



Ana Laura Huerta Valdovinos

Diputada Local



Honorable Asamblea Legislativa:

La suscrita Diputada Ana Laura Huerta Valdovinos, integrante de la Representación Partidista del Partido Verde Ecologista de México de la Legislatura 66 del Congreso del Estado Libre y Soberano de Tamaulipas, con fundamento en lo dispuesto en los artículos en 64 fracción I, de la Constitución Política del Estado de Tamaulipas; 89 párrafo 1 y 93 párrafos 1, 2 y 3 inciso b) de la Ley sobre la Organización y Funcionamiento Internos del Congreso del Estado Libre y Soberano de Tamaulipas, someto a consideración del Pleno de este Honorable Cuerpo Legislativo, la presente **INICIATIVA DE DECRETO DE REFORMAS A LOS ARTÍCULOS 418, FRACCIÓN XIX; Y 419, FRACCIÓN III; Y SE ADICIONAN LAS FRACCIONES XX AL ARTÍCULO 418 Y IV AL ARTÍCULO 419, DEL CÓDIGO PENAL PARA EL ESTADO DE TAMAULIPAS.**

OBJETO DE LA INICIATIVA

La presente iniciativa de decreto tiene por objeto tipificar el delito de fraude de comercio electrónico, para garantizar la protección de los derechos de los ciudadanos promoviendo un entorno digital más seguro y confiable para las tamaulipecas y tamaulipecos.

EXPOSICIÓN DE MOTIVOS

En las actividades diarias que realizamos las Tecnologías de la Información y la Comunicación (TICs), tienen una gran participación, debido a que han facilitado la forma de hacer las cosas. El concepto de Tecnologías de la Información y la Comunicación (TICs) se refiere al conjunto de herramientas que permiten la transmisión, el procesamiento y el almacenamiento de información. En este concepto se encuentran las computadoras y los elementos que la integran como



Ana Laura Huerta Valdovinos

Diputada Local

los programas de cómputo (software) y el hardware; los teléfonos inteligentes; las tabletas; las redes como Internet; sistemas informáticos y otros.¹

Las TICs se emplean para ejecutar actividades cotidianas de trabajo, educación, entretenimiento, transacciones comerciales, financieras, etcétera, y son usadas por un gran número de individuos, desde menores de edad hasta personas de la tercera edad, así como por las empresas y el gobierno. Desafortunadamente estas herramientas también son objeto e instrumento de conductas ilícitas que causan afectación a otras personas físicas o morales, y a sus patrimonios.

En este sentido, encontramos el llamado fraude cibernético o electrónico el cual es el uso de tecnologías digitales, principalmente a través de Internet, con el objetivo de cometer delitos o engañar a personas o empresas para obtener un beneficio económico de forma ilegal. Este tipo de fraude puede involucrar diversos métodos, como el robo de identidad, el phishing, el malware, el acceso no autorizado a cuentas bancarias, el fraude en compras en línea y otras actividades fraudulentas que explotan la confianza y las vulnerabilidades del entorno digital.

Las víctimas de fraude cibernético pueden ser individuos, organizaciones o incluso gobiernos, y los métodos utilizados por los ciberdelincuentes suelen ser cada vez más sofisticados y difíciles de detectar.

Las compras en línea se han consolidado como un medio práctico y eficiente para adquirir productos y servicios, permitiendo a los consumidores acceder a una vasta oferta de bienes desde la comodidad de su hogar. Sin embargo, junto con las ventajas que ofrece este nuevo paradigma, también surgen riesgos significativos relacionados con el fraude cibernético, un fenómeno que ha proliferado en el entorno digital.

¹ *Delitos Informáticos*. (2024). JUSTIA México. <https://mexico.justia.com/derecho-penal/delitos-informaticos/>



Ana Laura Huerta Valdovinos

Diputada Local

Asimismo, este lleva de la mano a la publicidad engañosa para atraer y hacer caer al consumidor, la cual puede ser por acción u omisión, la primera alude a información falsa que hace al consumidor caer en un error, como mostrar un número muy grande y creer que es el precio, pero no se refiere a eso. La segunda se refiere al ocultamiento de datos vitales, como las dimensiones del producto o garantía. Esta publicidad aprovecha que los consumidores suponen o asumen cosas que pueden parecer lógicas acerca del producto o servicio, pero luego se protegen indicando en que no se especificaron aquellos atributos.²

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), menciona que existen diferentes modalidades de fraude cibernético que afectan las compras en línea y dentro de los más comunes se encuentran:³

1. **Phishing:** Consiste en el uso de correos electrónicos o sitios web falsificados que imitan a empresas legítimas para robar datos sensibles, como contraseñas, números de tarjetas de crédito, datos bancarios u otros detalles personales, con el fin de usarlos de manera ilícita.

