

PROPOSICIÓN CON PUNTO DE ACUERDO, PARA EXHORTAR A LA SRE A INFORMAR SOBRE LA VIABILIDAD DE QUE EL ESTADO MEXICANO SE ADHIERA AL CONVENIO SOBRE CIBERDELINCUENCIA, O CONVENIO BUDAPEST, A CARGO DEL SENADOR MIGUEL ÁNGEL LUCERO OLIVAS, DEL GRUPO PARLAMENTARIO DEL PT

Del senador Miguel Ángel Lucero Olivas, integrante del Grupo Parlamentario del Partido del Trabajo de la LXIV Legislatura del honorable Congreso de la Unión, con fundamento en lo dispuesto por el artículo 58 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, somete a consideración del pleno de la Comisión Permanente la siguiente proposición con punto de acuerdo, por el que se exhorta respetuosamente a la Secretaría de Relaciones Exteriores a que rinda un informe detallado sobre la viabilidad de que el Estado mexicano se adhiera al Convenio de Ciberdelincuencia también llamado Convenio de Budapest y su protocolo adicional, al tenor de las siguientes

Consideraciones

La internet es un fenómeno globalizado del cual hemos obtenido grandes beneficios, han cambiado las formas de comunicar, acceder y compartir información, es así como la manera de interactuar se ha vuelto más rápida y sin límites fronterizos.

El Instituto Nacional de Estadística y Geografía nos muestran las siguientes estadísticas a propósito del día mundial del internet el 17 de mayo de 2019 datos nacionales; “Según los datos de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, en 2018 el 65.8% de la población de seis años o más en México es usuaria de Internet, 18.3 millones de hogares (52.9% del total nacional) disponen de conexión a Internet, 95.1% de los usuarios con estudios de nivel superior se conectan a la red, así como 54.9% de los que tienen estudios de educación básica.”¹

Con lo anterior el número de usuarios que cada día crece no es pequeña, sin embargo, así como sus beneficios han impactado en nuestra vida cotidiana también existen perjuicios que se podrían evitar, reparar o castigar.

El manual de Delitos Informáticos del Departamento de Justicia de los Estados Unidos de Norteamérica establece lo siguiente: “El delito informático es cualquier violación de la ley penal que implique el conocimiento de la tecnología informática para su perpetración o investigación”²

La legislación correspondiente para enfrentar y prevenir este tipo de conductas contiene un gran vacío legal en nuestro marco jurídico mexicano.

Con objeto de fortalecer el marco jurídico en materia de ciberseguridad se debe reforzar la cooperación internacional para prevenir estos delitos, México debe buscar la manera de hacer posible la ampliación de las herramientas de investigación, prevención y sanción.

Diversas naciones e instituciones como la Organización de las Naciones Unidas, el G8, la Unión Europea, el Consejo de Europa entre otras organizaciones regionales se han ocupado de la tarea para regular los delitos informáticos y ponerle freno a la ciberdelincuencia.

El Convenio de Budapest del 23 de noviembre del 2001 establece diversas acciones para tener un marco jurídico nacional adecuado con la tipificación de distintas conductas como ilícitas, dotar a las autoridades en materia de justicia penal con facultades y protocolos necesarios para la investigación y promueve la cooperación internacional.

El protocolo adicional del 28 de enero de 2003 establece en su artículo 1º la finalidad de completar, entre las Partes en el Protocolo, las disposiciones del Convenio sobre la Ciberdelincuencia, por lo que respecta a la tipificación penal de los actos de índole racista y xenófoba cometidos mediante sistemas informáticos.

El convenio ha sido ratificado por 64 países y otros 3 países han firmado sin ratificación, que son los siguientes:³

Albania, Andorra, Armenia, Austria, Azerbaiyán, Bélgica, Bosnia, Bulgaria, Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Georgia, Alemania, Grecia, Hungría, Islandia, Irlanda, Italia, Liechtenstein, Lituania, Luxemburgo, Malta, Mónaco, Montenegro, Países Bajos, Macedonia del Norte, Noruega, Polonia, Portugal, República de Moldova, San Marino, Serbia, Eslovaquia, Eslovenia, España, Suecia, Suiza, Turquía, Ucrania, Reino Unido, Argentina, Australia, Cabo Verde, Canadá, Chile, Costa Rica, República Dominicana, Ghana, Israel, Japón, Islas Mauricio, Marruecos, Panamá, Paraguay, Perú, Filipinas, Senegal, Sudáfrica, Sri Lanka, Tonga, Estados Unidos de América.

En México han existido distintos esfuerzos por distintos estados de la República, así como a nivel Federal en el ámbito de ciberseguridad y ciberdelincuencia.

Para incrementar su presencia en Internet, la Policía Federal Preventiva (PFP) desarrolló a inicios del gobierno del presidente Vicente Fox Quesada, una unidad especializada en el combate a delitos cibernéticos denominada Policía Cibernética, teniendo como objetivos principales localizar personas dedicadas a cometer delitos informáticos e identificar y desarticular organizaciones dedicadas al tráfico y corrupción de menores.⁴

En diciembre de 2002 la entonces Secretaría de Seguridad Pública instaló la Coordinación Interinstitucional de Combate a Delitos Cibernéticos formado por la Presidencia de la República, la Procuraduría General de la República, la Procuraduría General de Justicia del Distrito Federal, la Policía Federal Preventiva, el Centro de Investigación y Seguridad Nacional, la Secretaría de la Defensa Nacional, la Secretaría de Marina, la entonces Secretaría de Seguridad Pública, E-México, la Universidad Nacional Autónoma de México, Avantel, Alestra y la Alianza Mexicana de Cibercafés, AC. Entre sus actividades de patrullaje en la red están el rastreo de hacker, sitios de internet y chat room en los que promuevan pornografía y el turismo sexual infantil.

