INFORME DE INVESTIGACIÓN CIJUL

TEMA: FRAUDE INFORMÁTICO

RESUMEN: En el presente informe, se aborda el tema de los fraudes informáticos, desde la perspectiva penal y de la novedosa rama del derecho informático. A los efectos, primeramente se hace un análisis doctrinal, donde se examina la concpepción de fraude informático, así como las generalidades de este tipo de delitos, junto con las clasificaciones de lo que se ha llamado *hacking*. Poosteriormente se incorpora el artículo 217 bis del Código Penal, donde se tipifica el delito, así como un extracto jurisprudencial donde se abordan los requisitos para que se configure el delito informático.

Índice de contenido

DESARROLLO:

1. Doctrina

a. Concepto de Fraude Informático

[REYES VÁSQUEZ, Juilo R.][1]

“Dentro de nuestras fronteras, el delito de fraude informático esta regulado en el artículo 217 bis del Código Penal, siendo la reforma más relevante en materia de criminalidad informática.

Es menester mencionar que este tipo penal fue una copia casi íntegra del artículo del Código Alemán denominado "estafa por computadora" por ende le sería oponibles las mismas críticas que se realizaron antes de la sexta ley de reforma del Código Penal Alemán.

Dicha reforma "fue aprobada por el Deutsche Bundestag (Parlamento alemán) el 14.11.1997, se publicó en el BGBI (Diario Oficial alemán) 1998/1 164 ss. El 26.1.1198, entró en vigencia el 1 de Abril de 1998."

Se señala que el término "fraude informático" puede prestar a confusión y no esta 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...). 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."

"Por su parte, cuando se hace alusión a las "defraudaciones", se refiere al perjuicio económico ocasionado mediante fraude. Cuando se ha habla de "fraude informático" se hace referencia, en forma específica, 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."

Por lo anteriormente mencionado, es que algunos autores como Chinchilla Sandí prefiere la utilización de un término más preciso y completo, sugiriendo 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 que no propiamente se trata de específicas "estafas informáticas", sino de conductas fraudulentas realizadas con la utilización de elementos informáticos, como podría ser el caso del sabotaje informático."

De distinta forma piensa la autora Gutiérrez Francés la 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."

En otro sentido señala Camacho Losa que el fraude informático lo configura "como 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."

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."

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

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 perjuicio en otro.”

b. Generalidades sobre el Delito Informático

[LIBANO MANZUR, Claudio][2]

"Previo al análisis de esta especial modalidad comisiva debemos detenernos en dos precisiones de especial pronunciamiento.

En primer término, corresponde precisar que entendemos por delitos informáticos, para lo cual me permitiré citar la definición elaborada en conjunto con mi amigo y colega don Marcelo Huerta y plasmada en nuestra primera obra Delitos Informáticos.

Para ello diremos que Delitos Informáticos son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.

Estimamos que la definición entregada cumple con el requisito de ser omnicomprensiva de las distintas modalidades delictivas que con motivo de esta obra nos ha tocado conocer y de las distintas motivaciones que ellas tienen. Desde este punto de vista, la definición es de carácter amplio y especialmente operativa en el mundo del derecho. Por otra parte, es flexible y no restrictiva, toda vez que permite adscribirla a todo sistema de técnica legislativa que pretenda utilizarse, sea en la realidad nacional o en la experiencia extranjera como más adelante, y por primera vez, se entregará a la comunidad nacional interesada. Por otro lado, la definición es consecuente con nuestros postulados de internacionalización del derecho informático, así como con el necesario uso de una terminología clara y precisa sobre los conceptos técnicos y jurídicos que abraza.

En segundo término, y a grosso modo, me parece pertinente entregar nustra propia definición de los delitos informáticos. Así proponemos proponemos la siguiente clasificación de los delitos informáticos, a la luz del derecho comparado:

1. La manipulación indebida de datos a través de la utilización de un sistema de tratamiento de la información. El fraude informático.

Tal manipulación puede realizarse en la entrada de datos al sistema (input), en los programas, en la salida de datos del sistema (output), y siguiendo a Romeo, en el caso de manipulaciones a distancia, mediante la conexión telemática vía

módem a un computador.

