

INICIATIVA QUE ADICIONA DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL, EN MATERIA DE USO INDEBIDO DE DATOS PERSONALES, A CARGO DE LA DIPUTADA VALERIA SANTIAGO BARRIENTOS, DEL GRUPO PARLAMENTARIO DEL PVEM

La que suscribe, diputada Valeria Santiago Barrientos, integrante del Grupo Parlamentario del Partido Verde Ecologista de México de la LXV Legislatura de la Cámara de Diputados del honorable Congreso de la Unión, con fundamento en lo dispuesto en el artículo 71, fracción II, y 72 de la Constitución Política de los Estados Unidos Mexicanos; 6, numeral 1, 77 y 78 del Reglamento de la

Cámara de Diputados, somete a consideración de esta asamblea la presente **iniciativa con proyecto de decreto por el que se adiciona un Capítulo III Quáter y un artículo 391 Bis 1 al Código Penal Federal**, al tenor de la siguiente:

Exposición de Motivos

El artículo 6o. constitucional en su apartado A, fracción segunda, establece el derecho humano que garantiza que la información relativa a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

En el mismo sentido, el artículo 16 constitucional establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Como se observa, nuestra Carta Magna integra el derecho humano a la protección, de la información confidencial, íntima o privada de las personas como una garantía que debe estar bajo tutela jurídica.

Derivado de este derecho consagrado en la Constitución, existe normativa especial que establece las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección y al debido tratamiento de los datos personales, es decir, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ambas normativas conceptualizan los datos personales en dos vertientes:

-Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

-Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud

presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Ahora bien, la Ley Federal de Transparencia y Acceso a la Información Pública establece lo que se considerará como información confidencial:

De la Información Confidencial

Artículo 113. Se considera información confidencial:

La que contiene datos personales concernientes a una persona física identificada o identificable;

I. (...)

II. Los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos, y

III. Aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales. La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello.

(...)

No obstante lo anterior, no existe una regulación que sancione la sustracción uso o transmisión de datos personales con el propósito de cometer delitos.

Como se observa, tenemos legislación que garantiza la protección de datos personales y de la información confidencial de las personas, pero no una que sancione el uso de la misma para la comisión de delitos.

De manera irreductible, los insumos tecnológicos que día a día van apareciendo en nuestra vida pasan a formar parte de los accesorios necesarios que cada sector de la sociedad utiliza para desarrollarse, interactuar, desenvolverse y acceder a las necesidades básicas para facilitar sus actividades.

Si bien este avance tecnológico es utilizado para satisfacer los requerimientos actuales de todas y todos, como algo útil para facilitar la vida cotidiana, también es cierto que éstos son utilizados para acceder a información personal y privada con el fin de cometer conductas antijurídicas y causar algún tipo de daño.

En México, debido a la pandemia, se detonaron un sinnúmero de hechos que dan cuenta de la problemática que implica la vulneración de los datos personales o de la información privada.

De manera reciente, las aplicaciones de mensajería instantánea como WhatsApp, Telegram o Messenger han sido vías que utilizan los delincuentes para cometer actos ilícitos.

Un ejemplo es el robo de cuentas que se ha hecho común para pedir a los contactos de la víctima sumas de dinero a nombre de ésta; los criminales también aplican otro método que consiste en enviar un mensaje vía WhatsApp a su víctima, asegurando que son de la policía y que debe pagar una suma de dinero a cambio de no detenerlo por un delito grave. Pese a que no dicen la cantidad que quieren señalan que “se puede llegar a un acuerdo” antes de pasar el caso, pues aseguran que están a unos metros de su hogar y le envían supuestos documentos oficiales como una ficha de aprehensión en su contra.¹

Este tipo de conductas aterrizan en los llamados delitos cibernéticos o delitos informáticos, que han sido definidos por la Organización para la Cooperación y Desarrollo Económicos como “cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos”.²

La Organización de las Naciones Unidas, por su parte, reconoce diversos delitos vinculados con el tema informático, entre otros:

1. Acceso no autorizado a servicios o sistemas informáticos;
2. Falsificación de documentos de uso comercial;
- 3.- Fraude efectuado por manipulación informática; y
4. Manipulación de datos de salida.

En México, si bien existen hipótesis normativas que se acercan a tipificar algunas de las conductas antijurídicas vinculadas con temas afines con la tecnología, al día de hoy no existe reglamentación que sancione de manera particular los delitos realizados a través de medios tecnológicos cotidianos y que causan perjuicio en las personas que son susceptibles de estos delitos.

Según estadísticas de la Comisión Nacional para la Defensa de Usuarios de Servicios Financieros, conforme avanza el uso de las tecnologías de la información a través de dispositivos móviles, los delitos cibernéticos van en aumento. Algunas de las conductas que utilizan los delincuentes para cometer algún ilícito son:

-*Phising*. Son técnicas que utilizan los delincuentes para robar información personal o corporativa a través del correo electrónico o vía telefónica. En esta técnica se utiliza el engaño o violencia psicológica para que el sujeto pasivo entregue información cuando los usuarios no se dan cuenta de lo que está sucediendo. Es uno de los métodos más utilizados en México para delinquir.

-Pharming. Consiste en crear sitios web falsos, como si fuera un sitio web oficial, con la intención de conseguir la información que se introduzca en esos sitios, es decir, a través de un link falso redirigen al usuario a una página falsa para recabar información y poder cometer ilícitos.

-Spam. Son comunicaciones no solicitadas que se envían de forma masiva por Internet o mediante otros sistemas de mensajería electrónica. El spam es utilizado también para circular archivos que contienen algún tipo de virus que puede tener como intención acceder y robar la información del dispositivo en donde se descargó.

