

VI. ALGUNOS CASOS QUE NO ENCUADRAN EN LA ESTAFA

Se extrae de lo anterior, que el delito de estafa que actualmente tenemos en nuestro código no supe las necesidades para la protección del patrimonio contra cierto tipo de manipulaciones o delitos informáticos, quedando una serie de actos que no podrían ser encuadrados en el delito de estafa, sin dejar de lado una explicación posterior de las clases más comunes de manipulaciones.

Por ejemplo el caso del sujeto que saca provecho de su posición dentro de una oficina determinada para cambiar en la computadora los rubros correspondientes a su salario aumentándolo. En este caso y bajo las explicaciones anteriores no entraría dentro de la estafa a menos que participara una persona que pudiera caer en error. Otro caso que nos podría llevar a una solución similar fue en Australia, donde un contable de una empresa, desde una terminal de su domicilio, accedía ilegítimamente al programa de pagos de la compañía, sustrayendo de cada uno de los sueldos un penique (a este se le condenó por del delito de "fraude por computadora")⁶¹.

También en los Angeles el Vicepresidente de la New York Based Service Bureau, alteró los datos de una compañía rival en los Angeles, accediendo al sistema y dañándolo y alterando algunas de sus funciones. Por otra parte en Madrid, una sucursal de un banco, perdió tres millones y medio de pesetas que fueron abonadas a tres individuos en Nueva York, alguien había accedido al sistema del banco manipulándolo, para que realizara las operaciones en forma automática defraudando así a la entidad bancaria⁶². Dentro de la lista de

defraudaciones el autor Klaus Tiedemann, cita también algunos ejemplos dignos de mencionar, como el caso del empleado técnico de la sección de Asignaciones Familiares, que transfirió ilegalmente a sus hijos montos entre 5000 y 10000 marcos alemanes, o el caso del sujeto que introducía datos de manera ficticia logrando que las sumas giradas a estas se depositarían finalmente a una cuenta personal.

Recientemente Citibank, sufrió una serie de incursiones a su sistema; el intruso Vladimir Levin, y otros cómplices transfirieron desde una pequeña compañía de software en St. Petersburg, 11 millones de dólares desde las computadoras centrales de Citibank en Nueva York a Finlandia, Israel y California⁶³.

En todas estas manipulaciones se alteran máquinas para que realicen o no realicen funciones. No participa en ningún momento un ser humano capaz que pueda caer en error, en virtud del engaño al que es sometido, solo se programa una máquina para generar un perjuicio patrimonial a un sujeto.

A pesar de todo la situación en nuestro país no es del todo crítica, pues con la aplicación de ciertos tipos penales se puede dar una solución momentánea al problema de las manipulaciones. El primer delito es el de peculado, que permite la imputación por estas actividades a los funcionarios públicos, pues lo único que requiere, la sustracción o distracción de dinero y tener la calidad de funcionario público. De esta forma se podrían castigar estos delitos en perjuicio de la administración pública que parece ser el sujeto que más se ve afectado por estas defraudaciones, sin embargo quedan

61. PERNA PEREYRA (Elena M.) y otro, "Informática Jurídica y conductas punibles", Uruguay, *Revista del Instituto Uruguayo de Derecho Penal*, año VIII, Nº 10

62. DE LORENZO (Esperanza), "El Delito Informático", España, *Policia* (revista técnico-profesional), Nº 15, mayo de 1986.

63. ROTHFEDER (Jeffrey), "Seguridad, proteja sus archivos de los intrusos", Centroamérica, *Revista PC World*, Nº 11, año 2, Noviembre 1996, p. 42 ss. Sobre la seguridad de sistemas informáticos el autor cita algunos lugares en Internet que podrían ser consultados como. Secure Computing Corp. <http://www.Soto.com>, Security dynamics Inc. <http://www.Securid.com>, RSA Data Security Inc. <http://www.rsa.com.>, Computer Security Institute, <http://www.gocsi.com.>, Ellashim, <http://www.ellashim.com.>, y otras más, v.p. 46.

fuera de la aplicación de este delito las personas que no ostentan el cargo de funcionarios públicos y logran la manipulación desde fuera o a distancia. Otro delito que puede ser aplicado es el de la apropiación indebida, cuando no se ha podido demostrar la defraudación dolosa, pero si el destinatario del dinero defraudado. Sin embargo el artículo 223 del Código Penal da un plazo de 5 días para devolver o entregar el bien, de manera que tendremos manipuladores informáticos haciendo defraudaciones

y si son descubiertos, devolviendo el dinero en el plazo que da la ley. También podría hablarse de una posible aplicación del delito de hurto, sin embargo independientemente de la discusión acerca de si habría un apoderamiento en ciertos casos o no, no sería una buena práctica aplicar la pena de este delito al delincuente informático, que no es igual desde un punto de vista criminológico al delincuente ocasional de hurto⁶⁴.

