El delito informático

Álvaro Burgos-Mata *

Algunos juristas se han referido al fraude informático como un fenómeno de gran magnitud y trascendencia en el ámbito de la criminalidad mediante computadoras y núcleo central del delito informático desde el punto de vista criminológico, es por esta razón que existe una dimensión de la delincuencia informática a la que a la doctrina presta una especial atención, por considerarla el terreno hasta ahora más inexplorado y el que mayores dificultades presenta para su prevención y detención. Por ello, no extraña descubrir con frecuencia (en el lenguaje común, pero también en el mundo jurídico) la confusión entre *ilícito informático* y *fraude informático*, identificándolos como una sola cosa.

En un inicio, el término *fraude informático* venía a considerarse como *aquel delito que era cometido a través de ordenadores*, con lo cual se constituía en un grupo uniforme de delitos, que eran mayoritariamente de índole económicos, con el gran inconveniente de que se llegó a similar o equiparar con la conceptualización de los delitos informáticos.

* Dr. Derecho Penal y Criminología, Máster en Psicología Forense, Especialista en Ciencias Penales. Juez Coordinador del Tribunal Superior Penal Juvenil y Juez de Juicio del II Circuito Judicial de San José; Catedrático de Derecho Penal Especial y Criminología de la UCR, Profesor de la Maestría en Ciencias Penales de la UCR., del Programa Doctoral en Derecho Penal de la U. Escuela Libre de Derecho y de la Maestría en Psicología Forense de la UNIBE.

Consecuentemente y debido a la progresiva diversificación de conductas y finalidades perseguidas por los delincuentes informáticos, el término *fraude informático* se fue restringiendo para ser utilizado de la siguiente manera:

> *…En la descripción del ilícito económico vinculado a la información por excelencia, pero limitándose inicialmente al ámbito del fraude patrimonial mediante manipulaciones por medios informáticos, es posteriormente, a finales de los ochenta, cuando este ilícito va nuevamente extendiéndose conceptualmente para describir un espectro de varios supuestos distintos dentro del campo de los delitos económicos…*[1]

Para poder definir lo que se entiende por *fraude informático*, es necesario primero aproximarse a una definición de lo que es *el fraude*, y segundo, a una definición de lo que es *la informática*, con la intención de lograr una mayor delimitación del concepto en conjunto.

El Artículo 217 bis de nuestro Código Penal establece:

> *Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener u beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.*

Con respecto a la palabra *fraude*, en el lenguaje común (así como sus derivados *defraudar, fraudulento, defraudación*) se identifica con la idea del engaño, aquel en el que media malicia y que se dirige a provocar algún tipo de perjuicio (generalmente patrimonial). El diccionario de la Real Academia Española lo define así:

> *1) Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete. Se trata de inducir, mantener o reforzar el error en la víctima, con el designio de lograr de ella una disposición patrimonial.*[2]

1 ROVIRA DEL CANTO (Enrique), *Delincuencia Informática y fraudes informáticos,* Granada, Editorial Comares, 2002, p.242.

2 *Diccionario de la Real Academia Española,* vigésima primera edición, tomo 1. Madrid, Editores Espasa Calpe, 2002, p. 994.

Se señala que el término *fraude informático* puede prestar a confusión y no está bien utilizado. Al referirse a la palabra *fraude* tanto en su lenguaje cotidiano como jurídico, se pretende hacer referencia a la realización de un *modus operandi* que se caracteriza por un determinado comportamiento, que implica la presencia dominante de un montaje o artimaña ideal que desencadena determinada modalidad de acción (astuta, artera, subrepticia, engañosa, falsa, etc.). Según esto, el fraude y lo fraudulento presuponen el empleo primordial de artificios o medios intelectuales para elaborar cierta maquinación que, aunque encuentran en el engaño su máxima expresión, no quedan en el mismo agotados.

Es importante mencionar que para que exista fraude como categoría autónoma, es decir, como defraudación, se precisa algo más. La conducta astuta, engañosa, subrepticia, realizada con *animus decipiendi*, no interesa al derecho penal si no existe lesión o puesta en peligro de un bien jurídico, que es lo que justifica la intervención punitiva estatal.

Desde este punto de vista, señala el autor Reyes Vásquez[3], la necesidad de considerar el término *defraudación* en un sentido amplio, refiriéndose a la causación de un perjuicio económico (no necesariamente patrimonial) mediante una dinámica comitiva ideal, intelectiva (modus operandi fraudulento, con un fuerte componente subjetivo, intencional).

Por su parte, cuando se hace alusión a las *defraudaciones*, se refiere al prejuicio económico ocasionado mediante fraude. Cuando se habla de *fraude informático* se hace referencia, en forma especifica, no a cualquier tipo de acción fraudulenta que surge con la utilización de medios informáticos, sino únicamente, cuando lo dirigimos por la definición de contenido brindada a las defraudaciones.

Con respecto al término *informátic*a, ésta es el conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información. Por *informático* el tipo penal se refiere a aquellas conductas delictivas que son favorecidas, potenciadas o convertidos

3 REYES VAZQUEZ (Julio), *El delito de fraude informático en Costa Rica*, Tesis (licenciatura en derecho)- Universidad de Costa Rica. Facultad de Derecho, 2005. p. 98.

en más dañosos, y la vez más lucrativos, por la peculiaridad de los elementos informáticos y sus funciones propias (procesamiento, almacenamiento, tratamiento y transmisión de datos).