En lo que respecta a la regulación en la legislación los “delitos informáticos” existen en el Código Penal Federal desde el 17 de mayo de 1999, sin embargo, se fue quedando pequeña, puesto que en su articulado no se contemplan las actualizaciones que desde entonces se han hecho tanto en la tecnología como las nuevas redes sociales o la evolución de relaciones que se han inventado.

En la Ciudad de México actualmente tenemos a la policía de ciberdelincuencia preventiva que establece lo siguiente como sus principales líneas de acción:⁵

- Monitoreo de redes sociales y sitios web en general.
- Pláticas informativas en centros escolares e instituciones del Distrito Federal, con el objetivo de advertir los delitos y peligros que se cometen a través de internet, así como la forma de prevenirlos, creando una cultura de autocuidado y civismo digital.
- Ciber-alertas preventivas las cuales se realizan a través del análisis de los reportes recibidos en las cuentas de la Policía de Ciberdelincuencia Preventiva.

En el vigente ordenamiento jurídico y con la reforma en materia penal se crea la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, y se establecen sus atribuciones:

“Que el Sistema de Justicia Penal Adversarial requiere que el personal policial de la Agencia de Investigación Criminal realice investigaciones fortalecidas con elementos científicos y cibernéticos con el fin de contar con más información criminal que pueda ser incorporada como dato de prueba, medios de prueba y prueba al Ministerio Público de la Federación y con ello sustentar las acusaciones, por lo que he tenido a bien expedir el siguiente acuerdo:

Primero. Se crea la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas como la instancia de inteligencia encargada de la ejecución y supervisión de las acciones policiales que apoyen las investigaciones relacionadas con medios electrónicos y tecnológicos bajo la conducción y mando del Ministerio Público de la Federación.”⁶

Como observamos existen distintas autoridades y organismos que se están ocupando de la tarea, sin embargo, el poder legislativo tiene la tarea de coadyuvar con estos para otorgar efectivos resultados.

Con fecha del 8 de agosto de 2017 y número de oficio “SELAP/300/1959/17, se recibe en la Comisión Permanente del Congreso de la Unión la respuesta al punto de acuerdo por parte de la Secretaría de Relaciones Exteriores en el que establece lo siguiente: “Para responder a la invitación del Consejo de Europa a México a fin de que nuestro país se adhiera al Convenio de Budapest, las autoridades competentes del Ejecutivo Federal se encuentran evaluando si el marco jurídico vigente permitiría cumplir cabalmente con las obligaciones contenidas en el Convenio. Una vez que este análisis concluya, se podrá determinar la viabilidad de que el Estado mexicano se adhiera al Convenio o bien identificar las medidas legislativas que sería necesario implementar para poder ser Parte del mismo... Toda vez que no existe un foro multilateral único con el mandato para concentrar las deliberaciones sobre la ciberseguridad, la Secretaría de Relaciones Exteriores está comprometida a seguir privilegiando la concertación multilateral al abordar este tema, y a participar activamente en las discusiones en el marco de la ONU, así como en otros mecanismos de cooperación internacional como el Foro Global sobre Experiencias Cibernéticas y la Conferencia Global del Ciberespacio, o a nivel regional en el seno de la Organización de los Estados Americanos (OEA), dentro del programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo.”⁷

Con base en los trabajos legislativos que anteriormente se exponen, se debe seguir tanto con esfuerzo y seguimiento para alcanzar el objetivo de la concretización de la adherencia y así avanzar a tener un marco jurídico que garanticen la protección de los usuarios para terminar con las graves condiciones de inseguridad e impunidad que impera en la materia. El interés para que se concrete sería un gran paso en favor de los derechos humanos vulnerados.

La formación de un marco jurídico para la regulación de internet representa un grande reto de indudable relevancia y de gran urgencia, pues entre más esperamos su evolución es imparables. Si observamos en comparación los avances que hemos tenido y los esfuerzos que se han realizado para resolver esta problemática

En la actual legislatura el 24 de octubre del 2019 se discutió en el pleno el dictamen de las comisiones unidas de Seguridad Pública y Estudios Legislativos Primera, por el que se aprueba la iniciativa con proyecto de decreto por el que se declara el mes de octubre como “el mes nacional de la ciberseguridad”, es así como se remarca la intención en la actual legislatura para seguir con el trabajo antes mencionado en el Senado de la República que se traduzca en el fortalecimiento de instituciones y la creación de facultades en los órganos operativos del Estado para prevenir, enfrentar y castigar amenazas en los entornos digitales.

Por lo anteriormente expuesto, se somete a la consideración del pleno de la Comisión Permanente de esta soberanía el presente

Punto de Acuerdo

Único: La Comisión Permanente del honorable Congreso de la Unión exhorta respetuosamente a la Secretaría de Relaciones Exteriores a que rinda un informe detallado sobre la viabilidad del Estado mexicano para adherirse al Convenio de Ciberdelincuencia también llamado Convenio de Budapest y su protocolo adicional.

Notas

- 1 https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2019/internet2019_Nal.pdf
- 2 <https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf>
- 3 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=heJyDqZI
- 4 https://www.senado.gob.mx/64/gaceta_del_senado/documento/1196
- 5 <http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html>
- 6 http://dof.gob.mx/nota_detalle.php?codigo=5496125&fecha=05/09/2017
- 7 https://www.senado.gob.mx/sgsp/respuestas/63/2/2017-06-21-1/CP2R2A-2275-2275%20SEGOB_SRE

Dado en el pleno de la Comisión Permanente de la Cámara de Diputados el día veintidós de enero del año dos mil veinte.

Senador Miguel Ángel Lucero Olivas (rúbrica)