|  |
| --- |
| De la Sen. Margarita Villaescusa Rojo, del Grupo Parlamentario del Partido Revolucionario Institucional, la que contiene punto de acuerdo para solicitar a las Comisiones de Justicia y Ciencia y Tecnología de ambas Cámaras impulsar la firma de un convenio de colaboración en materia de delitos cibernéticos con la UNAM. |
| ***SE TURNÓ A LA COMISIÓN DE CIENCIA Y TECNOLOGÍA. Documento en Tramite*** |
|  |
| |  | | --- | |  | |
| **PROPOSICIÓN CON PUNTO DE ACUERDO QUE PRESENTA LA SENADORA MARGARITA VILLAESCUSA ROJO, INTEGRANTE DEL GRUPO PARLAMENTARIO DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL EN LA LXI LEGISLATURA DEL H. CONGRESO DE LA UNIÓN, PARA SOLICITAR A LAS COMISIONES DE JUSTICIA Y CIENCIA Y TECNOLOGÍA DE AMBAS CÁMARAS, A IMPULSAR LA FIRMA DE UN CONVENIO DE COLABORACIÓN EN MATERIA DE DELITOS CIBERNÉTICOS CON LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, EL CONSEJO NACIONAL DE CIENCIA Y TECNOLOGÍA, EL PODER JUDICIAL DE LA FEDERACIÓN Y LAS PROCURADURÍAS ESTATALES Y DEL DISTRITO FEDERAL, CON LA FINALIDAD DE REALIZAR FOROS, SEMINARIOS Y CONSULTAS NACIONALES E INTERNACIONALES PARA** **EMPRENDER ACCIONES Y PROPUESTAS DE REFORMAS LEGISLATIVAS A NIVEL FEDERAL QUE, POSTERIORMENTE, PUEDAN SER REPLICADAS Y HOMOLOGADAS EN CADA UNA DE LAS ENTIDADES FEDERATIVAS.**  La que suscribe, **MARGARITA VILLAESCUSA ROJO**, Senadora de la República, integrante del Grupo Parlamentario del Partido Revolucionario Institucional en la LXI Legislatura del H. Congreso de la Unión, en ejercicio de la facultad que me confieren los artículos 8, numeral 1, fracción II y 276 del Reglamento del Senado de la República, someto a la consideración de esta Honorable Asamblea, la siguiente proposición con punto de Acuerdo que se fundamenta con base en la presente:  **Exposición de Motivos**  La legislación nacional tiene obstáculos por jurisdicción y lagunas legales para la sanción de las conductas delictivas que se realizan en el ciberespacio.  Diversos datos confirman que México ocupa el último lugar en materia de ciberseguridad entre los países que conforman la OCDE, va rezagado en la tipificación de delitos informáticos y no cuenta con recursos humanos preparados (agentes del Ministerio Público, policías investigadores y jueces) para hacer frente a fraudes electrónicos, clonación de tarjetas, robo de base de datos, bloqueo de portales o *jaqueo* de cuentas de correo, entre otros ilícitos de este tipo.  México es una de las naciones donde se registran delitos graves respecto a la pornografía infantil donde se procura, obliga, facilita o induce a un niño a realizar actos sexuales lesivos por medios electrónicos como Internet, y donde también, se oculta el *ciberbullying,* una conducta de acoso entre estudiantes de secundaria y preparatoria, y que amerita una regulación especial por las graves consecuencias sociales entre las que se encuentra el suicidio que puede generar entre los menores de edad a causa de la depresión, el acoso y el rechazo de que son objeto en el entorno estudiantil.  La pornografía infantil va ligada al *sexting* (contracción de sex y texting), que se refiere a la generación o envío de contenidos eróticos o sexualmente explícitos que están en la frontera de lo pornográfico, y al *grooming,* que consiste en que un adulto se hace pasar por un menor de edad con la finalidad de ganarse paulatinamente su confianza y, posteriormente, concertar una cita para cometer con su víctima otra conducta delictiva.  El spam es otro caso donde los delitos cibernéticos se manifiestan, ya que se trata de un correo no deseado o no solicitado que puede ser *fishing* (hacer que los usuarios piquen el anzuelo) y *farming* (un simulador). En el primer caso, se pide información para actualizar una supuesta base de datos, lo que permite a los ciberdelincuentes acceder a cuentas bancarias y vaciarlas; el segundo, nos conduce a un portal que simula ser de una institución bancaria, donde otra persona sustrae los recursos.  Uno de los delitos más frecuentes lo encontramos en la clonación de tarjetas bancarias. Es común que en los cuentahabientes registren en sus estados de cuenta disposiciones o compras que ellos no efectuaron.  Por su parte, existen en el lavado de dinero múltiples subterfugios para blanquear el dinero mal habido y, a pesar de las disposiciones restrictivas emitidas por las autoridades, el problema no se ha combatido eficazmente.  Muchas de las modalidades que adquieren los delitos informáticos no están tipificadas en el Código Penal por el cambiante mundo de la tecnología. Mientras tanto, nuestro país enfrenta el reto de las distintas codificaciones que marcan las jurisdicciones locales, ante un problema que no sólo se circunscribe al ámbito nacional, sino que se erige como un fenómeno global.  El *spam* es uno esos delitos que asumen esa categoría, porque vía correo electrónico o redes sociales se busca infiltrar *spyware*, que son programas que se alojan en nuestra computadora y permiten que otros a distancia puedan controlarla, es decir, además de tener acceso a toda nuestra información, el *ciberdelincuente* puede usar una PC como un mini servidor para enviar *spam* o virus informáticos sin que el o los usuarios de esa computadora se den cuenta. Esto convierte a nuestra computadora en el lenguaje de los especialistas en un *zombie*.  Uno de los delitos informáticos más graves es la usurpación de identidad, recientemente se tipificado en el Distrito Federal, el Estado de México y en Colima.  La usurpación de identidad consiste en que alguien obtiene información personal de una persona para subirla a las redes o a algún otro sitio, y se ostenta como esa persona para delinquir, ya sea mediante extorsión, chantaje, secuestro u otro tipo de actividades.  