ANÁLISIS AL DELITO DE FRAUDE INFORMÁTICO

ANALISYS TO COMPUTER-RELATED FRAUD

Anderson Abraham Ávila Trivelli
ORCID: 0000-0002-3224-4646
Universidad Tecnológica del Perú
abrahamavilatrivelli@gmail.com
Perú

DOI: https://doi.org/10.24265/voxjuris.2024.v42n1.13

Recibido: 12 de mayo de 2022. Aceptado: 16 de abril de 2023.

SUMARIO

RESUMEN

El presente trabajo de investigación contempla un análisis al tipo penal de *fraude informático* en la legislación peruana, analizando también la tipificación establecida en el Convenio sobre la Ciberdelincuencia o Convenio de Budapest, haciendo además referencia a las legislaciones Argentina y Española para lo cual se aplica el método cualitativo, orientado al análisis de los tipos penales de las normativas antes mencionadas, obteniendo como resultado que nuestra normativa se encuentra en estricta consonancia con lo determinado en la norma internacional; siendo una tipificación idéntica a la establecida en el Convenio de Budapest. Es así como se puede concluir además que el tipo penal de fraude informático resulta ser más amplio en nuestra legislación que en las legislaciones argentina y española, encontrándonos frente a un delito pluriofensivo, destacándose la atipicidad al mediar el consentimiento por parte del sujeto pasivo en la ejecución de la conducta del ilícito penal desarrollado por el sujeto activo.

PALABRAS CLAVE

fraude informático, sistema informático, dato informático, Convenio de Budapest.

ABSTRACT

The present research work contemplates an analysis of the criminal type of Computer Fraud in Peruvian legislation, also analyzing the classification established in the Convention on Cybercrime or Budapest Convention, also making reference to the Argentine and Spanish legislation for which the qualitative method, oriented to the analysis of the criminal types of the aforementioned regulations, obtaining as a result that our regulations are in strict accordance with what is determined in the international standard; being a classification identical to that established in the Budapest Convention. Thus, it can also be concluded that the criminal type of computer fraud turns out to be broader in our legislation than in Argentine and Spanish legislation, finding ourselves faced with a multi-offensive crime, highlighting the atypicality in mediating consent on the part of the passive subject in the execution of the conduct of the criminal offense carried out by the active subject.

KEYWORDS

computer-related fraud, computer system, computer data, Budapest Convention.

INTRODUCCIÓN

El presente artículo de revisión abarca la problemática en el derecho penal vinculada al delito defraude informático, lacual es establecida como consecuencia del avance de la tecnología pues, como es de conocimiento general, desde hace unos años podemos observar que se ha incrementado la realización de diversos delitos a través de las tecnologías de la información y de las comunicaciones, materializados por medio de los sistemas informáticos; de ahí que resulta importante, en primer lugar, comprender la definición de sistema informático, por ello, al observar la legislación peruana, encontramos en la Ley N° 30096 (2013), modificada por la Ley N° 30171 (2014) y que se encuentra en armonía con lo establecido en el Convenio

de Budapest (2001), que en su artículo 1.A define al sistema informático como "todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa." (Pág. 4).

Consideramos que al haber optado el legislador peruano por utilizar de manera completa la definición desarrollada en el Convenio de Budapest, busca con la amplitud de ésta, abarcar diversas conductas ejecutadas por los delincuentes en la actualidad, a fin de evitar la impunidad sobre estos comportamientos delictivos. Es importante tener presente que en nuestro quehacer diario se ha tornado cotidiano el uso de diversos sistemas informáticos, mencionamos como ejemplo los siguientes: el teléfono móvil, la computadora, etc. Es importante señalar que, en el Perú, a través de la Resolución Legislativa N° 30913 de fecha 12 de febrero de 2019; y su ratificación dada mediante el Decreto Supremo N° 010-2019-RE del 9 de marzo de 2019 se dispone la entrada en vigor del Convenio de Budapest a partir del 1 de diciembre de 2019.

Después de haber señalado el concepto de sistema informático, debemos destacar, otro elemento denominado dato informático, el cual también se encuentra definido en la legislación peruana y en el Convenio de Budapest, debiéndose considerar, conforme a la definición establecida en el artículo 1.B., como dato informático a "toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función" (Pág. 4).

Estos conceptos nos demuestran que no somos ajenos a las tecnologías de la información y las comunicaciones, por el contrario, éstas han servido para facilitarnos el desarrollo de diversas actividades, entre las cuales podemos destacar a la comunicación con personas que se encuentran separadas físicamente de nosotros, usualmente en un lugar distante de donde nos ubicamos, sea en la misma ciudad, sea alrededor del mundo, generando de esta manera una reducción del tiempo utilizado para tomar conocimiento de algún evento que se suscite y garantizando un beneficio en la disminución de costos para la realización de diversas actividades, tales como el pago de diversos productos que buscamos adquirir, el estudio de cursos, diplomados, maestrías y doctorados, como también la participación en foros, conferencias o eventos no sólo académicos, si no también sociales, de esta forma podemos señalar que actualmente nos ayudan en la realización de actividades laborales, comerciales, educativas y de ocio, además, también sirve para que podamos tomar conocimiento de los diversos acontecimientos que ocurren a diario en todos los países.

Tras esta breve introducción, es importante mencionar que el fraude informático, es un delito que, desde el punto de vista del autor, se ha convertido y continuará siendo por mucho tiempo uno de los delitos más recurrentes como consecuencia del avance de la tecnología no sólo en el Perú, sino a nivel regional y mundial.

Teniendo en cuenta lo señalado en los párrafos precedentes, cabe identificar el siguiente problema ¿cuál es la tipología del delito de fraude informático aplicable en nuestra legislación? Pues bien, este trabajo tendrá como objetivo dotar de respuesta a esta pregunta, la cual se desarrollará a continuación, donde se postulará qué consideramos se debe entender por este delito. Para ello, se abordarán cuestiones generales comunes a las normas por analizar, luego se precisarán las leyes que se compararán y, posteriormente, se continuará con el análisis de este tipo penal, disgregando cada uno de los elementos que conforman la tipicidad objetiva de este ilícito penal. Finalmente se esbozarán las conclusiones a las que se arribará como consecuencia del análisis cualitativo efectuado.

CONSIDERACIÓN PREVIA

Debe tenerse presente que en nuestra legislación se establece en el primer supuesto de este ilícito penal, que la conducta prohibida debe recaer sobre los datos informáticos que pueda contener el sistema informático en perjuicio del propietario o poseedor del mismo, ocasionando un perjuicio para el titular del patrimonio; por otro lado, en el segundo supuesto que contempla este delito, la conducta debe recaer sobre los sistemas informáticos, respecto de los cuales se debe efectuar algún tipo de manipulación o se debe interferir de manera indebida; este delito contempla sobre cuáles implementos debe recaer la conducta, lo cual necesariamente conlleva, para que nos encontremos frente a un delito consumado, que exista un provecho ilícito en favor del sujeto activo o de un tercero ocasionando necesariamente un perjuicio económico en detrimento del patrimonio del afectado.