VII. PANORAMA DEL PROYECTO DEL CÓDIGO PENAL

El Proyecto del Código Penal establece como delito de estafa, en su artículo 226 que reza "Quien lesione el patrimonio ajeno, induciendo a error a otra persona o manteniéndolo en el, mediante la simulación de hechos falsos o por medio de la deformación o el ocultamiento de hechos verdaderos, será sancionado de la siguiente forma:" y como supuesto de delito de estafa agravada "Cuando se realice manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos"(art. 227). El delito de estafa es prácticamente el mismo, de manera que arrastre las deficiencias que venimos explicando. Sin embargo se trata de conciliar esta laguna en el artículo de la estafa agravada, que tiene como supuesto las manipulaciones. Pero debemos entender que las manipulaciones entran en dos supuestos diferentes; primero cuando hay participación de una persona (que pueda caer en

error), y segundo, cuando no hay participación de una persona. El ejemplo del artículo 227 del proyecto, cuadra dentro del primer supuesto y deja de lado el segundo en virtud de la redacción casi idéntica con el tipo penal de estafa del código penal vigente. En realidad no consideramos necesario la implementación de este nuevo inciso en el delito de estafa, pues no todas las manipulaciones generan grandes ganancias, y no siempre el autor es un experto en informática(manipulaciones en la salida de datos). El proyecto al poner este inciso, parece, trata de cubrir los delitos informáticos, sin embargo el problema es un asuntos de medios para realizar el delito, cuestión que no es tan importante como la existencia de una persona que sea engañada y llevada a error. Pero antes de pronunciar posibles soluciones al problema, debemos comprender el sentido de la palabra manipulaciones.

VIII. TIPOS DE MANIPULACIONES

Las manipulaciones informáticas las podemos clasificar en cuatro grupos, de acuerdo a Romeo Casabona. A pesar de haber algu-

nas clasificaciones más específicas esta que es genérica facilita el entendimiento del tema de las manipulaciones.

64. Ver sobre el perfil del delincuente informático JIJENA LEIVA (Renato Javier), "Chile, la protección penal de la intimidad y el delito informático", Editorial Jurídica Chile.

a) Manipulaciones en la entrada de datos

Se da esta manipulación cuando los datos suministrados a la computadora son falsos, o cuando se modifican datos reales. Aunque la computadora procesa los datos correctamente la disposición final va a ser inexacta por serlo así los datos de partida. Podríamos hablar en este caso del sujeto que incluye en la cartera de proveedores de una empresa proveedores ficticios, girándoles abonos —también ficticios— correspondientes a sus cuentas —que en realidad son las del autor u otro beneficiado—, con el fin de sustraer bienes o mercancías.

El descubrimiento de esta práctica no es fácil, salvo que haya sospecha previa o si se cuenta con procedimientos de control.

b) Manipulaciones en el programa

En este caso se parte de una entrada de datos correcta, pero a partir de esta se logra interferir el programa, para que produzca resultados falsos, o mejor dicho resultados que no son perseguidos por la entidad que es perjudicada. Estas nuevas instrucciones al programa implican modificación, introducción o eliminación de partes del programa, además de medidas oportunas para evitar que el supuesto de un control o auditoría pueda ser descubierta la manipulación. Casabona manifiesta que esta clase de delitos requiere de conocimientos cualificados en informática, y su descubrimiento puede ser muy difícil pues una vez terminada la manipulación se puede restituir al estado normal el programa.

Como ejemplo se puede citar el caso del sujeto que adiciona a cada recibo de cobro de un determinado servicio (luz, agua, etc.) una cantidad despreciable de dinero, que va a ir luego a una cuenta destinada al efecto. Es un proceso de "goteo", pero las ganancias y la seguridad que esta manipulación permite genera grandes ganancias para el infractor. Más adelante se hará mención sobre el tema en la llamada "técnica salami", o "redondeo de cuentas".

c) Manipulaciones en la Salida de Datos

En este caso los datos son incluidos de manera correcta y son procesados de igual forma, pero en su última fase no se corresponde con ellos por una manipulación en la salida de estos, ya sea cuando se hace una impresión de datos en papel, o cuando va a ser transmitidos a otra computadora o a un disquete. Para este caso no se requiere grandes conocimientos por parte del autor. Podría citarse el caso de quien modifica un registro de cuentas o una planilla antes de ser impresa, o cuando se va a pasar a otra computadora.

d) Manipulaciones a distancia

Casabona explica que en los casos anteriores es posible tales actos, por parte de los servidores de empresas públicas o privadas que tienen acceso a claves o a la computadora en sí. Sin embargo cabe la posibilidad por los avances de la telemática de conectarse vía teléfono mediante módem con otra computadora. El autor hace referencia a los medios de transferencia cifrada y "encriptada", lo cual permite mayor seguridad en caso de particulares que pretendan entrar sin autorización al sistema. Sin embargo puede ser que servidores o exservidores puedan realizar estas manipulaciones desde su casa. Un tema muy relacionado a este tipo de manipulaciones es el de la red "Internet", donde prácticamente se puede realizar una manipulación que afecte a un banco, una persona u otro tipo de entidad al otro lado del mundo estando en su propio domicilio, y donde las transacciones económicas⁶⁵ se proyectan en aumento para los años venideros. La preocupación principal de esta modalidad de transacciones, es acerca de la transmisión de números de tarjeta de crédito u otra información, de ahí que algunas compañías ya se hayan preocupado sobre el tema. Sobre la compra en línea (sistema de compra en internet de productos por medio de tarjeta de crédito o cuenta bancaria determinada), se han recomendado ciertas normas de

65. Algunos proveedores de efectivo digital en la red son: Cybercash (<http://www.cybercash.com>), Digicash (<http://www.digicash.com>), First Virtual (<http://www.firstvirtual.com>), etc. ver RUPLEY (Sebastian) "¿Efectivo Digital?", PC Magazine en Español.

precaución para no ser defraudado, como conocer datos físicos sobre la empresa con la que está negociando (teléfono, dirección), consultar el historial de la empresa (Comisión Federal de Comercio en los Estados Unidos ([hppt://fte.gov/](http://fte.gov/)), o también Better Business

Bureau ([hppt:// www.bbb.org/bbb./](http://www.bbb.org/bbb/)), verificar los términos de la venta y el tipo de propaganda que puede denotar ilicitud, y además tener en cuenta que sus movimientos pueden estar siendo rastreados por algún defraudador⁶⁶.

