

El fraude informático en la legislación penal de Puebla, México. Estudio dogmático

POR XAVIER NÁJERA GONZÁLEZ (*)

Sumario: I. Introducción.- II. Bien jurídico penal.- III. Elementos del delito.- IV. La conducta típica y el resultado material.- V. Dolo directo, indirecto y eventual.- VI. Elemento subjetivo específico de índole volitivo distinto al dolo.- VII. Acción y omisión.- VIII. La tentativa.- IX. Punibilidad.- X. Conclusiones.- XI. Referencias.

Resumen: el trabajo analiza el delito de fraude informático tipificado como una modalidad del fraude específico de la legislación penal poblana. Se analiza el bien jurídico patrimonio y su relación mediata con la protección económica de índole colectiva. Se reflexiona sobre su forma de ejecución por acción y omisión impropia, tanto en su vertiente consumada como tentada, pero siempre de manera eminentemente dolosa, bajo el específico elemento subjetivo de obtención de lucro indebido, en beneficio propio o de un tercero. Se critica la punibilidad establecida apriorísticamente conforme al monto de lo defraudado, en lugar de acudir a una individualización de la pena basada en la peligrosidad de la conducta misma.

Palabras claves: fraude informático - estudio dogmático - estafa

Computer fraud in the criminal legislation of Puebla, Mexico. Dogmatic study

Abstract: *this paper analyses the crime of computer fraud, classified as a specific type of fraud in the Puebla criminal legislation. The legal asset, patrimony, and its mediate relationship with collective economic protection are analysed. It reflects on its form of execution by improper action and omission, both in its completed and attempted form, but always in an eminently malicious manner, under the specific subjective element of obtaining undue profit, for one's own benefit or that of a third party. The punishability established a priori according to the amount of the fraud is criticised, instead of resorting to an individualisation of the penalty based on the dangerousness of the conduct itself.*

Keywords: computer fraud - dogmatic study - scam

(*) Doctor en Derecho penal, procesal penal y Derechos humanos, Universidad de Salamanca, España. Maestro y Doctor en Derecho, Benemérita Universidad Autónoma de Puebla, México. Ex Secretario de Juzgado y de Tribunal en el Poder Judicial de la Federación. Catedrático de Derecho Penal y Criminología, Benemérita Universidad Autónoma de Puebla, México. Miembro del Sistema Nacional de Investigadoras e Investigadores del CONAHCYT (México), Nivel I. Abogado en ejercicio.

I. Introducción

El cibercrimen o delito informático es aquella conducta punible que se ejecuta a través de una computadora o que afecta el funcionamiento de los sistemas informáticos. Es un concepto que abarca tanto las conductas que son efectuadas *por medio* de los ordenadores, como aquéllas otras que tienen como *objeto material* un sistema de naturaleza informática (Suárez, 2006. p. 200).

Así, por ejemplo, mediante los denominados *spywares* o programas espía, el sujeto activo obtienen claves de acceso mediante el ingreso a un sistema operativo de la computadora del ofendido. Estas claves pueden ser obtenidas, ya sea de manera remota, o bien, mediante la instalación de estos archivos espías en el ordenador de la víctima. Por otra parte, con apoyo en los denominados *keyloggers* o registradores de teclas, que son programas que registran datos de lo que se digite en una determinada computadora por una víctima, el sujeto activo puede obtener claves de acceso que emplea la víctima (Giménez, 2023, p. 28), o cualquier otra información que puede luego utilizar con fines desleales o ilícitos.

A pesar de que la imaginación y el actuar criminal en materia cibernética puede ser inmenso, por razones estructurales, este trabajo sólo se centrará en el análisis del delito de fraude informático, según la legislación penal de Puebla, México. De esa manera, debe decirse que el delito de fraude informático se encuentra tipificado en el artículo 404, fracción IX, del Código Penal del Estado Libre y Soberano de Puebla, México, como una modalidad específica del fraude, que se sanciona según el monto del perjuicio patrimonial vulnerado, conforme a lo establecido en el diverso 403, fracciones I a IV, de igual ordenamiento sustantivo penal local.

Tales disposiciones legales establecen lo siguiente:

Artículo 404. Las mismas sanciones señaladas en el artículo anterior, se impondrán: **XIX.** Al que dolosamente y con el propósito de procurarse un lucro ilícito, para sí o para un tercero, dañe o perjudique el patrimonio de otro, mediante el uso indebido de mecanismos cibernéticos, que provoque o mantenga un error, sea manipulando datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos.

Artículo 403. El delito de fraude se sancionará: **I.** Con multa de cinco a cincuenta Unidades de Medida y Actualización y prisión de seis meses a tres años, si no se puede determinar el valor de lo defraudado o este valor no es superior a cien Unidades de Medida y Actualización. **II.** Con multa de cincuenta a doscientas cincuenta Unidades de Me-

dida y Actualización y prisión de tres a cinco años, si el valor de lo defraudado excediere de cien Unidades de Medida y Actualización, pero no de quinientas; **III.** Con multa de doscientos cincuenta a quinientas unidades de medida y actualización y prisión de cinco a siete años, cuando el valor de lo defraudado excediere de quinientas unidades de medida y actualización, pero no de mil; **IV.** Con multa de quinientas a mil unidades de medida y actualización y prisión de siete a diez años, cuando el valor de lo defraudado excediere de mil unidades de medida y actualización.

De la lectura de la exposición de motivos de la reforma que creó este tipo penal autónomo, publicada el lunes, 30 de diciembre de 2013, en la Trigésima Séptima Sección del Periódico Oficial del Estado de Puebla, México (1), se advierte que el legislador poblano tomó en cuenta que los fraudes por internet, robo de información, y otros delitos informáticos similares, causaron un detrimento patrimonial a nivel mundial superior a ciento diez mil millones de dólares, de los cuales, dos mil millones de dólares afectaron a México concretamente. Tales cifras, aunadas a que existen más de 1,800 millones de usuarios conectados a Internet, ha provocado que anualmente, aproximadamente 556 millones de personas de todo el mundo se vean afectadas por esta clase de delitos. Situación que arroja un detrimento patrimonial promedio de 197 dólares por víctima, derivado de estos delitos (Periódico Oficial, 2013, p. 4).

Así, antes estos elevados costos de afectación económica en el ámbito mundial, nacional e individual, el legislador penal poblano decidió tipificar el fraude informático, dentro de los delitos de fraude específico, que afectan al bien jurídico patrimonio de las personas.

En ese sentido, debe destacarse que, en términos generales, al fraude cibernético se le ha entendido como: “Todo aquel acto de engaño que se realice con la finalidad de obtener beneficios económicos indebidos en agravio de instituciones o personas usuarias del sistema financiero mediante el uso de las tecnologías de la información” (Medina, Velasco y Velázquez, 2021, p. 12).

Esta definición se inspira en el artículo 8° del “Convenio sobre la Ciberdelincuencia”, también conocido como Convenio de Budapest del Consejo de Europa (23 de noviembre de 2001) (2), “que establece la obligación de tipificar en el derecho interno a quien cometa actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante introducción, alteración, borrado o

(1) Ver en <https://legislacion.scjn.gob.mx/Buscador/Paginas/wfOrdenamientoDetalle.aspx?q=39x2p4n8t00y5p+GGKuZgtSWuSpf8KpjI5tfw5Ds5HwrK71rua+HhXhEbdmit0pp>

(2) Ver en https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

supresión de datos informáticos, y cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva, de obtener ilegítimamente un beneficio económico para uno mismo o para terceros” (Medina, Velasco y Velázquez, 2021, p. 12).

No obstante, cabe señalar que México aún no se adhiere a este convenio (Piña, 2019, p. 65), e incluso, ha mostrado poco interés por hacerlo (Centeno, 2018, p. 5), por razones centradas en diferentes exigencias normativas de este instrumento internacional, que aún están por cumplirse en cada estado de la República.

Esto resulta de suma importancia tenerlo en consideración, si se toma en consideración que además, el fraude informático casi siempre se dirige directamente contra los usuarios de la banca, mediante lo que se conoce como *phishing* y *pharming*, afectando con ello, de manera indirecta a los propios bancos (Cassou, 2009, p. 229). Aunque también, se han registrado ataques cibernéticos diversos, mediante otras técnicas fraudulentas conocidas como *malware*, *ransomware*, *suplantación o robo de identidad en la web*, *hackeo*, *espionaje corporativo*, *DDos o de denegación de servicio* (Rodríguez, 2023 p. 278-280).

En este sentido, resulta importante distinguir entre los términos “*phishing*” y “*pharming*”, como las dos principales herramientas que se utilizan para cometer fraude informático. Esto es así, pues en ambos casos, los delincuentes manipulan cibernéticamente programas, para servir de trampa para obtener los datos personales de las víctimas (Kaspersky, s.f., párrafos 15-23).

Sin embargo, en el “*phishing*” los delincuentes cibernéticos se valen de correos electrónicos, mensajes de texto o utilizan redes sociales, para enviar vínculos maliciosos que llevan a un sitio web falso, para que el usuario ingrese ahí su información personal verdadera, casi siempre relacionada con su nombre de usuario y contraseña. Una vez obtenidos tales datos, los utilizan para provocar quebrantos patrimoniales ilícitos (Kaspersky, s.f., párrafos 15-23).

En tanto que en el *pharming*, los delincuentes cibernéticos instalan un código malicioso en la computadora o servidor de la víctima. Posteriormente, este código automáticamente envía al usuario a un sitio web falso, donde los sujetos activos obtienen información personal que luego utilizan para obtener ganancias ilícitas. Es una técnica defraudatoria muy similar al *phishing*, pero sin señuelo, ya que funciona automáticamente (Kaspersky, s.f., párrafos 15-23).