Esta primera clasificación es de carácter general y envolvente, pues, por regla casi absoluta, todo delito informático se cometerá a través de una manipulación en cualquiera de las fases mencionadas.

2. Delitos de espionaje informático.

Se incluyen las formas de acceso no autorizado a un sistema de tratamiento de la información.

3. Delitos de sabotaje informático.

Incluyen las formas de destrucción y alteración de datos, así como los programas virus.

4. Delitos de piratería de programas.

Sólo en cuanto se traduzca en la copia indebida de programas por medios informáticos.

5. Delitos de hacking, en sus distintas manifestaciones que se analizarán más adelante.

Luego de estas prístinas distinciones, nos encontramos en condiciones de abordar el quizás el más fulgurante de los delitos informáticos. Para ello es menester formular ciertas precisiones aclaratorias.

El delito de hacking, por constituir fundamentalmente un acceso indebido o no autorizado, induce a la creencia, no errada por cierto, de que este ilícito se presentará como medio o herramienta de comisión de otros delitos informáticos ya tratados, y que, por lo tanto, su característica podría ser la de configurarse como un hecho delictivo necesario para la comisión de otros.

Tal hipótesis en cierta medida es verdadera y comprobable. En efecto, gran parte de las veces los daños o deterioros sufridos por un programa, el espionaje de datos, los fraudes informáticos o la piratería de software, se realizarán a través de un acceso indebido o contra derecho en los sistemas. En tal caso, estimamos que el acceso indebido, léase hacking, sería un delito que se perpetra como medio necesario para la comisión de un ilícito diverso, situación en que, para los efectos sancionatorios y de penalización, se aplicarían las normas generales del derecho penal que rigen el llamado concurso ideal de delitos.

Sin embargo, es legítimo preguntarse acerca de la originalidad e independencia criminológica y típica del delito de hacking, o de otra forma, sobre la posibilidad de que un delito como el que tratamos surja y se consume de manera no asociada o vinculada con los otros delitos informáticos.

Previo a responder directamente esta interrogante, es preciso deternernos a razonar sobre el problema de las motivaciones que entran en juego en la mente del delincuente y que lo inducen a cometer delito.

Es indudable que muchas veces el HACKER (persona que comete el delito de hacking) utiliza el acceso indebido a un sistema de tratamiento de la información con el fin de cometer un fraude informático, un espionaje de datos, piratería o sabotaje en sus distintas manifestaciones. En estos casos el ánimo del delincuente será cometer estos delitos y la violación a la prohibición de acceso no será más que un medio de consumación. Ante esta primera situación motivacional es necesario precisar que para que exista hacking, éste debe estar tipificado de alguna forma en una ley. Por ello, pueden presentarse algunas situaciones que es necesario revisar. En primer término, es posible que el delincuente, al acceder indebidamente a un sistema para cometer, por ejemplo, sabotaje informático, se enfrente a un tipo penal que sanciona el sabotaje y que incluye como elemento del delito el acceso indebido. En este caso, no será posible hablar de delito de hacking ya que el acceso contra derecho era parte integrante del tipo sabotaje. Puede también suceder que la disposición que tipifica el sabotaje informático no considere el acceso indebido como uno de sus elementos objetivos, situación muy probable por cierto en atención a que muchas veces los delitos se cometen por operadores que cuentan con una autorización que les franquea el ingreso a los sistemas, y en tal caso podría considerarse la posibilidad de aplicar un concurso de delitos de sabotaje y hacking en el evento que otra disposición legal regulara separadamente el acceso indebido como delito. Si tal norma no existe, se deberá sancionar exclusivamente el sabotaje.

Un segundo supuesto motivacional del hacker estará determinado por un ánimo que podríamos llamar "no dañoso". En efecto, es posible, y así ha ocurrido muchas veces, que el delincuente busque la violación de la negativa al acceso, entiéndase códigos, passwords, etc., como una forma de autoratificación de sus capacidades técnicas e intelectuales. El hacker perseguirá la satisfacción de lograr vencer un obstáculo y de demostrar que los programadores que dispusieron las medidas de seguridad no pudieron contra su inteligencia. Asimismo, dentro de esta motivación "no dañosa", se encuentran los hackers que buscan burlar los códigos de acceso con la finalidad del simple divertimiento o por razones de curiosidad. Estas conductas, a pesar de no causar un daño directo y tangible, son delitos en si mismas y deben, necesariamente, estar reguladas y sancionadas.