IX. CLASIFICACIÓN ESPECÍFICA DE TIPOS DE MANIPULACIONES

Algunos autores han hecho diversas clasificaciones de modos de realizar maniobras con la informática⁶⁷, pero una de las clasificaciones que más se puede destacar es la del norteamericano Don B. Parker, que expone Renato Javier Jijena. El autor hace referencia a varias modalidades de las cuales vamos a citar algunas:

a) El Caballo de Troya (*Trojan Horse*): que consiste en la inserción de operaciones u órdenes dentro de la codificación de un programa, de manera que a determinada señal u orden realice una función para la que no estaba destinado originalmente. Es decir el programa actúa en forma distinta a la que estaba prevista. "En este caso el programa original no es destruido, y pasa a coexistir con el programa anormal"⁶⁸

b) Bomba lógica (*logics Bombs*): es una manipulación similar al caballo de troya, sólo que las ordenes que son introducidas se ejecutan en fechas o circunstancias determinadas. Es el caso del virus computacional.

c) Datos engañosos (*data diddling*): puede consistir en la omisión del ingreso de ciertas informaciones, la alteración de su contenido, la inclusión de datos no autorizados o el procesamiento duplicado de datos. Jijena, explica que es una de las formas más seguras y eficientes, pues al realizarse mediante la entrada de datos es más difícil de detectar.

d) Técnica Salami o Redondeo de Cuentas (*Salami Techniques o rounding down*): Como ya se vio en algunos ejemplos supra, esta acción consiste en sustraer pequeñas cantidades de cuentas determinadas para que se abonen a una cuenta específica. Las sumas de dinero sustraídas son prácticamente despreciables, de ahí que el perjudicado no reclame el faltante.

e) Superzapping: Esta manipulación inicia con la utilización no autorizada de programas de uso universal, como consecuencia de la copia de los mismos. A partir del sistema copiado se alteran, borran o adicionan datos al sistema original para pasarlos a un soporte magnético

66. FURGER (Roberta), "Comprando en línea: Lo que necesita saber", PC Word, año II, Nº 6, Junio de 1996.

67. Sobre el tema de los tipos de manipulaciones, ver JIJENA LEIVA (Renato Javier), "Chile, la protección penal de la Intimidad y el delito informático", Editorial Jurídica Chile, p. 95 ss. FALCON (Enrique), "¿Qué es Informática Jurídica?", Buenos Aires, ABELEDO-PERROT, p. 145 ss.; CASTRO FERNANDEZ (Juan Diego), "Abogacía e Informática, el delito informático", *Revista del Colegio de Abogados Penalistas del Valle*, Colombia, Vol. IX, Nº 16 y 17. SZNICK (Valdir), "Crimes Cometidos com o computador", *Justitia*, Sao Paulo, 66-70, jan-mar, 1984., LIMA (María de la Luz), "Delitos Electrónicos", Anuario de Derecho, Panamá, año XII, Nº12, 1983. GONZALEZ RUS (Juan José), "Informática y Derecho: Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", *Revista de la Facultad de Derecho de la Universidad Complutense*, Madrid, setiembre de 1986.

68. SZNICK (Valdir), "Crimes Cometidos com o computador", *Justitia*, Sao Paulo, 66-70, jan-mar, 1984, p. 68.

original para pasarlos a un soporte magnético que crea un superzap que permite el ingreso al ordenador en cualquier momento por muy protegido que se encuentre.

d) Otra técnica que no suele ser citada por los autores que nombrados en la nota al pie N° 67 mencionan, es la llamada **Jineteo**, o **Jineteo de cuentas**, que consiste en la manipulación de cuentas que presentan movimientos cada cierto tiempo. Por ejemplo, piénsese en el caso de que hay dos cuentas distintas de sujetos distintos. La cuenta A, registra movimientos

cada 15 del mes, y la cuenta B, realiza movimientos cada 1° del mes. Estos movimientos son de depósitos o retiros parciales. Entonces tenemos que el manipulador sacará una determinada cantidad de la cuenta B luego de la transacción que realiza el usuario y cuando este vuelve a realizar otra transacción se toma de la cuenta A, el dinero para que el usuario no ve error alguno en su cuenta. Cabe agregar que esta es una práctica muy compleja y por lo general el infractor cae por sí mismo al introducir más y más cuentas lo cual dificulta su control.

X. PROPUESTAS. NECESIDAD DE UNA REGULACIÓN ESPECÍFICA ACERCA DE DELITOS INFORMÁTICOS

Bajo todo el análisis referente al delito de estafa, no cabe duda de la necesidad de crear un delito específico para las "estafas por computadora", como la denominan los alemanes, o "estafa por ordenador", como lo hacen los españoles, o "computer crime", como lo determinan los estadounidenses, que es un concepto más amplio que los anteriores.

