

DICTAMEN POR EL QUE SE SOLICITA A LA PROCURADURÍA GENERAL DE LA REPÚBLICA, AL COMISIONADO NACIONAL DE SEGURIDAD Y AL CONSEJERO JURÍDICO DEL EJECUTIVO FEDERAL UN INFORME SOBRE LOS AVANCES DE LA INTEGRACIÓN DE MÉXICO EN LOS DISTINTOS ORGANISMOS, ACUERDOS, TRATADOS Y CONVENIOS INTERNACIONALES EN MATERIA DE SEGURIDAD CIBERNÉTICA.

HONORABLE ASAMBLEA

A la Segunda Comisión de Trabajo de la Comisión Permanente del Congreso de la Unión, Relaciones Exteriores, Defensa Nacional y Educación Pública, en el Segundo Receso del Tercer Año de Ejercicio Constitucional de la LXII Legislatura, le fue turnada para su análisis y dictamen la Proposición con Punto de Acuerdo a fin de que el Secretario de Gobernación, el Secretario de Relaciones Exteriores, la Procuradora General de la República, el Comisionado Nacional de Seguridad y el Consejero Jurídico del Ejecutivo Federal informen sobre los resultados obtenidos en base a la participación de nuestro país en organismos, acuerdos, tratados y convenios internacionales en materia de seguridad cibernética, y la posición de esas dependencias federales respecto a la adhesión al Convenio de Cibercriminalidad de Budapest.

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, los legisladores integrantes de esta Segunda Comisión, sometemos a la consideración del Pleno el presente Dictamen, de conformidad con los siguientes:

ANTECEDENTES

1. Con fecha 22 de julio 2015, la Diputada Lizbeth Rosas Montero, integrante del Grupo Parlamentario del Partido de la Revolución Democrática, presentó ante el Pleno de la Comisión Permanente del Congreso de la Unión la proposición de mérito.

2. En esa misma fecha la Presidencia de la Mesa Directiva de la Comisión Permanente del Congreso de la Unión, dispuso que dicha proposición con Punto de Acuerdo se turnara para su estudio y dictaminación a la Segunda Comisión, de Relaciones Exteriores, Defensa Nacional y Educación Pública, por lo que en este acto se emite el Dictamen correspondiente, de conformidad con lo siguiente:

CONTENIDO DE LA PROPOSICIÓN

La legisladora proponente del punto de acuerdo que se dictamina, señala expresamente en sus consideraciones:

“Un delito informático es toda aquella acción, típica, anti jurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como un delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática. A partir de los atentados del 11 de Septiembre esta definición se amplió y hoy día es, básicamente, cualquier delito perpetrado a través de un ordenador, sea cual sea su fin. Hay cientos de tipos de ciberdelitos, los más frecuentes son el Phising, el Fraude bancario, el uso de redes para el tráfico de drogas y el SPAM.

México es una de las naciones de América Latina y el Caribe más afectadas por los ciberdelitos, tan sólo en el 2013 las pérdidas económicas ascendieron a 3,000 millones de dólares. De acuerdo con el informe “Tendencias

de Seguridad Cibernética en América Latina y el Caribe", México es el segundo país más vulnerable, sólo después de Brasil, cuyas pérdidas por estos delitos alcanzaron 8,000 millones de dólares en ese año.

La Policía Federal ha reconocido públicamente un aumento del orden del 300% en incidentes de seguridad cibernética en 2014 en relación con la incidencia delictiva observada en 2013. Atribuyendo el incremento a las mejoras de los procesos de identificación de incidentes a nivel nacional y en la generación de nuevos vectores de ataque provenientes del exterior, según Eduardo Sánchez, en su carácter de vocero del Gobierno de la República.

El vocero del Gobierno Federal aseguró además ante diversos medios de comunicación que de diciembre del 2012 a enero del 2015 se recibieron 30,000 reportes telefónicos ligados con delitos cibernéticos, de los cuales 53% fueron contra dependencias de los tres niveles de gobierno, 26% contra ámbitos académicos y 21% contra sector privado (empresarios).