Este tipo de fraude implica la creación de correos electrónicos, mensajes de texto o sitios web que parecen provenir de una fuente confiable, como una entidad bancaria, una tienda en línea popular o una empresa legítima. Estos correos o páginas web fraudulentas están diseñados para que la víctima los confunda con páginas oficiales. El objetivo de estas, es engañar al usuario para que ingrese sus credenciales personales, lo que permite a los ciberdelincuentes acceder a sus cuentas y realizar transacciones fraudulentas.

² ¿Cómo evitar el fraude de compras por Internet? (2022). BBVA. <https://www.bbva.mx/educacion-financiera/creditos/fraude-de-compras-por-internet.html>

³ CONDUSEF. (2021). *Comercio electrónico, tipos de fraudes*. Gobierno de México. <https://www.condusef.gob.mx/?p=tipos-de-fraude>



Ana Laura Huerta Valdovinos

Diputada Local

El phishing tiene un impacto considerable tanto para los consumidores como para las empresas. Para los individuos, los riesgos son elevados: el robo de datos bancarios puede llevar a pérdidas financieras, el acceso a cuentas personales puede ser utilizado para cometer fraude o realizar compras no autorizadas, y la obtención de contraseñas puede facilitar el acceso a otras cuentas vinculadas, como correos electrónicos, redes sociales o servicios de pago.⁴

2. **Falsificación de productos:** Los delincuentes crean sitios web fraudulentos que ofrecen productos a precios mucho más bajos que los del mercado, con el fin de engañar a los consumidores y venderles productos falsificados o inexistentes.

La falsificación de productos constituye uno de los fraudes más perjudiciales y comunes en el ámbito del comercio electrónico. Los delincuentes cibernéticos crean sitios web fraudulentos que imitan a marcas y empresas legítimas con el fin de engañar a los consumidores y ofrecerles productos falsificados, de mala calidad o, incluso, inexistentes. Estos fraudes se aprovechan de la confianza y la comodidad que los compradores depositan en las plataformas de comercio en línea, y tienen consecuencias tanto económicas como legales para los afectados.⁵

Dentro de los métodos utilizados para que los sitios web donde se ofertan parezcan legítimos y cometer este tipo de fraude. Encontramos:

- Imitación de sitios web de marcas conocidas: Los fraudes se presentan a menudo con sitios web que utilizan el mismo diseño y las mismas imágenes que los sitios oficiales de marcas populares. Incluso pueden emplear dominios de direcciones web similares, con

⁴ *How to report a scam website fast.* (2023). F-secure. <https://www.f-secure.com/en/articles/how-to-report-a-scam-website-fast>

⁵ *Delitos informáticos.* (2020). Oficina de las Naciones Unidad Contra la Droga y el Delito. <https://www.unodc.org/e4j/es/cybercrime/module-2/key-issues/computer-related-offences.html>



Ana Laura Huerta Valdovinos

Diputada Local

pequeños cambios en la URL, para que los consumidores no detecten la falsificación.

- Ofertas atractivas y precios irrealmente bajos: Una de las tácticas más efectivas de los ciberdelincuentes es ofrecer productos a precios significativamente más bajos que los del mercado. Esto atrae a los consumidores que buscan descuentos y promociones, sin cuestionar la autenticidad del sitio.
- Reseñas falsas y testimonios falsificados: Muchos sitios fraudulentos utilizan reseñas y testimonios falsos de clientes para crear una apariencia de legitimidad. Estas reseñas pueden ser escritas por los propios delincuentes o compradas en plataformas que venden comentarios falsos.
- Falta de información de contacto o políticas claras: Las tiendas fraudulentas suelen carecer de información de contacto verificable, como números de teléfono o direcciones físicas. Además, sus políticas de devolución o reembolso son ambiguas o inexistentes, lo que hace que sea casi imposible recuperar el dinero después de una compra fraudulenta.

La CONDUSEF indica una serie de ventajas y desventajas sobre las compras en línea.⁶

Ventajas

- Facilita comparar precios y características de los productos.
- Se pueden realizar compras las 24 horas del día los 365 días del año.
- Se evitan los desplazamientos hacia las tiendas físicas y las filas al momento de pagar.
- Existen algunas opciones internacionales de compra.