Siendo esto así, es importante resaltar que, a través de este tipo penal, es posible inferir que se pretende sancionar a los denominados *crackers*, *este* término, que no es tan común para nosotros, la Real Academia Española (RAE) lo define como "pirata informático" término que a su vez es definido por la RAE como "persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos y obtener información secreta"; por otro lado, es necesario considerar que a nivel doctrinario, Miró (2012, Pág. 302) lo define como "hackers que utilizan el acceso informático para robar información relevante, defraudar o causar algún otro tipo de daño."

Asimismo, corresponde efectuar la distinción entre el *cracker* y el *hacker*, debido a que este último es, de acuerdo con la definición realizada por la RAE "la persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora"; mientras que, a nivel doctrinario, Miró (2012), lo define como:

> Experto informático (y apasionado por Internet y las nuevas tecnologías) que busca superar barreras por el mero hecho de su existencia sin entrar en el campo de lo delictivo, en ocasiones incluso usando sus conocimientos para la mejora de la seguridad de las redes y los sistemas (también denominados samuráis). También se utiliza el término para referirse al sujeto que accede de forma ilícita al sistema informático ajeno. (Pág. 304)

Cabe resaltar de lo expresado por el profesor Miró en su definición, que de manera coloquial se suele utilizar de manera indistinta los términos *hacker y cracker*, pese a las diferencias expresadas en la definición de ambos términos.

Se puede comprender que esta distinción ha sido realizada tomando como base la finalidad con que el experto informático desarrolla su actividad, ya que por un lado, el *cracker* ostenta una finalidad maliciosa, es decir, perniciosa 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; mientras, que el *hacker* lo que busca es usar sus conocimientos para superar obstáculos sin buscar pretender cometer delitos en el ciberespacio.

Asimismo, considero que debemos tener en cuenta lo expresado por Miró (2012) al referir que:

> Son muchas las formas en las que se puede lograr acceder al patrimonio de terceros, utilizando las múltiples formas de relación comercial existentes en el ciberespacio, así como las propias debilidades de seguridad de los sistemas informáticos que dan directamente acceso al patrimonio o indirectamente a él, al contener las claves o datos bancarios de los usuarios. (Pág. 69)

En este punto, resulta necesario hacer mención que la División de Investigación de Delitos de Alta Tecnología - DIVINDAT, ha establecido estadísticamente que entre los meses de enero y abril del año 2021 se han recibido 1,188 denuncias, debemos destacar que, de ellas, 600 corresponden al delito de fraude informático, conforme se aprecia de la imagen que se presenta a continuación, la cual ha sido extraída del Diario Oficial El Peruano de 26 de agosto de 2021

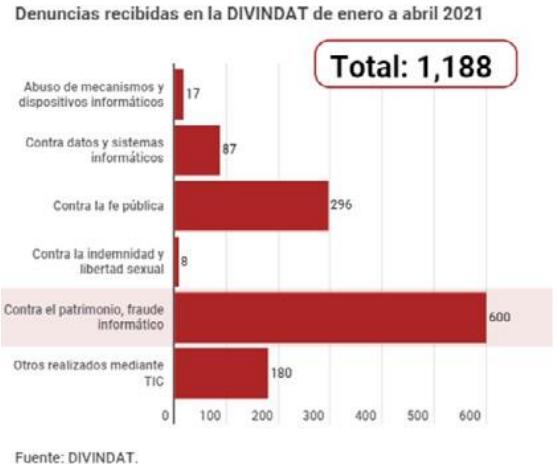

Figura 1. El dato proporcionado por la DIVINDAT demuestra la problemática que conlleva este ilícito penal, lo cual fundamenta la necesidad de establecer en el presente artículo de investigación, lineamientos básicos a efectos de interpretar válidamente este tipo penal.

EL TIPO PENAL DE FRAUDE INFORMÁTICO

Previo a realizar el análisis del tipo penal de *fraude informático*, corresponde observar la manera en que este delito ha sido definido por diversas legislaciones: la argentina, la española, la peruana y a nivel internacional.

Es así que el tipo penal de fraude informático se encuentra regulado a nivel internacional en el Artículo 8° del Convenio de Budapest, coincidentemente, en la legislación peruana también se le ha ubicado en el Artículo 8° de la Ley de Delitos Informáticos (Ley N° 30096 modificada por Ley N°30171); mientras que en la legislación argentina se ubica en el artículo 173º del Código Penal de la Nación

Argentina y finalmente, en la legislación española, está regulado en el artículo 248º del Código Penal español, como podemos apreciar a continuación:

Tabla 1. Normativa analizada

Convenio de Budapest	**Artículo 8º - Fraude Informático**	El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.
Legislación peruana – Ley 30096 (Modificada por Ley 30171)	**Artículo 8º. Fraude informático**	El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.
Legislación Argentina -	**Artículo 173º**	Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece: 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.
Legislación Española- Código Penal Español	**Artículo 248º**	2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Fuente y elaboración: propia.

ANÁLISIS DE LA TIPICIDAD DEL DELITO DE FRAUDE INFORMÁTICO

Corresponde analizar los elementos de este ilícito penal a efectos de poder determinar de modo concreto cuando aparecen hechos que sean pasibles de una imputación, de acuerdo con Sánchez (2008, Pág. 51) "la imputación se presenta como la operación en virtud de la cual se identifica un sujeto como artífice de un hecho", pues es esencial determinar cuáles son los elementos que constituyen el tipo penal para una adecuada subsunción de los hechos en la norma.

Lo fundamental del contenido de este artículo académico correspondiente al tipo penal de Fraude Informático se manifiesta en este punto, donde en primer lugar se podrá determinar quién puede ser sancionado por desplegar la conducta prohibida; es decir, quién pasará a ser responsable de la misma, el sujeto que ejecuta el delito; así como también quien puede ser considerado como sujeto pasivo. Luego, en segundo lugar, se establecerá cuál es el bien jurídico protegido o cuáles son los bienes jurídicos protegidos. Después, en tercer lugar, se analizará la conducta delictiva. Posteriormente, en cuarto lugar, nos referiremos sobre el elemento subjetivo del tipo penal. Tras ello, en quinto lugar, se abordará la autoría y participación para culminar con la punibilidad, es decir, la sanción penal y la agravante que recoge el texto legal correspondiente a este delito.

Debemos considerar lo expresado por Miró (2012, Pág. 119), quien nos indica que "la principal categoría de delitos en el ciberespacio es aquella que engloba a todos los comportamientos criminales llevados a cabo con la finalidad de obtener un beneficio patrimonial directo o indirecto del mismo". A su vez, el autor es de opinión que este delito contempla una variedad de supuestos pretendiendo punir las conductas de los agentes que afecten de ese modo el patrimonio de otros.