Lo informático del fraude está en el aprovechamiento, utilización o abuso de las características funcionales de los sistemas informáticos como instrumento para realizar una conducta astuta, engañosa, artera, subrepticia, con *animus decipiendi*.

Por lo anteriormente mencionado, es que algunos autores, como Chinchilla Sandí, prefieren la utilización de un término más preciso y completo, surgiendo, por ejemplo, el concepto *estafa informática* con el cual se lograría circunscribir de una mejor manera el campo de acción, con lo que se lograría una mayor seguridad jurídica, *"puesto que* fraude informático *"es un concepto muy amplio, donde se logran incluir conductas fraudulentas realizadas con la utilización de elementos informáticos, como podría ser el caso de sabotaje informático."*[4]

De distinta forma piensa el autor Reyes Vásquez[5], el cual prefiere aludir al término *fraude informático,* ya que a pesar de su ambigüedad, resulta a priori más conveniente que cualquier otra alternativa, por incompletas como la estafa informática o por excesivas como manipulaciones de datos, incapacitada para destacar la esencia criminal de estas conductas. Considera el fraude informático como el *término medio* ya que, por un lado, reúne lo informático y, por otro, el comportamiento defraudatorio criminal, lo adjetivo y lo sustantivo, respectivamente.

Por su parte, el autor Marcos Salt define el fraude informático como *"la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizadas con el objeto de obtener ganancias indebidas."*[6]

En otro sentido, señala Camacho Losa:

4 CHINCHILLA SANDÍ (Carlos), *Delitos informáticos, Elementos básicos para identificarlos y su aplicación.* 1 ed. San José, C.R: Ediciones Farben, 2004. p.112.

5 REYES VAZQUEZ (Julio), op.cit., supra, p.104.

6 SALT (Marcos G.), *Delitos no convencionales, artículo Delitos de carácter económico,* Editores del puerto, Buenos aires, 1994, p. 236.

> *[El fraude informático lo configura] el bloque de la delincuencia informática integrado por usos indebidos o manipulaciones fraudulentas de elementos informáticos de cualquier tipo (hardware, software, líneas de comunicación, información mecanizada, etc.), que posibilitan un beneficio ilícito.*[7]

Posteriormente simplifica la noción de *fraude informático* diciendo: *"toda conducta fraudulenta realizada a través o con la ayuda de un sistema informático por medio de la cual alguien trata de obtener un beneficio ilícito."*[8]

De dicha conceptualización se puede afirmar que se presentan las notas características del fraude informático que se aprecian en la mayoría de las definiciones:

1- Conducta fraudulenta (sin profundizar en lo que debe entenderse por fraudulento): consiste en un uso indebido o una manipulación fraudulenta de elementos informáticos.
2- La presencia de los componentes físicos y/o lógicos del sistema informático como instrumento de auxilio de la conducta.
3- La finalidad perseguida de obtener un beneficio ilícito (elemento subjetivo que se concreta en el ánimo de lucro injusto).
4- La producción de un prejuicio a otra persona.

En el fraude la naturaleza del medio ejecutivo para llevar a cabo el delito exige un actuar de modo consiente, meditado, pensado y no improvisado ni negligente.

De esta forma se puede concluir que el *fraude informático* es la acción en la cual el sujeto activo modifica o adultera, por cualquier medio, la información o los datos contenidos en el equipo de computo del sujeto pasivo, a fin de inducir al mismo a un error en su procesamiento, o bien obtener de ella un beneficio económico para sí o un tercero. Requiere, por un lado, la conducta fraudulenta, la cual necesita cierta maquinación, engaño, donde se tiene que considerar la intención de defraudar, es decir,

7 CAMACHO LOSA (L), *El delito informático*, Madrid, 1987, p. 25-27.
8 CAMACHO LOSA (L), op. cit., supra, p.28.

refiriéndose a la causación de un perjuicio económico, y, por otro lado, este perjuicio económico se causa única y exclusivamente por medio o sobre algún ordenador, es decir siempre va a estar presente algún medio informático para la comisión del ilícito.

Bien jurídico tutelado

Con relación al bien jurídico tutelado, se puede afirmar que, por la naturaleza del fraude informático, es un delito de carácter patrimonial, pero, por sus peculiaridades de dinámica comisiva y el que, por algunos de sus elementos aparecen también grandes similitudes con los delitos de sustracción o apoderamiento patrimonial, puede llegar a ser considerado como un delito de naturaleza mixta (apoderamiento-defraudatoria).

Se trata de una defraudación patrimonial realizada por medios informáticos o sobre estos, la cual atenta contra el patrimonio económico de un individuo y, generalmente, de personas jurídicas. Sin embargo, parte de la doctrina cree que simultáneamente se tutelan la intimidad y la propiedad.

La intimidad se ve conculcada por el simple ingreso de un tercero no autorizado a un equipo informático ajeno; es un delito que ataca expresamente la privacidad al penetrar en una esfera de conocimientos reservada expresamente a su titular; y si el sujeto activo produce además alguna anomalía funcional o extrae información de forma ilegítima de ese equipo al cual ingresa, se ve profanada la propiedad, pues se produce un detrimento patrimonial y se produce un daño. Incluso, aunque el sujeto pasivo no pierda la posesión efectiva de los datos extraídos, esta estaría también en posesión de otra persona.

