INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL PARA TIPIFICAR EL DELITO DE USURPACIÓN DE IDENTIDAD A TRAVÉS DE ALGÚN SISTEMA O MEDIO INFORMÁTICO

La suscrita, **Senadora Juanita Guerra Mena**, perteneciente a la LXVI Legislatura del H. Senado de la República, ejerciendo la facultad consagrada en el artículo 71 fracción II de la Constitución Política de los Estados Unidos Mexicanos, así como por los artículos 8 numeral 1, fracción I, 164 numeral 1 y 169 del Reglamento del Senado de la República, someto a la consideración de esta H. Asamblea la siguiente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL PARA TIPIFICAR EL DELITO DE USURPACIÓN DE IDENTIDAD A TRAVÉS DE ALGÚN SISTEMA O MEDIO INFORMÁTICO,** al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

La vida actual no podría ser concebida sin la existencia de Internet, que prácticamente revolucionó la interacción social en todas sus formas, las industrias dedicadas a la comunicación como los medios audiovisuales, la telefonía, periódicos, revistas, han tenido que ser redefinidos por Internet, naciendo así nuevos servicios y formas de comunicar, como el correo electrónico, las llamadas y video llamadas, la transmisió de radio y televisión, el consumo de música y videos y las redes sociales. Asimismo, el comercio y los servicios financieros tradicionales han adoptado Internet como una herramienta fundamental a nivel mundial.

De acuerdo con el informe que presentan We Are Social y Hootsuit, 4.021 millones de personas tienen acceso a Internet, es decir el 53% de la población mundial, de los cuales el 68% procede de dispositivos móviles, un crecimiento del 4% en comparación con los datos arrojados el año anterior. Los Emiratos Árabes Unidos y

Qatar, encabezan la lista de los países en los que Internet tiene una mayor penetración, logrando un 99% de población conectada, a éstos le siguen Kuwait, Bahréin, Bermudas, Islandia, Noruega, Andorra, Luxemburgo y Dinamarca con una tasa de penetración superior al 97%.

Otro dato interesante que arroja el estudio, es que tres cuartas partes de personas con acceso a Internet son usuarios activos de redes sociales, es decir, 3.2 billones, lo que representa el 42% de la población mundial, 13% más que en 2017. Asimismo, 9 de cada 10 usuarios activos de redes sociales acceden a ellas a través de un teléfono móvil, 14% más que el año anterior.

Durante 2017, el 74.7% de los usuarios que acceden a Internet desde un dispositivo móvil lo usaron para acceder a redes sociales, actividad conformada por el 82.5% de conexiones móviles. No obstante, según datos de GlobalWebIndex, "un usuario normal ahora ocupa seis horas diarias desde algún dispositivo o servicio con conexión a Internet. Esto representa la tercera parte del tiempo que permanecen despiertos".

En cuanto a la popularidad de las redes sociales, Facebook sigue encabezando la lista con más del 62% de los usuarios totales de redes sociales en el mundo, y se mantuvo con un crecimiento de usuarios del 15% durante el año pasado. Mientras tanto, WhatsApp y Facebook Messenger tuvieron un crecimiento del 30% cada uno, siendo la primera la aplicación de mensajería principal en 128 países, entre ellos toda Latinoamérica, Brasil y España.

América Latina tiene una penetración de Internet superior a la que se registra a nivel mundial, el 67% de los latinoamericanos se conecta a la red de manera habitual, contra el 54% a nivel global. Los países que cuentan con un mayor número de usuarios son Ecuador con un 81%, Argentina con 78.6%, Chile 77%, Brasil 65.9% y México con un 65.3%.

Con estas cifras, prácticamente más de la mitad de la población mundial se encuentra interconectada, compartiendo información, fotos, videos, música, proyectos, productos, servicios, entre otros; eliminando así las barreras del tiempo y el espacio,

de una forma relativamente económica y accesible para muchos, convirtiéndose en una de las herramientas más importantes de la sociedad moderna.

