PROPOSICIÓN CON PUNTO DE ACUERDO DE URGENTE U OBVIA RESOLUCIÓN POR EL QUE SE EXHORTA RESPETUOSAMENTE A LA SECRETARÍA DE RELACIONES EXTERIORES A ADHERIRSE Y RATIFICAR EL CONVENIO DE CIBERDELINCUENCIA TAMBIÉN LLAMADO CONVENIO DE BUDAPEST Y SU PROTOCOLO ADICIONAL.

El suscrito, Diputado Raúl Eduardo Bonifaz Moedano, integrante del Grupo Parlamentario de Morena, en la LXIV Legislatura del Honorable Congreso de la Unión y con fundamento en lo dispuesto en los artículos 58 y 59 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, someto a consideración del Pleno de la Comisión Permanente del Congreso de la Unión, la presente Proposición con Punto de Acuerdo al tenor de las siguientes:

CONSIDERACIONES

La creación de un espacio nuevo y virtual inimaginable hace pocas décadas, en el que transita cualquier tipo de información, desde los datos personales más sensibles hasta todo género de operaciones comerciales, supone una auténtica revolución tecnológica. La conectividad universal y la apertura del espacio apuntan directamente a un nuevo escenario de regulación e intervención que supera las fronteras nacionales, con los complejos problemas que ello supone. Los instrumentos normativos parten de la consideración de lo esencial de la cooperación internacional y la coordinación no sólo entre Estados, sino, con el sector privado en la lucha contra la ciberdelincuencia[i].

El ciberespacio cuenta con un aproximado de dos mil millones de usuarios en todo el mundo, de los cuales 431 millones han sido afectados por delitos hechos mediante computadoras, un millón de víctimas cada día a escala mundial[ii]. Los delitos cibernéticos, delitos informáticos o delitos hechos mediante computadoras han sido definidos por la Organización de Cooperación y Desarrollo Económicos (OCDE) como “cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos”.

El ciberdelito es una forma de delincuencia transnacional en evolución que se ve agravada por la creciente participación de grupos del crimen organizado. Los autores y las víctimas de los delitos cibernéticos pueden estar ubicados en diferentes regiones y sus consecuencias pueden afectar a sociedades de todo el mundo, lo que pone de relieve la necesidad de su medición para generar una respuesta institucional adecuada y dinámica a nivel nacional, regional e internacional[iii].

La Organización de las Naciones Unidas reconoce varios tipos de delitos cibernéticos, entre los cuales los más comunes son los relacionados con la identidad. Los delitos se dividen en:

a) Fraudes cometidos mediante manipulación de computadoras.
b) Falsificaciones informáticas.
c) Daños o modificaciones de programas o datos computarizados[iv].

Según estadísticas de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, en el primer semestre del año de 2019, los fraudes cibernéticos crecieron un 35% con respecto de 2018. El monto reclamado de los fraudes ascendió a 5,908 millones de pesos; se bonificó sólo el 42% y 87 de cada 100 fraudes cibernéticos se resolvieron a favor del usuario.

Existen diferentes tipos de fraudes cibernéticos, los cuales son:

1) *Phising.* Haciéndose pasar por alguna institución financiera, mediante correo electrónico se solicitan datos de cuentas bancarias con la alusión de que existe un problema en dichos datos y es necesario rectificarlos. También existe de forma telefónica, en donde los delincuentes simulan ser empleados de dicha institución financiera. Es el método más común de fraude en México.

2) *Pharming*. Por medio de un link redirigen al usuario a una página falsa para proceder a la estafa.

2) *Spam*. El famoso “correo basura” es un correo electrónico que es enviado a varias personas con el propósito de que descarguen un archivo, generalmente un virus, que roba la información del dispositivo en donde se descargó.

Incluso la misma Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, mencionó que el fraude financiero en México se ha incrementado de manera importante, de tal forma que del año 2011 al 2018 se han registrado 30.8 millones de reclamaciones imputables a un posible fraude, en tanto en el primer semestre de 2018, se registraron 3.5 millones, por un monto de 9 mil 231 millones de pesos. “En 2020, se incrementaron las compras en línea, por lo que se incrementaron las quejas por transferencias electrónicas no reconocidas, consumos vía internet no reconocidos y envío y/o retiro de dinero móvil no reconocido, en los que se incluyen las modalidades de phishing, vishing y smishing”[v]

Antes de continuar con los antecedentes que remarcan el constante aumento de ciberdelitos, es imperante especificar que el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest), el cual no ha sido ratificado por el Estado Mexicano, es el acuerdo internacional de uso más extendido para desarrollar la legislación de combate al cibercrimen. El tratado ha sido ratificado por 60 Estados, incluidos los Estados miembros de la Unión Europea, junto a Estados Unidos, Canadá, Australia y Japón.