El desarrollo de la informática y la producción legal tendiente a regularla no es algo nuevo, aunque la última es más reciente que la primera. La preocupación de regular la materia de los delitos informáticos se empieza a notar en los 80's, de ahí la producción legal en este tema en algunos países como Alemania, y posteriormente España. En Costa Rica, el Dr. Francisco Castillo ya había recomendado la creación de ese nuevo artículo en el código penal para regular la estafa por computadora⁶⁹,

sin embargo tal recomendación no prosperó.

a) Algunos tipos penales y propuestas

El código penal Alemán en su artículo 263, establece que "El que, con intención de obtener un beneficio patrimonial ilícito para sí o para un tercero, lesiona el patrimonio de otro interfiriendo en el resultado de un tratamiento de datos, mediante una estructuración incorrecta del programa, la utilización incorrecta o incompleta de datos, la utilización de datos sin autorización, o la intervención de cualquier otro no autorizada en el proceso, será castigado con la pena de privación de libertad de hasta cinco años o con multa", siendo su acción típica el interferir en un procesamiento de producción de datos, que no siempre se realiza sirviéndose directamente de una computadora. El concepto de "programa", supone una clara referencia a la informática, lo que se considera puede generar problemas dogmáti-

69. Con oportunidad de la reforma que implantó la Ley N° 7337 de 10 de marzo de 1993.

Por otra parte al referirse a la "utilización incorrecta o incompleta de datos", se refiere a la manipulación en la entrada de datos. Además el artículo deja un portillo abierto a las posibles lagunas, cuando establece "o la intervención de cualquier otro no autorizada en el proceso...".

El artículo del Código penal Alemán establece todos los supuestos de manipulaciones de los que se ha hablado, salvo algunas de las cuales no constituyen en sentido estricto hechos semejantes a la estafa⁷⁰, como es el caso del espionaje informático. Además el artículo hace remisión a conceptos que deben ser definidos tanto doctrinalmente como jurisprudencialmente. Ya algunos penalistas alemanes han hecho propuestas para mejorar esta situación⁷¹.

Por su parte y con una solución un poco más acertada, el Código Penal Español, en su artículo 248 inc. 2, establece: "También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero", sin embargo el artículo comete algunos errores. En primer lugar cabe preguntarse que se entiende por transferencia "*no consentida*", si se refiere a la inexistencia de este consentimiento del todo, o se refiere a el no asentimiento en el momento de la transacción. Si nos referimos a la segunda opción, podemos decir que al haber una voluntad expresada (consentimiento o no), hay una persona interviniente, de manera que se pueda aplicar el tipo común de estafa. Sin embargo esta no parece ser la interpretación que se da en el Código Penal Español, más bien parece que se habla de una falta de autorización. Pero solucionado este problema se presenta otra interrogante, pues el artículo habla de transferencia no consentida de cualquier "*activo patrimonial*".

Podemos decir que las transferencias son realizadas sobre activos, es decir no se puede transferir pasivos de mi cuenta a otra. De manera que las actividades del sujeto, que con ánimo de lucro y por cualquier medio de manipulación generen pasivos o produzcan el no actuar de determinado sujeto produciendo así un perjuicio patrimonial, no parecen ser cubiertas por el artículo español. Por ejemplo el caso del empresario que modifica por alguna manipulación los sistemas de su empresa enemiga y cambia datos para generar un perjuicio patrimonial en beneficio de su empresa o su persona, creado por el acto negativo (no actuar), de esta, o puede ser el caso del sujeto que para sustraer dinero de una entidad bancaria, genera deudas a distintos sujetos, es decir les aumenta el sus pasivos. Estos son algunos de los problemas que consideramos contiene este artículo, sin embargo usa un concepto más amplio y en nuestra opinión más adecuado que el del art. 263 del Código Penal Alemán, pues habla de "manipulación informática", concepto que se desarrolló ya en la parte VIII de este trabajo.

El último proyecto de Código Penal, presentado a la Asamblea Legislativa de nuestro país, por parte del diputado Gerardo Trejos, y elaborado por el Prof. Wolfgang Schöne, establece un tipo específico para la estafa por computadora. El artículo reza: "El que, con la intención de obtener para sí o para otro un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante: 1. programación falsa, 2. utilización de datos falsos o incompletos, 3. utilización indebida de datos, u, 4. otras influencias indebidas sobre el procesamiento y, por ello, perjudicara el patrimonio, será castigado con pena privativa de libertad hasta cinco años o pena de multa". Como se puede ver el artículo en estudio es en su primera parte similar al código alemán, sin embargo la parte objetiva del tipo

70. ROMEO CASABONA (Carlos María), op, cit. p. 115.

71. *Ibidem*.

alemán, sin embargo la parte objetiva del tipo varía un poco. Al igual que el código penal alemán, este artículo hace una necesaria referencia a la informática como ciencia, al hablar de "procesamiento de datos", "programación falsa", lo que puede causar problemas a la hora de la aplicación del tipo, pues se debe contar con doctrina y jurisprudencia que desarrolle el tema a nivel jurídico, sin dejar de lado la informática.