Sin embargo, el auge de Internet no podía estar exento de adversidades y junto con el uso de la red llegaron los delitos cibernéticos o ciberdelitos.

Ciberdelito "es un término genérico que hace referencia a la actividad delictiva llevada a cabo mediante equipos informáticos o a través de Internet"[1].

Los ciberdelitos atentan contra las libertades, bienes o derechos de las personas; debido al alcance internacional de algunos de ellos, en 2001 se firmó el Convenio de Ciberdelincuencia en Budapest, a fin de fomentar la cooperación internacional y que cada nación firmante llevara a cabo las medidas legislativas y de otro tipo que resulten necesarias para tipificar los ciberdelitos en su derecho interno y se garantice la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables[2].

El Convenio sobre la Ciberdelincuencia, es el primer tratado internacional, creado por el Consejo de Europa en 2001; en el año 2007, México manifestó su interés por trabajar en conjunto con otros países para luchar contra el cibercrimen, sin embargo, nunca finalizó el procedimiento para adherirse al Convenio de Budapest[3].

Entre los ciberdelitos más comunes se encuentran los siguientes[4]:

- Cyberbulling o ciberacoso, es el uso de medios telemáticos para ejercer el acoso psicológico entre iguales;

---

[1] https://www.avast.com/es-es/c-cybercrime

[2] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

[3] https://www.excelsior.com.mx/hacker/2016/12/07/1132670

[4] http://nicestream.com/blog/ciberdelitos/

- Revenge Porn o porno vengativo, es el contenido sexual explícito que se publica en internet sin el consentimiento del individuo que aparece representado;

- Grooming, se trata de una serie de conductas y acciones emprendidas por un adulto con el objetivo de ganarse la confianza de un menor de edad, creando una conexión emocional con el fin de disminuir las inhibiciones del menor y poder abusar sexualmente de él, o bien su introducción a la prostitución infantil o a la producción de material pornográfico;

- Pharming, es la explotación de una vulnerabilidad en el software de los servidores DNS (o en el de los equipos del propio usuario) que permite al atacante redirigir un nombre de dominio a otra computadora distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para el nombre de este dominio;

- Phishing o suplantación de identidad, es el modelo de abuso informático que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta. El ciberdelincuente, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica. Por lo general, es una acción que va de la mano con una estafa, los canales más susceptibles para poner en práctica este delito son el correo electrónico y las redes sociales.

Este último, phishin o suplantación de identidad ha ido en aumento a nivel mundial, este tipo de delito informático creció 20% durante el tercer trimestre del año 2017, los países más vulnerables a este ciberdelito son Brasil, Australia, Nueva Zelanda, China, Francia, Perú, Canadá, Qatar y Georgia, según el último informe de la empresa rusa de ciberseguridad Kaspersky.

Este tipo de ciberataque tiene dos vertientes, la primera consiste en engañar a los usuarios con mensajes de correo electrónico fraudulentos o sitios web que parecen legítimos para conseguir contraseñas, número de tarjeta de crédito, datos bancarios y cualquier tipo de información confidencial o sensible.

De acuerdo con datos de Kaspersky, entre los sitios más usados para llevar a cabo el delito se encuentran Facebook, Microsoft Corporation y Yahoo. Recientemente hubo un incremento en la utilización de Whatsapp y Netflix, debido a su creciente popularidad, en el caso del segundo los delincuentes obtienen la información de la tarjeta bancaria con el pretexto de un pago que no se completó u otros problemas con la renovación de la suscripción.

Siguiendo con información de Kaspersky, durante el segundo trimestre de 2017, la mitad de las detecciones de fraude se dieron mediante páginas fraudulentas que mencionaban nombres de bancos (24,1%), sistemas de pago (13,94%) y tiendas online (9,49%). También, es común el redireccionamiento y entrega de datos con el pretexto de haber ganado un premio, y así llevar a las víctimas a un sitio web falso[5].