Aunque la Comisión Nacional para la Defensa de Usuarios de Servicios Financieros emite regularmente información relativa a medidas de seguridad, estas acciones no son suficientes y se necesita tomar medidas más formales para contener este tipo de conductas. En tal sentido, resulta necesario comenzar a adecuar la legislación penal a fin de actualizar y adaptar la ley a los nuevos tiempos, dado que la tecnología avanza a pasos agigantados y los delincuentes no pueden estar delante de nosotros, por lo que es necesario regular estas conductas a fin de inhibir que estas acciones se sigan reproduciendo en perjuicio de la ciudadanía.

Aunado a las recomendaciones que las autoridades dan a la ciudadanía, resulta necesario sumar y fortalecer el marco legal para evitar, o bien, inhibir los delitos informáticos, por lo que se debe dar más importancia y fortalecer el andamiaje penal para establecer reglas específicas para estas hipótesis.

Es menester recordar, como se señaló con antelación, que si bien existen algunas similitudes en algunos tipos penales, el conjunto de características y componentes esenciales que constituyen un delito informático son diferentes a los elementos de las hipótesis que actualmente se encuentran en la ley, por ello es necesario adecuarnos a los nuevos tiempos y actualizar la norma a fin de evitar que los delincuentes escapen a la aplicación de la ley.

De manera particular, la iniciativa que se presenta tiene como finalidad integrar al Código Penal Federal tipos penales específicos y sanciones para quienes vulneren el ámbito privado de las personas y sustraigan, utilicen o transmitan datos personales e información confidencial con el propósito de cometer delitos.

La presente reforma es necesaria en razón de que el avance y expansión de las nuevas tecnologías de la información ha impactado de manera significativa en cada uno de los ámbitos de la vida de las personas, particularmente, en el entorno de la vida privada de quienes tienen acceso a dispositivos digitales con los cuales interactúan de manera constante con otras personas.

Es en ese sentido, es indispensable transitar hacia la regulación de las nuevas tecnologías a fin de inhibir que éstas sean utilizadas para cometer delitos, por lo que es momento de poner manos a la obra y a empezar a legislar sobre la materia; los tiempos que hoy vivimos y la sociedad así lo exigen.

Por lo anterior, se propone la siguiente adición al Código Penal Federal:

Texto Vigente	Texto Propuesto
Código Penal Federal	
SIN CORRELATIVO	<p style="text-align: center;">CAPÍTULO III Quáter Utilización indebida de datos personales o información confidencial</p> <p>Artículo 391 bis. 1.- Comete el delito de uso indebido de datos personales o información confidencial quien, sin consentimiento, mediante engaño, amenaza o violencia, sustraiga, utilice o transmita datos personales o información confidencial, contenidos en dispositivos electrónicos personales móviles u ordenadores personales fijos, con la intención de obtener un lucro indebido o con el propósito de cometer un delito.</p>
	<p>La sustracción y transmisión ilegal de datos personales o información confidencial se castigará con pena de tres a cinco años de prisión y de 200 a 500 días multa.</p> <p>En la utilización ilícita de datos personales o información confidencial, con la intención de realizar transacciones, operaciones financieras o actos de comercio, para obtener un beneficio personal se aplicarán las penas y multas establecidas en el artículo 386 de este Código.</p>

Es importante manifestar que la reforma propuesta en esta iniciativa no genera impacto económico en el presupuesto de la nación, ya que no necesita recursos para su aprobación, publicación y ejecución.

Por los razonamientos y argumentos aquí vertidos y con el fin de fortalecer las leyes en materia de delitos informáticos, someto a la consideración de esta honorable Asamblea la siguiente iniciativa con proyecto de:

Decreto por el que se adiciona un Capítulo III Quáter y un artículo 391 Bis 1 al Código Penal Federal

Artículo Único. Se adiciona un Capítulo III Quáter y un artículo 391 Bis 1 al Código Penal Federal, para quedar como sigue:

Capítulo III Quáter Utilización indebida de datos personales o información confidencial

Artículo 391 Bis. 1. Comete el delito de uso indebido de datos personales o información confidencial quien, sin consentimiento, mediante engaño, amenaza o violencia, sustraiga, utilice o transmita datos personales o información confidencial, contenidos en dispositivos electrónicos personales móviles u ordenadores personales fijos, con la intención de obtener un lucro indebido o con el propósito de cometer un delito.

La sustracción y transmisión ilegal de datos personales o información confidencial se castigará con pena de tres a cinco años de prisión y de 200 a 500 días multa.

En la utilización ilícita de datos personales o información confidencial, con la intención de realizar transacciones, operaciones financieras o actos de comercio, para obtener un beneficio personal se aplicarán las penas y multas establecidas en el artículo 386 de este Código.

Transitorio

Único. El presente Decreto entra en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Notas

1 [1] Véase, “Alerta por hackeo de WhatsApp: cómo evitar ser víctima”, Infobae, 16 de diciembre de 2021. Disponible en: <https://www.infobae.com/america/tecno/2021/12/16/alerta-por-hackeo-de-whatsapp-como-evitar-ser-victima/>

2 [1] Véase, Diana Medina Gómez, “Los delitos cibernéticos y los problemas a enfrentar”, Hechos y Derechos, número 55 enero-febrero 2020. Disponible en: <https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14381/15543>

Palacio Legislativo de San Lázaro, a 26 de abril del 2023.

Diputada Valeria Santiago Barrientos (rúbrica)