Por otro lado, el autor no está de acuerdo con lo señalado por Riquert (2020, Pág. 88), quien indica que, "Se trata de una de las previsiones del Convenio que ha recibido críticas en la doctrina, en vistas a que no proporciona una definición de estafa ni brinda una respuesta clara a la utilización abusiva de tarjetas", debido a que este delito no busca reprimir únicamente las conductas que contemplen como elementos el ardid, el engaño, la astucia o alguna forma fraudulenta ni que se requiera necesariamente haber inducido en error al agraviado; considero que nos encontramos frente a una figura independiente del delito de estafa, por lo que no se debía materializar una definición acorde a ese tipo penal; es así, que ha sido legislada con la finalidad de sancionar un abanico de conductas en las que existía un vacío en su regulación y que en algunos casos no resultaban ser subsumibles en tipos penales contra el patrimonio.

Sujetos del delito de Fraude Informático

Es importante indicar que conforme a la redacción establecida para el delito de fraude informático es posible concluir que es un delito común, conforme indican Roxin y Meini (citados en García, 2019, Pág. 396), para esta clase de ilícitos señala "En los delitos comunes, el tipo penal no exige una cualidad especial para ser autor del delito, de manera que cualquier persona que reúna las condiciones generales de imputabilidad podrá responder como autor", lo cual implica que puede ser cometido por cualquier persona, no se exigiéndose que el sujeto activo cuente con alguna cualidad especial para que pueda atribuírsele la conducta ilícita, de este modo, basta con que el agente reúna las condiciones generales de imputabilidad para que pueda ser sujeto activo de este delito; sin embargo, al momento de reflexionar sobre éste elemento del tipo penal, resulta importante tener en cuenta lo expresado por Azaloa (citado en Villavicencio, 2014, Pág. 284) "El perfil del ciberdelincuente (sujeto activo) en esta modalidad delictual requiere que este posea ciertas habilidades y conocimientos detallados en el manejo del sistema informático".

De este modo se coincide con lo señalado debido a que para poder realizar esta conducta el agente debe tener algún tipo de conocimiento o *expertis* técnico en informática, puesto que el sujeto activo es aquel que desarrolla la conducta prohibida por el tipo penal a través del uso de las tecnologías de la información y comunicaciones.

No obstante, se debe precisar que la Convención de Budapest del 23 de noviembre de 2001, en su Artículo 12. indica:

> Artículo 12 – Responsabilidad de las personas jurídicas
>
> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:
>   a. Un poder de representación de la persona jurídica;
>   b. Una autorización para tomar decisiones en nombre de la persona jurídica;
>   c. Una autorización para ejercer funciones de control en el seno de la persona jurídica.
>
> 2. Además de los casos previstos en el párrafo 1 del presente artículo, Cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad.
>
> 3. Dependiendo de los principios jurídicas de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.
>
> 4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Al hacerse mención a la responsabilidad de las personas jurídicas en la comisión de esta clase de ilícitos penales; debemos considerar que si bien no existe para este tipo de ilícitos penales una responsabilidad penal de la persona jurídica determinada expresamente mediante una norma

en nuestra legislación, ello da la posibilidad de considerar como autor de este ilícito penal a algún funcionario o representante de una persona jurídica que tenga dentro del ámbito de control y/o supervisión o cautela el bien jurídico protegido; esto es, el patrimonio; vg., una entidad financiera, sea, un banco, una caja, una cooperativa, etc. El mismo que se encontraría respecto de la cual exista un vínculo con el titular del patrimonio, mediante un contrato legítimo, con las condiciones establecidas por la normativa sobre la materia respectivas.

Resulta interesante lo señalado en la convención donde se ha considerado quiénes pueden resultar responsables de la comisión de esta clase de delitos, debido a que se llega a establecer que ante la ausencia de vigilancia o de control por parte de una persona física que se encuentre vinculada con la persona jurídica, sea ejerciendo funciones de control, sea autorizada a tomar decisiones en nombre de la persona jurídica u ostente un poder de representación de la persona jurídica, con la redacción actual del tipo penal de fraude informático, nos encontraríamos frente a un delito donde se infringe un deber, por incumplir el rol de control o vigilancia dentro de la persona jurídica, sea por parte de la persona que ejerza las funciones encomendadas, que podría establecerse cuando un funcionario de la entidad financiera omita la realización de sus funciones de supervisión y/o control. Este supuesto, no exige que la conducta realizada por algún funcionario de la persona jurídica sea necesariamente ejecutada por persona que ostente la calidad de órgano de representación o de socio representante de la sociedad.

Sin embargo, es de destacar lo expresado en la legislación peruana con relación al actuar en nombre de otro; que se encuentra regulado en el artículo 27° del Código Penal Peruano, cuyo texto se comparte a continuación:

> Artículo 27.- El que actúa como órgano de representación autorizado de una persona jurídica o como socio representante autorizado de una sociedad y realiza el tipo legal de un delito es responsable como autor, aunque los elementos especiales que fundamentan la penalidad de este tipo no concurran en él, pero sí en la representada.

Es en este artículo donde se determina la responsabilidad de aquel que actúa como órganos de representación de una persona jurídica o como socio representante de una sociedad y realiza el tipo penal, es responsable como autor, aunque los elementos especiales no concurran en él, pero si, en la persona jurídica por la que actúa en su nombre. Puesto que la responsabilidad por la afectación al patrimonio de una persona natural, patrimonio que se encuentra bajo el nivel de supervisión o control de la persona jurídica, recaería en el órgano de representación de la persona jurídica.

Asimismo, a las personas con poder de decisión en la persona jurídica se les puede atribuir la comisión de este tipo de ilícitos penales cuando la conducta sea ordenada o ejecutada por éstos, puesto que, por ejemplo, una entidad financiera posee el deber jurídico de cautelar el patrimonio de las personas físicas o jurídicas que encomiendan bajo las diversas modalidades reconocidas por el ordenamiento jurídico, la custodia de su patrimonio, el deber de cautelar las cuentas tanto de crédito como de débito que una persona física o jurídica posea en la entidad financiera.

Con lo señalado por la Convención y avalado en la legislación peruana, se puede contemplar que se está también frente a una infracción de un deber; en tanto y en cuando el sujeto activo sea parte de la organización; ergo, de la persona jurídica encargada de cautelar el patrimonio de otros o de la misma persona jurídica. En este supuesto, podemos ubicar al insider definido por Miró (2012, Pág. 305) como el "Cibercriminal que pertenece o trabaja para la institución o empresa víctima de la infracción."

Para comprender ¿quién es el *insider*?, se abordarán dos ejemplos, en el primero de ellos, el sujeto activo labora en la propia persona jurídica, siendo éste el *insider*, denominado como "A" quien se encuentra encargado del área de recursos humanos de una entidad financiera y percibe US$ 2000.00 (dos mil dólares americanos) mensuales, realiza una manipulación al sistema informático de la entidad financiera, efectuando una modificación a la base de datos de la entidad financiera, consignando en ésta información falsa que establecería la compra de sus vacaciones por parte de la empresa en el mes de febrero, periodo en el que se encontraba ejerciendo sus funciones de manera regular, percibiendo de esta manera doble remuneración; esto es, US$ 4000.00 (cuatro mil dólares americanos en el mes de febrero.