Luego de estas breves consideraciones, es factible pasar al estudio del delito de hacking, sus modalidades, y la casuística

que entregan los autores de las doctrinas comparadas.”

c. Clasificaciones del *Hacking*

[LIBANO MANZUR, Claudio][3]

“De acuerdo a lo expuesto, podemos decir que el delito de hacking admite ser clasificado en dos grandes grupos:

A. HACKING PROPIAMENTE DICHO O HACKING DIRECTO.

El hacking propiamente dicho, es un delito informático que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor.

La voluntad de divertirse generalmente se traduce en paseos por el sistema haciendo alarde de la intromisión. Es lo que se ha llamado JOY RIDING, o paseos de diversión.

Características de esta clase de hacking.

a. El hacker es una persona experta en materias informáticas, y generalmente sus edades fluctuarán entre los 15 y los 25 años. Es por ello que esta delincuencia se ha nominado "SHORT PANTS CRIMES", es decir, crímenes en pantalones cortos.

b. Su motivación no es la de causar un daño, sino que se trata de obtener personales satisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos. Por ello, el hacker siempre buscará notoriedad pública desde el anonimato. Asimismo, perseguirá objetivos cada vez más difíciles de vencer, y elegirá sus víctimas entre empresas y organismos de trascendencia nacional e incluso internacional.

c. Esta clase de hacking no representa un importante nivel de riesgo, toda vez que el hacker no busca causar un daño.

d. Desde un punto de vista estrictamente jurídico, estimamos que se trata de un delito de resultado que se consuma al momento de ser descifrados los códigos de acceso secretos, aún cuando los usuarios no tomen conocimiento del hecho.

Sobre la modalidad del hacking propiamente dicho, el economista español Alfredo Sneyers, en su libro "Fraude y Otros Delitos Informáticos", entrega un caso digno de análisis ocurrido en Inglaterra.

"Dos hackers, Steve Gold y Robert Schifreen, encontraron una brecha en el sistema de seguridad del sistema Prestel de la

British Telecom. En octubre de 1985, tuvieron acceso a varias cuentas confidenciales y uno de ellos, Schifreen, pudo introducirse en la casilla de correo electrónico del duque de Edimburgo. Schifreen logró tener acceso no autorizado al sistema Prestel porque empleados de la British Telecom habían dejado las contraseñas privilegiadas del sistema Prestel en las páginas electrónicas principales del sistema de prueba. Gold y Schifreen informaron a Prestel acerca de esta anomalía y Prestel la corrigió.

Ambos hackers fueron detenidos y, a finales de 1986, fueron juzgados culpables de falsificación y condenados a pagar multas por un total de 1.350 libras (unas 300.000 pesetas) y costas del juicio por unas 1.000 libras (unas 200.000 pesetas)".

Sin embargo, el Tribunal de Apelaciones, al revisar el fallo, estimó pronunciarse por la absolución de los condenados. Textualmente el presidente de aquel alto Tribunal sostuvo: "Su conducta fue la de ganar acceso deshonesto al banco de datos de Prestel mediante un ardid. Esto no constituye una ofensa criminal. Si se desea considerarlo así, es una cuestión de la legislatura más que de los tribunales".

Esta sentencia conduce a que podamos formular ciertas precisiones.

En primer término, el fallo recurrido condenó a los Sres. Gold y Schifreen en calidad de autores del delito de falsificación. Lo que ocurrió, es que ante la ausencia de ley que regulara la actividad de los accesos indebidos, el Juez se vio en la necesidad de recurrir al tipo que pensó más podía asemejarse a las conductas expuestas. La verdad es que debió forzar las características incriminatorias del delito de falsificación, de manera de propiciar el encuadramiento necesario para condenar.

En segundo lugar, el Tribunal de Apelaciones fue más sensato y justo. Consideró que las conductas de los acusados no constituían delito, sin perjuicio de que merecieran un juicio de reprochabilidad. Menciona asimismo que el problema es de la legislatura y en eso tiene la razón. La tipicidad es de competencia de los legisladores, los cuales deben recoger las necesidades sociales de tutela jurídica frente a ciertos hechos no regulados como delitos.