Se han diferenciado diferentes tipos de modalidades de fraude informático en el ámbito patrimonial, atendiendo al objeto sobre el cual recae:

1) Manipulaciones informáticas directas: consiste en las principales conductas que figuran en el fraude informático, como lo son las manipulaciones en la llevanza, tratamiento o procesamiento informático de operaciones mercantiles, facturas,

pagos de sueldos o salarios de empresas, de cuentas y anotaciones bancarias, así como en asientos contables, balances o incluso inventarios.

En este tipo de modalidad, las principales víctimas son las grandes empresas y entidades bancarias tanto en las propias terminales como también en sus propios sistemas internos, posterior y, aproximadamente en la década de los noventas, se comenzaron a dar los delitos desde puntos externos a dichos sistemas a través de las redes informáticas y telemáticas.

Con las conexiones de ordenadores a las redes internacionales de telecomunicación se facilitó en gran medida la comisión de ilícitos informáticos desde la planta física de la empresa-victima del delito.

Como ejemplo de lo anterior, se dio un caso en Estados Unidos en 1994 donde un grupo de delincuentes rusos, operando desde San Petersburgo, logró acceder al sistema informático del Banco Norteamericano y efectuar una transferencia a su favor de diez millones de dólares.

Como consecuencia del avance tecnológico y la necesidad imperiosa de ser competitivo en el mundo globalizado, la mayoría de las grandes empresas, sin dejar de lado las medianas y pequeñas compañías, están conectadas a internet y a otras redes informáticas con el objeto de facilitar la realización de trámites o negocios de distintas índoles. Con el gran inconveniente de que internet cada vez es más utilizada para cometer todo tipo de manipulaciones por medio o sobre ordenadores.

Frecuentemente los autores de estos tipos de delitos se aprovechan de las insuficientes y limitadas medidas de seguridad en los sistemas informáticos o bien de la inexperiencia de los administradores de los mismos sistemas.

2) Abusos de tarjetas magnéticas de crédito y de debito y otros medios similares de pago: conforman el segundo grupo de fraudes informáticos, los cuales se han desarrollado a finales de los ochenta. Con respecto a esta modalidad de ilícito, es necesario mencionar que el perjuicio causado la mayoría de las veces responde a pequeñas cuantías económicas.

Las formas como se lleva a cabo este delito se extienden desde el uso simple de tarjetas robadas, pasando por la manipulación de las mismas con la ayuda de ordenadores, hasta la fabricación independiente de tarjetas auténticas. Aparte de estas tarjetas, se manipulan otras tarjetas magnéticas, como las tarjetas telefónicas o las tarjetas para las apuestas hípicas.

Para la realización del delito los autores consiguen el *pin* necesario para el uso de la tarjeta, llevando a cabo una llamada telefónica falsa, preparando y manipulando el teclado, usando un teclado falso o, incluso, interviniendo las líneas telefónicas de datos.

Con relación al uso de tarjetas telefónicas, el caso de unos jóvenes alemanes que, con éxito, en 1994, copiaron unas tarjetas telefónicas con *chips* integrados, descodificaron las señales de las tarjetas usando cables de adaptador y ordenadores pequeños con los que entonces simularon las señales de sus propias tarjetas inteligentes, pudiendo ser usadas en forma permanente.

3) Abuso de la red telefónica y de telecomunicaciones: constituye el tercer grupo de modalidad defraudatorios por medios informáticos. Ha sufrido a través de los años cambios cuantitativos, llegando a convertirse en un delito en masa.

En los años sesenta los autores de este tipo de ilícito solo buscaban evitar el pago de sus propias llamadas telefónicas. Sin embargo, a finales de los años ochenta, surgieron técnicas que fueron creadas por *hackers* y fueron usadas también por empresas que ofrecían conversaciones telefónicas intercontinentales. Y en los años noventa empezaron a surgir manipulaciones financieras donde se daba la transferencia de dinero a través de compañías telefónicas.

En los años sesenta se desarrolló lo que se denominó la caja azul o blue box, la cual se basaba en el hecho de que en la red telefónica analógica tradicional, los tonos de control para establecer conexión transmiten a través de la misma línea que la información y, por tanto, pueden manipularse con la ayuda de la blue box. De esta forma, se hacía uso de la red telefónica internacional, pero el servicio nunca era pagado, ya que se hacían una o varias llamadas libres de recargo.

Actualmente, se usan otras técnicas de manipulación donde se llevan a cabo llamadas telefónicas a expensas de otros usuarios de la red, mediante la intervención de sistemas de mensajes de voz protegidos de manera inadecuada, lo cual permite la función de marcado directo.

Otra forma de manipulación consiste en el comercio de números de tarjetas de prepago, los cuales son vendidos por empleados de las compañías telefónicas o los números de las tarjetas son interceptados introduciéndose en un ordenador o escuchando las llamadas telefónicas en forma secreta. Con este tipo de manipulación en los años noventa afloró sobre todo en Alemania el uso indebido de *las líneas sexuales*. Con respecto a este tipo de delitos, obviamente el elemento configurador es el ánimo defraudatorio.

4) Manipulaciones telemáticas: es una modalidad de fraude informático que ha ido creciendo cada vez más con la utilización de internet, donde se logra engañar al usuario y consumidor en general, mediante anuncios falsos e incluso paginas web simuladas, llamadas *web spoofing*.