Algunos autores ya han manifestado su opinión al respecto de tener un artículo específico para regular la estafa por computadora. Así el Dr. Francisco Castillo, propuso el siguiente texto: "Será reprimido con la pena establecida en el artículo 216 el que, con la finalidad de obtener un beneficio patrimonial antijurídico para sí o para un tercero, lesione el patrimonio ajeno mediante la alteración de un proceso de computación, sea que esta se produzca por medio de la construcción incorrecta del programa, por medio del empleo indebido de datos del programa o por medio de cualquier otra manipulación indebida en el proceso de computación", al igual que el código penal, hace remisiones a la informática que pueden presentar problemas en su aplicación, pero mayores problemas presenta el artículo que plantea Rodolfo Bolaños Ramírez⁷², que dice "Estafa Mediante medios mecánicos o tecnológicos. Quien utilizando un medio mecánico o tecnológico y con conocimientos de informática procediere a aplicar cualquiera de los métodos existentes, en la comisión de un hecho, que directa o indirectamente defraudare en su patrimonio a otro, en perjuicio propio o ajeno será sancionado con... (deja a criterio del legislador)", este artículo presenta una amplitud tremenda, pero su problema principal radica en el elemento objetivo de tener conocimientos de informática, porque ¿quién puede ser el que tenga conocimiento de informática, un profesional en la materia, o un

simple funcionario que se aprovecha de sus conocimientos empíricos sobre el tema?. Esto es importante definirlo, pues no todos los tipos de manipulaciones requieren de amplios conocimientos de informática como el caso de las manipulaciones de salida de datos. Más reciente, en nuestro ordenamiento jurídico, la Ley de Aduanas estableció un tipo llamado "delito informático", que reza en su artículo 221 "Será reprimido con prisión de uno a tres años quien:

- a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el **Servicio Nacional de Aduanas**.
- b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el **Servicio Nacional de Aduanas**, siempre que hayan sido declarados de uso restringido por esta autoridad.
- c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del **Servicio Nacional de Aduanas**, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona.
- d) Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La pena será de seis meses a un año si el empleo se facilita culposamente y como agravante establece en el artículo 222, "Agravante La pena será de tres a cinco años cuando, en alguna de las causales del artículo anterior, concurra una de las siguientes circunstancias:
 - a. Intervengan en el hecho tres o más personas, en calidad de autoras.
 - b. Intervenga, en calidad de autor, instigador o cómplice, un funcionario público en ejercicio de sus funciones, con ocasión de

72. BOLAÑOS RAMIREZ (Rodolfo), "Delito Informático como nueva figura jurídica", *Organismo Judicial*, vol. II, N°2, Abril 1988, p. 50.

ellas o con abuso de su cargo". (Lo resaltado es nuestro), ciertamente el artículo tiene una depurada elaboración, aún mejor que cualquier tipo en estudio, sin embargo se le pueden hacer algunas anotaciones: el inciso a) del 221 se refiere a un tipo de delito informático que encierra acción típica que no corresponde a la estafa. Hace referencia al inciso de los problemas de "tiempo de la computadora", "acceso sin autorización", que no son estrictamente tipos de estafa. También habla de "por cualquier medio", es decir permite su aplicación a las llamadas "manipulaciones a distancia", lo mismo hace el inciso d). En su inciso b), el mismo artículo enumera una serie de verbos típicos, sin embargo es importante aclarar el "apoderamiento". Se entiende por apoderamiento aquella acción de sujeto activo por medio de la cual logra sacar el bien de la esfera de disposición del sujeto pasivo, es decir "objetivamente requiere, en primer lugar, el desapoderamiento de quien ejercía la tenencia de la cosa, lo cual implica quitarla de la llamada esfera de custodia, que no es otra cosa que la esfera dentro de la que el tenedor puede disponer de ella; no se trata, pues, de una noción necesariamente referida a un determinado lugar, sino a una determinada situación de la cosa, que permite el ejercicio del poder de disposición de ella: hay desapoderamiento cuando la acción del agente, al quitar la cosa de aquella esfera de custodia, impide que el tenedor ejerza sobre la misma sus poderes de disposición."⁷³, el desapoderamiento no es tal en materia de estos delitos, pues en muchos casos lo que se hace es una copia del material y realmente no se está sacando el objeto de la esfera del sujeto pasivo. El problema parece resuelto con el verbo "copiar", sin embargo sería bueno dar una determinación doctrinaria al verbo apoderar, que es evidente no es la misma que se utiliza en el robo. El inciso c) me parece es una de las mejores proposiciones

típicas del delito, pues no es en sentido estricto una manipulación, pero es claro su referencia a los delitos informáticos. El único problema que presenta el artículo, lamentablemente, se refiere a el elemento objetivo que establece el Servicio Nacional de Aduanas, pues solo se podrán perseguir dichos delitos en cuanto estén en contra de dicha entidad, lo cual resulta bastante lamentable, pues como dije antes el artículo goza de una rica técnica legislativa en materia de delitos informáticos. Con respecto a las agravantes, son problemas de valoración jurídica que no merece mayor discusión.

La preocupación acerca de este tema en el derecho penal, no es de unos pocos. Sin embargo considero que algunas de las soluciones no son tan viables, como otras. Es importante anotar que no es bueno ser tan casuístico a la hora de definir el tipo de la estafa. Recordemos que las tendencias con respecto a los tipos de estafa, eran por un lado las que contienen normas minuciosas y detalladas que se traducen en una multiplicidad de figuras del delito y por otro las que establecían menos normas pero de mayor amplitud. Nuestro Código pertenece a esta segunda tendencia, de tal forma que lo que importa es que haya un engaño que produzca error en la víctima, para que realice una disposición patrimonial que le perjudique. No importa el medio con que se realice el engaño, sino que este exista, de manera que sea este el punto medular de la estafa. En el caso de las manipulaciones informáticas podemos prescindir del elemento del error y el de la disposición patrimonial, pero para hacer lo mismo con el engaño hay que sustituirlo por un concepto igual de amplio que este, de manera que pueda cubrir varias hipótesis delictivas de la misma naturaleza. Es por eso que creo que sería mejor la utilización de un concepto genérico, y desarrollado por la doctrina (tanto alemana como española), como es el caso de "manipulaciones", que com-