Existen otras variantes similares al *phishing* y *pharming* como el *malware*, que consiste en utilizar un software que mediante correos electrónicos o ficheros adjuntos, provocan que, al ser abiertos por la víctima, se infecte su dispositivo electrónico con virus, troyanos, u otros similares, que permiten que el delincuente

sustraiga la información necesaria para defraudar, o suplantar la identidad de la víctima (Rodríguez, 2023, pp. 278-280).

Además, está el *ransomware* (traducido como “secuestro de datos”), que se vale de la misma dinámica comisiva, pero que tiene un propósito diferente más cercano a la extorsión, pues una vez que se logra infectar el equipo de la víctima, el delincuente se apodera del mismo en forma remota mediante un cifrado de datos del disco duro. Hecho lo anterior, el delincuente bloquea el acceso al dispositivo o a determinados archivos de forma que, si la víctima quiere recuperar los datos (*soft-ware*) debe de pagar un rescate (*ransom*) en forma económica. Y en algunos casos, además, en caso de no pagarse la suma exigida, existe la amenaza de filtrar a la red, documentos, fotos, o material sensible de la víctima (Rodríguez, 2023, pp. 278-280).

Aunado a ello, a través de los ataques DDos o de denegación de servicio, mediante diferentes herramientas se satura el acceso a una determinada página web, aplicación o servicio. Uno de ellos es el denominado *smurf* (pitufo), en el delincuente ubica la dirección IP de la víctima y deja inoperante su servidor, tras crear un paquete de datos falsificados que manda a todos los dispositivos conectados dentro de la misma organización para saturarla (Rodríguez, 2023, pp. 278-280). Luego, puede obtener alguna ganancia ilícita o simplemente causar ese daño.

De ahí la necesidad de prevenir tales conductas fraudulentas en forma adecuada, a través del uso del derecho penal. Y más aún, si se tiene en consideración que estos comportamientos antijurídicos dan pauta a formas de colaboración posterior a la consumación del hecho, por personas que se conocen como “money-mules” o “muleros”. En efecto, estos denominados “muleros”, son aquellos que, en fase posterior al hecho delictivo consumado de fraude informático, sirven como blanqueadores o lavadores de los montos defraudados en el territorio nacional. Esto es así, ya que posteriormente al hecho consumado de fraude en territorio nacional, hacen remesas al extranjero, mediante casas de cambio, paquetería postal y empresas de envíos de dineros, extrayendo el monto defraudado fuera de lugar de comisión del evento (Oxman, 2013, p. 218). Todo lo cual, hace que las consecuencias de este delito de fraude informático, pasen de cometerse en el ámbito meramente local, para tener repercusiones legales en el orden internacional; lo que dificulta su persecución y castigo.

Explicada que ha sido la mecánica comisiva y trascendencia de muchos fraudes informáticos, que incluso, pueden tener propósitos diversos cercanos a otros delitos, ahora es menester reflexionar cuál es el bien jurídico penal que se afecta por esta clase de delitos cibernéticos (Hernández, 2009, pp. 240-241), ya que algunos consideran que, además del bien jurídico individual de índole patrimonial, también se afectan bienes jurídicos colectivos como la integridad y el funcionamiento

ordenado de los sistemas informáticos (García y Pilco, 2024, p. 53). Es por ello, que resulta necesario analizar el concreto bien jurídico protegido por este delito de fraude informático, que de *lege lata* se contempla en la legislación sustantiva penal poblana. Lo que resulta de particular interés, si se toma en cuenta que México es el décimo país a nivel mundial más atacado cibernéticamente (Albarrán, 2021, p. 95).

II. Bien jurídico penal

El tipo penal de fraude informático se encuentra descrito dentro del elenco de delitos que se enumeran bajo el “*Capítulo decimoctavo*”, intitulado “*Delitos contra las personas en su patrimonio*”, sección cuarta denominada “*Fraude*”. Esta situación nos conduce a determinar que el patrimonio es el bien jurídico penalmente protegido (3).

Por patrimonio —en su quinta acepción referida al derecho, según la Real Academia de la Lengua Española— debe entenderse: “El conjunto de bienes pertenecientes a una persona natural o jurídica, o afectos a un fin, susceptibles de estimación económica” (RAE, 2001).

Tradicionalmente se ha entendido que el *patrimonio* de una persona se conforma con un conjunto de bienes, derechos reales, derechos personales, obligaciones reales, obligaciones personales, y cargas susceptibles de valoración pecuniaria. Y en este sentido, también se estima que los derechos de la persona o de la personalidad, son extrapatrimoniales (Herrera, 2014, p. 69).

En materia penal, la protección del patrimonio afecta diferentes derechos que lo integran como: la posesión, la propiedad y el derecho de crédito. Por ello, existen ocasiones en que la lesión de alguno de estos elementos patrimoniales, no implica necesariamente la disminución del activo de una persona (Azzolini, 2013, p. 193). Sin embargo, la tutela penal surge porque la afectación de alguno de estos elementos patrimoniales, vulnera la integridad misma del patrimonio en su conjunto; cosa que el Estado no debe permitir en forma alguna respecto de quien resulte ser su titular.

Incluso, desde una perspectiva más novedosa, se sostiene que el patrimonio representa una entidad personalmente estructurada que sirve para el desarrollo económico de una persona (Navarrete, 2023, p. 38). Este concepto vincula la protección patrimonial con la posibilidad de desarrollo económico, por tanto, puede

(3) Es importante señalar que, para prevenir diversos delitos informáticos, en Puebla, México, funciona la Policía Cibernética. Tal institución cuenta con una página electrónica que brinda información básica para la ciudadanía. <https://planeader.puebla.gob.mx/documentos/capacitacion-municipal/1erSemestre2024/Material.%20Viernes%2012%20de%20abril/6.%20Polic%C3%ADa%20Cibernetica>

establecerse que el patrimonio, como bien jurídico individual, contribuye a la protección de la economía personal, sin la cual, la economía en general, como bien jurídico colectivo, tampoco puede desarrollarse en plenitud. Lo que resulta imprescindible para el desarrollo de los derechos humanos de segunda generación, que son imprescindibles en un estado social y democrático de derecho.

Aquí, coincido con quien estima que “Hay varios factores que conducen a la incorporación de bienes jurídicos colectivos a la protección del Derecho penal, el más determinante es la propia evolución del modelo de Estado, que trae consigo el reconocimiento constitucional de los denominados derechos humanos de segunda generación, que están unidos al Estado social de Derecho” (Berdugo, 2024, p. 25).

En ese sentido, la doctrina alemana de la llamada teoría económica del patrimonio (*wirtschaftliche Vermögenstheorie*), converge incluso, con la idea de que la totalidad de los bienes pertenecientes a una persona es su patrimonio, sin que sea relevante el que dichos bienes le pertenezcan conforme a derecho o tengan reconocimiento jurídico (Schlack, 2008, p. 269).

Dicho lo anterior, es conveniente analizar esa vinculación entre la lesión patrimonial-económica, y la conducta típicamente protegida.

III. Elementos del delito

Los elementos del delito de fraude informático en Puebla, esquemáticamente pueden desglosarse de la siguiente manera:

a) Hacer uso de mecanismos cibernéticos (*conducta típica*), que provoque o mantenga un error, sea manipulando datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos (*medios comisivos alternativos*).

b) Que la realización de alguna de tales conductas tenga como consecuencia el daño o perjuicio del patrimonio de otro (resultado típico).

c) Ejecutar la acción típica en forma dolosa (dolo directo, indirecto y eventual), y con el propósito de procurarse un lucro ilícito, para sí o para un tercero (elemento subjetivo específico distinto al dolo).

Cada uno de tales elementos típicos deben acreditarse mediante el uso de pruebas idóneas para tal fin. Y, hecho lo anterior, corresponderá al juez determinar en el caso concreto, si esto aconteció o no; por supuesto, con base en la versión de los hechos que le dieron las partes. Lo anterior resulta ser así, pues, la prueba en el sistema penal acusatorio busca transmitir información al juzgador, pero sobre todo, influir en forma persuasiva y cognoscitiva en su ánimo. Situación que implica que el sujeto procesal no busca llegar a la verdad material del evento

delictuoso, sino sólo convencer al juez sobre su versión de los hechos. Lo que, por tanto, pone en duda que, con el desahogo del proceso, verdaderamente se busque el esclarecimiento de los hechos (Zeferín, 2016, p.18).

Precisado lo anterior, lo primero que se debe demostrar para acreditar con pruebas idóneas el delito de fraude informático en Puebla, México, es demostrar que la conducta típica consistente en *hacer uso indebido de mecanismos cibernéticos*, que es el núcleo del delito, precisamente, fue a través de un uso indebido. Para ello, es menester probar que el sujeto activo materializó tal comportamiento antijurídico logrando provocar con ello un error o mantener ese error en la información contenida en el ese equipo computacional, a través de alguno de los tres siguientes medios comisivos alternativos (4): a) *sea manipulando datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral*; b) *sea presentando como ciertos hechos que no lo son*; o c) *deformando o disimulando hechos verdaderos*.

Como dice (Mayer y Oliver, 2020, p. 153): “si por hacking entendemos el acceso indebido a datos o programas de sistemas informáticos, podrá advertirse que para cometer un fraude informático resultará necesario acceder (en forma indebida) a los datos o programas referidos”.

Logrado que haya sido esto, que equivale a demostrar la *causa* de este hecho delictuoso, debe acreditarse la consecuencia, que consiste en que esta causa sea *idónea o suficientemente apta* para la producción del *resultado típico*, consistente en *dañar o perjudicar el patrimonio de otro*. Esto es sumamente importante, porque a través de ese daño o perjuicio causado por la conducta típicamente antijurídica, se lesiona al bien jurídico *patrimonio* que se protege legalmente. Mientras esto no se logre, estaremos en el ámbito de la tentativa, como una forma imperfecta de la ejecución del hecho.