La otra vertiente de la suplantación de identidad, difiere del robo, el delincuente no busca acceder a las contraseñas o datos personales de la víctima, simplemente crea perfiles paralelos con información publicada particularmente en redes sociales. Los motivos para crear perfiles falsos son diversos y pueden dar pie a que se cometa otro delito conocido como ciberacoso o ciberbullying, en esta vertiente el delincuente genera contenidos negativos de la víctima para afectar su reputación online, se lleva a cabo por periodos largos para finalmente solicitar dinero a cambio de eliminar la información falsa; en algunas ocasiones se usa el nombre e imagen de la persona para encontrar pareja o amigos en el ciberespacio; también se crean para ofertar préstamos de dinero o servicios, solicitando dinero por adelantado para gastos de gestión.

Las redes sociales son el espacio más común donde las suplantaciones de identidad dan lugar, ya que es fácil y accesible obtener la información personal de un usuario

[5] https://www.eleconomista.com.ar/2017-11-pais-top-10-ranking-phishing/

específico, así como fotos y en algunos casos hasta videos. Las personas más susceptibles de ser víctimas son aquellas que tienen su información personal como el nombre y apellidos, fecha y lugar de nacimiento, fotografías, videos, etc. de manera pública en alguna red social; es común pensar que esto solo les ocurre a figuras públicas, no obstante, cualquiera puede ser víctima de este ciberdelito.

La usurpación de identidad no solo afectan a la persona o empresa suplantada, también a aquellos que consideran verdaderas y confiables las cuentas falsas.

En América Latina los ataques de phishing han sido constantes, con un incremento del 60%, donde Venezuela registra el mayor número de los ataques en proporción a su población con un total de 70.4%, seguido por Bolivia con un 66.3% y Brasil con 64.4%, lo anterior se dio a conocer durante la Octava Cumbre de Analistas de Seguridad para América Latina que se llevó a cabo en Panamá. Una gran parte de los ataques ocurren mientras la víctima está navegando, descargando archivos o cuando se reciben archivos adjuntos de correos electrónicos fraudulentos[6].

Según datos del Banco de México, nuestro país ocupa el octavo lugar global en el delito de robo de identidad, el cual ocurre porque las personas pierden sus documentos, les roban carteras y portafolios o porque los delincuentes toman su información directamente de una tarjeta bancaria.

Por su parte, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), manifiesta que, el robo de identidad se puede dar si no tomas las debidas precauciones al realizar compras, pagos de servicios, de impuestos o transacciones bancarias vía internet; robo de teléfonos celulares; si proporcionas demasiada información a través de redes sociales; en estados de cuenta o documentos personales que tiras sin precaución a la basura; robo de correspondencia y robo de carteras o bolsos con tarjetas de crédito e identificaciones. Y emite las siguientes recomendaciones: no ingresar nombres de usuario y contraseñas en sitios desconocidos; evitar compartir información financiera; utilizar

---

[6] https://latam.kaspersky.com/about/press-releases/2018_panorama-de-amenazas-phishing

sólo páginas electrónicas que cuenten con certificados de seguridad; entre otros, que no están ligados al uso de sistemas informáticos.

En lo que va del año, la Asociación de Sociedades Financieras de Objeto Múltiple (Asofom) ha detectado que entre 10 y 12 de sus agremiados sufrió algún caso de suplantación de identidad, lo que supone un incremento considerable en la incidencia de este ciberdelito. De acuerdo con información del presidente de la Asofon, Adolfo González Olhovich, la suplantación de identidad es el ciberdelito que más afecta actualmente a las 171 sociedades financieras de objeto múltiple (sofomes) agremiadas en la asociación. "En el caso de los intermediarios financieros, la suplantación de identidad se lleva a cabo cuando una persona ajena a la institución financiera crea un sitio web similar al oficial, con lo que pueden ser alteradas formas de contacto, el nombre de los representantes de la sociedad y hasta los datos financieros de la misma"[7], lo cual permite a los ciberdelincuentes defraudar a los clientes que confían en que están accediendo a un sitio web legítimo.