De acuerdo a Sneyers, el Computer Fraud & Security Bulletin criticó la sentencia del Tribunal de Apelaciones expresando que de esta forma el hacking sólo sería sancionado cuando el hacker, a través del acceso indebido cometa fraude u otros delitos, tratando de significar que debe sancionarse el hacking propiamente dicho. Es cierto lo manifestado por tan prestigiosa revista, sin embargo no comprenden que en el caso de Inglaterra el problema pasaba por

la ausencia de Ley.

Sin perjuicio de nuestra posición, se han levantado voces expresando que el hacking propiamente tal no es una conducta que pueda ser considerada como delictiva. Se fundan en que tal clase de hacking no constituye ofensa alguna y que castigar al hacker por el simple hecho de acceder significaría pisotear el derecho a la intimidad del hacker. Lo dicho no resiste mayores comentarios si se piensa solamente en que el hacker viola la intimidad de sus víctimas al acceder sin derecho a los programas ajenos.

Al respecto, Ulrich Sieber, se pronuncia en favor de la atipicidad del hacking propiamente dicho, en el caso de que luego del acceso, el hacker de noticia a las víctimas de la manera en que ingresó.

Creemos que tal posición no es sustentable jurídicamente, toda vez que la sóla situación de revelar la técnica comisiva no exime al hacker de la mala utilización que realiza de las técnicas informáticas, las cuales deben ser puras e idóneas de acuerdo a la tendencia chilena que nosotros compartimos. Por otro lado, si nos basamos en los bienes jurídicos múltiples que intentan proteger en el derecho comparado con los delitos informáticos, concluiremos que el hacker que no causa daños o fraudes, si viola la privacidad de los datos, afectando la intimidad entrando, de manera no autorizada, en la propiedad ajena.

Ahora bien, es evidente que la penalización de esta clase de hacking no debe ser de gran magnitud, precisamente atendiendo a que no causa mayores daños y a que el ánimo involucrado no es extremadamente riesgoso. La circunstancia de que el hechor revele a sus víctimas el modus operandi en la violación de la prohibición de acceso, puede ser vista desde dos ángulos: por una parte existe la posibilidad de que el ánimo del hacker sea efectivamente poner a resguardo a las víctimas de nuevas intromisiones; por otro lado, es posible que el agente delictivo sólo busque vanagloriarse y hacer aún más sarcástica su burla. Sea como fuere, el acceso indebido se produjo y el delito se consumó.

A modo de corolario del presente acápite, citaremos las palabras del experto Sneyers :

"La sociedad debe tomar conciencia de que el hacker es una persona que comete un acto ilegal con pleno conocimiento de causa sólo por el mero hecho de introducirse, sin autorización, en un sistema informático ajeno, exista o no intención de causar un daño o ánimo de lucro".

B. HACKING COMO MEDIO DE COMISION DE OTROS DELITOS O HACKING INDIRECTO.

Como se ha dicho, es usual que el hacking, en cuanto acceso

indebido, se realice como medio para la comisión de otros delitos como fraude, sabotaje, piratería, y espionaje.

Es usual que los delincuentes informáticos se valgan de accesos indebidos a los programas para cometer ahí sus fechorías.

Los delitos de fraude, sabotaje, etc., pueden cometerse, en general, por dos tipos de personas: en primer término, por aquellos que tienen autorizado el acceso al sistema y que, por ende, conocen, legítimamente, los códigos de seguridad. Se tratará generalmente de trabajadores del área informática de bancos, empresas u organismos del estado. En estas personas se ha depositado un nivel de confianza importante. En segundo lugar, están aquellos que tienen el acceso prohibido o cerrado y que ingresan al sistema a través del desciframiento malicioso del password. Es en este último caso donde el agente comete hacking indirecto.

Como se dijo, lo que determina si el hacking es propiamente dicho o medio de comisión de otros ilícitos es el ánimo o motivación que induce a la comisión del delito. En el caso del hacking que tratamos, el ánimo del delincuente está determinado por su intención de dañar, de defraudar, de espiar, etc. Es por ello que en el hacking indirecto el acceso indebido cede su rol protagónico frente al delito "principal" que se busca cometer.