⁶ CONDUSEF. (2021a). Comercio electrónico. Gobierno de México. <https://www.condusef.gob.mx/?p=lo-que-debes-saber>



Ana Laura Huerta Valdovinos

Diputada Local

- Se puede encontrar una mayor oferta de productos y precios más bajos.

Desventajas

- Si bien toda transacción comercial implica cierto riesgo, en compras por comercio electrónico se deben tomar mayores precauciones debido a que no se tiene un contacto presencial con el oferente.
- Algunos negocios no ofrecen un nivel adecuado de seguridad al realizar pagos electrónicos.
- En ocasiones las páginas web están en otro idioma.
- Se debe validar cual es la forma para hacer las devoluciones o hacer válida la garantía.

3. **Robo de identidad:** A través del acceso no autorizado a información personal de los usuarios, los ciberdelincuentes pueden realizar compras a nombre de las víctimas, afectando directamente su bienestar económico.

El robo de identidad puede tener efectos devastadores tanto a nivel económico como personal, afectando la reputación y el bienestar financiero de quienes lo sufren.

Los ciberdelincuentes pueden obtener esta información de diversas formas:

- **Phishing y otras técnicas de ingeniería social:** Los atacantes engañan a la víctima para que proporcione sus datos personales a través de correos electrónicos falsificados, mensajes de texto o sitios web fraudulentos que imitan a instituciones legítimas. Estos mensajes suelen indicar problemas de seguridad o la necesidad de actualizar información en una cuenta.
- **Robo de datos mediante vulnerabilidades de seguridad:** Los ciberdelincuentes también pueden obtener información personal a través de ataques a plataformas de comercio electrónico, bases de



Ana Laura Huerta Valdovinos

Diputada Local

datos de empresas o incluso dispositivos personales que no cuentan con la seguridad adecuada, como computadoras o teléfonos móviles sin protección.

- Acceso a redes sociales y otros servicios en línea: Los delincuentes pueden extraer datos personales de redes sociales y otros servicios en línea, donde las personas suelen compartir información sensible. El uso de técnicas como la recopilación masiva de datos a través de "scraping" o el análisis de perfiles públicos también contribuye al robo de identidad.⁷

4. **Estafas de pago:** En este tipo de fraude, los consumidores realizan pagos por productos que nunca reciben o que no corresponden a lo que fue prometido en la transacción.

Las estafas de pago se han vuelto cada vez más sofisticadas debido a la expansión del comercio en línea y al uso generalizado de plataformas digitales que no siempre ofrecen las garantías necesarias para evitar este tipo de engaños.⁸

Los tipos más comunes de estafas de pago incluyen:

- Pago por productos inexistentes: En este caso, el consumidor paga por un producto que no existe, es decir, realiza un pago por un artículo que no será entregado. Los estafadores suelen crear sitios web fraudulentos que imitan tiendas legítimas y venden productos a precios atractivos, para luego desaparecer una vez realizado el pago.

⁷ Mayne, M. (2024). *¿Qué es eso de scraping? Cómo merman los bots de scrapers web la rentabilidad del comercio electrónico.* Akamai. [https://www.akamai.com/es/blog/security-research/2024-commerce-soti-web-scrapers-bots#:~:text=%C2%BFQu%C3%A9%20es%20un%20bot%20de,inventario\)%20de%20un%20sitio%20web.](https://www.akamai.com/es/blog/security-research/2024-commerce-soti-web-scrapers-bots#:~:text=%C2%BFQu%C3%A9%20es%20un%20bot%20de,inventario)%20de%20un%20sitio%20web.)

⁸ Instituto Nacional de Ciberseguridad (INCIBE). (2023). *Prevención de estafas en el comercio electrónico: Recomendaciones para consumidores y empresas.* <https://www.incibe.es/>



Ana Laura Huerta Valdovinos

Diputada Local

- Productos no conformes a lo prometido: El consumidor puede recibir un producto, pero este no es el que se había anunciado en el sitio web. Este tipo de estafa puede implicar productos de mala calidad, artículos defectuosos o incluso copias de baja calidad de productos originales.
- Estafas de pago anticipado: En algunas ocasiones, los estafadores exigen el pago completo o una parte significativa del monto por adelantado, prometiendo el envío del producto en una fecha futura. Sin embargo, una vez que el pago se realiza, el estafador no envía el producto y desaparece con el dinero.
- Estafas de servicios no prestados: En este caso, el consumidor paga por un servicio que nunca se lleva a cabo. Las estafas relacionadas con servicios en línea, como la contratación de servicios de diseño web, asesoramiento o cursos en línea, son bastante comunes. Tras el pago, el proveedor desaparece sin ofrecer el servicio contratado.⁹

En este sentido de acuerdo con el documento "Retail Report 2024"¹⁰, revela que el fraude por comercio electrónico en México ha ido en aumento, tan solo en nuestro país en él 2023 se estafó a los consumidores en un 160% más de dinero que el año anterior. Con el tiempo ha aumentado este tipo de fraude, por ello se considera de suma importancia tipificar este delito, para garantizar una respuesta efectiva ante la creciente amenaza digital.