Así mismo el citado servidor público señaló que la suplantación y el robo de identidad acaparan 68% de los delitos cibernéticos; el fraude cibernético ocupa el 17% de los ataques, mientras que los hackeos representan 15%, todas las cifras durante el año 2014. Estas cifras colocan a México en el tercer lugar mundial con víctimas por crímenes cibernéticos, solo por debajo de China y Sudáfrica, con el 85% y 84% de usuarios víctimas, respectivamente. El país también es una de las capitales mundiales con mayor cantidad de crímenes cibernéticos cometidos a través de virus informáticos: siete de cada 10 usuarios.

Es claro que en México existe la necesidad de crear Leyes específicas respecto del uso del Ciberespacio y homologar la tipificación de los delitos cibernéticos, pero también resulta apremiante la adhesión a organismos, convenios, acuerdos y tratados internacionales para la desarticulación de redes de delincuentes mundiales que cometen delitos en internet. Lo anterior toda vez que hoy nuestro país está imposibilitado a sancionar las acciones ilegales que sean perpetradas desde fuera del territorio nacional.

El Estado Mexicano forma parte de Organizaciones Internacionales que atienden y coordinan las políticas domésticas e internacionales en diversos sectores, incluyendo el área de tecnología de información y comunicación, en los que se discuten políticas públicas para solucionar problemas comunes entre sus miembros, como al caso resultan la Unión Internacional de Telecomunicaciones (UIT) dependiente de la Organización de Naciones Unidas (ONU) y tiene como función primordial la creación de políticas y recomendaciones en el sector de las telecomunicaciones y donde participan 191 Países. La Unión Internacional de Telecomunicaciones (UIT) tiene además la encomienda de coordinar los esfuerzos internacionales en materia de ciberseguridad y fungir como facilitador para la implementación de tecnologías de la información.

Nuestra nación es también miembro de la Organización Internacional de Policía Criminal (INTERPOL) que entre sus prioridades tiene la de combatir los delitos que derivan del uso de las nuevas tecnologías. México es igualmente integrante de la Organización para la Cooperación y el Desarrollo Económico (OCDE) que entre sus tareas tiene la de buscar soluciones a la problemática común entre sus miembros como resultan ser los ciberdelitos y en los que se ha venido trabajando desde el año 2008 con la reunión ministerial denominada "El Futuro de la Economía en Internet" en la que se trataron aspectos sobre la ciberdelincuencia y el robo de identidad en los países miembros.

Sin embargo aún con la mencionada inclusión en los foros y organismos mundiales referidos se sigue observando la vulnerabilidad del Gobierno Mexicano en materia de seguridad informática, misma que ha quedado evidenciada en diversas acciones llevadas a cabo por grupos de ciberactivistas como el denominado "Anonymus" que el 15 de septiembre de 2011 en plena fecha de la conmemoración de la Independencia bloquearon el acceso a varias páginas web del Gobierno Federal que estuvieron caídas por varias horas.

Al Gobierno que encabeza Enrique Peña Nieto le corresponde entender y asumir que el ciberdelito es un fenómeno global y que su investigación y persecución exige métodos adecuados basados en una dimensión internacional, esto se debe a que no es necesario que el delincuente se ubique físicamente en el lugar donde se comete el crimen o se localiza la víctima.

La cooperación internacional permitirá que se robustezcan las capacidades de investigación, mejoren las estructuras institucionales en atención a la adopción de políticas de avanzada en materia seguridad informática. Nuestro país requiere la inmediata adopción de políticas basadas en la experiencia global y el trabajo coordinado con naciones que encabezan el combate a los peligros del mundo virtual de Internet.

La Convención de Budapest como se le identifica habitualmente a The Convention on Cybercrime (ETS) 185 o Convenio sobre Cibercriminalidad de Budapest (traducción no oficial) o “Convención sobre Delitos Informáticos” o “Convenio sobre Cibercriminalidad” conforma el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre cibercriminalidad (derecho penal, derecho procesal y cooperación internacional) y trata con carácter prioritario una política penal contra la cibercriminalidad.