Así, por ejemplo, un sujeto activo a través del *phishing* o del *pharming* (Aguilar, 2011, pp. 126-140), puede hacer uso indebido del sistema cibernético, bien sea, **a) manipulando datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral**; **b) sea presentando como ciertos hechos que no lo son**; o **c) deformando o disimulando hechos verdaderos**.

De ahí que el *phishing* o el *pharming*, como técnicas defraudatorias, sirven como medios comisivos para atacar al bien jurídico patrimonio del sujeto pasivo, que aquí son tipificados en forma autónoma, y que se castigan en forma de

(4) En ese sentido, coincido con la postura que señala que “los medios comisivos del delito constituyen un grupo específico de conductas ejecutivas que, perteneciendo a la categoría del tipo, están dotadas de singularidad propia” (De la Herrán, 2024, p. 29).

tentativa si sólo se pone en peligro al patrimonio, o como delito consumado de fraude, si efectivamente se logra el daño de dicho bien jurídico.

A pesar de lo aquí indicado, cabe señalar que el uso indebido de los sistemas informáticos, puede dar paso a otra clase de delitos que no sólo tengan como propósito una afectación patrimonial propiamente dicha. Esto es así, pues tal como señala (Acurio, 2015, pp. 10-11), la manipulación indebida de sistemas cibernéticos, puede ser efectuada con otros fines delictivos diversos, ya que tales atentados pueden recaer sobre hospitales, aeropuertos, parlamentos, sistemas de seguridad, sistemas de administración de justicia, entre otros. De ahí la peligrosidad de tal clase de conductas que, a través del uso indebido de sistemas informáticos, afecten a otros bienes jurídicos diversos, e incluso, en algunos casos, puedan dar ocasión a la perpetración de actos de ciberterrorismo (Sánchez, 2012, p. 74).

Asimismo, el verbo típico materializado en el *uso indebido de mecanismos cibernéticos*, a través de alguno de los medios comisivos que describe el tipo como: *manipulación de datos o falseamiento, deformación o simulación de hechos* (es decir, lo que computacionalmente se conoce como *pharming* o *phishing*, u otros similares), debe ser realizado en forma dolosa, lo que automáticamente excluye la punición de la modalidad imprudente de este delito.

Delito que además, exige que en el ánimo del sujeto activo, se aprecie la existencia de un *elemento subjetivo específico de índole volitivo distinto al dolo*, consistente en tener el *propósito de procurarse un lucro ilícito, para sí o para un tercero*.

Cabe señalar que el sujeto activo de tales delitos, se conoce en el mundo computacional como *cracker*, que se define como aquella persona que “ostenta una finalidad maliciosa, es decir, pernicioso para los intereses de la víctima, sea persona natural o jurídica, lo cual puede derivar en un perjuicio patrimonial, de su honor o buena reputación e incluso afectar su intimidad, dependiendo mucho del acto ilícito que realice”. En tanto que el término *hacker*, más bien, se refiere a aquella persona que busca usar sus conocimientos para fines nobles, como son, superar obstáculos en el mundo de la informática, pero, sin pretender cometer delitos en el ciberespacio (Ávila, 2024, p. 161).

IV. La conducta típica y el resultado material

El uso indebido de mecanismos cibernéticos como verbo nuclear típico del fraude informático en Puebla, obliga a realizar un análisis gramatical del sentido de esas palabras para su mejor entendimiento.

Usar gramaticalmente es definido por la Real Academia de la Lengua Española, como *hacer servir una cosa para algo*. Esto implica entender que el sujeto activo debe servirse de los mecanismos cibernéticos, pero para que dicho uso informático

sea típico, es uso debe ser *indebido*. Esto implica demostrar que la utilización de tales medios debe realizarse fuera de los rangos o parámetros legalmente establecidos.

Ilícitud que deriva de entender que lo *indebido* de dicha utilización, tiene que ver con la *provocación o mantenimiento de un error*, que propiamente debe entenderse como *una alteración que se realiza en la información que se resguarda en el propio mecanismo cibernético*, con lo que se logra el daño o menoscabo patrimonial del sujeto pasivo, propio de esta modalidad específica del fraude. En este sentido, el sujeto activo falsamente hace aparecer un error en la información contenida en el mecanismo computacional que deriva en el daño patrimonial aludido.

En efecto, dicho error provocado o mantenido por el uso indebido de mecanismos cibernéticos, debe ser la consecuencia de la realización de alguno de los medios comisivos antes descritos.

Por tanto —en el primer caso—, el *error que se provocó o se propició mantener a través del uso indebido de mecanismos cibernéticos*, debe ser consecuencia de *una manipulación de datos de entrada a un equipo de informática*, y dicha manipulación puede tener dos objetivos, *producir movimientos falsos* —lo que implica que dichos movimientos no eran existentes en forma previa a su manipulación, y gracias al actuar del sujeto activo estos son creados o producidos en forma falsa—; o bien, *lograr movimientos falsos* —lo que implica que ya existían movimientos reales y verdaderos, pero debido al actuar del sujeto activo, se logró que estos fueran falseados—, todo lo cual debe referirse precisamente, a las *transacciones de una persona física o moral*. De tal manera que en este primer supuesto, el sujeto activo manipula datos de entrada a un equipo informático, para falsear las transacciones patrimoniales de un sujeto pasivo.

En el segundo caso, el *error que se provocó o se propició mantener* mediante el *uso indebido de medios cibernéticos* es debido a que se *presentan como ciertos hechos que no lo son*. Certeza que se demostrará en juicio, mediante pruebas de las que se constata que, efectivamente, los hechos que fueron manipulados por el sujeto activo no eran los verdaderos, dada su franca y abierta contradicción con los que a todas luces resultaron verdaderos. En ese sentido, si esto no logra ser demostrado plenamente, aplica el principio de que, en caso de duda, se le debe absolver.

En el tercer caso, el *error que se provocó o se propició mantener* mediante el *uso indebido de medios cibernéticos*, es debido a que se *deforman o disimulan hechos verdaderos*. Esto se traduce en que el sujeto activo hace que algo verdadero pierda su forma, porque la tergiversa, la oculta, o la finge de algún modo.

En un sentido clásico, según (Manero, 1995, pp. 46-47), todo esto puede ser llevado a cabo a través de diversas técnicas conocidas en habla inglesa como: *data*

diddling (5), *trojanhorse* (6), *roundingdown* (7), *scavenging* (8), *superzapping* (9), *logicbomb* (10), *trapdoors* (11), *data leakage* (12), *piggybacking* (13), *wiretap* (14), y *simulation and modeling* (15).

(5) Introducción de datos falsos: Es el más común y sencillo de los métodos empleados para defraudar cibernéticamente, y consiste en manipular las transacciones de entrada para introducir movimientos falsos o eliminar transacciones que se deberían haberse introducido.

(6) Caballo de Troya: Consiste en introducir en un programa un conjunto de instrucciones o rutina no autorizada para que este programa actúe de una forma distinta a la prevista en determinados casos. Un ejemplo de esta técnica sería realizar un cálculo erróneo de una nómina aumentando el importe.

(7) Salami: Consiste en la manipulación de un gran número de pequeños importes. Situación que se equipara al salami, porque el fraude se realiza en pequeños cortes. Como ejemplo de esta técnica defraudatoria, piénsese en una entidad bancaria en que se añaden unas líneas adicionales de código en un programa de cálculo de intereses con el objetivo de redondearlos, desviándose de esta forma la cifra redondeada, a una cuenta controlada por el sujeto activo del fraude.

(8) Recogida de información desechada: Cuando se desecha información en la papelera por contener errores o ser obsoleta, pero con datos confidenciales de interés para otros. El fraude consiste en recoger estos datos confidenciales y venderlos a otras empresas competidoras, o gente que puede hacer mal uso de los mismos. En la práctica internacional, ha sido problemático demostrar la propiedad de estos datos, sobre todo, porque provienen de un desechamiento efectuado por el propio usuario.

(9) Esta técnica defraudatoria hace referencia a utilidades que permiten modificar archivos y bases de datos sin acceder a ellos por el programa que los gestiona. El peligro surge cuando estas utilidades están al alcance del público ajeno y derivado de una utilización no controlada. Como ejemplo se cita la alteración del saldo de una cuenta modificando este dato directamente en el archivo donde se encuentra.

(10) Bomba lógica: Esta técnica consiste en establecer una rutina no autorizada sobre un programa que posteriormente produce consecuencias destructivas en una fecha, tiempo o evento predeterminados. Como ejemplo, el empleado despedido que coloca una de estas rutinas para que se ejecute posteriormente, con el objetivo de producir daños en la información, o incluso, pérdida patrimonial para la empresa, con independencia que de ello obtenga un lucro o no.

(11) Puertas falsas: La utilización indebida de los puntos de control (puertas falsas) dejados en un programa determinado, por un programador, que en principio sólo los usa para comprobar que los resultados intermedios han sido correctos. Pero que, - casi siempre por olvido -, no fueron eliminados al finalizar la programación de dicha aplicación. Así, el hecho de haber dejado puertas de entrada no documentadas en las aplicaciones durante su normal ejecución, que no están documentadas, y que, por ende, tampoco forman parte de las especificaciones del programa establecido, es aprovechado por el sujeto activo para su utilización con fines defraudatorios.

(12) Fuga de información: Tiene que ver con la divulgación no autorizada de datos reservados. Muchas veces tiene que ver con el famoso espionaje industrial. Dicha sustracción de información confidencial es uno de los principales peligros que corren los sistemas informáticos en general. Y, es muy común, pues normalmente, es muy sencillo realizar una copia de un fichero con datos privados, por quien tenga acceso a los mismos.

(13) Acceso no autorizado: Consiste en acceder a áreas restringidas, ya sean físicas (salas de ordenadores), o bien, dentro del ordenador mismo (dispositivos, discos, etc.).