Las modalidades de fraudes que afectan a la población mexicana son numerosas, ejemplo de ello son clasificaciones que refieren conductas denominadas como monta deudas, pirámides financieras, llamadas de extorsión, falsos premios, engaños, venta de productos apócrifos, suplantación de identidad, comercio

⁹ Ídem

¹⁰

https://www.adyen.com/es_ES/index-reports/retail?utm_medium=OnlineAdvertising&utm_source=Google&utm_campaign=gad_source=1&gclid=EAIaIQobChMIplb30Z3giwMV_iZECB1QcSOWEAAAYASAAEgIT5vD_BwE



Ana Laura Huerta Valdovinos

Diputada Local

electrónico, entre otras, las cuales son medios para enganchar a las víctimas y buscar obtener un beneficio económico de manera ilegal. Por estas razones, algunos gobiernos de los estados de la República han creado fiscalías especializadas para investigar estos delitos. Ejemplo de ello es la Fiscalía de Investigación Estratégica de Delitos Financieros de la Fiscalía General de Justicia de la Ciudad de México. Dicho organismo tiene la facultad de conocer “los delitos de fraude y abuso de confianza cuando el monto sea superior a quince mil veces el salario mínimo vigente en el Distrito Federal, y delitos cometidos contra las instituciones financieras”.¹¹

Dentro del marco Legal Nacional, el fraude en nuestro país se encuentra tipificado en el Código Penal Federal¹² (CPF) en su título vigésimo segundo denominado “delitos en contra de las personas en su patrimonio”. En específico, el capítulo III aborda estas conductas ilícitas. El artículo 386 lo define como: “comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido” (CPF, 2023. p. 123). Asimismo, los artículos 387 al 389 bis mencionan las agravantes para las diferentes modalidades de este ilícito.

En nuestro Estado el personal de la Guardia Estatal Cibernética ha realizado campañas, en las cuales brindan orientación a las y los tlaulipecos que hayan sido víctimas de algún delito cibernético, o bien, requieran verificar algún sitio y prevenir estas situaciones.

Dentro de estas campañas para realizar acciones preventivas visitan planteles educativos y grupos gestionados por la sociedad civil organizada, para llevar a cabo pláticas informativas respecto a diferentes prácticas de las cuales pudieran constituirse delitos cibernéticos.

¹¹ Aguirre Quezada, J.P. (2023). “El fraude en México: daños patrimoniales y trabajo legislativo para enfrentarlo” Cuaderno de investigación No.99, Instituto Belisario Domínguez, Senado de la República, Ciudad México, 27p.

¹² <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf>



Ana Laura Huerta Valdovinos

Diputada Local

En Tamaulipas los municipios con más reportes en fraudes cibernéticos son Tampico, Reynosa y Ciudad Victoria.

En nuestro marco jurídico se encuentra tipificado en el Código Penal para el Estado de Tamaulipas en artículo 417 el delito de fraude, el cual menciona lo siguiente:

“ARTÍCULO 417.- *Comete el delito de fraude el que engañando a alguien o aprovechándose del error en que éste se halla, se haga ilícitamente de una cosa o alcance para sí o para otro un lucro indebido.*”¹³

Tipificando también en el artículo 420 al fraude laboral y en el artículo 421 Bis al fraude familiar, por lo que se considera de suma importancia añadir a nuestro Código Penal el delito de Fraude de comercio electrónico, para sí brindar una mayor seguridad a las personas y organizaciones en línea, incluyendo la protección de datos personales, financieros y de propiedad intelectual que son vulnerables en el ámbito digital, proporcionando respuestas legales eficaces, previniendo futuros delitos y promoviendo un entorno digital más seguro y confiable para todas y todos los tamaulipecos.