Lamentablemente nuestro país no es miembro de la referida convención y eso conlleva a la falta de coordinación estratégica con las naciones líderes en el combate a los ciberdelitos a pesar de estar incluidos entre los países con mayor incidencia delictiva en internet. Un total y absoluto contrasentido en materia de procuración de justicia generado desde las altas esferas gubernativas.

Para apoyar el necesario esfuerzo de adhesión de México a The Convention on Cybercrime (ETS) 185 o Convenio sobre Cibercriminalidad de Budapest (traducción no oficial) o “Convención sobre Delitos Informáticos” o “Convenio sobre Cibercriminalidad” se requiere la participación decidida de la Secretaría de Relaciones Exteriores al ser ésta la encargada de conducir la política exterior e intervenir en toda clase de tratados, acuerdos y convenciones en los que nuestra nación deba ser parte, como al caso resulta. Asimismo resulta necesaria la participación comprometida de la Consejería Jurídica del Ejecutivo Federal para llevar a cabo la revisión y validación de cualquier instrumento jurídico que sea sometido a su consideración y conlleve a la indispensable adopción de políticas internacionales en materia seguridad informática.

Por lo expuesto solicitamos la urgente intervención del Secretario de Gobernación, el Secretario de Relaciones Exteriores, la Procuradora General de la República y el Comisionado Nacional de Seguridad, para que en el ámbito de sus facultades y atribuciones analicen y resuelvan en forma urgente la posible adhesión de nuestro País al Acuerdos Internacionales mencionado con antelación.

Por lo anterior es menester que esta H. Cámara de Diputados realice un posicionamiento institucional, para EXHORTAR en forma oportuna la PROPOSICION CON PUNTO DE ACUERDO A FIN DE QUE EL SECRETARIO DE GOBERNACION, EL SECRETARIO DE RELACIONES EXTERIORES, LA PROCURADORA GENERAL DE LA REPUBLICA, EL COMISIONADO NACIONAL DE SEGURIDAD Y EL CONSEJERO JURIDICO DEL EJECUTIVO FEDERAL INFORMEN SOBRE LOS RESULTADOS OBTENIDOS EN BASE A LA PARTICIPACION DE NUESTRO PAIS EN ORGANISMOS, ACUERDOS, TRATADOS Y CONVENIOS INTERNACIONALES EN MATERIA DE SEGURIDAD CIBERNETICA, Y LA POSICION DE ESAS DEPENDENCIAS FEDERALES RESPECTO A LA ADHESION AL CONVENIO DE CIBERCRIMINALIDAD DE BUDAPEST (THE CONVENTION ON CYBERCRIME-ETS-185).”

Ante lo expuesto, la proposición que nos ocupa establece los siguientes puntos resolutivos:

PUNTO DE ACUERDO

“PRIMERO.- La Comisión Permanente del Congreso de la Unión exhorta al Secretario de Gobernación, a la Procuradora General de la República, al Comisionado Nacional de Seguridad y al Consejero Jurídico del Ejecutivo Federal informen sobre los resultados obtenidos en materia de seguridad cibernética en base a la participación de nuestro país en organismos, acuerdos, tratados y convenios internacionales en materia de seguridad cibernética, y la posición de esas dependencias federales respecto a la adhesión al convenio de cibercriminalidad de Budapest (The Convention on Cybercrime-ets-185).

SEGUNDO.- La Comisión Permanente del Congreso de la Unión exhorta al Secretario de Relaciones Exteriores y al Consejero Jurídico del Ejecutivo Federal informen sobre la posición de esas dependencias federales respecto a la adhesión al convenio de cibercriminalidad de Budapest (The Convention on Cybercrime-ets-185).

TERCERO.- La Comisión Permanente del Congreso de la Unión solicita informar a esta Soberanía, en un término no mayor a diez días hábiles lo especificado en los puntos PRIMERO y SEGUNDO.”