Tal situación no implica que el acceso indebido como delito desaparece. Sin embargo, para que esta materia quede absolutamente clara, es necesario plantearse algunas hipótesis legislativas.

Un primer supuesto estará determinado por la posibilidad de que una ley sobre la actividad informática, o bien la que introduzca modificaciones relativas a estas materias en los códigos penales, contemple, de manera expresa, en una norma independiente de aquellas que tipifican el fraude, el espionaje, el sabotaje, etc., el acceso indebido o hacking en sus dos clases, como una forma delictiva aislada, es decir, un delito per se.

La segunda posibilidad radica en el supuesto de que la ley incluya el acceso indebido como elemento del tipo fraude, sabotaje, piratería, etc. Por ejemplo, "El que a través de un acceso indebido al sistema de tratamiento de los datos destruya, modifique o altere el contenido de programas o ficheros...". En este caso, no será correcto hablar de hacking como delito independiente, toda vez que el acceso indebido pasa a ser uno más de los elementos objetivos del tipo. Dentro de esta segunda hipótesis, cabe también la posibilidad de que el legislador, en atención a las especiales características de ciertos tipos delictivo informáticos, incluya el elemento acceso indebido sólo en algunas de las figuras y no en todas, y al mismo tiempo exista

una norma general e independiente que sancione el hacking en sus modalidades.

La tercera situación es la que se relaciona con la atipicidad del hacking. Es decir, el acceso indebido, cualquiera sea la motivación que presente, no estará sancionado. Esta es, sin duda, la más peligrosa de las alternativas.

Sostenemos que la mejor forma de regular el hacking, en general, es su tipificación en una norma independiente. De esta manera se evitan confusiones y se hace más exiguo el campo de los intérpretes. Por lo tanto el acceso no autorizado será siempre un delito cualquiera sea el ánimo con que se cometa, sin perjuicio de que tal motivación deba ser un elemento a considerar al graduar la pena aplicable. De esta forma, se salva el problema de los delitos cometidos por personas autorizadas a ingresar a un sistema determinado, los cuales sólo serán sancionados por el delito que cometieron, sin perjuicio de que pueda constituirse una circunstancia agravante de la responsabilidad criminal por el eventual abuso de confianza empleado en la comisión del ilícito.

Así, en el caso de que una persona cometa sabotaje ingresando ilícitamente al sistema, se le sancionará por el concurso delictivo ideal que se produce en el hecho, debido a ser el acceso indebido el medio necesario para cometer otro delito.

Siempre resulta interesante citar un caso. Para ello citaremos a Alfredo Sneyers, quien, de acuerdo a la revista Computer Fraud & Security Bulletin, narra la siguiente hazaña delictual.

"Hoxie, un programador de 24 años de edad, de Houston, Texas, de buena posición económica, fue acusado de robo y arrestado. Negó toda responsabilidad y fue puesto en libertad bajo fianza de 30.000 dólares.

Los hechos:

Según el fiscal, Robert J. Hoxie accedió sin autorización a una base de datos de Greater Houston Credit Bureau de la que extrajo las historias personales completas de cierto número de presidentes de bancos, altos ejecutivos de compañías de petróleo y otros prominentes hombres de negocios. Obtuvo así los números de sus cuentas bancarias y de sus saldos y, lo que es muy importante, información sobre las tarjetas de crédito que tenían.

Se alegó que hoxie solicitó las tarjetas de crédito Master Card y Visa en nombre de sus víctimas; el First City Bank de Dallas las concedió y envió a sus direcciones, en el área de Houston, que figuraban en las solicitudes.

Hoxie reunió un total de 76 tarjetas de crédito en las direcciones que había dado y, disfrazado para no ser reconocido, las utilizó

para efectuar retiros de fondos en cajeros automáticos por un importe total de 100.000 dólares.

El fraude duró desde Julio hasta Octubre de 1984, fecha en que un empleado del First City Bank examinó la lista de las "tarjetas delincuentes" y vio el nombre de uno de sus colegas del banco. Habló con él y, naturalmente, éste no sabía nada de la tarjeta concedida a su nombre.

El banco, entonces, examinó todas las tarjetas de crédito en las que los nombres no correspondían a las verdaderas direcciones de sus poseedores y se descubrió que las pérdidas ascendían a un importe total de 100.000 dólares.