Por lo anteriormente expuesto y para tener una mejor apreciación de la iniciativa a presentar, se puede visualizar el siguiente cuadro comparativo:

Código Penal para el Estado de Tamaulipas (vigente)	Dip. Ana Laura Huerta Valdovinos (propuesta)
ARTÍCULO 418.- Las sanciones a que se refiere el Artículo 419 se aplicarán:	ARTÍCULO 418.- Las ...

¹³<https://www.congresotamaulipas.gob.mx/Parlamentario/Archivos/Codigos/Codigo%20Penal%20para%20el%20Estado%20de%20Tamaulipas%2012-feb-2025.pdf>



Ana Laura Huerta Valdovinos

Diputada Local

<p>I. a la XIX. ...</p> <p>SIN CORRELATIVO</p>	<p>I. a la XVIII;</p> <p>XIX Al que se coloque en estado de insolvencia, con el objeto de eludir las obligaciones a su cargo con respecto a sus acreedores; y</p> <p>XX. A quienes, por medio de plataformas digitales, tiendas en línea, o cualquier medio electrónico, engañen o inciten al error al consumidor, mediante la venta de productos o servicios falsos.</p> <p>Así como también a quienes, tras recibir un pago o depósito, no cumplan con la entrega del producto o servicio.</p>
<p>ARTÍCULO 419.- Al responsable ...</p> <p>I y II.- ...</p> <p>III.- ...</p> <p>SIN CORRELATIVO</p>	<p>ARTÍCULO 419.- Al responsable ...</p> <p>I y II.- ...</p> <p>III.- De seis a doce años de prisión y multa de ochenta a ciento cuarenta veces el valor diario de la Unidad de Medida y Actualización, cuando el valor de lo defraudado exceda de trescientas veces el valor diario de la Unidad de Medida y Actualización; y</p> <p>IV.- Al responsable de delito de fraude previsto en la fracción XX del</p>



Ana Laura Huerta Valdovinos

Diputada Local

	<p>artículo 418, se le impondrá sanción de seis meses a 3 años de prisión y de ciento cuarenta y cinco a cuatrocientas veces el valor diario de la Unidad de Medida y Actualización, de la Unidad de Medida y Actualización. Cuando el sujeto . . .</p>
--	--

Por lo anteriormente fundado y expuesto me permito someter a la consideración de este Honorable Congreso el siguiente:

PROYECTO DE DECRETO DE REFORMAS A LOS ARTÍCULOS 418, FRACCIÓN XIX; Y 419, FRACCIÓN III; Y SE ADICIONAN LAS FRACCIONES XX AL ARTÍCULO 418 Y IV AL ARTÍCULO 419, DEL CÓDIGO PENAL PARA EL ESTADO DE TAMAULIPAS

Artículo Único: Se reforman los artículos 418, fracción XIX; y 419, fracción III; y se adicionan las fracciones XX al artículo 418 y IV al artículo 419, del Código penal para el Estado de Tamaulipas, para quedar como sigue:

ARTÍCULO 418.- Las ...

I. a la XVIII;

XIX Al que se coloque en estado de insolvencia, con el objeto de eludir las obligaciones a su cargo con respecto a sus acreedores; y

XX. A quienes, por medio de plataformas digitales, tiendas en línea, o cualquier medio electrónico, engañen o inciten al error al consumidor, mediante la venta de productos o servicios falsos.



Ana Laura Huerta Valdovinos

Diputada Local

Así como también a quienes, tras recibir un pago o depósito, no cumplan con la entrega del producto o servicio.

ARTÍCULO 419. – Al responsable . . .

I y II.-

III.- De seis a doce años de prisión y multa de ochenta a ciento cuarenta veces el valor diario de la Unidad de Medida y Actualización, cuando el valor de lo defraudado exceda de trescientas veces el valor diario de la Unidad de Medida y Actualización; y

IV.- Al responsable de delito de fraude previsto en la fracción XX del artículo 418, se le impondrá sanción de seis meses a 3 años de prisión y de ciento cuarenta y cinco a cuatrocientas veces el valor diario de la Unidad de Medida y Actualización, de la Unidad de Medida y Actualización.

Cuando el sujeto . . .

Transitorios

ÚNICO. – El presente decreto entrará en vigor al día siguiente de su publicación en el Periódico oficial del Estado.



Ana Laura Huerta Valdovinos

Diputada Local

Dado en el Recinto Oficial del Congreso del Estado Libre y Soberano de
Tamaulipas, a los 04 días del mes de marzo del año 2025.

ATENTAMENTE

Ana Laura Huerta Valdovinos
DIP. ANA LAURA HUERTA VALDOVINOS