Esta modalidad consiste en la simulación de una pagina web ya existente, normalmente de una entidad bancaria o financiera, que, aprovechando la falta de conocimientos del usuario que pretende contactar con el servidor de esta, las deficiencias de programación del equipo o sistema informático que de forma automática efectúa el contacto y va a materializar la operación, o la ausencia de medidas de seguridad para garantizar la autenticidad de la web, cae en el servidor falso y le facilita sus datos bancarios o información de contenido económico patrimonial, lo que va a permitir al delincuente informático el aprovecharse de tal información para efectuar en su beneficio y en perjuicio de aquel transacciones, pagos, transferencias electrónicas de fondos o cualquier tipo de operación bancaria o mercantil.

A pesar de las anteriores modalidades de fraudes informáticos, el mismo va a estar subordinado a una mayor amplitud de conocimientos informáticos, como pueden ser violentados nuevos bienes jurídicos (por ejemplo programas, datos, la información en sí misma, así como su almacenamiento,

tratamiento, procesamiento transferencia en las redes y sistemas informáticos), donde necesariamente se diferenciaría de los otros delitos informáticos por la concurrencia del elemento específico del ánimo defraudatorio.

Análisis del tipo penal

Elementos objetivos:

Pertenecen al aspecto objetivo el sujeto activo, pasivo, la acción por el medio informático, el resultado producido mediante el fraude y la relación de causalidad.

Se puede afirmar que el fraude informático es el delito más común y conocido dentro de los llamados *delitos informáticos*:

> *Y probablemente el más antiguo, pues se tienen noticias de fraudes cometidos con computadoras que datan de la tercera generación, cuando estas hicieron su aparición en la vida laboral de empresas de tipo financiero y bancario.* [9]

Las formas en que se puede llevar a cabo un delito de fraude informático pueden ser muy variadas, pero siempre van a tener como común denominador el uso ilegítimo de los medios informáticos, ya que los medios para llevar a cabo estos ilícitos derivan propiamente de la naturaleza intrínseca de los sistemas informáticos.

Existen cinco presupuestos fundamentales para poder llevar a cabo un delito de fraude informático:

- Debe tratarse de un sistema automatizado por lo que consecuentemente los sistemas manuales quedan excluidos.
- El sistema debe ser capaz de almacenar información óptica o magnética.[10]

9 Opinión jurídica de la Procuraduría General de la República, número OJ-154-2001, del 24 de octubre de 2001, p. 26.

10 De manera óptica consiste en almacenar información por medio de discos compactos, CD de lectura o escritura o en general sobre cualquier superficie que tenga la capacidad de transformar la información a números y pueda ser recuperado por medio de instrumentos que pueden leer por medio de rayos láser. La magnética consiste en guardar en superficies metálicas o que se tenga la posibilidad de almacenar información electromagnética, ejemplos, discos duros o disquetes.

- El ordenador debe utilizar un programa particular que es exclusivo para manejo de información por medio del sistema de base de datos.
- El sistema tiene que residir en una plataforma de computadoras.
- Deben existir usuarios que tengan posibilidad de acceder al sistema para introducir, modificar, borrar o consultar información.

Sujeto Activo y Pasivo

En cuanto al estudio de sujetos en este tipo de delitos se encuentra como sujeto activo lo que la doctrina denomina como *delicta communia* y se deduce de la frase del artículo *la persona que*, con lo que se hace referencia a que se puede tratar de cualquier persona, no necesita el autor tener una condición especial para calificar dentro del supuesto, sin embargo, hay que considerar que este tipo de infractores tienen capacidades intelectuales un poco más arriba del promedio, incluso se les ha llegado a calificar de esta manera[11]:

- *Hacke*r: la persona que disfruta explorando detalles de los sistemas programables y aprendiendo a usarlos al máximo, al contrario del operador común, que en general se conforma con aprender lo básico. Estos sujetos tienen altos conocimientos de informática. Su mayor motivación la encuentra en la vulneración de *passwords* o claves de acceso. El *hacker* realiza el llamado *intrusismo informático* o *conductas de hacking*. Estas conductas se refieren al conjunto de comportamientos de acceso o interferencia no autorizados a un sistema informático o red de comunicación electrónica de datos y a su utilización de forma oculta.
- *Cracker:* se trata de un autodidacta de la informática, que compite con el *hacker*, pero no cuenta con sus conocimientos. El *cracker* desconoce los sistemas informáticos y se limita a la vulneración de los programas (software); realiza acciones de piratería informática, como la copia ilegal de programas informáticos con violación a los derechos de autor.
- *Preacker*: se trata del arte y la ciencia de *crackear* la red telefónica para obtener beneficios personales. Por ejemplo, llamadas gratis de larga distancia.

11 CHINCHILLA SANDÍ, op.cit., supra, p. 55-56.

En este caso cabe la figura de la autoría mediata, coautoría, del instigador y el cómplice.

Se ha señalado, por lo mismo, la necesidad de que el tipo contemple distintas penas dependiendo del sujeto activo que cometió el delito. Es decir, no es lo mismo que el delito lo cometa un sujeto que sea especialista en delitos informáticos y, por ende, tenga a su cargo la revisión y mantenimiento del equipo informático de cualquier entidad estatal o privada, con lo cual aprovechándose de su cargo y las facilidades que este le brinda cometa el delito, a un sujeto que no cuente con dichas características.

El tipo penal podría, en este sentido, prever tres tipos de sujetos activos de conformidad con la teoría de los sistemas, la cual indica que existen tres fases de los sistemas informáticos: la manipulación en el ingreso de los datos (*insiders*), la manipulación de datos ingresados, que es propiamente el procesamiento (conocida como *técnica del caballo de Troya*) y la manipulación en los datos de salida (*outsiders*).