(14) Pinchazo de líneas: Se trata del irrumpir en cualquier clase de líneas de comunicación, ya sean telefónicas, cibernéticas o de datos.

(15) Simular y moldear: Consiste en utilizar un equipo de cómputo para simular y moldear un delito. Por ejemplo, realizar asientos contables falsos a través de la utilización de una copia de la contabilidad de la empresa.

Demostrado que ha sido alguna de tales medios comisivos alternativos de la conducta típica, restará comprobar procesalmente, que el error que se provocó o que se mantuvo en los datos del propio mecanismo cibernético alterado, tuvieron como consecuencia directa o indirecta el menoscabo patrimonial del sujeto pasivo, con la consecuente lesión en el hecho consumado, o puesta en peligro en el caso de la tentativa, del bien jurídico protegido.

Cabe señalar que el verbo rector *uso indebido de mecanismos cibernéticos*, directamente referido a los medios comisivos alternativos, referidos a que *se provoque o mantenga un error, sea manipulando datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos*, fueron diseñados en este fraude específico, para evitar caer en la falacia de engañar a la máquina misma. Pues con ello, se deja a salvo el añejo criterio de que las máquinas no pueden ser engañadas en virtud de carecer de juicio y de criterio de decisión al limitarse a ejecutar las conductas para las que fueron preprogramadas (Gómez, s/a, pp. 15-16). Situación por la cual, resulta más adecuado hablar de manipulación, pues de ello, sí pueden ser objetos los mecanismos cibernéticos de los que en este delito en particular, hace uso indebido el sujeto activo.

V. Dolo directo, indirecto y eventual

El tipo penal expresamente exige que el comportamiento sea doloso. Por tanto, se excluye en automático la modalidad imprudente. Esto es indicativo que el legislador poblano quiso abarcar las diversas modalidades de dolo directo, dolo indirecto, y dolo eventual.

Si atendemos a la redacción actual del Código Penal poblano, se advierte que estas tres clases de dolo están comprendidas en la descripción de este elemento típico realizada por el artículo 13 de dicho cuerpo normativo, que dispone:

Artículo 13. La conducta es dolosa, si se ejecutó con intención y coincide con los elementos del tipo penal o se previó como posible el resultado típico y se quiso o aceptó la realización del hecho descrito por la Ley.

Lo anterior resulta ser así, pues de la lectura de dicho numeral, se puede advertir que hay **dolo directo**, cuando el sujeto tiene plena *intención* de realizar *los elementos del tipo penal (dolo directo)*. Intención dolosa, que presupone, un conocimiento previo del hecho que se va a realizar por el sujeto activo, quien además, tiene plena voluntad (*intención*) de llevar a cabo.

Por su parte, también se contiene al **dolo indirecto**, al disponer dicho numeral, que *la conducta es dolosa, si se previó como posible el resultado típico* (esto implica que el sujeto activo tiene un conocimiento probable o incierto del hecho por realizar), pero a pesar de ello, de todos modos, el sujeto activo **quiere realizar el hecho típico** (dolo indirecto).

Y, finalmente, también dicho precepto 13 de la legislación punitiva poblana, contiene al **dolo eventual**, al disponer que el sujeto activo prevé *como posible el resultado típico* (es decir, sólo alberga la posibilidad de lograrlo), pero, a pesar de ello, continúa en su propósito criminal, y **acepta** (dolo indirecto) la realización del hecho delictivo descrito por la ley (lo que abarca sus *consecuencias necesarias o inherentes*).

No obstante, Hassemer califica de “fossilizadas” las consideraciones del dolo como algo relativo al mundo cognoscitivo y volitivo, prefiriendo determinaciones sustentadas en expresiones como “decisión a favor de la lesión del bien jurídico”, “decisión contra el bien jurídico”, “punto de vista estrictamente personal”, “negación de una situación protegida por la norma penal”, “asunción de circunstancias del hecho constitutivas del injusto” (Hassemer 1990, p. 916).

Dicho lo anterior, al contemplarse tales hipótesis dolosas en la ley penal poblana, habrá fraude informático con dolo directo, cuando se demuestre que el sujeto activo *hizo uso indebido de mecanismos cibernéticos (conducta típica)*, con la intención de provocar un resultado patrimonial lesivo en un sujeto pasivo (ofendido), y con plena voluntad de provocar o mantener un error en la información ahí contenida. Aunado a ello, debe comprobarse que dicho sujeto activo *conoció y tuvo intención* de manipular datos de entrada al propio equipo informático, de tal manera que con dicha manipulación se produjeran o se crearan movimientos falsos en transacciones del sujeto pasivo; o bien, que el sujeto activo efectúa tal manipulación informática con el conocimiento y voluntad (*intención*) de presentar como ciertos hechos que no lo son; o bien, que el sujeto activo manipula tal información con *conocimiento e intención* de deformar o disimular hechos verdaderos. Todo ello, además, demostrándose que el sujeto activo tuvo la firme intención de *dañar o perjudicar el patrimonio de otro*. Es decir, debe demostrarse fehacientemente que el sujeto activo la plena *intención* de vulnerar el bien jurídico patrimonio que se tutela por este tipo especial de fraude (16).

El error de tipo vencible o invencible (Moya, 2014, p. 14), sobre cualquiera de tales elementos, excluirá o atenuará, en su caso, el actuar doloso del sujeto activo

(16) Es importante tener en cuenta que, en términos generales, el dolo y la culpa se sustentan en factores subjetivos. Así, el dolo se sustenta en el querer, en tanto la culpa en la previsibilidad; sin embargo, dichas concepciones han venido cediendo paso a una concepción de índole más normativa (Díaz-Aranda, 2007, p. 577).

(Chirino *et. al.*, 1992, p. 29). Lo que ocurrirá, si se advierte que el sujeto activo tuvo la viciada voluntad de cometer la conducta típica antes descrita (uso indebido de mecanismos cibernéticos), debido a un error invencible sobre alguno de tales medios comisivos, que, por ende, vician, además, la voluntad de causar el daño patrimonial ilícito. En este caso, se deberá demostrar que el error recayó sobre la *manipulación de datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos.*

En lo que atañe al *dolo indirecto*, referido a la hipótesis de que la conducta es dolosa, **si se previó como posible el resultado típico y se quiso la realización del hecho descrito por la Ley.**

En el caso concreto, para que este dolo indirecto o, de segundo grado, se actualice, en el fraude informático que nos ocupa, es menester que se demuestre mediante pruebas idóneas, que el sujeto activo **previo como posible** el daño o menoscabo patrimonial de un sujeto pasivo (*resultado típico*) —aunque no haya tenido la firme intencionalidad de realizarlo a plenitud—, pero, a pesar de ello, *quiso* además, hacer uso defraudatorio de los mecanismos informáticos que tenía a su alcance, de alguna de las maneras antes detalladas, es decir, con *voluntad (intención)* de *manipular datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos.*

En lo que atañe al *dolo eventual*, que se actualiza cuando el sujeto activo **previó como posible el resultado típico y aceptó la realización del hecho descrito por la Ley.**

En este caso, el sujeto activo sólo **prevé** el resultado típico lesivo del patrimonio (pues, no tiene la certeza de que éste ocurrirá), sin embargo, continúa encaminando su actuar aceptando las consecuencia inherentes al hecho delictuoso, como serían la *manipulación de datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos.*

Tanto en el dolo directo, como en el dolo indirecto y el dolo eventual, el sujeto activo tiene la voluntad de realización del uso indebido de mecanismos cibernéticos en perjuicio patrimonial de alguien. Lo único que varía es que en el dolo directo el conocimiento y la intención de realización del hecho es plena. Por su parte, en los otros dos dolos, el sujeto activo no tiene certeza que logrará el resultado típico, sin embargo, quiere realizarlo (dolo indirecto) o bien, acepta realizarlo

(dolo eventual), lo logre o no. Son tres grados de decisión a favor del tipo de injusto (Hassemer, 1990, p. 931), que deben demostrarse en el caso concreto, pues de ellos dependerá el nivel de mayor rigor o menor rigor de punición que éstos puedan alcanzar.

VI. Elemento subjetivo específico de índole volitivo distinto al dolo

En todos esos casos, además, debe demostrarse que, en el comportamiento típico del sujeto activo, consistente en el uso indebido de mecanismos cibernéticos, tuvo como propósito específico *procurarse un lucro ilícito, para sí o para un tercero*. Este último elemento constituye un elemento subjetivo específico de índole volitivo, que debe entenderse como “un determinado ánimo o intención que ha de guiar la actuación del sujeto activo en el momento de realizar una conducta penalmente típica” (Martínez-Bujan, 2013, p. 234). Por tanto, no debe ser abarcado por el dolo, y debe demostrarse en el caso concreto, en forma independiente a éste. Esto es así, pues al igual que el dolo, este elemento subjetivo específico *ánimo de procurarse un lucro ilícito, para sí o para un tercero*, también forma parte del tipo subjetivo, y debe referirse a los elementos que integran el tipo de objetivo (Martínez-Bujan, 2013, p. 240).

Sin embargo, ya este malintencionado propósito u ánimo que impregna el comportamiento delictivo, debe advertirse desde el momento en que se realiza el uso indebido de los mecanismos cibernéticos, aunque dicho lucro no llegue a materializarse en perjuicio de nadie. Por tanto, no basta que en el caso concreto se demostrara que se actuó dolosamente al momento de usar tales mecanismos informáticos, pues, además, es menester demostrar que el sujeto activo tenía la firme intención de lograr un lucro ilegal con todo ello, aunque éste no llegase a concretarse en ningún momento (Herzberg, 2008, p. 12) (17). Pues caso contrario, nos enfrentaríamos a una forma de atipicidad de la conducta.