73. Sobre el punto se puede consultar, Resolución N° 519 del 06/09/1995 10h 50m. Sala Tercera de la Corte.

prende las hipótesis de entrada y salida de datos, o su alteración a distancia y la alteración del programa, "no se pretende hacer códigos sofisticados y casuísticos para que sólo respondan a una realidad pasajera, y pronto queden obsoletos. Es preferible seguir el camino de las definiciones genéricas que no es limitativo ni casuístico"⁷⁴. Valga decir que esta es una simple opinión que debe ser mejorada con especialistas tanto de informática como de derecho penal y de informática jurídica. Sin embargo podríamos proponer como solución el siguiente artículo "El que, con la intención de obtener un beneficio patrimonial ilícito para sí o para un tercero, mediante cualquier tipo de manipulación de datos informáticos, será sancionado con prisión o con multa". Como se puede notar el artículo esta basado en el art. 263 del Código Penal Alemán, sin embargo se cambian los supuesto objetivos que este propone por una genérico(manipulaciones).

La primera parte de "...con intención de obtener un beneficio patrimonial ilícito", hace referencia al ánimo de lucro y al principio de que no es posible que se de el delito de estafa en relaciones ilícitas, cuando hace referencia a "para sí o para un tercero", no es otra cosa que las discusiones ya mencionadas en el tema del sujeto activo. La frase "mediante cualquier tipo de manipulación de datos informáticos", hace referencia a los diversos tipos de manipulaciones que tutelan prácticamente todos los ámbitos posibles, de comisión del delito de estafa por computadora. Sin embargo hay que determinar que el concepto de "datos informáticos", por el cual podemos entender aquel que se encuentre, entre o salga de una computadora. Pueden existir otras maniobras o manipula-

ciones que no encuadren en este delito, pero por ser propias de otro tipo de conducta dolosa, como es el caso del sabotaje informático, la piratería de programas, el hurto de horas de la computadora, la difamación y hasta el acoso⁷⁵ que en nuestra opinión deben ser regulados en el Código Penal ya sea creando nuevos tipos o reformando los existentes.

b) Problemas de Investigación

"El control de la criminalidad (ley computer), será siempre un problema social además que criminológico y legal. Más los sistemas judiciales del mundo occidental, proyectados hacia la represión de la criminalidad tradicional, no parecen estar en grado de enfrentar ese tipo de "desafío tecnológico"⁷⁶. El problema que plantea López Muñoz, se refiere principalmente a los mecanismos y preparación para investigar la materia de informática. Pues de nada sirve, tener un cuerpo legal idóneo para reprimir los delitos informáticos si no se tiene la capacidad para investigarlos, de la manera correcta. La informática presenta características que nos pueden desligar de la investigación común, de testigos, firmas borradas, manchas de sangre, huellas dactilares, etc., pues las facilidades para deshacerse de cualquier elemento incriminador son increíbles. Por ejemplo en las manipulaciones del programa, los infractores realizan su manipulación de tal forma que al final de la tarea todo lo hecho se borra y no queda rastro alguno de la manipulación. "A diferencia de los delitos patrimoniales la acción y efecto se producen por separado, a menudo con intervalos de cierta entidad lo que dificulta de sobremanera su descubrimiento"⁷⁷, de un lado esta la tarea de descubrir

74. LIMA (María de la Luz), "Delitos Electrónicos", Anuario de Derecho, Panamá, año XII, Nº 12, 1983, p. 182.

75. Sobre el acoso, difamación y derechos de autor se puede consultar el artículo "Lo que puede y lo que no puede hacer en línea", por Roberta Furger, PC World, agosto de 1996.

76. LÓPEZ-MUÑIZ (Goñi Miguel), "El Derecho y la Electrónica", *Revista de Derecho Judicial*, año XII, Nº 46, abril-junio de 1971, Madrid, p. 99, citado por LIMA (María de la Luz), "Delitos Electrónicos", *Anuario de Derecho*, Panamá, año XII, Nº 12, 1983, p. 179.

77. GONZÁLEZ RUS (Juan José), "Informática y Derecho: Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", *Revista de la Facultad de Derecho de la Universidad Complutense*, Madrid, setiembre de 1986, p. 111.

los hechos y por otro más complicado la de probarlos. De ahí que sea importante la capacitación tanto de los investigadores como de los aplicadores del derecho. Es así como en los Estados Unidos el F.B.I, inició en 1973, la capacitación de policías y luego esta capacitación se extendió a los magistrados encargados de procesos⁷⁸, de esta forma es importante notar la necesidad de instruir a los investigadores en esta rama tan novedosa del derecho.