Con respecto a la manipulación en el ingreso de datos, resulta ser la conducta más común en el fraude informático, de fácil comisión y con mucha dificultad para descubrir el delito.

En esta fase no se requiere que el sujeto activo posea especiales conocimientos informáticos, sino que tenga acceso a las normales funciones de procesamiento de datos en la fase de adquisición de los mismos:

> *La introducción y el almacenamiento de datos, corresponde al paso inicial del procesamiento de los mismos por medio de la computadora. Una vez ingresada la información, la misma computadora, con aplicación de los programas que posee, procede a ordenarla, para posteriormente ser utilizada.*[12]

Para ejemplificar, se puede citar un caso en Costa Rica donde una empleada del poder judicial tenía bajo su poder el ingreso de datos a la planilla, con lo que incluyó como juez a un compañero de ella, sin que el mismo realizara nunca dicha labor y, mucho menos, haya sido nombrado para tal cargo, recibiendo el salario respectivo que le correspondería eventualmente a un juez.

12 CHINCHILLA SANDI, op. cit., supra, p.41.

En tanto a la manipulación de datos ingresados, el sujeto activo controla los datos que contiene el computador, *"alterando los programas existentes en el sistema de la computadora y, también, en insertar nuevos programas o nuevas rutinas."*[13]

Menciona el autor Chinchilla Sandi el ejemplo del sujeto que manipula la información aduanera, logrando que no se pague la totalidad de derechos de aduana que corresponde por la importación de materia prima al país, por lo que se pagaría solo parte de los impuestos que debía pagar.[14]

El método conocido como *Caballo de Troya*[15] es utilizado por aquellas personas que tienen conocimientos especializados en programación informática. Dicho método consiste en insertar instrucciones de computadora en forma encubierta en un programa informático para que se pueda realizar una función no autorizada al mismo tiempo que su función normal.

Con base en lo anterior y analógicamente *Caballo de Troya* consiste en *"un programa legítimo que contiene una sección de código oculto, a simple vista parece inofensivo, pero cuando se procesa, se activa el mismo y provoca graves distorsiones a los sistemas informáticos"*.[16]

La última fase de la teoría de los sistemas es la manipulación en los datos de salida, conocida también como *outsiders*. Cuando los datos se transfieren a otra computadora, en los programas de impresión (*output*), o en programas de actualización, es decir, una vez que los datos son ingresados, ordenados y los procesos de cálculos elaborados, la información final, por lo general se imprime y se almacena. Es posible manipular la información que se imprime y se almacena, de manera tal que la alteración no pueda detectarse, durante el procesamiento de datos.

13 Ibidem.

14 En este caso se aplicaría el artículo 221 inciso b de la ley de aduanas cuya pena oscila de uno a tres años.

15 El nombre se debe al episodio de la Ilíada de Homero, Ulises diseñó una estratagema mediante la cual regala a los troyanos un gran caballo de madera que en el interior oculta soldados, con lo cual hacía creer que el ejército griego abandona el sitio de la ciudad. Confiando los troyanos que efectivamente se trataba de un regalo de los vencidos en guerra ingresan el caballo en el recinto amurallado de Troya y aprovechando la noche y confianza de los habitantes, los guerreros ocultos hicieron entrar a las tropas griegas que aguardaban en las puertas de la ciudad, la cual invadieron.

16 CHINCHILLA SANDI, op. cit., supra, p. 42.

El ejemplo más representativo:

> *[El caso del que se realiza] en los cajeros automáticos mediante falsificación de instrucciones para la computadora en la fase de adquisición de datos. Inicialmente, dichos fraudes se ejecutaban con tarjetas bancarias robadas, pero actualmente se utilizan equipos y programas especializados para las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.*[17]

Como se puede apreciar, fácilmente se requiere un conocimiento más especializado para cometer un fraude en la fase de procesamiento de datos que en la fase de ingreso o salida de datos, por esta razón se sostiene la necesidad de que existan distintas penalidades, debe castigarse, según la fase en la que se haya cometido el delito, bajo esta premisa deberían existir tres tipos de sujetos activos.

Bajo esta tesitura, aquella persona que cuenta con una mayor posibilidad de ingresar a un sistema informático debe ser acreedor de una pena más alta, tomando en consideración que el 90% de este tipo de delitos son cometidos por este tipo de personas.

Diferente regulación prevé el tipo penal 196 bis del código penal llamado *"violación de las comunidades electrónicas"*:

> *Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, acceda, modifique, altere, suprima, intercepte, interfiera, utilice, difunda, o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes. Electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.*

Como se puede apreciar fácilmente, este tipo penal prevé dos tipos de sujetos activos, aquellos que por la labor que realizan, cuentan con una mayor facilidad para llevar a cabo el delito y, por otro lado, los sujetos que no cuentan con estas características.

17 Ibidem.

Opina sobre lo tratado el Lic. Reyes Vásquez, diciendo que no comparte la tesis en el sentido que, al momento de penalizar la conducta del delito de fraude informático, la pena vaya a depender del sujeto que llevó a cabo el delito, sino que propone que la pena dependa del monto defraudado:

> *El delito de fraude informático establece una pena de prisión de uno a diez años sin especificar nada más. Considero más apropiado tipificar distintas penas dependiendo del monto que haya sido sustraído por medio del delito y aunado a lo anterior podría aumentar la pena en un determinado porcentaje, si el delito fuese llevado a cabo por un sujeto que tuviese una mayor facilidad para ingresar al sistema informatizado.*[18]

El delito de fraude informático establece como condicionante *"la intención de procurar u obtener un beneficio patrimonial para si o para un tercero…"*, razón por la cual se sugiere establecer las penas de dicho delito en razón del monto que fuese defraudado.