La pregunta es ¿Cómo hacer frente a esta moderna delincuencia? Que por desgracia cobran más auge en la actualidad y son ilícitos que están en la impunidad. De ahí que, en principio, sea clave tipificarlos.  Es indispensable también, contar con más y mejores equipos tecnológicos, así como más grupos policíacos especializados, que puedan identificar estos fenómenos.  De ahí la importancia para que desde el Congreso de la Unión y, en especial a través de las comisiones de Justicia y Ciencia y Tecnología de ambas cámaras, se puedan emprender acciones y reformas legislativas a nivel federal que puedan ser replicadas y homologadas en cada una de las entidades federativas, con el fin de destinar más recursos tecnológicos a la indagatoria de los delitos cibernéticos, así como la formación de policías investigadores, agentes del ministerio público y jueces especializados para poder enfrentar esta nueva forma de delincuencia.  Por otra parte, México es observador del Consejo Europeo desde 1999 y, en virtud de ello, fue invitado a ratificar la firma del Convenio europeo sobre cibercriminalidad, que ya han ratificado 32 de las 47 naciones miembro de este organismo, entre los que se encuentran Canadá, Estados Unidos, Japón y Sudáfrica.  El Convenio europeo sobre cibercriminalidad tiene como objetivo prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de los mismos, asegurando la incriminación de dichos comportamientos y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel nacional como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiable.  Asimismo, el Convenio está fundamentado en la necesidad de garantizar un equilibrio adecuado entre los intereses de la acción represiva y el respeto de los derechos fundamentales del hombre, como los garantizados en el Convenio para la protección de los derechos del hombre y de las libertades fundamentales del Consejo de Europa (1950), en el Pacto internacional relativo a los derechos civiles y políticos de las Naciones Unidas (1966), así como en otros convenios internacionales aplicables en materia de derechos del hombre, que reafirman el derecho de no ser perseguido por la opinión, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar informaciones e ideas de toda naturaleza, sin consideración de fronteras, así como el derecho al respeto de la vida privada.  El Convenio considera igualmente complementarlos convenios existentes del Consejo de Europa sobre la cooperación en materia penal, así como otros tratados similares suscritos entre los Estados miembros del Consejo de Europa y otros Estados, con el fin de hacer más eficaces las investigaciones y procedimientos penales relativos a las infracciones penales vinculadas a sistemas y datos informáticos, así como permitir la recopilación de pruebas electrónicas de una infracción penal.  En declaraciones recientes el responsable de Protección de datos y delitos cibernéticos del Consejo de Europa, Alexander Seger, instó a México a ratificar el Convenio sobre cibercriminalidad, con el objetivo de fortalecer la legislación nacional en esta materia, pues dijo, con la situación actual hay muchas dificultades para que haya una cooperación internacional efectiva.  Es por lo anterior que creemos pertinente, solicitar a las comisiones de Justicia y Ciencia y Tecnología de esta Cámara, celebrar reuniones con las dependencias del Ejecutivo Federal involucradas, para impulsar la firma, aprobación y ratificación del Convenio europeo sobre cibercriminalidad.  Por lo anteriormente expuesto y fundado en los artículos 8, numeral 1, fracción II y 276 del Reglamento del Senado de la República, someto a la consideración de la Asamblea, la siguiente proposición con  **Puntos de acuerdo**  **Primero.-** El Senado de la República solicita respetosamente a las comisiones de Justicia y Ciencia y Tecnología de ambas cámaras, a impulsar la firma de un convenio de colaboración en materia de delitos cibernéticos con la Universidad Nacional Autónoma de México, el Consejo Nacional de Ciencia y Tecnología, el Poder Judicial de la Federación, las procuradurías estatales y del Distrito Federal, con la finalidad de realizar foros, seminarios y consultas nacionales e internacionales para emprender acciones y propuestas de reformas legislativas a nivel federal que, posteriormente, puedan ser replicadas y homologadas en cada una de las entidades federativas con el fin de destinar más recursos tecnológicos a la indagatoria de los delitos cibernéticos, así como la formación de policías investigadores, agentes del ministerio público y jueces especializados para poder enfrentar esta nueva forma de delincuencia.  **Segundo.-** El Senado de la República solicita a las comisiones de Justicia y Ciencia y Tecnología de ambas cámaras, para que en el uso de sus atribuciones, puedan dejar sentadas las bases y los consensos necesarios para lograr que los delitos informáticos puedan estar tipificados en los códigos Penal y de Procedimientos Penales y, que las distintas codificaciones que marcan las jurisdicciones locales puedan homologarse para la persecución eficaz de este delito ante un problema que no sólo se circunscribe al ámbito nacional, sino que se erige como un fenómeno global.  **Tercero.-** El Senado de la República solicita a las comisiones de Justicia y Ciencia y Tecnología de esta Cámara celebrar reuniones con las dependencias del Ejecutivo Federal involucradas, para impulsar la firma, aprobación y ratificación del Convenio europeo sobre cibercriminalidad.  S u s c r i b e,  **SEN. MARGARITA VILLAESCUSA ROJO**  Dado en el salón de sesiones del Senado de la República, a los 13 días del mes de marzo de 2012. |