Hasta la fecha de la publicación, los investigadores no habían podido establecer aún cómo se había realizado este hacking. Por la evidencia disponible, parece que alguien pudo acceder a la contraseña del jefe de los sistemas, ya que datos tan detallados como los obtenidos por Hoxie no podían haber estado a disposición de los suscriptores normales del Greater Credit Bureau".

Por último, parece ser que el hacking comenzó como un hacking de desafío intelectual o de divertimiento. Con el paso de los años esta modalidad delictiva ha ido pasando a un segundo plano frente al impulso que ha adquirido el hacking delincuencial o indirecto."

2. Normativa

a. Código Penal[4]

Artículo 217-bis.- Fraude informático (*)

Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un 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.

(*) El presente artículo 217-bis ha sido adicionado mediante Ley No. 8148 de 24 de octubre del 2001. Alcance No. 81 a LG# 216 de 9 de noviembre del 2001.

3. Jurisprudencia

a. El fraude informático en relación con la sustracción y uso de tarjeta.

[SALA TECERA][5]

"III.- En el motivo por inobservancia de normas sustantivas se reprocha indebida aplicación del artículo 217 bis del Código Penal, e inaplicación del numeral 209. Considera la impugnante, que el hecho tenido por cierto no es constitutivo de la conducta descrita en el numeral 217 bis del Código Penal, que se refiere a una estafa informática, aunque se titule fraude informático. Afirma, que cuando el tipo penal habla de "influir", se refiere a quien de alguna forma altere el normal funcionamiento de un procesamiento, o altere el resultado de los datos de un sistema de cómputo. Indica que en este caso el sujeto activo se limitó a seguir los pasos que realizaría el propietario de la tarjeta, para obtener el dinero, sin que en forma alguna influenciara en el sistema. Sostiene que la actuación del tercero que obtiene dinero de un cajero, será o no legal, no porque esa persona influya en el cajero, sino si tiene o no autorización del propietario de la tarjeta para sacar el dinero. Alega que la acción que se configura es la de hurto agravado, con utilización de "llave", sea la tarjeta. Se acoge el reclamo. Al realizar el análisis jurídico penal, el Tribunal afirma que la encartada hizo uso indebido de la tarjeta – al sustraerla de la cartera de la ofendida – así como de los datos del sistema de cómputo para ingresar a su cuenta, sea la clave o pin de esa tarjeta. Esa acción la considera constitutiva del delito contemplado en el artículo 217 bis del Código Penal, el cual dispone: " Se impondrá prisión de uno a diez años a la persona que, con la intención de procurar u obtener un 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 ". A juicio de esta Sala, la conducta tenida por probada – sustracción de la tarjeta de débito, obtención de la clave de ingreso, y uso de la tarjeta para conseguir en el cajero automático, dinero de la cuenta de la ofendida –, no es propia de dicha ilicitud, en vista de que Barrantes Barrantes no manipuló los datos del sistema, ni influyó en su procesamiento. Como se señaló en un caso similar: "En sentido amplio, el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como medio o como fin; como medio en el caso del fraude informático, y como fin, en el sabotaje informático (artículo 229 bis del Código Penal). "Por una parte, el National Center for Computer Crime Data