Así la acción típica de *usar indebidamente mecanismos cibernéticos*, debe ir revestida de ese específico propósito de *procurarse un lucro*, que además, debe ser *ilícito*, sin importar en el caso concreto que sea obtenido para beneficio propio o de una tercera persona. Y, en este sentido, por lucro, debe entenderse según la definición de la Real Academia de la Lengua, “la ganancia o provecho que se saca de algo”. Por tanto, es menester demostrar en el caso concreto, a través de pruebas idóneas (18), que el sujeto activo con el específico propósito de obtener una ganancia o provecho de la misma, aunque ésta no llegara a concretarse, pues el

(17) Pues, como dice Herzberg, cualquiera que sea el diccionario que se consulte, actuar “dolosamente” equivale a actuar “intencionadamente”.

(18) La idoneidad o conducencia de la prueba tiene que ver con la idea de que la prueba deberá ser apta para probar determinado hecho (Vázquez y Fernández, 2022, p. 156).

tipo penal no nos exige que se obtenga en forma efectiva, sino sólo que se tenga la intención de obtenerla en el caso concreto.

Aquí, al igual que acontece con el juicio de imputación dolosa, es importante tener en cuenta el propio juzgamiento que hace el sujeto activo de su conocimiento acerca de hechos, las propias capacidades físicas y las conexiones nomológicas. Todo ello, bajo un criterio objetivo sustentado en el uso defectuoso que hace el autor de su propia capacidad individual de acción; situación toda ella, que justificaría sobradamente, la imposición de una pena en su contra. (Kindhäuser, 2008, p. 18)

Esto nos lleva a su vez, a la reflexión, que, en el caso concreto, haya sido factible obtener dicha ganancia o provecho, pues, si se llegara a demostrar que la obtención de un lucro ilícito era algo imposible de efectuar (verbigracia, la cuenta crackeada estaba vacía), esto podría tener como consecuencia la atipicidad de la conducta. Esto es así, pues, a pesar de que el móvil ambicioso del sujeto activo, traducido en *el propósito de procurarse un lucro ilícito, para sí o para un tercero*, fuera totalmente comprobable, sin en el caso específico, la obtención del lucro estuviera totalmente fuera de su alcance, faltaría la idoneidad de la meta antijurídica planteada por el agente del delito.

Tan es así, que dicho propósito se ve complementado con el hecho de que el tipo penal, describe a continuación la concreta exigencia de *dañar o perjudicar el patrimonio de otro*. Situación que denota que si en el caso concreto, no se advierte un daño o perjuicio patrimonial, que le era factible obtener al sujeto activo, entonces, no se podría actualizar la acreditación del elemento subjetivo específico distinto al dolo que aquí nos ocupa comentar. Finalmente, cabe hacer énfasis que, si el ánimo del sujeto activo fuera la obtención de un lucro, que no fuera ilícito, carecería de sentido hablar de tipicidad de la conducta, y por ende, también de antijuricidad de la misma. Y, por ello, tampoco podría hablarse de ningún daño o perjuicio en el patrimonio de otro.

VII. Acción y omisión

El fraude informático es una conducta típica dolosa, que puede ser realizada por acción o en comisión por omisión (al tratarse de un delito de resultado material). De ahí que no sea posible hablar de omisión pura o simple en ningún caso.

En este sentido, resulta aplicable lo dispuesto por el artículo 23 del Código Penal para el Estado Libre y Soberano de Puebla, México, dispone:

Artículo 23. En los delitos de resultado material será atribuible el resultado típico producido a quien omita impedirlo, si éste tenía el deber jurídico de evitarlo, si:

I.- Es garante del bien jurídico:

II.- De acuerdo con las circunstancias podía evitarlo; o

III.- Su inactividad es, en su eficacia, equivalente a la actividad prohibida en el tipo. Para efectos de este artículo, se entiende por garante del bien jurídico quien:

a) Aceptó efectivamente su custodia;

b) Voluntariamente forma parte de una comunidad que afronta peligros de la naturaleza;

c) Con una actividad precedente, culposa o fortuita, generó el peligro para el bien jurídico; o

d) Se halla en una efectiva y concreta posición de custodia de la vida, la salud o integridad corporal de algún miembro de su familia o de su pupilo.

No perderá la calidad de garante el que se comportó de manera culposa o negligente respecto al bien jurídico.

Dicho lo anterior, en el caso concreto, se deberá demostrar que el sujeto activo que a título de comisión por omisión, dolosamente (en forma de dolo directo, indirecto o eventual) y con el propósito de procurarse un lucro ilícito, para sí o para un tercero, *deja que otro haga uso indebido de su mecanismo cibernético, que provoque o mantenga un error, sea manipulando datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos.*

En este caso, el sujeto activo le será atribuible el resultado típico que se produjo en perjuicio del patrimonio ajeno, *por haber omitido impedirlo*; siempre que se demuestre en el caso concreto, que dicho sujeto activo *tenía el deber jurídico de evitar dicho resultado* lesivo del patrimonio de otra persona.

Téngase en consideración que respecto de la injerencia como factor condicionante de la comisión por omisión “es relevante la actividad precedente en cuanto antecedente que constituye en garante, pero lo típicamente relevante es la omisión de la acción esperada, en otras palabras, la acción omitida que hubiera evitado el resultado” (Izquierdo, 2006, p. 335).

Para lo cual, será menester demostrar que el sujeto activo omiso es garante del patrimonio ajeno afectado, porque *en forma previa o concomitante al hecho típico,*

había aceptado efectivamente su custodia; o, bien, que dada su específica condición con relación al patrimonio afectado, puede demostrarse objetivamente que éste había voluntariamente aceptado afrontar peligros cibernéticos, por ejemplo, por ser empleado de aquél que con el uso de su mecanismo cibernético fue afectado en su patrimonio; lo que habría hecho suponer, que no tendría por qué permitir que otro afectara el patrimonio que custodiaba de su patrón, con el uso de tales equipos, que permitió a otro utilizar en forma dolosa, y con ánimo de obtención de lucro, para sí o para un tercero.

Y, en todos los casos anteriores, claro está, siempre que se demuestre que de acuerdo con las circunstancias particulares y específicas del caso concreto, dicho sujeto activo podía evitar haber incurrido en la comisión por omisión que realizó; y que por ello mismo, su inactividad fue eficaz, equivalente a la actividad prohibida en el tipo que nos ocupa.

A manera de aclaración, cabe señalar que:

- En este delito de fraude informático, automáticamente, se descartaría la hipótesis de considerar garante a título de comisión por omisión, a aquel sujeto activo que permitiera mediante su inactividad el uso indebido de mecanismos cibernéticos por otro sujeto, con motivo de una actividad precedente, culposa o fortuita, que generara el peligro para el bien jurídico patrimonio, porque el tipo penal expresamente exige la comisión dolosa de este delito.

- Y lo mismo acontecería, con la hipótesis de calidad de garante, referida a que el sujeto activo que con su inactividad, se hallara en una efectiva y concreta posición de custodia de la vida, la salud o integridad corporal de algún miembro de su familia o de su pupilo; porque en el delito que nos ocupa, el bien jurídico es el patrimonio.

- Tampoco sería aplicable la hipótesis de calidad de garante, referida a que el sujeto activo no perderá la calidad de garante si se comportara de manera culposa o negligente respecto al bien jurídico; porque por disposición expresa del propio tipo penal, sólo se admite la comisión dolosa del fraude informático que nos ocupa.

VIII. La tentativa

Por esto mismo, es un delito que admite la tentativa acabada e inacabada, y dependiendo la mayor o menor proximidad en el ataque al bien jurídico patrimonio, la tentativa podría ser idónea e inidónea.

Sin embargo, esta última, que propiamente hace referencia a un delito imposible, muestra su inidoneidad en *el objeto, en los medios, o en el sujeto*. Por ello, se

considera incapaz *ex ante* (desde un primer momento), para lograr la consumación, que por supuesto, tampoco se logra *ex post* (Ovalle, 2003, p. 26).

El artículo 20 del Código Penal del Estado Libre y Soberano de Puebla, México, define a la tentativa de la siguiente manera:

Artículo 20. Existe tentativa, cuando usando medios eficaces e idóneos, se ejecutan o exteriorizan total o parcialmente actos encaminados directa o inmediatamente a la realización de un delito, o se omiten los que deberían evitarlo, si no se consuma por causas ajenas a la voluntad del agente. Si el sujeto activo desiste espontáneamente de la ejecución o impide la consumación del delito, no se le impondrá pena alguna por lo que a este se refiere.

De la lectura de dicho numeral, se advierte que el ordenamiento sustantivo penal local, admite la *tentativa acabada e inacabada*, al hablar de usar *medios eficaces*, a través del *ejecutar o exteriorizar total o parcialmente actos* encaminados a la realización del delito (tentativa por acción), o bien, omitir los que deberían evitarlo (tentativa en comisión por omisión), en ambos casos, si no se consuma el resultado típico por causas ajenas a la voluntad del agente del delito.

En este sentido, coincido con el criterio de que una tentativa es acabada, cuando el autor ha aprovechado *exhaustivamente* la oportunidad de realizar un comportamiento que, desde su concreta apreciación de sus circunstancias, tendría que haber concretado eficazmente la realización antijurídica del tipo en cuestión, a pesar de no haberlo logrado consumir, por causas externas a su voluntad. Por el contrario, si no se ha aprovechado *exhaustivamente* tal oportunidad delictiva, se estará ante una tentativa inacabada. (Mañalich, 2022, pp. 29-30)

Y también hace referencia a lo que dogmáticamente se conoce como tentativa idónea e inidónea, cuando hace referencia a *usar medios idóneos* por ser *directa e inmediatamente* encaminados a la realización del hecho delictuoso. Situación que se realiza a través de la exteriorización de actos o de exteriorización de omisiones impropias, que tiene que ver con la mayor o proximidad lograda en el ataque concreto al bien jurídico protegido, que en el caso del delito que nos ocupa, que es el fraude informático, es el patrimonio.

