Fecha de recepción: 31 de julio de 2012 / Fecha de aprobación: 12 de septiembre de 2012

Revista de Derecho Comunicaciones y Nuevas Tecnologías

El delito de transferencia no consentida de activos

Ricardo Posada Maya

Universidad de los Andes
Facultad de Derecho
Revista de Derecho, comunicaciones y Nuevas Tecnologías
N.º 8, Diciembre de 2012. ISSN 1909-7786

El delito de transferencia no consentida de activos

Ricardo Posada Maya*

Resumen

El Código Penal colombiano prevé en el artículo 269J las figuras típicas de *Transferencia no consentida de activos* y *tenencia de software destinado al fraude*, propias de los delitos informáticos en sentido estricto que, además de la seguridad de la información informatizada, protegen el patrimonio económico. Así las cosas, la presente contribución busca realizar un estudio breve en relación con el concepto de "*ciberdelito*", el bien jurídico protegido por la norma citada y los elementos objetivos y subjetivos que estructuran este tipo de incriminaciones jurídicas que, en nuestro medio, constituyen un avance imprescindible para completar el "microsistema" de seguridad de la información y los datos en el CP penal vigente.

Palabras clave: fraudes informáticos, delito informático, trasferencia no consentida de activos, delitos contra la seguridad de la información.

Abstract

The Criminal Code provided in article 269J the *typus* of not consensual transfer of assets and possession, manufacture, introduction and facilitation of cheat's software to commit frauds, as characteristic figures of computer-related crimes in the strict sense, in addition to protect the security of computerized information and the economic heritage. This contribution seeks a brief in relation to the concept of cybercrime study, the interest protected by the cited standard, and the objective and subjective elements that make up this class of legal prosecutions that certainly constitute a major advance to complete the "Microsystems" of security of the information and data in the existing criminal law.

Keywords: Computer fraud, computer crime, not consensual transfer of assets, offences against the security of the information.

* Profesor y Director del Área de Derecho Penal, Procesal Penal y Criminología, y Director del Grupo de Estudios en Derecho Penal "Cesare Beccaria" de la Universidad de los Andes, Bogotá-Colombia. Conjuez de la Sala Penal de la Corte Suprema de Justicia de Colombia. Doctor en Derecho por la Universidad de Salamanca y especialista en derecho penal por la Universidad de Antioquia..

Sumario

I. CONSIDERACIONES GENERALES

La Ley 1273 de 2009/art. 1° adicionó el Código Penal de 2000 (en adelante CP) con un nuevo título VII *bis* denominado "De la protección de la información y de los datos", encaminado a proteger de manera integral la "seguridad de la información informatizada" y los sistemas que utilicen para su funcionamiento las tecnologías de la información y las comunicaciones (TIC). Dicho título se compone de dos capítulos: el primero, alusivo a "Los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" (ello es, las funciones informáticas propiamente dichas), y, el segundo, relativo a "Los atentados informáticos y otras infracciones", siguiendo la distribución de la convención contra la cibercriminalidad de 2003 (Budapest)[1].

La doctrina mayoritaria considera la inclusión de las normas sancionatorias de acciones defraudadoras informáticas patrimoniales, como un progreso jurídico y político-criminal[2] importante que complementa el "microsistema" de seguridad (defensa) de la información y los datos preexistente en las leyes 599 de 2000 y la estatutaria de *Habeas Data* núm. 1266 del 2008 (Diario Oficial núm. 47.219 del 31.12.2008. CConst., Sent. C-1011 de 2008). Dicho progreso se refleja en la regulación de modalidades criminales que, además del bien jurídico de la seguridad de la información y el funcionamiento confiable de los sistemas informáticos o telemáticos, protegen asimismo el patrimonio económico (*vid. infra* II, B). Regulación que dista de ser completa, como lo demuestra la impunidad de la falsedad informática (en documentos privados).

Precisamente, a partir del principio de legalidad y sus garantías sustanciales (en particular, la prohibición de la analogía in malam partem y la exigencia de lex certa: CP/art. 10), antes de la reforma era posible comprobar las dificultades para adecuar los delitos informáticos básicos en tipos penales "tradicionales", especialmente, en las figuras de hurto, daño en bien ajeno y estafa que, desde luego, no están diseñadas para proteger la información y los datos informatizados como objetos inmateriales[3], susceptibles y necesitados de protección jurídico-penal específica. Una omisión jurídica que condescendía la impunidad de comportamientos propios del tratamiento automatizado de activos, que funcionan sobre la base del procesamiento, almacenamiento y transmisión automático de datos e información digital[4]. Antes de la L. 1273 de 2009, Colombia era un verdadero paraíso informático.