En el segundo ejemplo, el *insider*, sujeto "A" a través de la infracción de un deber especial; omitiendo actualizar el software del antivirus contratado por la entidad financiera que hubiera protegido algún tipo de acceso indebido al sistema informático de la misma, permite con esta conducta que un tercero "X" acceda a la

base de datos de la misma e introduzca en esta un algoritmo que realice el débito automático de las cuentas de todos los clientes que cuentan con una tarjeta de crédito y que esas cantidades; aunque sean minúsculas (1 dólar americano) pero realizadas en las cuentas de todos los clientes generen un perjuicio millonario y que estos cargos sean trasladados hacia una determinada cuenta en el exterior de propiedad de "C", quien finalmente se ve beneficiado indebidamente con estas conductas. Teniendo en cuenta que "A" no cumple con su función, ante los clientes, resulta ser responsable la entidad financiera puesto que no ha cumplido a cabalidad con el deber de cautelar el patrimonio de sus clientes. Este ejemplo corresponde a un caso de comisión por omisión u omision impropia, puesto que el agente no ha desarrollado la conducta esperada, pese a encontrarse en posición de garante respecto del bien jurídico protegido, debiéndosele considerar coautor del ilícito penal.

Es evidente la deslealtad desarrollada por el *insider* al momento de ejecutar los actos destinados a obtener un beneficio patrimonial mediante una manipulación al sistema informático, llegando a percibir una remuneración indebida. Así como la conducta realizada al momento de omitir cumplir con su deber y de esta manera permitir que un tercero acceda a la base de datos y ocasione un perjuicio en las cuentas de los clientes de la entidad financiera.

Desde mi punto de vista, podríamos considerar como autor al *insider* debido a que el rol que ejerce determina una deslealtad dentro de las funciones encomendadas, la cual no escapa de que consecuentemente se impongan en contra de éste sanciones administrativas, civiles y penales, debido a que determinan la afectación del desarrollo de las actividades propias de la persona jurídica.

Por otro lado, como se ha podido observar cuando se ha hablado sobre el sujeto activo, en el delito de fraude informático se debe tener en cuenta lo señalado por el desaparecido profesor Mir (2008, Pág. 220) quien ha mencionado que: "Sujeto pasivo es el titular o portador del interés cuya ofensa constituye la esencia del delito. (…) Según esto, el sujeto pasivo no coincide necesariamente con el sujeto sobre el que recae físicamente la acción, ni con el perjudicado", por lo que, en este delito, al no determinarse de manera expresa sobre quien recae la acción, se considera que también puede ser cualquier persona, independientemente de si el sujeto sobre el cual recae la acción es una persona natural o jurídica.

Esta afirmación se da porque que cualquier persona natural o jurídica puede ser el sujeto pasivo de la conducta prohibida debido a que el tipo penal de fraude informático no exige que el sujeto pasivo ostente una calidad especial, en contraposición a delitos como el parricidio[1]o los delitos de corrupción de funcionarios[2], etc. En estos ilícitos penales si se exige que el sujeto pasivo ostente una calidad determinada para que podamos subsumir la conducta en estos delitos.

Es importante mencionar que en este tipo penal, no necesariamente en todos los casos el sujeto sobre el cual recae la acción delictiva será el mismo sujeto respecto del cual se afecta el patrimonio, tal como también puede ocurrir en el delito de estafa; en otras palabras, este tipo penal puede contemplar la concurrencia de un sujeto pasivo del delito y de un sujeto pasivo de la acción, por ello, el sujeto sobre el que recae la conducta no es siempre el sujeto perjudicado patrimonialmente, un claro ejemplo de esto se presenta cuando el sujeto activo, una persona que ha ingresado a un sistema informático de un banco, altera los datos informáticos de éste, es decir realiza una modificación en las cuentas que poseen diversas personas en la entidad financiera, siendo ésta última quien la cautela, modificando el contenido dinerario de las mismas a través de una transferencia del patrimonio a una cuenta del sujeto activo o de una tercera persona, que también puede ser natural o jurídica, ocasionando de esta forma la disposición patrimonial de las cuentas de los clientes del banco estableciéndose que el sujeto sobre el que recayó la acción típica (banco) es distinto del sujeto cuyo patrimonio se ve mermado (cliente de la entidad financiera).

Lo señalado en este acápite resulta plenamente aplicable no solo para la legislación peruana, sino también para el Convenio de Budapest y las legislaciones argentina y española, puesto que, en todos estos instrumentos jurídicos, no se ha considerado que el sujeto activo ni el sujeto pasivo posean una cualidad específica para la ejecución del delito.

---

1 En este tipo penal, el sujeto pasivo es el ascendente o descendente, natural o adoptivo, con quien sostenga o haya sostenido una relación conyugal o de convivencia el sujeto activo.

2 En esta clase de delitos, el sujeto pasivo es el Estado; siendo ejercida la defensa de sus intereses mediante los procuradores públicos. Conforme a lo dispuesto en el Decreto Legislativo 1068 – Decreto Legislativo de Defensa Jurídica del Estado, en el artículo 2º: El Sistema de Defensa Jurídica del Estado es el conjunto de principios, normas, procedimientos, técnicas e instrumentos, estructurados e integrados funcionalmente mediante los cuales los Procuradores Públicos ejercen la defensa jurídica del Estado.

Bien jurídico protegido

De acuerdo con la redacción de la Convención y los tipos penales argentino, español y peruano, estoy plenamente convencido que en este tipo penal nos encontramos frente a un delito pluriofensivo, teniendo en cuenta lo señalado por García (2019), se debe considerar que:

> Los tipos penales pueden clasificarse también en función de si la conducta típica está configurada en atención a la afectación de un solo bien jurídico o de varios bienes jurídicos. En el primer caso al tipo penal se le denomina delito uniofensivo, mientras que en el segundo caso la calificación utilizada es la de delito pluriofensivo. (Pág. 405)

En sentido contrario se expresa Aboso (2020, Pág. 317), quien considera como único bien jurídico protegido al patrimonio, refiriendo que "El bien jurídico tutelado es el patrimonio individual. No se tutela acá el normal funcionamiento de los sistemas informáticos o de transmisión de datos, tampoco la privacidad de estos últimos"

Desde mi punto de vista, a este tipo penal le corresponde la protección no sólo del patrimonio; sino también, de la integridad de los datos informáticos y de la integridad de los sistemas informáticos, debido a que son bienes jurídicos que se encuentran interrelacionados en este tipo penal, exigiéndose su necesaria afectación para que se consume el delito de fraude informático o las figuras reconocidas en las legislaciones argentina y española, teniendo en definitiva presente que la conducta típica debe recaer sobre los datos informáticos o sobre los sistemas informáticos, siendo evidente que no solamente se va a afectar al patrimonio del agraviado. Con relación a estos bienes jurídicos protegidos se debe tener en cuenta que:

En primer lugar, el patrimonio, entendido por Salinas (2018, Pág. 1145) como "la situación de disponibilidad que tienen las personas sobre sus bienes, derechos o cualquier otro objeto, siempre que tal situación tenga una protección jurídica de relevancia económica"; debemos destacar que el patrimonio en este ilícito penal se encuentra representado, por ejemplo, a través de depósitos bancarios, fondos electrónicos, etc.