El Convenio sobre la Ciberdelincuencia (Convention on Cybercrime), conocido como Convenio de Budapest (COE, Serie Tratados Europeos N° 185), fue suscrito en dicha ciudad el 23 de noviembre de 2001 en el marco de los Estados miembros del Consejo de Europa, y se encuentra en vigor a partir del 1 de julio de 2004.

La adhesión al tratado, según establece su Artículo 37°, se encuentra abierta a la incorporación de países que no sean miembros del Consejo de Europa. A la fecha, Budapest ha sido ratificado por 60 Estados, junto a los Estados miembros de la Unión Europea, el Convenio ha sido ratificado por países no europeos , entre ellos Estados Unidos, Canadá, Australia, Japón, Israel, República Dominicana, Chile, Argentina y Colombia. Otras organizaciones internacionales se han adherido a él, tales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Organización de los Estados Americanos (OEA), la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), y la Unión Internacional de Telecomunicaciones (UIT).

Se trata del único tratado internacional vinculante en la materia y constituye una especie de guía, “ley modelo” o “acuerdo marco” para que los Estados Parte: i) implementen dentro de su ordenamiento jurídico nacional la legislación pertinente para investigar y perseguir penalmente aquellos delitos cometidos en contra de sistemas o medios informáticos o mediante el uso de los mismos y ii) faciliten la cooperación internacional en este sentido[vi].

En forma complementaria al tratado, en abril de 2003 se suscribió el Protocolo Adicional al Convenio sobre Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems) (STE N°189), que tiene por objeto armonizar la legislación penal sustantiva en relación a la lucha contra el racismo y la xenofobia en Internet, y mejorar la cooperación en esta materia (COE, 2003).

A nivel interno, las Partes contratantes deberán tomar medidas legislativas o de otra índole para evitar la difusión de material racista y xenófobo mediante sistemas informáticos, impedir que mediante las redes se den amenazas o insultos con motivación racista o xenófoba y también impedir que se utilicen sistemas informáticos para negar o justificar genocidios o crímenes contra la humanidad[vii].

Conforme al Artículo 15 del Convenio, las medidas que los Estados adopten para combatir la "ciberdelincuencia" deberán diseñarse de tal forma que garanticen el pleno respeto al Estado de Derecho y a los principios internacionales en materia de derechos humanos[viii]. Esto implica que cada país que decida adherirse al Convenio se asegure de implementar dentro de su ordenamiento interno las condiciones y salvaguardas necesarias para prevenir el uso abusivo de los poderes y procedimientos previstos en el mismo por parte de las autoridades, garantizando una efectiva y adecuada protección de los derechos humanos.

Cabe mencionar que su completa implemetación en el Estado Mexicano radicaría en la legislación nacional que se determine, al momento de aplicar las obligaciones internacionales vinculantes. Es decir, se podría garantizar la carga de protección adecuada en materia de derechos humanos y de transparencia.

Además, se debe tener en consideración que durante la pandemia provocada por el SARS-CoV-2, que transmite la enfermedad COVID-19, ha incrementado el tiempo que la población navega en internet y eso implica algunos riesgos, como la ciberdelincuencia[ix].

La proliferación de productos de innovación digital que permiten a las personas trabajar desde casa y realizar transacciones a través de internet ha sido clave para mitigar algunos de los retos del coronavirus. Sin embargo, este cambio digital también ha aumentado la amenaza de los ciberataques, especialmente en los mercados emergentes.[x] Si bien, el aumento de la adopción de soluciones digitales ha desempeñado un papel importante en la reducción del riesgo de contraer el virus, además de permitir que las personas sigan trabajando y estudiando, también ha aumentado los problemas de seguridad cibernética.[xi]

Por ejemplo, un ataque de phishing en la India pretendía ofrecer a la gente una suscripción gratuita a Netflix durante el cierre si rellenaban una encuesta y reenviaban el mensaje a 10 personas. En agosto, la Organización International de Policía Criminal, observó que había sido testigo de un número considerable de amenazas cibernéticas relacionadas con la COVID-19, como estafas en línea con temática de coronavirus y correos electrónicos de suplantación de identidad que suplantan a las autoridades gubernamentales y sanitarias[xii].