1 La estructura del código penal sigue la ordenación de *The Convention on cybercrimen* (ETS. núm. 185/2003), en: http://conventions.coe.int/Treaty/EN/ Reports/Html/185.htm; *Rapport explicatif* de la convención, Párr. II sobre los trabajos preparatorios §§ 7-15 en: www.coe.int. Schwarzenegger, C, "Computer crimes in cyberspace. A comparative analysis of criminal law in Germany, Switzerland and northern Europe", en: http://www.weblaw.ch/jusletter/artikel.jsp?articleNr=1957.ok.2002. Jusletter 14, Oktober 2002, www.jusletter.ch.

2 Sobre la importancia y la necesidad de regular los delitos informáticos, *vid*. Möhrenschlager, M. (1992, p. 50); Borja Jiménez (2003, pp. 304 y 305); Picotti (2006, p. 364); Rodríguez Gómez (2003); XV Congreso universitario de alumnos de derecho penal (2003, pp. 139 -140); Sanz Mulas (2003, p. 11 y ss.).

3 *Vid*. Dto. 351 de 1993 (C.A.N.)/art. 3°, Dto. Reg. 1360 de 1989, L. 23 de 1982 y Dto. 486 de 2000 (C.A.N.) y L. 75 de 1990/art. 45, sobre información privilegiada.

4 Cfr. Posada Maya (2006, pp. 11-60); Castro Ospina, (2002, pp. 127-162.

La importancia de estas modalidades típicas se advierte, no solo porque estas fenomenologías delictivas se han incrementado exponencialmente durante los últimos años, precisamente por la actuación de criminales organizados muy difíciles de controlar por parte de las autoridades y la sociedad (muchos de ellos terroristas), sino también por las características propias de las TIC, por la fragmentariedad del control judicial y policivo en la materia, y porque la información circulante y el número de usuarios de la red es considerable[5]. Por tal motivo, Morón Lerma (2002, p. 21) advierte que "(...) las opciones ante el futuro propuesto por las nuevas tecnologías discurren entre la utopía y la paranoia".

En este sentido, el presente escrito examina las figuras típicas de *transferencia no consentida de activos y fabricación, posesión, introducción y facilitación de software defraudatorio*. Para ello, en primer lugar, se realizan algunas consideraciones generales; en segundo lugar, se abordan las cuestiones de las acciones informáticas defraudadoras y el bien jurídico de la seguridad de la información; en tercer lugar, se estudian las normas previstas en el CP/art. 269J, y se analizan sus elementos dogmáticos, sus variantes y se precisan sus relaciones sistemáticas con los delitos de hurto por medios informáticos y estafa; finalmente, en cuarto lugar, se hacen algunas consideraciones a título de conclusión. Todo ello, con el propósito de ofrecer al operador jurídico elementos dogmáticos y político-criminales que le permitan su adecuada aplicación en nuestro medio.

II. LAS ACCIONES INFORMÁTICAS DEFRAUDATORIAS Y EL BIEN JURÍDICO DE LA SEGURIDAD DE LA INFORMACIÓN

A continuación se abordan dos temas fundamentales para comprender a cabalidad el tema analizado; por un lado, el concepto de "ciberdelito", lo que permitirá elaborar un estudio dogmático de la acción informática defraudadora en particular y, por el otro, el concepto del bien jurídico objeto de especial protección en el CP y su correlación con los objetos materiales protegidos por los delitos de Transferencia no consentida de activos en el tráfico automático de pagos y la fabricación, posesión, introducción y facilitación de *software* defraudatorio.

A. *El concepto de "ciberdelito"*

La doctrina especializada reconoce dos manifestaciones fenomenológicas de este sofisticado problema, que algunos de manera equivocada tratan como hipótesis jurídicas equivalentes: 1) la criminalidad informática en sentido amplio[6] y 2) la cibercriminalidad.

1) La *criminalidad informática* cubre todas aquellas figuras punibles tradicionales que, debido a su estructura modal abierta, son realizadas por el sujeto activo empleando de modo

5 Borja Jiménez (2003, p. 305 y ss.): "con el agravante de que la brecha generacional, convierte a cierto sector social, verdaderos o potenciales "analfabetas informáticos", en grupos vulnerables, por su escaso dominio de técnicas de seguridad informática"; De la Mata Barranco/Hernández Díaz (2010, p. 181); Mata y Martín, (2006, p. 97 y ss.); Quintero Olivares (2005, p. 647); Romeo Casabona (2006, pp. 3 y 5); Tiedemann, K. (2007, p. 217-219).