En este sentido, se debe distinguir entre el dolo de consumir el hecho poniendo en peligro al bien jurídico, y la intención subjetiva específica de concretar todos los pasos que llevarán al sujeto a tal ejecución consumada. O, dicho de otro modo: “una cosa es el dolo de la tentativa, que ha de abarcar el conocimiento y la voluntad de realizar una parte de los actos ejecutivos, y otra cosa diferente es la intención de consu-

mar el hecho típico (o de completar la ejecución)". (Martínez-Bujan, 2013, p. 246)

Cabe señalar que la ley penal local poblana, hace referencia a la figura del arrepentimiento activo y eficaz, por la vía del desistimiento (Mañalich, 2020a, p. 263) (19), o a través del impedimento que hace el agente del delito de la consumación típica ya emprendida (Mañalich, 2020b, párr. 4) (20), como formas de exclusión de la punibilidad de la conducta. El primero, guarda cierta relación con la tentativa inacabada, y el segundo, a la tentativa acabada (Cuello, 2007, p. 82), desde el punto de vista de los requisitos que se exigen para estimar relevantes, tanto el desistimiento (tentativa inacabada), como el impedimento de la producción del resultado por el propio agente del delito (tentativa acabada).

Explicados han sido los alcances de la ley penal poblana, es menester reflexionar sobre la actualización de hipótesis típicas en que el sujeto activo, a través de la acción, o de la comisión por omisión, ejecute un delito de fraude informático, en perjuicio patrimonial de un tercero.

Así, en el caso de la **tentativa por acción**, esta será posible, de las siguientes maneras:

Cuando el agente del delito dolosamente y con el propósito de procurarse un lucro ilícito, para sí o para un tercero, *ponga en peligro de dañar o perjudicar* (idóneamente, y no sólo, inidóneamente) el patrimonio de otro, mediante el *intento de usar indebidamente mecanismos cibernéticos*, que provoquen o mantengan un error, sea a través del *intento de manipular* datos de entrada a un equipo de informática con el fin de *tratar de producir o lograr* movimientos falsos en transacciones de una persona física o moral; o bien, sea *intentando presentar* como ciertos hechos que no lo son; o *intentando deformar* o *intentando disimular* hechos verdaderos.

En este punto, es importante resaltar que para efectos prácticos, debe comprobarse con base en pruebas objetivas, que el sujeto activo tuvo la intención de consumir el hecho en perjuicio patrimonial del sujeto pasivo, precisamente, a través del uso indebido de mecanismos cibernéticos que realizó para tal fin.

Para ello, debe tomarse en cuenta que tales intentos que efectúa el sujeto activo, deben ser ejecutados a través del uso indebido de mecanismos cibernéticos,

(19) Quien al seguir un modelo basado en la teoría de las normas, entiende al desistimiento como una caracterización general de la tentativa como delito imperfecto.

(20) Autor que da a entender que el desistimiento tiene que ver con la tentativa inacabada, y el impedimento del propio agente del delito con la tentativa acabada.

que se traduzcan en la utilización de un medio eficaz (verbigracia: *el equipo cibernético, las capacidades del que lo manipula y el programa utilizado deben ser aptos para tal fin*), pues de otra forma no se podrá hablar de eficacia. Y, el número de pasos que ejecuta el sujeto activo debe ser exteriorizado de tal manera, que, realizados en forma parcial o en su totalidad (parte de ellos o todos), directa e inmediatamente (idóneamente) pongan en peligro al patrimonio del sujeto pasivo.

Aquí, coincido con (Serrano-Piedecabras, 2003, p. 25.), cuando señala que:

En definitiva, toda tentativa requiere de la aparición de un peligro en el resultado. Por lo que, todo resultado de peligro requiere de un doble análisis: uno *ex ante* sobre la peligrosidad de la acción y uno *ex post* sobre la plasmación de esa peligrosidad en el peligro concretamente acaecido, atribución verificada por la vía de un juicio objetivo de imputación. El estado de peligro debe manifestar externamente dos características interdependientes: la proximidad de lesión del bien jurídico y la ausencia de una normal dominabilidad de las posibles causas salvadoras.

En este sentido, se debe comprobar que el sujeto activo ha sido capaz de intentar (en forma eficaz e idónea) *manipular* datos de entrada a un equipo de informática con el fin de *tratar de producir o lograr* movimientos falsos en transacciones de una persona física o moral; aunque esto no lo logre por causas ajenas a su voluntad.

O bien, se debe demostrar que el sujeto activo haciendo uso indebido de un mecanismo cibernético, ha ejecutado total o parcialmente actos (eficaces e idóneos) para *presentar* como ciertos hechos que no lo son, sin lograrlo, por causas ajenas a su voluntad.

O bien, se debe demostrar que el sujeto activo haciendo uso indebido de un mecanismo cibernético, ha ejecutado total o parcialmente actos (eficaces e idóneos) para *deformar o intentar disimular* hechos verdaderos, sin lograrlo, por causas ajenas a su voluntad.

Todo lo cual, requiere demostrar en el caso concreto, que desde una perspectiva *ex ante* (visión misma del sujeto activo) y *ex post* (lo que efectivamente aconteció), que su intento de hacer uso indebido de mecanismos cibernéticos a través de tales *manipulaciones, presentaciones, deformaciones o simulaciones*, ha sido suficientemente próximo al bien jurídico patrimonio del sujeto pasivo, para ponerlo en peligro en forma real y efectiva (idónea, y no sólo hipotética). Situación que sólo podría ser posible, si dicho sujeto activo externamente mostró la ausencia de una normal dominabilidad de las posibles causas salvadoras para dicho patrimonio, porque dicho resultado lesivo de este bien jurídico no se logró, precisamente, por causas ajenas a su voluntad.

Ahora bien, para el caso de la **tentativa, en forma de comisión por omisión**, en el caso concreto, se deberá demostrar lo siguiente.

Que el sujeto activo tendiendo la calidad de garante sobre el patrimonio puesto en peligro de un tercero, haya omitido actos que deberían haberlo evitado, bien sea porque permitió que otro u otros, hicieren uso indebido de mecanismos cibernéticos, en forma eficaz e idónea, ejecutando o exteriorizando total o parcialmente actos encaminados directa o inmediatamente a la realización de la puesta en peligro de ese patrimonio ajeno, porque el sujeto activo dolosamente y con el propósito de procurarse un lucro ilícito, para sí o para un tercero, permitió que otro u otros intentaran provocar o mantener un error, sea intentado manipular datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral; o bien, sea intentando presentar como ciertos hechos que no lo son; o intentando deformar o disimular hechos verdaderos; pero que en cualquier caso no consumaron el daño o perjuicio patrimonial deseado por el sujeto activo, por causas ajenas a la voluntad del quien permitió que lo hiciera (21).

Cabe señalar que, en estos casos, la peligrosidad de dichos actos omisivos impropios nace *ex ante* de la evitación del sujeto activo de actuar conforme a la norma. Por ende, dicha evitación no debe aparecer *ab initio* como improbable, pues de otra manera, sería inidónea (Ovalle, 2003, p. 37), y por ende, impune.

IX. Punibilidad

Para el delito de fraude informático que nos ocupa, al igual que sucede con el fraude genérico, y todos los demás fraudes específicos contemplados en la legislación sustantiva penal poblana, el legislador optó por seguir un sistema que se basa en una cuantificación de las penas a imponer, con base en el monto de lo defraudado.

De esa manera, si se siguen los márgenes de punibilidad establecidos por el artículo 403 del Código Penal para el Estado Libre y Soberano de Puebla, México, se obtiene que el fraude informático se sancionaría de la siguiente manera:

a) *Si no se puede determinar el valor de lo defraudado o este valor no es superior a 100 Unidades de Medida y Actualización*, (que para el año 2025 equivalen a \$11,314.00 pesos mexicanos — equivalentes a unos 500 dólares americanos aproximadamente—) (22); se impondrá una multa será de 5 a 50 Unidades de Medida

(21) Siempre téngase en consideración -como dice Nieves-, que en el *itercriminis*, la tentativa del delito debe ubicarse después de la preparación, pero antes de la consumación (Nieves, 2000, p. 272).

(22) Resultado de multiplicar una Unidad de Medida y Actualización que para 2025 es de \$ 113.14 pesos mexicanos diarios por 100. <https://www.littler.com/publication-press/publication/mexico-incremento-al-valor-de-la-unidad-de-medida-y-actualizacion-4>

y Actualización (que oscilan entre \$565.70 pesos mexicanos y \$5,657.00 pesos mexicanos), más una pena de prisión de 6 meses a 3 años.

b) Y, si el valor de lo defraudado excediere de 100 Unidades de Medida y Actualización (que comienzan desde \$11,314.01 pesos mexicanos), pero no de 500 (equivalentes a \$56,570.00 pesos mexicanos —que son aproximadamente unos \$2,500 dólares americanos—); la sanción pecuniaria será de multa de 50 a 250 Unidades de Medida y Actualización (que oscila entre \$5,657.00 a \$28,285.00 pesos mexicanos), más pena de prisión de 3 a 5 años.

c) Cuando el valor de lo defraudado excediere de 500 unidades de medida y actualización (equivalentes a \$56,570.01 pesos mexicanos), pero no de 1000 (equivalentes a \$113,140.00 pesos mexicanos, que son aproximadamente unos \$5,500 dólares americanos); la pena será de multa de 250 a 500 unidades de medida y actualización (que oscilan entre \$28,285.00 a \$56,570.00 pesos mexicanos), más pena de prisión de 5 a 7 años.

d) Finalmente, cuando el valor de lo defraudado excediere de 1000 unidades de medida y actualización (equivalentes a \$113,140.01 pesos mexicanos, es decir, más de \$5,500 dólares americanos aproximadamente), la pena será una multa de 500 a 1000 unidades de medida y actualización (que oscilan entre \$56,570.00 y \$113,140.00 pesos mexicanos), más una pena de prisión de 7 a 10 años.