CONSIDERACIONES

I.- Los legisladores que integramos esta Segunda Comisión de Trabajo de la Comisión Permanente coincidimos con la proposición de mérito, Los delitos realizados a través de una computadora o dispositivo informático, mejor conocidos como ciberdelincuencia o delitos informáticos, han estado en constante crecimiento y mutación en la sociedad actual. Por delito informático, suele entenderse toda aquella conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático. La OCDE lo define como cualquier conducta, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos; distribución de códigos maliciosos, robo de información, distribución y almacenamiento de pornografía infantil, acoso, extorsión, estafas comerciales y bancarias son algunas de las actividades que actos delictivos cometidos utilizando medios informáticos. La rapidez de la difusión, el anonimato, la comodidad y la amplitud de alcance no sólo nacional, sino mundial que facilitan las nuevas tecnologías, hacen que los delincuentes aprovechen las mismas para llevar a cabo diversas actividades delictivas.

II.- Esta Dictaminadora considera que los avances tecnológicos obligan a realizar mayores esfuerzos para proteger a la sociedad y al Estado de actividades del ciberespacio, y que afecta el orden y el Estado de derecho, por ejemplo la velocidad de los crímenes en esta materia es alarmante frente a los instrumentos tradicionales de investigación del Estado mexicano, debido a la velocidad de la transmisión de la información y la rapidez con la que se llevan a cabo la mayoría de estos delitos informáticos, así como la propagación de los mismos, ha sido de gran importancia para la mayoría de los países el regular y legislar para tratar de evitar y combatir estas actividades, es decir, establecer reglas básicas de comportamiento por parte del usuario, así como de los prestadores del servicio.

III.- La Segunda Comisión debe ubicar este dictamen y su discusión dentro de la nueva concepción de delitos informáticos en México es relativamente nueva. En 1977, en Estados Unidos se dio la primera propuesta para legislar este tipo de conductas. En 1983 la OCDE hizo una recomendación a sus países integrantes para legislar sus códigos penales e integrar los nuevos delitos informáticos. Para 1989, un comité del Consejo de Europa presentó una lista de delitos informáticos. En 1996, se estableció por el Comité Europeo para los Problemas de la Delincuencia, un nuevo comité para abordar el tema de los delitos informáticos. El 23 de noviembre de 2011, el Consejo de Ministros de Europa, compuesto por los ministros del interior de los estados que conforman la Unión Europea, Estados Unidos, Sudáfrica, Canadá y Japón, firmaron en Budapest, un convenio sobre delitos informáticos.

IV.- El Convenio de Budapest o Convenio sobre cibercriminalidad o ciberdelincuencia, es el primer tratado internacional sobre delitos cometidos a través de las redes de Internet y otra de computadora, que tratan sobre todo con las infracciones de los derechos de autor, el fraude relacionado con la informática, la pornografía infantil, crímenes de odio y violaciones de seguridad de la red. También contiene una serie de poderes y procedimientos

tales como la búsqueda de las redes informáticas y la interceptación legal. Su objetivo principal, que figura en el preámbulo, es seguir una política penal común destinada a la protección de la sociedad contra el delito cibernético, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Los principales objetivos de este tratado son los siguientes: la armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos; la prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, 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. Establece, entre otras cosas, cuestiones de derecho procesal como la preservación expedita de los datos almacenados, la preservación expedita y revelación parcial de los datos de tráfico, el orden de producción, el registro y la incautación de datos informáticos y la interceptación de datos de contenido. Además, la Convención contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados.

La Convención es el producto de cuatro años de trabajo de expertos europeos e internacionales. Se ha complementado por un protocolo adicional de hacer cualquier publicación de la propaganda racista y xenófoba través de redes informáticas un delito penal. Actualmente, el terrorismo cibernético también se estudia en el marco de la Convención.

V.- En el caso mexicano el Código Penal Federal se encuentran previstos entre otros, los delitos de revelación de Secretos, acceso ilícito a equipos y sistemas de informática, delitos contra los Derechos de Autor, *hacking* y *cracking* informático, etc. En la cuestión financiera la Ley de Instituciones de Crédito, dispone que se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que altere el medio de identificación electrónica y acceda a los equipos electromagnéticos del sistema bancario, con el propósito de disponer indebidamente de recursos económicos. En México los cambios más recientes a la legislación en materia de ciberdelincuencia se dieron en el año de 2009 cuando se publicó en el Diario Oficial de la Federación un cambio al Código Penal Federal en donde se adicionaron nuevas tipologías de delitos informáticos. Sin embargo, estos cambios presentan aún ciertas deficiencias considerando que sólo se contempla a los sistemas informáticos protegidos por mecanismos de seguridad, no se define que es un sistema de seguridad y no se consideran muchos ciberdelitos como los virus y el acoso cibernético.