6 Sobre los orígenes del concepto *vid*. Sieber, U. (1992, pp. 29 y ss.); Tiedemann K. (1985, pp. 481-492).

circunstancial redes de comunicación automatizadas o sistemas informáticos, electrónicos o telemáticos, con la consecuente lesión o peligro para bienes jurídicos individuales o supra individuales, como el patrimonio económico, la libertad, la intimidad, la formación sexual o el orden económico y social (p.e.: estafas o extorsiones comunes realizadas usando la Internet, casinos fraudulentos, falsificaciones de documentos públicos informáticos, pornografía con menores en la Web, actos sexuales por medios virtuales o utilizando redes globales de información, uso o facilitación de medios de comunicación vía Web para ofrecer servicios sexuales con menores de edad, entre otros hechos delictivos). Por tal motivo, la Ley 1273 de 2009/art. 2° adicionó un num. 17 al art. 58 del CP: "Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos ó telemáticos", como una circunstancia genérica de mayor punibilidad a tener en cuenta en la individualización judicial de la pena que, conforme al CP/art. 61, corresponde a un mayor desvalor de acción objetivo en la ejecución del delito tradicional.

2) Por el contrario, la *cibercriminalidad* cubre aquellas conductas punibles realizadas con fines ilícitos, no consentidas (facultadas) por el titular de la información o los datos, o abusivas de este consentimiento (facultad), que se orientan a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación y ejecución automática (Matellanes Rodríguez, 2000, p. 130) de programas de datos o información informatizada reservada o secreta de naturaleza personal (privada o semiprivada), empresarial, comercial o pública, que pongan en peligro o lesionen (CP/art. 11) la seguridad de las funciones informáticas en sentido estricto, esto es, la confiabilidad (calidad, pureza, idoneidad y corrección), la integridad y la disponibilidad de datos o información, y de los componentes lógicos de la programación de los equipos informáticos o de los programas operativos o aplicativos (*software*) (Posada Maya, 2006, pp. 10-11). Por consiguiente, no se trata de delitos comunes sino de tipologías especiales realizadas a través de procedimientos informáticos, que gozan de cierta riqueza técnica, aunque no abandonan los tipos penales ordinarios como referentes dogmáticos y criminológicos[7].

Más allá, esta definición se especifica todavía más en la noción de *acciones informáticas defraudadoras*[8], cuando el comportamiento incluya la (1) manipulación, introducción, falsificación, alteración o borrado lógico de datos o información informatizada contenidos en bases de datos, sistemas o redes; o (2) la interferencia, mal uso o uso indebido del almacenamiento, procesamiento o transferencia de datos o información informatizada o de programas de funcionamiento de sistemas informáticos y telemáticos, para ocasionar de manera fraudulenta una disminución del patrimonio de otra persona o de la administración pública y un perjuicio patrimonial injustificado -no consentido- para la víctima, generalmente con ánimo de lucro. Con

7 Puede cfr. Rovira del Canto (2002), Romeo Casabona (2002, p. 130); Matellanes Rodríguez (2000, p. 130). En contra: Choclán Montalvo (2006, p. 69).

8 Rovira del Canto (2002, pp. 248 y 249, 258 y 259), señala que este concepto se distingue en lo sustantivo de la noción de fraude informático, pues la última se refiere exclusivamente a la delincuencia económica tradicional realizada por medios informáticos. Sobre el concepto tradicional *vid*. Suárez Sánchez (2009, pp. 59 y ss.).

ello, se advierten al menos cuatro elementos de esta clase de conductas criminales: 1) la realización de un comportamiento fraudulento o *manipulación en sentido amplio*, 2) la existencia de un medio informático susceptible de manipulación, 3) una obtención patrimonial ilícita de activos con perjuicio de terceros, y 4) Dolo y un ánimo *decipendi* o de lucro (Matellanes Rodríguez, 2000, p. 139).

B. *El bien jurídico protegido*

Por lo que se refiere al bien jurídico, la normativa vigente supera la clásica discusión, al preguntarse todavía si la *cibercriminalidad* lesiona o pone en peligro un interés autónomo (el espacio informático como bien jurídico intermedio), o si lesiona o pone en peligro distintos bienes jurídicos tutelados, que comprenden intereses diversos de naturaleza colectiva o derechos personalísimos y personales (como el patrimonio económico) o ambos, que incluyen la seguridad de la información y las funciones informáticas[9]. Por ello, sin duda, hoy los delitos informáticos se pueden clasificar como *tipos pluriofensivos* (Rovira del Canto, 2002, p. 187) (colectivo-individuales) que protegen, no solo la seguridad de las funciones informáticas, los sistemas informáticos y los datos e información informatizada como valor económico y social, como un bien inmaterial público e intermedio[10], sino también otros bienes jurídicos de naturaleza personalísima o colectiva.