En segundo lugar, la integridad de los datos informáticos, por la cual se busca cautelar la inmutabilidad de los datos informáticos, lo cual implica la no alteración o modificación de las representaciones de hechos, información o conceptos expresados de cualquier manera que se preste a tratamiento informático, incluyéndose los programas diseñados para que un sistema informático ejecute una función.

En tercer lugar, la integridad de los sistemas informáticos, el cual, debe ser entendido como la no alteración o modificación de todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa, de esta forma este tipo penal también busca preservar la invariabilidad de los datos informáticos o de los sistemas informáticos éstos mediante algún empleo indebido de los mismos.

Análisis de la conducta delictiva

Continuando con el análisis a este tipo penal, conforme al texto de la Convención y el recogido en la legislación peruana, resulta necesario mencionar que la modalidad de ejecución de éste ilícito penal, diferencia la afectación de datos informáticos y de los sistemas informáticos; sin embargo, se debe considerar que cuando el legislador peruano asumió que se debía tipificar el delito de fraude informático, a través de la Ley 300963, no contemplaba que ésta debía ser desarrollada de manera deliberada e ilegítima, siendo que con la modificatoria realizada por la Ley 30171, éstos términos fueron incorporados como elementos del tipo para que podamos establecer de manera fehaciente la tipicidad en este delito; por ello, en primer lugar, definiremos estos términos:

Deliberadamente

Este término fue tipificado en nuestra legislación para que no nos apartemos de la conducta regulada en la Convención, debiéndose comprender por deliberada una conducta consciente y voluntaria por parte del sujeto activo en la realización de éste ilícito penal; puesto que nos encontramos frente a una conducta que necesariamente debe ser dolosa. Desde mi punto de vista, nos encontramos frente

3 El texto original establecido a través de la Ley 30096 fue el siguiente: Artículo 8. Fraude informático: El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

a la figura del dolo directo, pues el término deliberadamente determina consciencia plena del sujeto activo en la ejecución de la conducta prohibida y además ha previsto el desarrollo del resultado típico.

Se descarta la comisión de este delito de manera culposa, al no encontrarse prevista dicha modalidad de comisión en el tipo penal, lo cual se encuentra en estricta armonía con lo señalado en el Código Penal Peruano en su artículo 12: "Las penas establecidas por la ley se aplican siempre al agente de infracción dolosa. El agente de infracción culposa es punible en los casos expresamente establecidos por la ley.". Esta norma determina que la punición de las conductas culposas se realiza en los casos previstos expresamente por la ley.

Ilegítimamente

Por otro lado, para definir este término, recurriremos al Informe Explicativo del Convenio de Budapest (2001), donde se entiende que:

> …refleja la idea de que la conducta descrita no siempre es punible per se, sino que puede ser legal o justificada, no sólo en aquellos casos en que corresponde aplicar una defensa legal clásica, como el consentimiento, la defensa propia o la necesidad, sino también cuando otros principios o intereses conducen a la exclusión de la responsabilidad penal. El término "ilegítimo" deriva su significado del contexto en que está utilizado (…) puede referirse a una conducta realizada sin facultades para hacerlo (ya sean de orden legislativo, ejecutivo, administrativo, judicial, contractual o consensual) o a una conducta que no está de otro modo comprendida dentro de las justificaciones, excusas y defensas legales establecidas o los principios pertinentes con arreglo a las leyes nacionales. (Fundamento 38)

Como podemos observar que con relación al término ilegítimamente, es un elemento necesario para la configuración del tipo penal, resultando ser una exigencia que se corroborará en el caso concreto; a través de correos electrónicos, documentos, resoluciones judiciales, autorizaciones, etc., tal como el informe de la convención lo ha señalado.

Es necesario mencionar, que la legislación española si ha establecido de manera expresa la necesidad de que la conducta sea efectuada de manera no consentida; en tanto, que en la legislación argentina no se ha señalado esta exigencia; sin embargo, la misma se puede inferir de la lectura del tipo penal, puesto que al establecer el tipo penal argentino el término *defraudare* y que el artículo 173 Código Penal de la Nación argentina indica que nos encontramos frente a casos especiales de defraudación como enunciado general en esta clase de comportamientos, es preciso tener una definición de defraudación.

De acuerdo con Arocena & Balcarce (2018), sobre la defraudación señalan que:

> La defraudación *in genere* es el comportamiento consistente en un ardid o engaño que induce en error a un sujeto, previo a una disposición patrimonial perjudicial para el ofendido o, también, el abuso de confianza otorgada, de situación producida o frustración de un derecho concedido que, por regla, implica una disposición patrimonial perjudicial para el disponente o un tercero, o excepcionalmente, el peligro de que ella se produzca. (Pág.75)

Del concepto esbozado se puede observar que el elemento engaño determina una situación donde no existe consentimiento alguno por parte del sujeto pasivo.

Ahora bien, luego de haber analizado los dos primeros elementos que constituyen requisitos indispensables para que se ejecute este delito, en segundo lugar, se procederás a analizar los verbos rectores que determinan las conductas que afectan a los datos informáticos, de esta manera, se tendrá que la acción penal será ejercida cuando la conducta se despliegue a través del diseño, introducción, alteración, borrado, supresión clonación de datos informáticos, como podemos observar:

- *Alteración de datos informáticos*: Por alteración se entendería a la modificación de datos informáticos.
- *Borrado de datos informáticos*: Por borrado se comprendería la eliminación de los datos informáticos.
- *Clonación de datos informáticos*: Por clonar se comprendería a la creación de datos informáticos idénticos a los originales.
- *Diseño de datos informáticos*: Por diseño se entendería la manera cómo el dato informático está representado y almacenado.
- *Introducción de datos informáticos*: Por introducción se comprendería adicionar o agregar datos informáticos que no existían.
- *Supresión de datos informáticos*: Por Suprimir se entendería a que los datos informáticos serán erradicados o desaparecidos.

Luego, en segundo término, nos encontramos con que la norma sanciona las siguientes conductas:

- *Cualquier interferencia en el funcionamiento de un sistema informático*: Por interferir se entendería el interponerse en el funcionamiento del sistema informático; alguna forma de interposición para que el sistema informático no funcione de manera normal y adecuada.
- *Cualquier manipulación en el funcionamiento de un sistema informático*: Por manipular se comprendería el intervenir con medios hábiles distorsionando el funcionamiento del sistema informático.