Acción

La acción que es punible en este delito se estructura como una conducta de carácter doloso, siendo el mismo un delito de resultado, donde lo que se persigue es el beneficio patrimonial para sí o para un tercero.

Con respecto a la estricta configuración de la acción típica del delito, viene referida únicamente al verbo *influir*, por lo que la regulación de este delito es algo imprecisa y a la vez deja al juez la tarea de completar el contenido del verbo típico de la acción penal debido a que no se tiene claro dicho concepto.

Aunado al verbo *influir* como acción típica del delito, se describen los medios para lograr la obtención del resultado, esto es, en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos, cualquier otra acción que incida en el proceso de los datos del sistema como elementos descriptivos.

Un gran problema que presenta este tipo penal es que tipifica como delito el influir *"en el procesamiento o el resultado de los datos…"*.

18 REYES VAZQUEZ (Julio), op.cit., supra, p.221.

De acuerdo a la teoría de los sistemas, estaría fallando una parte fundamental para tutelar los delitos que son cometidos por medio del fraude informático. Aunado a lo anterior, el proyecto de reforma al código penal tampoco contempla alguna variante con relación a este tipo penal, por lo que seguiría contemplando las deficiencias típicas que he venido apuntando.

Dicha teoría señala tres fases en un sistema informático: la entrada, el procesamiento y el resultado de datos. Como se puede apreciar claramente, este tipo penal tutela únicamente la manipulación de datos en la segunda y última fase de un sistema informático, es decir, comprende la fase de procesamiento y resultado de datos, pero dejó excluida la parte más importante: la entrada de datos.

Es menester mencionar que casi todas las defraudaciones informáticas se generan en la entrada de datos, conocida también como *insiders*. Se cometió un grave error por cuanto se deja por fuera la mayoría de las conductas que deberían ser comprendidas por el tipo de fraude informático tal y como lo prevén otras legislaciones.

Se podría pensar que, con la simple inclusión de *procesamiento* se comprendería este *ingreso* de datos, lo cual resulta sumamente artificial y alejado de la realidad del quehacer informático, pues el *procesamiento* del tipo penal trata de la manipulación o alteración de los datos ya *ingresados* al sistema informático, como un paso posterior a ese olvidado *ingreso.*

Otro problema que presenta el artículo del fraude informático es la confusión de términos, dicho tipo describe el influir en el procesamiento o el resultado de los datos de un *sistema de cómputo.*

Por *sistema de cómputo* debemos entender cualquier conjunto de computadoras que se encuentran entrelazadas por medio de una red o bien en sí en la parte física del computador.

En otro sentido, *sistema de información* es un conjunto de datos, es decir, elementos descriptivos de algo (parte lógica) que por medio de una programación ya establecida en el sistema arrojan cierta información.

Una vez aclarados los términos, se puede apreciar que el tipo penal lo que debería regular es el sistema de información y no propiamente el sistema físico del ordenador. Un punto importante a señalar es que el tipo penal solo menciona *datos*, pero no se toma en cuenta que el resultado final que se obtiene por medio de los datos es información, por lo que también debería hablarse de información.

El proyecto de ley de delito informático define *dato informático* o *información* de la siguiente manera:

> *Toda aquella representación de hechos, manifestaciones o conceptos en un formato que puede ser interpretado y tratado por un sistema informático, además se incluyen los sistemas de bases de datos".*[19] *Con respecto a la descripción de las conductas para llevar a cabo el delito, se establece "mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema".*

La parte que indica "*mediante programación"*, va referida al acceso a la caja negra, el cual se logra mediante programas fuentes comprendiendo la fase de procesamiento de datos según la teoría de los sistemas.

El problema surge cuando se menciona "*empleo de datos falsos o incompletos, uso indebido de datos…"*, esto por cuanto solo se puede llevar a cabo mediante la entrada de datos, que es la parte dentro de la teoría de los sistemas que el tipo penal no comprendió.

En relación a la frase *"o cualquier otra acción que incida en el proceso de los datos del sistema,"* no hay mayor inconveniente, ya que esta parte va referida a la ultima etapa de la teoría de los sistemas, que corresponde a la fase de resultado de datos.

Es relevante mencionar que existe en tramite parlamentario un proyecto de ley denominado *"Ley de delito informático"*[20], el cual sugiere una nueva redacción del tipo fraude informático (denominado en dicho proyecto fraude por computadora, artículo 4).

19 CHINCHILLA SANDI op. cit., supra, p. 112.

20 Proyecto de Ley de Delito Informático no 15.397, del 8 de setiembre de 2009, de la Comisión permanente de asuntos jurídicos de la Asamblea Legislativa, artículo 1.

La redacción de dicho artículo está estructurada en tres incisos: el primer inciso tipifica la fase de entrada de datos, el segundo inciso comprende la fase de procesamiento de datos y el tercero pena la fase de resultado de datos. Cada uno tiene su respectiva pena.

En mi criterio resulta de una mejor tipificación y redacción dicho proyecto tomando en consideración las deficiencias que he venido señalando del actual tipo penal, máxime si el proyecto de reforma al código penal no contempla ningún cambio para este tipo.