En una declaración publicada a finales de abril del año 2020, la Organización Mundial de la Salud (OMS) dijo que había experimentado un aumento de cinco veces en el número de ciberataques desde el brote de la COVID-19, con las direcciones de correo electrónico y las contraseñas de miles de personas que trabajaban en tareas en respuesta al virus que se filtraba en línea[xiii].

El número de casos en los que se reportó robo de identidad en los Estados Unidos de América, se duplicó en 2020 en comparación con el año previo, dijo la Comisión Federal de Comercio (FTC, por sus siglas en inglés). En una publicación que marca el inicio de la Semana de Concientización sobre el Robo de Identidad en Estados Unidos, la FTC dijo que recibió aproximadamente 1.4 millones de reportes de casos de robo de identidad el año pasado. Este aumento en los casos se debe principalmente a que los ciberdelincuentes apuntan a personas que se han visto afectadas financieramente por la pandemia de COVID-19.

Incluso, Izumi Nakamitsu, jefa de desarme de la Organización de las Naciones Unidas (ONU), advirtió sobre un aumento de los ciberdelitos, entre ellos, los correos electrónicos maliciosos, que aumentaron 600% durante la actual emergencia sanitaria[xiv].

El 19 de mayo de 2021, el Presidente de la Asociación de Bancos de México, Daniel Becker, declaró que durante la pandemia, los bancos invirtieron en conjunto más de 20,000 millones de pesos en herramientas de ciberseguridad para blindar las operaciones digitales. De acuerdo con información de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, en el año 2020, los bancos concentraron 94% de las reclamaciones de los clientes con 6.3 millones de expedientes. De enero a diciembre de 2020, el porcentaje de Resolución Favorable del sector Bancos fue 36.1, lo cual sugiere que **en 6 de cada 10 casos, los clientes que reportan fraudes no obtienen una resolución a favor**[xv].

Actualmente, México se encuentra como observador del Convenio de Budapest y de manera formal ha sido invitado a ascender y adherirse al mismo y es imperante valorar los efectos en el ciberespacio durante una pandemia.

Por lo anteriormente expuesto y fundamentado, someto a la consideración de esta Honorable Asamblea, como asunto de urgente u obvia resolución y puesto a votación de inmediato, el siguiente:

Punto de Acuerdo

ÚNICO.- La Comisión Permanente del Honorable Congreso de la Unión exhorta respetuosamente a la Secretaría de Relaciones Exteriores a adherirse y ratificar el Convenio de Ciberdelincuencia también llamado Convenio de Budapest y su Protocolo Adicional.

Salón de sesiones de la Comisión Permanente del H. Congreso de la Unión a los 22 días del mes de mayo de 2021.

RAÚL EDUARDO BONIFAZ MOEDANO
DIPUTADO FEDERAL

---

[i] https://revistaciencias.inacipe.gob.mx/index.php/01/article/view/391/317
[ii] https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14381/15543
[iii] https://www.unodc.org/mexicoandcentralamerica/es/webstories/2020/09_10_CdE_ciberdelincuencia.html
[iv] https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14381/15543
[v] https://www.jornada.com.mx/notas/2021/02/22/economia/aumentaron-25-los-reclamos-por-fraudes-ciberneticos-en-2020-condusef/
[vi] https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf
[vii] https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf

[viii] Seger, A. The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web, 16 de febrero de 2012, disponible en: https://rm.coe.int/16802fa3e0

[ix] https://www.unodc.org/mexicoandcentralamerica/es/webstories/2020/09_10_CdE_ciberdelincuencia.html
[x] https://atalayar.com/content/aumenta-la-ciberdelincuencia-durante-la-pandemia-de-la-covid-19
[xi] Ídem
[xii] Ídem
[xiii] **Ídem**
[xiv] https://acis.org.co/portal/content/noticiasdelsector/un-600-ha-aumentado-los-ciberdelitos-en-pandemia-¡asegúrese-para-iniciar-el-2021
[xv] https://www.forbes.com.mx/negocios-bancos-paginas-web-falsas-abm-credito/?utm_source=nora-push&utm_medium=push-notifications&utm_campaign=new-nora-push