indica que “el delito informático incluye todos los delitos perpetrados por medio del uso de ordenadores y todos los delitos en que se dañe a los ordenadores o a sus componentes”. De igual forma, y siempre con ese carácter de generalidad y amplitud, la Organización para la Cooperación y Desarrollo Económico (OCDE) explica que el “delito informático es toda conducta ilegal, no ética o no autorizada, que involucra un proceso automático de datos y/o la transmisión de datos”. Asimismo, William Cashion – estadounidense experto en informática – señala que el “delito informático es cualquier acto inicuo que no puede ser cometido sin un ordenador o que no existiría sin un ordenador o su tecnología” (Delitos informáticos, Carlos Chinchilla Sandí, Farben, 2004, página 27). Si bien para la comisión de un delito informático se requiere un ordenador, ello no implica que siempre que en la comisión del hecho delictivo esté presente un computador, estaremos en presencia de un delito informático. Para mostrar un caso obvio, si se violenta un cajero automático para sustraer el dinero que guarda, no se cometerá un delito informático. De acuerdo a la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en influir en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas que han de incidir en el proceso de los datos del sistema. Influir en el procesamiento o resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema. Por ejemplo, en el proceso de pagar el salario a los empleados habrá una serie de pasos a seguir, que si alguno se altera fraudulentamente, incidirá en el resto del proceso. El usuario aparece al final de ese proceso, y en términos generales, no lo puede modificar. Para hacerlo, requiere el ingreso al sistema, y usualmente debe poseer ciertos conocimientos. Las personas que cometen delitos informáticos presentan algunas características que no tiene el común de las personas, como la destreza en el manejo de los sistemas informáticos, o una posición estratégica que le facilita el manejo de información restringida, o, en muchos casos, ambas ventajas. Por estos aspectos son considerados “delitos de cuello blanco”. Esto por cuanto, además de la tecnicidad en el manejo de los sistemas, éstos se encuentran protegidos por mecanismos de defensa cuya vulneración requiere, usualmente, de conocimientos técnicos: “Esta predisposición de medios defensivos en forma general y la limitación que se puso a los delitos electrónicos nos permite inducir en forma clara que para ingresar a cualquier sistema sin la debida autorización (para el caso la simple intrusión resultaría el delito subsidiario de otros más graves como hacking o robo de información, por citar algunos) implica necesariamente vencer una resistencia predispuesta del sistema

colocada allí expresamente por razones de seguridad, - según expresan los programadores y constructores -.” (Derecho Penal Informático, Gabriel Cámpoli, Investigaciones Jurídicas S.A., 2003, página 28). Según indica el doctor Chinchilla Sandí, dentro de esas conductas destacan la manipulación de los datos de entrada: conocido también como sustracción de datos, es el más común en vista de la facilidad para la comisión y la dificultad en el descubrimiento. No requiere de conocimientos técnicos en informática y puede realizarlo cualquier persona que tenga acceso al procesamiento de datos en su fase de adquisición; manipulación de programas: difícil de descubrir pues el sujeto activo ha de tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en introducir nuevos programas o nuevas rutinas. Un método muy usado es el denominado “Caballo de Troya”, el cual consiste en implantar instrucciones de computadora en forma subrepticia en un programa informático para que realice una función no autorizada al mismo tiempo que la normal; manipulación de los datos de salida: se lleva a cabo fijando un objetivo al funcionamiento del sistema informático, como el fraude a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos, lo que se hacía con tarjetas bancarias robadas. Ahora se usa equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y en las tarjetas de crédito” (Sala Tercera, sentencia # 148-2006) . Como se observa, el delito de fraude informático requiere algún manejo de los datos, o los programas, que afecta el proceso de los datos del sistema. Por su parte, la conducta tenida por acreditada, en el caso en estudio, es el apoderamiento ilegítimo de dinero ajeno, utilizando la tarjeta original, por medio de un ordenador, pero sin modificación, ni alteración de la información que éste contenía, de modo que indujera a error en el procesamiento o el resultado de los datos del sistema. La acción realizada es la misma que hubiera hecho la titular de la tarjeta de débito, para obtener el dinero, por lo cual la conducta tenida por cierta no se adecua al tipo penal considerado por el Tribunal."

FUENTES CITADAS:

1 REYES VÁSQUEZ, Julio R. El Delito de Fraude Informático en Costa Rica. Tesis para optar al grado de Licenciatura en Derecho. San José, Costa Rica: Universidad de Costa Rica, Facultad de Derecho, 2005. pp. 120-123.

2 LIBANO MANZUR, Claudio. Los Delitos de Hacking en sus Diversas Manifestaciones. *Revista de Derecho Informático Alfa-redi*. [En línea]. Consultada el 19 de setiembre de 2007. Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=453

3 LIBANO MANZUR, Claudio. Los Delitos de Hacking en sus Diversas Manifestaciones. *Revista de Derecho Informático Alfa-redi*. [En línea]. Consultada el 19 de setiembre de 2007. Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=453

4 Ley Número 4573. Costa Rica, 4 de mayo de 1970.

5 SALA TERCERA DE LA SORTE SUPREMA DE JUSTICIA. Resolución 763-2006, de las nueve horas con veinte minutos del dieciocho de agosto de dos mil seis.