Precisamente, Ley 1273 de 2009 reconoce como bien jurídico principal "La protección de la información y de los datos" informatizados con valor final o instrumental, con lo cual se protege la seguridad, disponibilidad y control, y la autenticidad e integridad de la información y los datos. Bien jurídico que igualmente preserva el "derecho fundamental a la protección de datos y autodeterminación informática", consagrado en la CN/art. 15[11], que igualmente codifica el *habeas data*.

Este bien jurídico debe distinguirse de los objetos jurídicos concretos protegidos por los tipos penales de contenido informático previstos en el CP, objetos estos que usualmente se sintetizan en la facultad de realizar funciones informáticas dirigidas a acceder, crear, procesar, adquirir, conocer, trasmitir, transferir, divulgar, manipular, disponer, tratar, almacenar y ejecutar, de manera automática, eficaz y segura programas de datos o información informatizada con valor para el individuo, el comercio, la industria, la colectividad y el Estado. Incluso, una ulterior distinción todavía es posible, pues los datos propiamente dichos[12], cualquiera que sea su sentido social o jurídico, constituyen uno de los objetos inma-

9 Cfr. Castro Ospina (s.f., p. 132 y ss.); Reyna Alfaro (2001, pp. 181-190) y Romeo Casabona (1987, p. 19 y ss.).

10 En Colombia ver: Suárez Sánchez (2010, p. 236).

11 Corte Constitucional, Sent. T-559/2007. *cfr*. Romeo Casabona (2006, pp. 181 y ss.).

12 El Convenio de Budapest de 2003, entiende por datos o información en el Ch. I, art. 1°, aquella "unidad básica de información, ello es, cualquier representación de información, conocimiento, hechos, conceptos o instrucciones que pueden ser procesadas u operadas por sistemas automáticos de computadores, y cuya unión con otros datos conforma la información en sentido estricto". La característica esencial es que este tipo de elementos no son susceptibles de visualización directa y para ello requieren un procesamiento digital que haga explicitas las señales que los integran. La Ley estatutaria núm. 1266 del 31.12.2008/ art. 3°, lit. e, f, g y h, y la Sentencia C-1011 de 2008, clasifican para Colombia los datos en: "e) dato personal, f) dato público, g) dato semiprivado, y h) dato privado".

teriales protegidos sobre los cuales recae la acción automatizada de carácter cibercriminal.

Finalmente, esta característica también implica, de manera desafortunada, que la mayoría de los tipos penales sean de amenaza o peligro en abstracto, es decir, de aquellos que suponen o presumen -*iure et de iure*- la afectación del bien jurídico tutelado por medio de acciones que recaen sobre los objetos protegidos, sin que ello admita prueba en contrario (Rovira del Canto, 2002, 187). Técnica de intervención legislativa que se considera abusiva porque lesiona garantías fundamentales y encubre los verdaderos intereses políticos y económicos protegidos por la norma jurídico-penal, ya que anticipa las barreras de protección del derecho penal vigente y castiga actividades preparatorias de infracción a la seguridad y al control, mediante una intervención máxima del sistema penal (Rovira del Canto, 2002, 17). A ello, añádase que estas *tipicidades* se sirven en exceso de elementos normativos que, a pesar del argumento de la *innovación tecnológica*, ponen en entre dicho los principios de legalidad y taxatividad o certeza (CP/arts. 6 y 10) (Rovira del Canto, 2002, 572).

III. ASPECTOS DOGMÁTICOS DE LA TRANSFERENCIA NO CONSENTIDA DE ACTIVOS Y LA FABRICACIÓN, POSESIÓN, INTRODUCCIÓN Y FACILITACIÓN DE *SOFTWARE* DEFRAUDATORIO

A. El legislador penal incorporó en el CP/art. 269J, el tipo penal autónomo de defraudación informática económica, que consiste en la Transferencia no consentida de activos, de la siguiente forma: "El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes"[13].