Pues bien, cualquiera de éstas ocho modalidades de comisión del ilícito penal necesariamente deben desarrollarse para que se configure el delito de fraude informático, asimismo, no se excluye la posibilidad de que puedan concurrir dos o más de ellas, pero si se exige necesariamente la afectación al patrimonio del sujeto pasivo o titular del bien jurídico, debido a que el texto de la norma determina que el sujeto activo busca obtener un beneficio económico con la ejecución de las conductas descritas, siendo el beneficio económico indefectiblemente ilegítimo el cual implica una disminución del patrimonio del agraviado.

En este momento, debemos destacar que la legislación argentina y española, a diferencia de la peruana y la convención, congregan como elemento típico de sanción la manipulación informática, asimismo, esta puede recaer en un sistema informático o en la transmisión de datos (argentina); en tanto, que se adiciona a dicha modalidad la conducta realizada a través de algún artificio que ocasione una transferencia de un activo patrimonial (española).

Para comprender el concepto de manipulación debemos considerar lo expuesto por Aboso (2019, Pág. 317), quien indica que "se comete cuando el autor utiliza una técnica de manipulación informática" y finaliza su definición señalando: al definir o desarrollar el concepto no debe utilizarse el mismo termino objeto de definición.

> La acción de manipular debe producir una alteración en el sistema de almacenamiento y tratamiento de datos. Esta alteración debe consistir en el funcionamiento anómalo del sistema, es decir, la acción de manipular debe incidir sobre el proceso mismo del funcionamiento del sistema provocando resultados inadecuados o extraños a los que debería arrojar. (Pág.319)

Esta definición se complementa con la de García (2008), quien menciona:

> … se define como toda acción que suponga intervenir en el sistema informático alterando, modificando u ocultando los datos que deban ser tratados automáticamente o modificando las instrucciones del programa, con el fin de alterar el resultado debido de un tratamiento informático y con el ánimo de obtener una ventaja patrimonial. (Pág. 294)

Con la definición del término manipular se pretendía abarcar el contenido de la conducta prohibida para este tipo penal; sin embargo, es evidente que resulta ser insuficiente para lo establecido mediante la convención, en razón a que los verbos rectores que se tipifican, tanto en nuestra legislación nacional como a nivel internacional son mayores y comprenden un mayor bagaje de conductas punibles.

También, se debe considerar en este delito, que el sujeto activo debe tener plena consciencia de que su conducta es contraria al ordenamiento jurídico y es opuesta a la voluntad del sujeto pasivo, así como que conociendo ello, debe desplegar la conducta lesiva. Como afirma Mayer (2007) al referirse sobre el dolo, este autor nos señala que:

> La producción contraria al deber de un resultado típico es dolosa, tanto si movió al autor a realizar la acción la representación de que el resultado va a tener lugar, como cuando esa representación no fue razón para que él se abstuviera de la actuación voluntaria. (Pág.320)

Tanto el Convenio, como las legislaciones española y peruana, si contemplan expresamente el elemento perjuicio en esta clase de delitos, a diferencia de la legislación argentina, donde no se contempla dicho término; sin embargo, por la ubicación del delito en el espacio referente a las defraudaciones, resulta evidente que es un elemento necesario para la configuración del delito de fraude informático, lo que evidencia que en todas ellas, se exija como elemento subjetivo del tipo, entendido por Jescheck (2002, Pág. 342) como "...delitos de intención (delitos de tendencia interna). Se habla de intención en este sentido cuando el autor persigue un resultado que tiene en consideración para la realización del tipo pero que en realidad no necesita ser alcanzado."

La tendencia interna trascendente en este delito hace referencia al ánimo de lucro, se debe

considerar la intención, según Wezel (1956, Pág. 84) como "tendencia hacia un fin ulterior. En ella el propósito de concretar el tipo objetivo es solamente el medio para un fin más amplio…" por parte del agente de obtener o que un tercero obtenga con la conducta prohibida un provecho o ventaja económica o patrimonial; como bien señala García (2008, Pág. 293) "…el fraude informático tiene como elemento común con la estafa genérica el ánimo de lucro…". Por lo que, si se logra demostrar la falta de este ánimo, nos encontraríamos frente a una conducta atípica.

Corresponde mencionar sobre el provecho en favor de tercero, la figura de los "*muleros*", de acuerdo con Gil & Hernández (2019):

> Se trata de la persona que recibiría en su cuenta el dinero obtenido de la víctima de la estafa, dificultando, de esta manera, el descubrimiento de los criminales. Si el mulero conoce que el dinero que recibe proviene de una estafa y forma parte por tanto de la organización del delito, será condenado como coautor o como cooperador necesario de un delito de estafa. Sin embargo, en la mayoría de las ocasiones no es así. En ocasiones los muleros son a su vez captados por las organizaciones criminales con engaños, como una oferta de trabajo con apariencia más o menos real, aunque con unas condiciones muy sugerentes, en la que se le dice al sujeto que, a cambio de una cantidad o un porcentaje, debe abrir una cuenta a su nombre, recibir una transferencia de dinero y reenviarlo después a los estafadores. (Pág. 249).

Por ello, la Convención, ha buscado sancionar también a estas personas que reciben el dinero ilícito en sus cuentas y que muchas veces sirven de nexo para el tránsito del dinero indebido hacia el beneficiario final.

Finalmente, es necesaria una breve mención de los ciberfraudes más comunes que se encuentran vinculados a esta figura delictiva:

- *Auction fraud*: Miró (2012, Pág. 70) lo define como "fraude en las subastas, consistente en la tergiversación de un producto o su no entrega conforme a lo pactado en los sistemas de subasta *online* tipo eBay"
- *Phishing*: Conforme a lo señalado por Miró (2012):

  > Definido por el grupo mundial *antiphishing* como el mecanismo criminal que emplea ingeniería social y subterfugios técnicos para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias. El uso de la ingeniería social se produce cuando se utiliza la identidad personal de otro (*spoofing*) mediante la falsificación de sitios web, para conducir a los consumidores a que confíen en la veracidad del mensaje y divulguen los datos objetivos. (Pág.72)

En este punto podemos subdividir las modalidades de *phishing*, de la siguiente forma:

- El *vishing*, que según Miró (2012, Pág. 309) es la: "Práctica consistente en la utilización de mensajes de telefonía basada en voz sobre IP para conseguir de la víctima información personal, financiera o cualquier otro tipo de datos confidenciales".
- El *smishing*, considero que esta práctica consiste en el envío de mensajes de texto "SMS" para conseguir datos de la víctima, por lo general se sustentan en premios que uno ha obtenido a razón de un sorteo, solicitando al "ganador" se comunique con determinado número telefónico donde le exigirán diversos datos de verificación, solicitándole por el premio la realización de un pago, generalmente vía transferencia, para dar conformidad a que es la cuenta del "ganador"; o se le solicita los datos de su cuenta bancaria; número de tarjeta de crédito/débito, CVV, fecha de expiración de la tarjeta y nombre de la persona a la que le pertenece ésta, para que los cibercriminales puedan realizar compras o transacciones.
- El *whaling*, según Miró (2012, Pág. 77) ocurre cuando "el *phisher* se centra en un pequeño grupo de personas de alto nivel de una organización concreta e intenta robar sus credenciales, preferiblemente a través de la instalación de *malware* que proporciona funcionalidades de <<puerta de atrás>> y *keylogging*" finalmente, también corresponde destacar los fraudes BEC (Business Email Compromise), donde en este tipo de fraude, el cibercriminal suplanta la identidad de un directivo de la compañía dirigiéndose a un empleado de la empresa que cuente con capacidad para realizar actos de disposición patrimonial ordenándole realizar un pago indebido o una transferencia. Por lo general ocurre a través de correos electrónicos. Si bien, algunas de estas modalidades podrían subsumirse en otro tipo penal, correspondería a una evaluación caso por caso para determinar la concurrencia de alguna figura concursal o la aplicación de los principios que resuelven el concurso aparente de leyes.