Resultado

Tenemos como *conditio sine qua non* que la lesión de los bienes jurídicos mencionados debe ser producto de engaño y la acción debe incidir en el proceso de los datos del sistema con el fin ya mencionado (fraude). Si hay consentimiento de su titular a sabiendas del resultado, hay atipicidad; así también si la única acción fuere la intromisión al sistema (acto preparatorio) sin influir en los datos de este, pues estamos ante un delito de resultado, no de peligro abstracto.

Con base en lo anterior se puede señalar que el bien jurídico tutelado en este delito es el patrimonio. Surgiendo el siguiente problema, aquel sujeto que "…influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de datos del sistema", pero sin la intención de procurarse un beneficio patrimonial para sí o para un tercero estaría quedando excluido del delito de fraude informático, esto por cuanto dicho delito establece como condicionante para llevarse a cabo el ánimo de lucro.

Razón por la cual sugiere la necesidad de ampliar el bien jurídico tutelado en este delito, ya que deja por fuera todas aquellas conductas que no tengan como finalidad el ánimo de lucro. Ante esta situación la posible solución inmediata sería la aplicación del delito de violación de las comunicaciones electrónicas, regulado en el artículo 196 del código penal.

La finalidad perseguida por el sujeto activo, con su acción de influir en el procesamiento o el resultado de los datos, es lograr directamente una transferencia real de objetos materiales o inmateriales existentes (de cualquier activo patrimonial), bien trasladándose de lugar (anotación contable, entre cuentas corrientes, entre entidades de crédito, su entrega material al autor o a un tercero) bien procediendo, cuando fuera posible, a la anulación o cancelación mediante la supresión o compensación de los datos, sea todo ello efectuado directamente por el autor; o a través de la programación, empleo de datos falsos, o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

Con base en lo anterior, no existe un acto de disposición por parte del sujeto pasivo, sino que el propio autor del delito mediante su manipulación en el sistema obtiene directamente la transferencia patrimonial, tomando en consideración que dicho desplazamiento patrimonial nunca fue consentido por el titular del bien que fue sustraído.

Nexo Causal

La misma debe existir entre la influencia que tiene el sujeto activo en el procesamiento o resultado de los datos de un sistema mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso y el beneficio patrimonial que se procura para sí o para un tercero.

El texto define la acción típica referida al verbo *influir* y a la vez opera una restricción al dársele relevancia penal únicamente cuando tal influencia es ilícita, es decir, va dirigida a obtener un beneficio patrimonial que nunca fue concebido y operó en perjuicio ajeno.

Vinculada la acción y el bien jurídico tutelado (patrimonio), lo importante es que el tipo prevea las posibles influencias o manipulaciones informáticas que tienen la capacidad de realizar una disposición o acto patrimonial dañoso para un tercero.

Es necesario mencionar que en este tipo de delito figura una relación de causalidad directa, es decir, basta con la manipulación

que realizó el sujeto activo sobre el ordenador para que se diera un beneficio patrimonial para este o un tercero.

Elementos subjetivos

Los elementos esenciales de carácter subjetivo, prácticamente coincidentes con los requeridos para la estafa genérica y los delitos defraudatorios y de enriquecimiento, así como para muchos otros delitos patrimoniales son dos: el dolo y ánimo de lucro.

Dolo

El dolo es el conocimiento y la voluntad de la realización del delito. Estamos ante un tipo doloso, en este caso el dolo sería de engañar, manipular o influir en el procesamiento de datos informáticos ajenos para obtener un beneficio patrimonial para sí o un tercero.

Aparece como un elemento subjetivo fundamental y esencial en este tipo delictivo, lo cual se refleja con la utilización en el texto de la frase *"con la intención de"*, en el sentido de que el sujeto tenga el conocimiento y voluntad de la realización de los restantes elementos del tipo, es decir, acción, resultado y relación de casualidad.

Aunado a lo anterior, el sujeto debe conocer y estar consciente de los medios a través de los cuales pretende llevar a cabo el resultado de la acción, es decir, por medio de la manipulación de un sistema informatizado dirigida a lograr la finalidad de obtener un beneficio patrimonial indebido, no consentido y perjudicial para un tercero.

> *Cierto que estadísticamente muchos supuestos de afectación o alteraciones de datos, programas, información informatizada, e intervención de la misma en las vías de transferencia y transmisión informática y telemática se producen de forma imprudente, negligente, incluso por parte de operadores o técnicos especializados.*[21]

No es necesario un dolo específico o directo, sino que incluso basta con un dolo genérico, siendo factibles todas las modalidades

21 ROVIRA DEL CANTO, op. cit., supra, p. 597.

de dolo, incluso el dolo eventual, o sea, que el sujeto activo se represente el resultado (el beneficio patrimonial) como posible y aunque no quiera producirlo, siga actuando y admita su eventual realización.

Es necesario que el actuar del sujeto activo sea de modo consciente y meditado no solo referido a la utilización del sistema informatizado, por la utilización del verbo *influir,* sino también en cuanto al resultado perseguido, es decir, obtener, procurarse, lograr, conseguir, alcanzar la finalidad previsto por el tipo penal que sería el beneficio patrimonial para sí o para un tercero. Con base en esto queda consecuentemente entendido que este tipo constituye única y exclusivamente un delito de acción dolosa.

Por ende, no podrían ser sancionables aquellas conductas imprudentes, negligentes o torpes en cuanto a la utilización o manipulación de un ordenador, ni en cuanto al logro del resultado, ya que el delito de fraude informático exige para su configuración en sus elementos subjetivos el ánimo de lucro que veremos seguidamente.