Otro problema que presenta la investigación de estos delitos es la "cifra negra", pues muchas de las empresas bancarias estatales o privadas, o empresas, por temor a que su prestigio caiga al poner una denuncia contra un infractor desisten pues puede que cause mayores perjuicios económicos de los que causó la defraudación⁷⁹. El Reporte informativo de la National Criminal Intelligence Service (la Haya, 1990.) explica algunos de los problemas principales de la investigación de estos delitos, como lo es la falta de experiencia producto de la poca

cantidad de casos que llegan a conocimiento de las autoridades, además de la gran variedad de tipos informáticos, y la particular personalidad del delincuente informático. Sin embargo propone algunas medidas para solucionar el problema de la investigación (algunas de las cuales ya se han implementado en Holanda), que van desde la "Prevención", con el Programa Nacional Contra la Delincuencia por Computadora, la "Corrección" (Reforma de el Código penal y del código de procedimientos penales), la "Detección" (basado en la preparación de los organismos judiciales o privados)⁸⁰. Otro de los problemas que presenta este tipo de criminalidad es la posibilidad de realizar delitos fuera del territorio nacional, de tal forma que no se podría incoar proceso por no tratarse de un caso de los que prevee el art. 7 del Código Penal y tampoco se podría extraditar al nacional que defraude a entidades internacionales desde el país, de ahí la importancia de una regulación internacional al respecto.

XI. CONCLUSIÓN

El derecho es una creación de seres humanos, y por tanto es cambiante. De manera que el legislador y el estudioso del derecho deben preocuparse por estar a la vanguardia de esta situación. La informática es en nuestros días uno de los instrumentos más útiles para el desarrollo del derecho, ya sea como informática Operacional, Registral o Documental. Aunque los dos primeros están iniciando su desarrollo, el último es toda una realidad en nuestro país con la implementación del Centro

Electrónico de Información Jurisprudencial⁸¹. Sin embargo no todo es para bien y hay personas que se valen de tan poderoso instrumento para crear perjuicios a terceros.

El derecho penal, está limitado al principio de legalidad en su expresión particular del principio de tipicidad, que es una forma, en casos muy excepcionales, de lograr la impunidad de ciertos sujetos, de manera que es importante realizar una regulación para todos estos casos que se relacionan con la informática, como es

78. GOLDSTEIN (Bruce), "Fraude Informático: el delito del futuro", *Revista Internacional de policía criminal*, INTERPOL, año. 40, octubre de 1985, N° 391.

79. "All studies in this area have indicate that the true extent of computer-related crime is unknown, since most crimes are either not detected or are not reported to the responsible authorities." *International Review of Criminal Policy*, Nos. 43 y 44, 1994, United Nations.

79. National Criminal Intelligence Service, CRI-INTERPOL. Reporte Informativo, La Haya, Holanda, 1990.

80. Sobre los avances de la informática documental y opcional se puede ver un análisis de derecho comparado del DELPIAZZO (Carlos) y otros, "Introducción a la Informática Jurídica y al Derecho Informático", Ediciones Jurídicas Amalio M. Fernández, Montevideo, p. 41 ss.

81. *International Review of Criminal Policy*, Nos. 43 y 44, 1994, United Nations.

el uso indebido de tiempo de la computadora, el sabotaje, el espionaje, los derechos de autor, el hurto de programas y algunos otros que al parecer no merecen mayor problema con la aplicación de los tipos tradicionales (como la difamación o el acoso), pero sería importante realizar un estudio para determinar tal situación.

Debemos recordar que como derecho penal considerado como la "ultima ratio", no quita la facultad de proponer acciones para evitar este tipo de criminalidad como sería la implementación de medidas de seguridad (auditorías, reportes, revisiones, códigos de acceso etc.) y en acuerdo al informe de la International Review of Criminal Policy, la implementación de códigos de ética⁸².

Nuestro país no está exento de la intervención de la informática que se a conver-

tido en parte de nuestra realidad, de manera que al igual que muchas invenciones en la vida del ser humano, deben ser reguladas para que las mentes inescrupulosas no saquen provecho de tan importante recurso para la humanidad. Este artículo presenta la problemática que enfrenta un tipo específico (estafa), en una materia determinada (derecho penal), dentro del amplio ordenamiento jurídico, de manera que sea necesario ir valorando paulatinamente la influencia de la informática en cada rama del derecho, como por ejemplo en Derecho Mercantil donde gracias a la informática las transacciones se hacen más efectivas y rápidas de un lugar a otro en el mundo entero, y así dar una respuesta razonable que mantenga en equilibrio las libertades del individuo y su protección ante posibles conductas ilícitas.

82. International Review of Criminal Policy, Nos. 43 y 44, 1994, United Nations.

BIBLIOGRAFÍA

- ARTEAGA SÁNCHEZ (Alberto), "La Estafa y otros Fraudes en la Legislación Penal Venezolana", UNIVERSIDAD CENTRAL DE VENEZUELA, 1971.
- BUSTOS RAMÍREZ (Juan), "Manual de Derecho Penal, Parte Especial", Barcelona, ARIEL, 2a edición,
- CUELLO CALON (Eugenio), "Derecho Penal Parte Especial", Barcelona, BOSCH, 14a edición, T. II, Vol. II.
- Diccionario de la Lengua Española, Madrid, Real Academia Española, vigésima edición, 1984, p.554.
- FALCON (Enrique),
"¿Que es Informática Jurídica?", Buenos Aires, ABELEDO-PERROT
- FINZI (Conrado), "La Estafa y Otros Fraudes", Buenos Aires, DEPALMA, 1961.
- FONTAN BALESTRA (Carlos), "Derecho Penal Parte Especial", Buenos Aires, ABELEDO-PERROT, 13va edición, p. 491.
- JIJENA LEIVA (Renato Javier), "Chile, la protección penal de la intimidad y el delito informático", Editorial Jurídica Chile.
- PÉREZ (Luis Carlos), "Derecho Penal, Partes General y Especial", Bogotá, TEMIS, 1988.
- PUIG PEÑA (Federico), "Derecho Penal, Parte Especial", Madrid, EDITORIAL REVISTA DE DERECHO, 1955, T. IV, 4a. Edición.
- RODRÍGUEZ DEVESA, "Derecho Penal Español, Parte Especial", Madrid, Artes Gráficas Carasa, novena edición, 1983.
- ROMEO CASABONA(Carlos María), "Poder Informático y Seguridad Jurídica", España, FUNDESCO, 1987, p. 47ss.
- SOLER (Sebastian), "Derecho Penal Argentino", p. 333 a 334.
- TIEDEMANN (Klaus), "Criminalidad Mediante Computadoras", publicado en la obra "La Droga en la Sociedad Actual", C.A.P Guipuzcoa-España.