- *Pharming*: Siguiendo a Miró (2012) afirma que se debe considerar la definición precedente, pues esta modalidad se da:

  > Cuando se utilizan otros artificios técnicos, como por ejemplo redireccionar un nombre de dominio de una página web verdadera situada en la memoria caché del sujeto o de otro modo a una página web falsa, o monitorizar la intervención del sujeto en la verdadera, se utiliza el término *pharming*. (Pág.72)

- *Scam* (Ciberfraudes burdos): De acuerdo con Miró (2012, Pág. 69), en esta clase de fraudes "Se prometen cantidades importantes de dinero a cambio de pequeñas transferencias relacionadas con ofertas de trabajo, loterías, premios u otros"

Como sepuede observar, todas estas modalidades de ciberfraudes son pasibles de subsumirse en el tipo penal de Fraude Informático regulado en nuestra legislación, siendo ejemplos de las formas de comisión de este ilícito penal.

Grado y desarrollo del delito

El autor considera que para este delito si cabe la figura de la tentativa toda vez que nos encontramos frente a un delito de resultado, en esta clase de delito se requiere que para la consumación del ilícito penal se debe ocasionar un resultado materializado en un perjuicio en desmedro del patrimonio del sujeto pasivo o agraviado; en palabras de Aboso (2020, Pág. 341) "Al desvalor del acto debe agregarse el desvalor de resultado, que consiste en este caso en el perjuicio patrimonial ajeno. Este perjuicio patrimonial se consuma cuando el autor puede disponer del dinero, valores o bienes." Con relación a los delitos de resultado coincido con la definición expuesta por Díaz (2018, Pág. 130) quien señala que "describen conductas cuya consumación implica la lesión de un bien jurídico tutelado"

Por ello, es evidente que dentro de las fases del desarrollo y ejecución del delito, en tanto, el sujeto activo ejecute cualquiera de las modalidades de conductas prohibidas previstas y no exista una disposición del patrimonio con la generación de perjuicio en agravio del titular del bien jurídico protegido patrimonio, nos encontraremos frente a un delito en grado de tentativa, siempre que se pueda demostrar que se buscaba obtener un beneficio patrimonial el beneficio propio o de tercero, caso contrario, podría subsumirse la conducta en otro ilícito penal como el acceso ilícito. De esta manera, el sujeto activo puede desplegar la conducta reprimible sin llegar a consumar el ilícito, la tentativa se manifiesta hasta el momento anterior a ocasionar el detrimento en el patrimonio del sujeto pasivo o agraviado; es decir, previo al traslado del patrimonio fuera de la esfera de dominio del sujeto pasivo.

Por último, con relación a las figuras concursales, en este punto coincido con lo expresado por Riquert (2014):

> El fraude informático es un tipo que ofrece diversas posibilidades de concurso de delitos. Como destacan con acierto Aboso y Zapata, concurrirá por lo general con la acción de ingreso indebido o no autorizado a un sistema informático (art. 153 bis, CP), caso que estiman como de simple relación medial y que, puede agregarse, está previsto expresamente como figura residual.

Generalmente nos podremos encontrar frente a esta calificación residual en los casos en los que no se llegue a consumar el delito de fraude informático, cabe acotar que, para la legislación peruana, el tipo residual sería el de acceso ilícito, tipificado en el artículo 2° de la Ley 30096, modificada por Ley 30171 del 10 de marzo de 2014, que a continuación indicamos:

> **Artículo 2. Acceso ilícito:** El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.

Autoría y participación

Para este ilícito penal en las legislaciones argentina, española y peruana, son aceptables todas las formas o modalidades de participación delictiva; esto es, la autoría, por un lado, es factible la figura independiente del autor, entendido por el profesor Villavicencio (2017, Pág. 104) como "aquel sujeto que tiene un poder de conducción de todos los acontecimientos de forma tal que le es posible encausarlo hacia el objeto determinado", la coautoría, definida por Roxin (2017, Pág. 146) como "realización del tipo mediante ejecución con división del trabajo", autoría mediata, considerando Roxin (2014) que:

> Se puede realizar también un tipo sirviéndose de otro (de "alguien que actúa como medio [en el hecho]") y empleando la persona de este

> para los fines propios de modo que, mediante su instrumentalización (su utilización como ¨instrumento¨), se denomina mediatamente (como ¨sujeto de atrás¨) al acontecer. (Pág.84)

También la participación, en la figura de la incitación o inducción, entendida por Roxin (2014, Pág. 226) como "el determinar provocando o incitando dolosamente un hecho ajeno." y la cooperación o complicidad Roxin (2014, Pág. 275) la define como "una acción de aumentar el riesgo, causal para el resultado típico y jurídicamente desaprobada."

En este punto, corresponde delimitar al cómplice primario, conceptualizado por el profesor Villavicencio (2017, Pág. 111) como "aquel que otorga un aporte sin el cual no se hubiera podido cometer el delito.". Y al cómplice secundario definido por Villavicencio (2017, Pág. 111) como "aquel que otorga un aporte que no es indispensable para la realización del delito, porque de cualquier otro modo este se hubiera consumado."

Por ello, se exige un análisis caso por caso a efectos de poder determinar en cada situación en específico frente a cuál de estas figuras nos encontramos.

Sanción

La sanción prescrita por el legislador peruano en el tipo penal base corresponde a una pena de 3 a 8 años de pena privativa de la libertad a imponer al autor del hecho punible y otra pena que se materializaría entre 60 a 120 días – multa.

Por otro lado, las sanciones establecidas en el tipo de fraude informático para las legislaciones argentina y española resultan ser penas más benignas (argentina de 1 mes a 6 años) y (España 6 meses a tres años).

Sobre el particular, podemos observar que nuestra legislación reprime con mayor intensidad la comisión del delito de fraude informático, a diferencia de las legislaciones española y argentina, siendo que en nuestra legislación se ha incorporado este tipo penal a través de una ley especial que se encuentra en concordancia con el Convenio de Budapest.

Asimismo, existe la posibilidad de imposición de dos penas principales, la privativa de libertad y la de multa, ambas deben ser materia de la aplicación del sistema de tercios para una adecuada determinación judicial de la pena, donde se individualicen las penas concretas y abstractas a imponer.