Lo anterior lleva a la reflexión de que tal escala de valores de punibilidad, tiene el desacierto de sancionar con una multa aproximada de la mitad del monto de lo defraudado como sanción pecuniaria, que pudiera llevar a pensar al sujeto activo del delito, que el cometer el hecho típicamente antijurídico, compensa su osadía. Sin embargo, tal aparente laxitud en esa escala de valores de punibilidad, se ve compensada con el agregado del número de años de prisión a que se haría acreedor en el caso concreto, lo que en cualquier caso, al tratarse de un delito en el que no media la violencia, puede ser conmutable en sentencia firme, por pago de dinero equivalente al monto diario de la condena individualizada al sujeto activo, que opera a favor del Estado, como un beneficio que puede obtenerse en lugar de compurgar esta última. Y, a esto, habrá que añadir, además, el pago de la reparación del daño material y moral, consistente en el monto efectivamente obtenido o puesto en peligro en perjuicio patrimonial del sujeto pasivo. Situación que desestima esa aparente laxitud de la sanción pecuniaria que obra en el diseño típico antes indicado.

Con independencia de la anterior, cabe señalar que este sistema basado en el *quantum* de lo obtenido, ha sido duramente criticado por la doctrina (Azzolini, 2005, p. 81), al señalar que no es muy equitativo basar el *quantum* de punibilidad en el monto de lo obtenido como botín por el sujeto activo, pues esto no refleja

con exactitud el mayor o menor grado de antijuridicidad de la conducta típica, ni del grado de culpabilidad del agente del delito, con relación a la mayor o menor lesividad o puesta en peligro del patrimonio, como bien jurídico protegido. Se ha dicho que simplemente se trata de un sistema arbitrario que tiene que ver con el *quantum* de afectación al patrimonio del sujeto pasivo, que no toma en cuenta, en modo alguno, la mayor o menor peligrosidad de la conducta del sujeto activo con relación a la efectiva puesta en peligro o lesión de un bien jurídico, que es lo que en realidad se debería punir. Todo ello, sin dejar de entender, la pena para el delito debe ser proporcional a la importancia social del hecho (Lara y Torres, 2021, p. 259).

A pesar de tales discusiones doctrinales, el legislador poblano decidió sancionar este delito con relación a la efectiva obtención de un monto, que según sea mayor o menor, incidirá directamente en la mayor o menor cantidad de pena que recibirá el sujeto activo por su conducta. Un aspecto que tiene que ver más con la doctrina de lo causado *ex post*, que de una doctrina penal más avanzada que tiene en cuenta la resolución interna *ex ante* del sujeto activo (Greco, 2023, p. 3), encaminada a lograr la efectiva lesión o puesta en peligro del particular bien jurídico protegido, que en el caso concreto es el patrimonio. Todo ello, en virtud de que “la amenaza penal no puede limitarse a cumplir la función de respuesta frente al delito una vez cometido, sino que ha de poder ser captada por el ciudadano en el momento de actuar, si es que la pena quiere incidir en su conducta” (Mir, 1983, p. 7).

Así, si un sujeto activo decidiera cometer defraudación informática, sabedor del monto de lo que podría obtener, sería igualmente sancionado, que alguien que lo hiciera por azar, sin saber exactamente cuánto podría obtener por su conducta delictuosa. Aquí, no se mediría la mayor o menor peligrosidad de la conducta del sujeto activo con relación a la mayor o menor puesta en peligro o lesión del bien jurídico protegido (patrimonio), sino la eventual obtención del monto de lo efectivamente defraudado, con total independencia de la actitud interna de quien dolosamente comete el delito (acción) o quien dolosamente permite que este sea cometido (comisión por omisión).

X. Conclusiones

Dentro del elenco de ciberdelitos destaca el fraude informático, debido a la gran afectación de índole patrimonial que produce en el ámbito global. De ahí que el legislador penal poblano haya decidido tipificarlo como una forma de fraude específico.

El bien jurídico protegido en el fraude informático es el patrimonio. Sin embargo, las concepciones teóricas más modernas lo vinculan con la economía en general, dada la afectación que indirectamente produce en el patrimonio de la

sociedad de un determinado Estado, e incluso, en el ámbito internacional. De ahí que pueda decirse que el objeto jurídico de tutela es el patrimonio, de manera inmediata, como bien jurídico individual; y al mismo tiempo, la economía, de manera mediata, como bien jurídico colectivo.

En términos generales, puede decirse que la mayoría de los fraudes informáticos se producen a través de lo que computacionalmente se conoce como *phishing* o *pharming* (aunque existen otras técnicas similares, pero que producen efectos diversos). Una vez que el sujeto activo a través de estos medios cibernéticos obtenidos en forma de manipulación del sistema computacional, logra hacerse de la información confidencial de la víctima, como datos personales, y claves de acceso, realiza la defraudación en perjuicio de su patrimonio. Información que al ser transferidas a los “muleros” estos se encargan de hacerla transnacional, afectado con ello la economía en general.

En el tipo penal poblano, el verbo típico *uso indebido* de mecanismos cibernéticos, se ejecuta a través de alguno de los medios comisivos consistentes en: la manipulación de datos o falseamiento, deformación o simulación de hechos (es decir, mediante *pharming* o *phishing*, u otras similares), y debe ser realizado en forma dolosa, e imbuido de un ánimo de obtención de lucro, en beneficio propio o de un tercero (elemento subjetivo específico distinto al dolo). Lo que es indicativo que la actuación de los llamados “muleros” se realiza en fase de agotamiento delictivo.

Al concebirse el tipo penal poblano de fraude informático en forma exclusivamente dolosa, se excluye en automático la modalidad imprudente. De esa manera, el fraude informático puede ser ejecutado a través del delito directo, del dolo indirecto y del dolo eventual. Por tanto, El error de tipo vencible o invencible, sobre cualquiera de tales elementos, excluirá o atenuará, en su caso, el actuar doloso del sujeto activo.

Y, en este sentido, cabe señalar además, que no basta que en el caso concreto se demuestre que el sujeto activo actuó dolosamente al momento de usar tales mecanismos informáticos, pues, además, es menester demostrar que el sujeto activo tenía la firme intención de lograr un lucro ilegal con todo ello, aunque éste no llegase a concretarse en ningún momento. De ahí que además, haya sido menester demostrar que era factible en el caso concreto la obtención de dicha ganancia ilícita por el autor delictivo.

El fraude informático en Puebla, responde al diseño típico de poder ser ejecutado en forma de acción, o de comisión por omisión, pues se trata de un delito de resultado material. De ahí que también es punible la conducta, si verbigracia, el sujeto activo teniendo la calidad de garante del patrimonio ajeno, dolosamente y

con ánimo de obtención de un lucro indebido para sí, o para un tercero, permite que otro (u otros) actué(n) en su perjuicio mediante la manipulación informática correspondiente. Conducta omisiva impropia que puede ser previa o concomitante al hecho, y que de cualquier manera, debió ser eficaz en sus particulares condiciones y circunstancias personales para la producción del resultado típico.

Además, al tratarse de un delito de resultado material, admite la tentativa acabada e inacabada, de acuerdo con la mayor o menor progresión de actos u omisiones ejecutivas encaminadas a la consumación típica. Y sólo admite la tentativa idónea, en cuando se exige la efectiva puesta en peligro del bien jurídico patrimonio que se protege por la ley, en el ataque por acción u omisión impropia que en contra del mismo realiza el sujeto activo. Ello conlleva a determinar que la llamada tentativa inidónea o irreal, carece de relevancia jurídica para la producción del resultado típico en el fraude cibernético que nos ocupa.

El diseño típico penal poblano del fraude cibernético sustenta el *quantum* de punibilidad con relación directa al monto de lo efectivamente defraudado. Situación que no está exenta de críticas desde un punto de vista dogmático más contemporáneo, dado que lejos de tomar en cuenta —con base en un esquema de valoración global del hecho—, la peligrosidad *ex ante* y *ex post* que tuvo la conducta típica con relación a la concreta puesta en peligro o lesión del bien jurídico; sólo atañe a un valor tasado objetivo de lo que por botín haya logrado obtener el sujeto activo. Situación que pudiera ser un desacierto en la punición de dicha figura, porque en lugar de medir la peligrosidad de la conducta delictuosa, toma en cuenta algo “aleatorio” a la misma, como lo es lo “efectivamente obtenido o no como producto del delito”. Situación que deja de lado un análisis más profundo de la individualización de la pena, con relación a la mayor o menor peligrosidad de la conducta desplegada por el sujeto activo que debe hacer el juzgador en el caso concreto; y que por tanto, sólo se contenta con el daño patrimonial efectivamente causado para medir este parámetro que ya viene de antemano determinado por el legislador.

XI. Referencias

Acurio del Pino, S. (2015). *Derecho Penal Informático. Una visión general del Derecho Informático en el Ecuador con énfasis en las infracciones informáticas, la informática forense y la evidencia digital*. Pontificia Universidad Católica del Ecuador.

Aguilar Olguín, C. C. (2011). *El delito de fraude cibernético y sus implicaciones jurídicas en México*. [Tesis de licenciatura, Universidad Nacional Autónoma de México]. <https://repositorio.unam.mx/contenidos/328496>

Albarrán Martínez, E. E. (2021). *Delitos cibernéticos. Transregiones*, (2), 93-104.

