordinación de la comunidad internacional. Por ejemplo, la INTERPOL ha diseñado la Estrategia contra la Ciberdelincuencia, con el objetivo de ayudar a los países miembros a identificar ataques cibernéticos y sus perpetradores. La Estrategia contiene cinco líneas de acción: [*]

- Evaluación y análisis de amenazas, seguimiento de las tendencias
- Acceso y explotación de datos digitales brutos
- Proceso de gestión de pruebas digitales
- Correlación de información digital y física
- Armonización e interoperabilidad

Ante este escenario, los Estados miembros del Consejo de Europa impulsaron en 2001 la firma del Convenio sobre la Ciberdelincuencia o Convenio de Budapest.

Este Convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otros medios digitales, que se centra en el fraude informático, la pornografía infantil y las violaciones de la seguridad en la red. También propone una serie de poderes y procedimientos como la búsqueda en redes de computadoras y la intercepción y conservación de información.

El principal objetivo del Convenio es buscar una política criminal común dirigida a la protección de la sociedad contra el delito cibernético, especialmente mediante la adopción de la legislación apropiada y el fomento a la cooperación internacional. [*]

El Convenio es resultado de cuatro años de trabajo de expertos internacionales y se complementa con un Protocolo Adicional que reconoce como ofensa criminal cualquier publicación de propaganda racista y xenófoba a través de las redes.

El 23 de noviembre de 2001, el Convenio fue dispuesto para la firma de todos los Estados miembros del Consejo de Europa, de los Estados no miembros que participaron en su elaboración, así como para la adhesión de otros Estados no miembros.

Hasta la fecha, de los 47 países miembros del Consejo de Europa, todos, con excepción de Rusia, lo han firmado; y 43 lo han ratificado. Además, se han adherido 18 países no miembros, incluyendo varias naciones latinoamericanas como Chile, Argentina, Costa Rica, República Dominicana, Panamá y Paraguay. [*]

México ha firmado y/o ratificado nueve tratados impulsados por el Consejo Europeo, incluyendo el Convenio Europeo de Información sobre Derecho Extranjero (ratificado en 2003); el Convenio de Derecho Penal sobre la Corrupción (firmado en 2002) y el Convenio del Consejo de Europa sobre los Delitos Relacionados con los Bienes Culturales (ratificado en 2018), entre otros. [*]

El enfoque del Convenio de Budapest se sustenta, por un lado, en prevenir los actos que pongan el peligro la confidencialidad, la integridad, y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de los mismos; y por otro lado, en reconocer la necesidad de proteger los intereses legítimos en la uso de las tecnologías de la información y la comunicación. [*]

Al concretar su adhesión al Convenio de Budapest, nuestro país estaría fortaleciendo las acciones nacionales en materia de ciberseguridad y colaborando con otros países en la lucha efectiva contra la ciberdelincuencia.

Tal como ha sido señalado por diversos actores en México [*], la adhesión a este Convenio tendría que ir acompañada de cambios en la legislación mexicana, particularmente en el Código Penal Federal, con el objetivo de proteger los derechos humanos y la seguridad jurídica de los y las ciudadanas.

Además, el combate y prevención efectivos de la ciberdelincuencia requiere actuar con un enfoque de múltiples partes interesadas. De acuerdo con la organización de Internet ISOC por sus siglas en inglés, "el enfoque de gobernanza de múltiples partes interesadas abarca tres componentes: innovación libre y sin límites, instituciones de gobernanza descentralizadas y procesos abiertos e inclusivos". [*]

El Convenio de Budapest es el único tratado multilateral que trata los asuntos de delitos informáticos, y es necesaria la adhesión de México puesto que ello traería una serie de beneficios, tales como:

- proporcionar herramientas para que las autoridades correspondientes investiguen y sancionen adecuadamente la ciberdelincuencia;
- garantizar la protección de los derechos humanos y las libertades de acuerdo con los documentos internacionales actuales;
- dotar de mecanismos flexibles para evitar conflictos jurisdiccionales a nivel internacional sobre la materia;

- propiciar un acercamiento nacional coherente a la legislación sobre ciberdelincuencia;
- armonizar las disposiciones penales nacionales sobre delitos informáticos con las de otros países; y
- articular estándares globales más ágiles y efectivos en materia de cooperación internacional sobre ciberdelincuencia.

La complejidad de los desafíos que enfrentamos para mantener un ciberespacio libre y seguro nos exige abordarlos conjunta y abiertamente. Solo así podremos construir conjuntamente, a través de un proceso democrático y participativo, una propuesta transparente, responsable, equitativa, sostenible y eficaz.

Por lo anteriormente expuesto, se somete a la consideración de esta soberanía el presente:

PUNTO DE ACUERDO

ÚNICO.- Se exhorta respetuosamente al Ejecutivo Federal a iniciar, a través de un proceso múltiples partes interesadas, los trabajos necesarios para la adhesión de México al Convenio sobre la Ciberdelincuencia, o Convenio de Budapest.

Salón de Sesiones del Senado de la República del H. Congreso de la Unión, abril de 2019.

SENADORA ALEJANDRA LAGUNES SOTO RUIZ

PARTIDO VERDE ECOLOGISTA DE MÉXICO

[*] https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

[*] "Cyber crime: Preventing young people from getting involved". National Crime Agency. http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved

[*] "Tendencias de Seguridad Cibernética en América Latina y el Caribe". Organización de los Estados Americanos. junio de 2014.https://www.sites.oas.org/cyber/documents/2014%20-%20tendencias%20de%20seguridad%20cibern%C3%A9tica%20en%20am%C3%A9rica%20latina%20y%20el%20caribe.pdf

[*] CONDUSEF. Estadísticas (consultado en septiembre de 2018) https://www.condusef.gob.mx/gbmx/?p=estadisticas

[*] Presidencia de la República. Sexto Informe de Gobierno 2017-2018 http://cdn.presidencia.gob.mx/sextoinforme/informe/6_IG_INFORME_COMPLETO.pdf

[*] Interpol. Estrategia Mundial contra la Ciberdelincuencia. Resumen https://www.interpol.int/es/Media/Files/Crime-areas/Cybercrime/Estrategia-mundial-contra-la-ciberdelincuencia-Resumen

[*] Council of Europe. Details of Treaty No.185 Convention on Cybercrime https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[*] Council of Europe. Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=efkXvpjI

[*] Council of Europe. Treaty list for a specific State https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/MEX?p_auth=giOxcqOS

[*] Council of Europe. Details of Treaty No.185 Convention on Cybercrime https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[*] "Danya Centeno. "México y el Convenio de Budapest: posibles incompatibilidades". Red de Defensa de los Derechos Digitales https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf

[*] "Gobernanza de Internet – Por qué funciona el enfoque de múltiples partes interesadas". Internet Society. "https://www.internetsociety.org/es/resources/doc/2016/gobernanza-de-internet-por-que-funciona-el-enfoque-de-multiples-partes-interesadas/