Por su parte, algunas Entidades Federativas, en sus Códigos Penales, enumeran algunos tipos de delitos cibernéticos tales como: la falsificación, producción, impresión, enajenación, distribución y alteración de documentos, principalmente aquellos referidos al crédito. El Código Penal de Sinaloa fue el primero en tipificar el “delito Informático” y es el único que lo denomina así.

VI.- De acuerdo con datos de la Asociación Mexicana de Internet AC, México está experimentando un considerable crecimiento en el número de usuarios de internet con más de 50% de la población, siendo la población joven, de entre 13 y 34 años, la que más hace uso de estas tecnologías con un 63% de los usuarios totales en México.

Las computadoras portátiles, teléfonos celulares, computadoras de escritorio y tabletas son los dispositivos más utilizados por los usuarios mexicanos. El uso más común es para acceder a las redes sociales, buscar información, enviar y recibir correos electrónicos, enviar y recibir mensajes instantáneos, comprar en línea, realizar operaciones de banca en línea, hacer video llamadas y buscar empleo. Ante un panorama de intensificación del uso de los dispositivos informáticos y el aumento en la adopción de estos instrumentos como medios de producción, de entretenimiento y de educación es importante un cambio en la legislación nacional siempre con una visión de transnacionalización de estas actividades.

Así pues, es cada vez más evidente la inserción de la informática en la vida diaria de los mexicanos más allá de lo laboral y, por tanto, la importancia de legislar y monitorear de manera económica, sociológica y psicológica las consecuencias del uso de estas tecnologías. En el caso de la legislación mexicana ante la adhesión de un convenio internacional como lo es el Convenio o Convención de Budapest, existen muchos aspectos que no son del todo asequibles pues, a diferencia de la legislación nacional en materia de cibercriminalidad, no existe un concepto como tal acerca de cibercriminalidad y tampoco se hace una diferencia entre crimen cibernético o delito cibernético y ataque cibernético, no se consideran muchos como delitos penales, no hay tampoco una contemplación de delitos por difusión, o almacenamiento de delitos raciales o religiosos, ciberacoso (tomando en cuenta que en México los problemas por acoso escolar y laboral han ido en aumento) y está en proceso una legislación para la responsabilidad penal de las personas morales.

Por otra parte, la infraestructura a nivel internacional en lo que respecta a la investigación y seguimiento de estos crímenes está creciendo y evolucionando pues, como ya se mencionó en un principio, los delitos cibernéticos se dan con gran rapidez.

VII.- Finalmente, esta Segunda Comisión reitera su compromiso por establecer y fortalecer nuestro marco jurídico frente al fenómeno de crímenes cibernéticos, y apoya la solicitud de la proponente de solicitar un informe a las dependencias federales sobre los acuerdos y avances con organismos internacionales en torno al Convenio de Budapest.

Por lo anteriormente expuesto, los legisladores integrantes de la Segunda Comisión, de Relaciones Exteriores, Defensa Nacional y Educación Pública, de la Comisión Permanente del Congreso de la Unión, someten a la consideración de esta Soberanía el siguiente:

PUNTO DE ACUERDO

ÚNICO. La Comisión Permanente del Congreso de la Unión solicita a la Procuraduría General de la República, al Comisionado Nacional de Seguridad y al Consejero Jurídico del Ejecutivo Federal un informe sobre los avances de la integración de México en los distintos organismos, acuerdos, tratados y convenios internacionales en materia de seguridad cibernética, y la posición de esas dependencias federales respecto a la adhesión al convenio de cibercriminalidad de Budapest.

Dado en la sala de reuniones de la Segunda Comisión de la Comisión Permanente del Congreso de la Unión, a los trece días del mes de agosto del año dos mil quince.