Con la finalidad de combatir este ciberdelito se han implementado diversas acciones, por ejemplo, la Asociación de Sociedades Financieras de Objeto Múltiple (Asofom) creó un Comité de Ciberseguridad que servirá para coordinar e informar a los agremiados sobre los incidentes que afecten a cada uno de ellos; además se ha elaborado una guía sobre usurpación de identidad; así como firma de acuerdos entre instituciones financieras y autoridades como Condusef, la Secretaría de Hacienda y la Comisión Nacional Bancaria y de Valores, y con la Asociación Internacional de Investigaciones de Crímenes Financieros (IAFCI), asociación experta en el tema de ciberseguridad.

En ese sentido, aunque se están llevando a cabo acciones para detener el ciberdelito de usurpación de identidad o phishing todavía queda mucho por hacer, particularmente desde el Poder Legislativo, si consideramos que México tiene una gran cantidad de usuarios, los cuales destinan más de 3 horas al día a las redes sociales y aplicaciones de mensajería instantanea. "Ochenta y tres millones de

[7] https://www.eleconomista.com.mx/tecnologia/Suplantacion-de-identidad-principal-ciberdelito-contra-sofomes-en-Mexico-20180812-0004.html

usuarios en México mensualmente presentan actividad en Facebook. De este número, más del 90% accede desde un móvil, siendo los perfiles de mujeres los que presentan un mayor número, así como usuarios entre los 18 y 34 años de edad"[8], y recordamos que particularmente esta red social es de las favoritas de los delincuentes para la usurpación de identidad, nuestro país se encuentra en riesgo latente de incrementar este ciberdelito.

Hoy, nuestra propuesta consite en reformar el Codigó Penal Federal para establecer el delito de usurpación de identidad a través de algún sistema o medio informático, con la finalidad de obtener un beneficio para sí mismo o un tercero, con una pena de cuatro a ocho años de prisión y una multa de 150 a 300 unidades de medida, a fin de inhibir dicha conducta delictiva que año con año va en aumento en nuestro país y que en gran medida se debe al vacio legal.

Por lo anteriormente expuesto, someto a consideración de esta H. Asamblea, la siguiente Iniciativa con:

PROYECTO DE DECRETO

ÚNICO. - Se **REFORMA** la denominación del TÍTULO NOVENO "Revelación de Secretos y acceso ilícito a sistemas y equipos de informática" y se **ADICIONA** un Capítulo III y un Artículo 211 bis 8 al Código Penal Federal, para quedar como sigue:

CÓDIGO PENAL FEDERAL

TÍTULO NOVENO

Revelación de Secretos**,** acceso ilícito a sistemas y equipos de informática **y uso ilícito de información**

Capítulo III
Uso Ilícito de Información obtenida de sistemas y equipos de informática

[8] https://www.internacionaldemarketing.com/blog/las-redes-sociales-mas-usadas-mexico-caracteristicas/

Artículo 211 bis 8.- A quien a traves de algún sistema o medio informático obtenga sin consentimiento expreso, datos personales de un tercero para usurpar o suplantar su identidad, con la finalidad de obtener un beneficio para sí mismo o un tercero, se le impondrá una pena de cuatro a ocho años de prisión y una multa de 150 a 300 unidades de medida.

Dicha pena se aumentará hasta en una mitad si la utilización de datos personales de terceros sin consentimiento constituye el medio comisivo de otro delito o si el sujeto activo genera con su actuar una afectación a los bienes, patrimonio, buena fama o prestigio laboral.

TRANSITORIOS

ARTICULO PRIMERO.- El presente decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Salón de Sesiones del Senado de la República, a 21 de abril de 2026.

SENADORA JUANITA GUERRA MENA
INTEGRANTE DEL GRUPO PARLAMENTARIO DEL
PARTIDO VERDE ECOLOGISTA DE MÉXICO