Ávila Trivelli, A. A. (2024). Análisis al delito de fraude informático. *Vox Juris*, 42(1), 159-173. <http://dx.doi.org/10.24265/voxxuris.2024.v42n1.13>

Azzolini Bíncaz, A. (2005). La regulación del robo en el nuevo código penal para el distrito federal. En S. García Ramírez, O. Islas de González Mariscal y L. A. Vargas Casillas (Coords.), *Temas de Derecho Penal, seguridad pública y criminalística* (pp. 79-86). Universidad Nacional Autónoma de México.

Azzolini Bíncaz, A. (2016). Los delitos patrimoniales en el código penal para el Distrito. En S. García Ramírez O. Islas de González Mariscal y L. A. Vargas Casillas (Coords.), *Código Penal para el Distrito Federal a diez años de su vigencia* (pp. 191-210). Universidad Nacional Autónoma de México.

Berdugo Gómez de la Torre, I. (2024). Sobre la protección penal del medio ambiente. Especial referencia al ecocidio. *Revista Penal*, (53), 22-37.

Cassou Ruiz, J. E. (2009). Delitos informáticos en México. *Revista del Instituto de la Judicatura Federal, Consejo de la Judicatura Federal, Poder Judicial de la Federación*, (28), 207-236.

Centeno, D. (2018). *México y el Convenio de Budapest: posibles incompatibilidades*. Red en defensa de los derechos digitales, Derechos digitales América Latina.

Cuello Contreras, J. (2007). Conceptos fundamentales de la responsabilidad por tentativa. *Anuario de Derecho Penal y Ciencias Penales, LX(1)*, 39-96.

Chirino Sánchez, E. A. y Houed Vega, M. A. (1992). El tratamiento del error en la legislación penal y en la jurisprudencia costarricense, Ciencias Penales. *Revista de la Asociación de Ciencia*, (6), 26-35.

De la Herrán Ruíz-Mateos, S. (2024). *Fundamentos de los medios comisivos en el tipo de injusto de los delitos compuestos*. (1ª ed.). Tirant lo Blanch.

Díaz Aranda, E. (2007). La normativización del tipo objetivo y subjetivo. En S. García Ramírez y O. Islas de González Mariscal (Coords.), *Panorama Internacional sobre Justicia Penal. Política Criminal, derecho penal y criminología. Culturas y sistemas jurídicos comparados* (pp. 567-584). Universidad Nacional Autónoma de México.

García Andrade, J. I. y Pilco Guamán, G. E. (2024). *El derecho a la propiedad privada y nuevas modalidades de delitos cibernéticos en la legislación Ecuatoriana: Phishing* [Trabajo final de grado, Universidad Nacional de Chimborazo]. <http://dspace.unach.edu.ec/handle/51000/13485>

Giménez García, I. (2023). *El delito de fraude informático (art. 248.2.a CP): aspectos problemáticos en relación con su interpretación y aplicación* [Trabajo final de grado, Universidad de Alicante]. <http://hdl.handle.net/10045/130801>

Greco, L. (2023). La dogmática del hecho punible con base en la teoría de las normas: ¿desde arriba o desde abajo? (Trad. N. Canard). *Revista Electrónica de Ciencia Penal y Criminología*, (25), 1-13.

Gómez Cervantes, J. (2007). El tipo penal de fraude informático. *Epitekia*, (4), 1-21.

Hassemer, W. (1990). Los elementos característicos del dolo. *Anuario de Derecho Penal y Ciencias Penales*, 43(3), 909-932.

Hernández Díaz, L. (2009). El delito informático. *Eguzkilore*, (23), 227-243.

Herzberg, R. D. (2008). Reflexiones sobre la teoría final de la acción. *Revista Electrónica de Ciencia Penal y Criminología*, (10), 1-30.

Herrera Villanueva, J. J. (2014). El patrimonio. *Revista Mexicana de Derecho. Colección Colegio de Notarios del Distrito Federal de México*, (16), 67-100.

Izquierdo Sánchez, C. (2006). Comisión por omisión. Algunas consideraciones sobre la injerencia como fuente de la posición de garante. *Revista Chilena de Derecho, Pontificia Universidad Católica de Chile Santiago*, 33(2), 329-343.

Kindäuser, U. (2008). El tipo subjetivo en la construcción del delito Una crítica a la teoría de la imputación objetiva (Trad. J. P. Mañalich-Raffo). *InDret, Revista para el Análisis del Derecho*, (4), 1-35.

Lara Patrón, R. J. y Torres Morán, A. (2021). La doble dimensión de la proporcionalidad de las penas en México. En D. B. González Carvallo y R. Sánchez Gil (Coords.), *El Test de Proporcionalidad en la Suprema Corte. Aplicaciones y desarrollos recientes* (1a ed., pp. 243-281). Centro de Estudios Constitucionales de la Suprema Corte de Justicia de la Nación.

Manero Font, E. (1995). El fraude informático. *Auditoría Pública: Revista de los Órganos Autónomos de Control Externo*, (2), 44-49.

Mañalich-Raffo, J. P. (2020a). El desistimiento de la tentativa como revisión del quebrantamiento de la norma. Una aplicación del modelo del delito imperfecto. *InDret, Revista para el Análisis del Derecho*, (3), 260-284.

Mañalich-Raffo, J. P. (2020b). El desistimiento de la tentativa como evitación o impedimento imputable de la consumación. *Política Criminal*, 15(30). <http://dx.doi.org/10.4067/S0718-33992020000200780>

Mañalich-Raffo, J. P. (2022). La estructura de la tentativa punible: el modelo del delito imperfecto. *Revista de Ciencias Penales Sexta Época*, XLVIII(3), 11-44.

Martínez-Bujan Pérez, C. (2013). Los elementos subjetivos del tipo de acción (Un estudio a la luz de la concepción significativa de la acción). *Teoría y Derecho. Revista de Pensamiento Jurídico*, (13), 233-279.

Mayer Lux, L. y Oliver Calderón, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología*, 9(1), 151-184. <https://doi.org/10.5354/0719-2584.2020.57149>

Medina Ruvalcaba, E., Velasco San Martín, C. y Velázquez Olavarrieta, A. (2021). *Recomendaciones para abordar la detección e investigación del fraude cibernético en México. Perspectiva desde el sistema judicial*. PA Consulting, Embajada Británica en México.

Mir Puig, S. (1983). La perspectiva “ex ante” en Derecho penal. *Anuario de Derecho Penal y Ciencias Penales*, 36(1), 5-22.

Moya Molina, A. F. (2014). *El error de tipo en la legislación ecuatoriana* [Trabajo final de grado, Universidad de las Américas]. <http://dspace.udla.edu.ec/handle/33000/2033>

Navarrete Morales, M. E. (2023). Reflexiones sobre el bien jurídico protegido en el delito de administración desleal. *Revista Internacional de Doctrina y Jurisprudencia*, (30), 29-49. <https://doi.org/10.25115/ridj.vi30.9653>

Nieves Luna Castro, J. (2000). La antijuridicidad y los elementos subjetivos del injusto, conforme a la doctrina tradicional y su evolución histórica. *Revista del Instituto de la Judicatura Judicial. Escuela Judicial*, (7), 257-280.

Ovalle Madrid, G. L. (2003). La tentativa inidónea en los delitos de omisión propios en el código penal español. *Revista Chilena de Derecho*, 30(1), 23-37.

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing” y el “pharming”. *Revista de Derecho*, (XLI), 211-262.

Piña Libien, H. R. (2019). Cibercriminalidad y ciberseguridad en México. *Ius-Comitalis*, (4), 47-69. <https://doi.org/10.36677/iuscomitalis.v2i4.13203>

Qué es el pharming y cómo protegerte. (s.f.). *Kaspersky*. Recuperado el 20 de febrero de 2025 de https://latam.kaspersky.com/resource-center/definitions/pharming?srsId=AfmBOoolq5HsvLoq2MosB05Pqv56uceWs0_So9K85g5_-Fr7AEyF00Pz

Real Academia Española. (2001). *Diccionario de la Lengua Española*. (22a ed.). RAE.

Rodríguez Almirón, F. (2023). El delito de estafa informática. ¿Es posible determinar la responsabilidad civil de la entidad financiera en base al artículo 120.3 del código penal como consecuencia del «phishing»? *Revista de Derecho Penal y Criminología*, (30), 273-304. <https://doi.org/10.5944/rdpc.JUNIO.2023.37387>

Sánchez Medero, G. (2014). Ciberespacio y el crimen organizado. Los nuevos desafíos del siglo XXI. *Revista Enfoques Ciencia Política y Administración Pública*, 10(16), 71-87. <https://doi.org/10.60728/zch2bv10>

Schlack Muñoz, A. (2008). El concepto de patrimonio y su contenido en el delito de estafa. *Revista Chilena de Derecho*, 35(2), 261-292. <http://dx.doi.org/10.4067/S0718-34372008000200003>

Serrano-Piedecasas, J. R. (2003). Prólogo. En E. D. Crespo, *La tentativa en la autoría mediata y en actio libera in causa* (pp. 13-20). Comares Editorial, Grupo Editorial Ibañez.

Suárez Sánchez, A. (2006). La estafa informática, Derecho penal y criminología. *Derecho Penal y Criminología*, 27(81), 195-223.

Vázquez, C. y Fernández López, M. (2022). La conformación del conjunto de elementos de juicio: admisión de pruebas. En J. Ferrer Beltrán (Coord.), *Manual de razonamiento probatorio*. (1ª ed., pp. 137-221). Suprema Corte de Justicia de la Nación, Derechos Humanos, Escuela Federal de Formación Judicial.

Zeferín Hernández, I. A. (2016). *La prueba libre y lógica. Sistema penal acusatorio mexicano*. (1ª ed.). Instituto de la Judicatura Federal.

Fecha de recepción: 07-03-2025

Fecha de aceptación: 28-06-2025