REVISTAS Y OTROS

- BOLAÑOS RAMÍREZ (Rodolfo)**, "Delito Informático como nueva figura jurídica", Organismo Judicial, vol. II, Nº 2, Abril 1988.
- CANCINO MORENO (Antonio José)**, "Es necesario crear en el Código Penal un capítulo para los denominados delitos informáticos", Colombia, Revista del Colegio de Abogados Penalistas del Valle, Nº 19, vol. XI, 2do semestre de 1988.
- CASTRO FERNÁNDEZ (Juan Diego)**, "Abogacía e Informática, el delito informático", Revista del Colegio de Abogados Penalistas del Valle, Colombia, Vol. IX, Nº 16 y 17.
- DE LORENZO (Esperanza)**, "El Delito Informático", España, Policía (revista técnico-profesional), Nº 15, mayo de 1986.
- Expediente de Reforma de los artículos 106, 152, 209, 212, 384 inc. 1 y 4 del Código Penal, folio 415 a 418. Audiencia al Dr. Francisco Castillo.
- FURGER (Roberta)**, "Comprando en línea: Lo que necesita saber", PC Word, año II, Nº 6, junio de 1996
- GOLDSTEIN (Bruce)**, "Fraude informático: el delito del futuro", Revista internacional de policía criminal, INTERPOL, año. 40, octubre de 1985, Nº 391
- GONZÁLEZ RUS (Juan José)**, "Informática y Derecho: Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", Revista de la Facultad de Derecho de la Universidad Complutense, Madrid, setiembre de 1986.
- International Review of Criminal Policy, Nos. 43 y 44, 1994, United Nations
- PERNA PEREYRA (Elena M.) y otro**, "Informática Jurídica y conductas punibles", Uruguay, Revista del Instituto Uruguayo de Derecho Penal, año VIII, Nº 10.
- LIMA (María de la Luz)**, "Delitos Electrónicos", Anuario de Derecho, Panamá, año XII, Nº 12, 1983.
- LÓPEZ-MUÑIZ (Goñi Miguel)**, "El Derecho y la Electrónica", Revista de Derecho Judicial, año XII, Nº 46, abril-junio de 1971, Madrid.
- National Criminal Intelligence Service, CRI-INTERPOL. Reporte informativo, La Haya, Holanda. 1990.
- Revista Internet, Nº 1, año 1, p. 6
- ROTHFEDER (Jeffrey)**, "Seguridad, proteja sus archivos de los intrusos", Centroamerica, Revista PC World, Nº 11, año 2, Noviembre 1996.
- SZNICK (Valdir)**, "Crimes Cometidos como computador", Justitia, Sao Paulo, 66-70, jan-mar, 1984., LIMA (María de la Luz), "Delitos Electrónicos", Anuario de Derecho, Panamá, año XII, Nº 12, 1983.

JURISPRUDENCIA

Tribunal Superior Penal, Alajuela, Sec. B,
No. 93 del 15 de abril, de 1986.

Sala Tercera de la Corte, No. 333 del 27/11/87

Tribunal Superior de Puntarenas, No. 148 de las
14,55 h del 5 de octubre de 1988.

Tribunal Superior Penal de Alajuela, Sec. Segun-
da, No. 236 del 10 de noviembre de 1989

Tribunal Superior Penal de Alajuela,
Sec. Tercera, Nº: 4 del 15/01/1991

Tribunal Superior Cuarto Penal, Sec. Segunda,
Nº: 2130 del 28/10/1991

Tribunal Superior Primero Penal, Sec. Segunda,
Nº: 18 del 28/01/1991

Tribunal Superior Penal de Alajuela,
Sec. Segunda, Nº: 68 del 13/05/1991,

Tribunal Superior Penal de Alajuela, Sec. Tercera,
Nº: 172 del 29/10/1991

Sala Tercera de la Corte, Nº: 690 del 20/12/1991

Tribunal Superior Penal de Alajuela,
Sec. Segunda, Nº: 98 del 26/06/1992

Tribunal Superior Tercero Penal, Sec. Segunda,
Nº: 160 del 17/09/1992

Sala Tercera de la Corte, Nº: 60 del 16/04/1993

Sala Tercera de la Corte Nº: 160 de 16/04/1993

Sala Tercera de la Corte Nº: 200 del 14/05/1993

Sala Tercera de la Corte, Nº: 160 del 16/04/1993

Sala Tercera de la Corte, Nº: 515 del 28/11/1994
Sala Tercera de la Corte, Nº: 508 del 28/11/1994

Sala Tercera de la Corte, Nº: 515 del 28/11/1994

Sala Tercera de la Corte, Nº: 565 del 12/12/1994

Sala Tercera de la Corte Nº: 519 del 06/09/1995.