Ánimo de lucro

Constituye el otro elemento específico subjetivo requerido por el tipo penal entendido como *"ánimo o intención de enriquecimiento injusto, propio o de un tercero, correlativo al perjuicio patrimonial ajeno."*[22]

El ánimo de lucro constituye, pues, la intención de obtener o procurarse para sí o para un tercero, una ventaja o beneficio de índole patrimonial, el cual es ilícito, no consentido y en perjuicio de un tercero. El ánimo de lucro va ínsito en el carácter de valor patrimonial del activo transferido.

La intención *"de procurar u obtener un beneficio patrimonial"* es una voluntad dirigida a una finalidad, como ocurre en el dolo directo de primer grado (llamado también *intención*). La intención es, entonces, una voluntad dirigida a un comportamiento futuro o a un resultado todavía no ocurrido.

22 ROVIRA DEL CANTO, op. cit., supra, p. 598- 599.

Desde el punto de vista volitivo, el autor debe pretender alcanzar el beneficio patrimonial ilícito. El sujeto activo debe representarse la ventaja patrimonial y dicha representación debe influir en la resolución de realizar la acción. Por ende, no podría cometerse un fraude informático cuando el sujeto activo obtiene un beneficio patrimonial, pero como consecuencia necesaria o posible de un comportamiento dirigido a otra finalidad. Siempre debe mediar la intención del sujeto activo de enriquecerse en perjuicio ajeno por medio de la manipulación sobre el sistema informatizado.

Es importante mencionar que la presencia de este elemento (ánimo de lucro) termina de acreditar que este delito se trata de un delito meramente doloso, de intención y, por ende, resulta totalmente incompatible toda actuación culposa.

Formas de ejecución y participación

El delito de fraude informático es un ilícito de resultado material, consecuentemente exige para su configuración un efectivo perjuicio patrimonial ajeno, a través del desplazamiento patrimonial no consentido, el cual fue logrado por medio de la manipulación sobre el ordenador.

Con base en lo anterior, se puede señalar que el momento en que se logra consumar el delito es cuando se materializa o consigue, por parte del sujeto activo, la transferencia o desplazamiento patrimonial, siempre que esta suponga un perjuicio para otra persona, sea jurídica o física, ajena al autor del delito.

Por otra parte, si bien al ser el perjuicio el resultado material, y la consumación no se va a producir hasta que este no se materialice, dice que la tentativa exigirá la ejecución de la manipulación informática y que, difícilmente, se podrá diferenciar la tentativa acabada y la inacabada dado que la transferencia del activo patrimonial producirá automáticamente el perjuicio, aunque no implique paralelamente la obtención del beneficio económico.

Considera el autor Rovira Del Canto que si bien es cierto es posible la tentativa, es sumamente difícil la delimitación exacta entre la tentativa acabada y la inacabada; se podría considerar

que la tentativa acabada se da cuando se han realizado todos los requisitos de la acción, pero no ya cuando se ha obtenido la transferencia no consentida del activo patrimonial.

Por su parte, la tentativa inacabada abarcaría en el *iter criminis* desde el inicio de la realización o utilización de medio idóneo o la manipulación en el sistema informatizado, sin llegar a practicar todos los pasos necesarios para obtener la transferencia del activo patrimonial.

En principio, no existe ningún problema relativo a la participación en el delito de fraude informático, por lo que también le serían aplicables las reglas generales en la materia de participación.

Sería entonces tan imputable el sujeto que realiza materialmente el delito de fraude informático como también aquel que coopera o instiga de la siguiente manera:

> *Sin participar directamente en la realización o utilización de la manipulación, y teniendo conocimiento o habiendo obtenido las claves de acceso al programa o sistema informático, o las de neutralización de las medidas de seguridad establecidas, las facilitará al que efectúe la manipulación del sistema informatizado.*[23]

23 ROVIRA DEL CANTO, op. cit., supra, p. 603.

Bibliografía

Código Penal de Costa Rica Ley N°4573. Artículo 217 bis.

CHINCHILLA SANDÍ (Carlos), Delitos informáticos, Elementos básicos para identificarlos y su aplicación. 1 ed. San José, C.R: Ediciones Farben, 2004.

REYES VAZQUEZ (Julio), El delito de fraude informático en Costa Rica, Tesis (licenciatura en derecho)- Universidad de Costa Rica. Facultad de Derecho, 2005.

CÁMPOLI (Gabriel), Derecho Penal Informático. San José, C.R: Investigaciones Jurídicas, 2003.

ROVIRA DEL CANTO (Enrique), Delincuencia Informática y fraudes informáticos, Granada, Editorial Comares, 2002.

SALT (Marcos G.), Delitos no convencionales, articulo Delitos de carácter económico, Editores del puerto, Buenos aires, 1994.

CAMACHO LOSA (L), El delito informático, Madrid, 1987.

Diccionario de la real academia española, vigésima primera edición, tomo 1. Madrid, Editores Espasa Calpe, 2002.

Procuraduría General de la República, número OJ-154-2001, del 24 de octubre del 2001.

JURISPRUDENCIA:

14997-07 SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA.

00763-2006 SALA TERCERA DE LA CORTE SUPREMA DE JUSTICIA. San José, a las nueve horas veinte minutos del dieciocho de agosto de dos mil seis.

00726-2007 SALA TERCERA DE LA CORTE SUPREMA DE JUSTICIA. San José, a las diez horas cuarenta y cinco minutos del veinte de julio de dos mil siete.