Agravante

Por último, respecto de la agravante, el legislador ha buscado proteger al patrimonio destinado por el Estado para gestionar su actuación en beneficio directo de personas que se encuentran en situación de vulnerabilidad, debiéndose considerar dos aspectos importantes, en el primero de ellos el patrimonio debe encontrarse bajo supervisión del Estado; por ende, el sujeto pasivo resulta ser el Estado, en tanto que el segundo requisito es la finalidad o destino que tiene dicho patrimonio, pues se busca sancionar la afectación a través del fraude informático del patrimonio destinado para atender los fines asistenciales y a quienes recurren a los diversos programas de apoyo social, tales como pensión 65, Juntos, Jóvenes Productivos, etc, o, sancionando las conductas que afecten el patrimonio con ésta finalidad específica a la que se encuentra destinado, por ello, la pena abstracta a imponer se debe ubicar entre 5 y 10 años de pena privativa de la libertad y otra pena entre 80 a 140 días - multa.

Sin embargo, debemos considerar que en el artículo 11 de la Ley 30096 también se han establecido agravantes para los delitos informáticos previstos en esta ley, siendo inaplicable par el delito de fraude informático, desde mi punto de vista, la tercera agravante (en su totalidad) y el primer supuesto de la cuarta agravante (en cuanto hace referencia a que debe comprenderse a los fines asistenciales para la imposición de una agravante). En tanto que, resulta aplicable la agravante en los supuestos en que nos encontremos frente a una organización criminal siempre y cuando el agente cometa el delito en calidad de integrante de la misma, como también si el agente abusa de su posición especial de acceso a la información a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función, respecto al ejercicio de un cargo o función, considero que debe interpretarse dentro del ámbito de la función pública para su correcta aplicación; y finalmente, cuando el delito comprometa la defensa, la seguridad y la soberanía nacionales, supuestos que para los que el legislador la obligación del juez de aumentar la pena hasta en un tercio por encima del máximo legal fijado para el delito.

CONCLUSIONES

La actual redacción del delito de fraude informático en la legislación peruana y que resulta similar a la esbozada en el Convenio de Budapest, busca proteger o resguardar datos informáticos vinculados a un contenido patrimonial, cuya afectación genere una disminución del patrimonio del titular del bien jurídico protegido, determinando de esta forma que nos encontramos frente a un delito pluriofensivo por no ser el patrimonio el único bien jurídico protegido. Para una mejor redacción de la conclusión podría eliminarse lo resaltado.

La actual regulación del tipo penal de fraude informático establecido en nuestra legislación evidencia que nos encontramos frente a un delito de resultado, puesto que para la consumación de este se exige una necesaria afectación que ocasione un detrimento en el patrimonio del afectado, materializado en la disminución del mismo.

Con relación a la agravante establecida en el segundo párrafo de éste ilícito penal, ésta pretende sancionar de manera gravosa a quienes afecten el patrimonio del Estado a través de las tecnologías de la información y las comunicaciones, en la medida de que este patrimonio haya sido destinado a satisfacer fines asistenciales o programas de apoyo social; entiendo que el fundamento de esta agravante radica en la situación de vulnerabilidad de las personas que requieren la asistencia del Estado peruano, siendo el agraviado el Estado.

Tanto la Convención como el tipo penal peruano; a diferencia de las legislaciones argentina y española no solamente pretenden sancionar las defraudaciones dadas a través de manipulaciones informáticas (caso argentino) o las defraudaciones realizadas mediante manipulación o algún artificio semejante a esta (caso español); si no que contemplan una mayor cantidad de supuestos de hecho, buscando sancionar conductas que previo a la dación de esta norma eran consideradas atípicas.

Si una persona desarrolla cualquiera de las conductas establecidas en el delito de Fraude Informático con autorización por parte del sujeto pasivo, podemos establecer que nos encontraríamos frente a la figura del consentimiento, lo cual determinaría la atipicidad de la conducta por parte del presunto sujeto activo en el presente delito debido a que el tipo penal exige que el agente debe actuar de modo ilegítimo, por lo que al actuar con consentimiento por parte del sujeto pasivo no es factible sancionar dicha conducta.

FUENTES DE INFORMACIÓN

Fuentes bibliográficas

Aboso, G. (2020). *Derecho penal cibernético.* Editorial Bdef.

Arocena, G & Belcarce, F. (2018). *Defraudaciones.* Editorial Hammurabi.

Díaz Aranda, E. (2018). *Manual de derecho penal*. Fondo de Cultura Económica.

García Cavero, P. (2019). *Derecho Penal. Parte General*. Ideas Solución Editorial.

Gil, A. & Hernández Berlinchez, R. (2019). *Cibercriminalidad.* Dykinson

Jescheck, H. (2002). *Tratado de derecho penal*. Editorial Comares.

Mayer, M. (2007). *Derecho Penal. Parte General.* Editorial Bdef.

Mir Puig. S. (2008). *Derecho Penal. Parte General*. Editorial Reppertor.

Miró Llinares, F. (2012). *El cibercrimen*. Marcial Pons.

Riquert Marcelo, A. (2020). *Ciberdelitos*. Editorial Hammurabi.

Roxin, C. (2014*). Derecho Penal. Parte General*. Editorial Civitas.

Salinas Siccha, R. (2013). *Derecho Penal. Parte Especial*. Editorial Grijley.

Sánchez Ostiz, P. (2008). *Imputación y Teoría del Delito*. Editorial Bdef.

Villavicencio Terreros, F. (2017*). Derecho Penal Básico*. Editorial de la Pontificia Universidad Católica del Perú.

Welzel, H. (1956). *Derecho Penal. Parte General*. Roque Depalma Editor.

Fuentes hemerográficas

García Cervigón, J. (2008). El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. Revista cuatrimestral de las facultades de derecho y ciencias económicas y empresariales. 74, 289-308.

Fuentes electrónicas

El Peruano (2021). Ciberdelitos en el Perú. https://elperuano.pe/noticia/121876-ciberdelitos-en-el-peru-se-elevan-denuncias-de-fraude-informatico-y-suplantacion-de-identidad

Riquert, M. (2014). Riquert Delincuencia Informática. http://riquertdelincuenciainformatica.blogspot.com/2014/11/estafa-o-fraude-informatico.html

Fuentes legales

Congreso de la República (1991). Código Penal Peruano.

Congreso de la República (2013). Ley N° 30096 – Ley de Delitos Informáticos

Congreso de la República (2014). Ley N° 30170 – Ley que modifica el artículo 1 de la Ley 29631

Congreso de la República (2014). Ley N°30191 – Ley que modifica la Ley de Delitos Informáticos

Consejo de Europa (2001). Convenio de Budapest.

Consejo Europeo (2022). Informe explicativo del Convenio de Budapest.

Jefatura del Estado (1995). Código Penal Español.

Ministerio de Educación y Justicia (1984). Código Penal de la Nación Argentina.