Se trata de una modalidad típica diferente a la estafa tradicional (CP/art. 356)[14], porque, aunque comparte algunos de sus elementos dogmáticos (objetivos y subjetivos), se caracteriza por sancionar operaciones automáticas realizadas por sistemas informáticos como resultado directo de manipulaciones defraudadoras impulsadas, desarrolladas o ejecutadas por el sujeto activo (Gutiérrez Francés, 1991, pp. 37-41, 91 y 588; Picotti, 2006, pp. 258-260). Precisamente, el inc. 2° del art. 269J distingue las dos

13 CB, Ch. I, art. Article 8–Computer-related fraud. "(...) cuando se produzcan intencionalmente y sin derecho, una pérdida de propiedad a otra persona por: una entrada, alteración, borrado o supresión de datos informáticos; b cualquier interferencia con el funcionamiento de un sistema informático, con intención fraudulenta o deshonesta y sin derecho, un beneficio económico para sí mismo o para otra persona" (T/L). El supuesto de hecho doméstico es una copia, aunque en otro contexto de protección, de la norma prevista en el CP de España/art. 248.2. A diferencia de este, allí se le considera de modo exclusivo un delito patrimonial.

14 Su naturaleza es muy disputada. Por una parte, se encuentran aquellos doctrinantes que afirman que la transferencia es una modalidad asimilada al tipo básico de estafa o un tipo especial de estafa (Orts Berenguer et al, 2004, p. 571), quienes hablan de estafas cometidas dentro y fuera del sistema; Serrano Gómez et al (2009, p. 435, hablan de estafa peculiar), por la otra, quienes sostienen que se trata de un tipo informático autónomo defraudatorio (Borja Jiménez 2003, p. 307; Faraldo Cabana 2009, p. 85; Polaino Navarrete et al, 2011, p. 98; Quintero Olivares et al 2011, p. 668, porque pretende criminalizar conductas lesivas para el patrimonio ajeno extramuros de la dinámica comisiva presidida por el engaño; Suárez Sánchez 2011, p. 245, entre otros autores).

modalidades típicas, cuando sanciona el comportamiento de *tenencia de software defraudatorio* para la comisión del "*delito descrito en el inciso anterior, **o de** una estafa*" (énfasis propio).

Además, la *trasferencia* no es un tipo de convergencia impropia de sujetos como la estafa, pues el sujeto pasivo (víctima) o el sujeto sobre el cual recae la acción en nada intervienen durante la producción del perjuicio patrimonial que es causa de una transferencia automática de activos generada por una máquina[15] instruida por el autor. De hecho, si llegase a existir un engaño al sujeto pasivo o al sujeto sobre cual recae la acción, de tal manera que se advierta una relación directa entre la disposición patrimonial voluntaria y el perjuicio por parte del sujeto pasivo, quedaría excluida la tipicidad de la conducta de *transferencia no consentida de activos* (Anarte Borallo, 2010, p. 237). De igual manera, quedaría excluida la figura cuando no haya una transferencia de activos sino un apoderamiento de dinero en los términos del CP/art. 239.

En fin, se trata de figuras diferentes como lo demuestra el que no existe una unidad típica relativa entre ellas, por lo que en caso de presentarse un concurso de tipicidades este sería heterogéneo y probablemente material por ausencia de unidad de conducta. Diferencias que también impiden configurar un delito continuado entre estas tipicidades, por la ausencia de homogeneidad en el *modus operandi* (CP/art. 31 y par.) e identidad de bien jurídico.

1. Aspecto objetivo: Sujeto Activo

Monosubjetivo y común: "*El que*": cualquier persona natural que realice la acción propia del tipo penal, sin que este requiera alguna calificación particular o especial (como ser cliente de una entidad financiera determinada (Superintendencia Financiera de Colombia, Concepto 2011005081-005 del 19 de abril de 2011)), o poseer especiales conocimientos técnicos en materia informática. Incluso, el sujeto activo puede ser el titular legítimo del sistema cuando lleve a cabo una manipulación informática a su favor y en perjuicio de otro (Rovira del Canto, 2002, p. 565). De todas maneras, no se puede confundir el sujeto activo del tipo con el beneficiario de la acción criminal, pues la práctica enseña que, ocasionalmente, los beneficiaros no son quienes realizan la conducta punible y, en muchos casos, ni siquiera están al tanto de la defraudación.

Téngase en cuenta, asimismo, que el CP/art. 269H modifica y agrava el tipo penal de la mitad a las tres cuartas partes, cuando el sujeto activo tenga la calidad de *servidor público en ejercicio de sus funciones* (num. 2), incremento punitivo que se fundamenta en la mayor exigibilidad que comporta tal cualificación; o cuando el sujeto activo se pueda considerar como un *insider* (num. 8), es decir, cuando sea el responsable de la administración, manejo o control de la información informatizada objeto del crimen (operadores, programadores, cajeros, etc.). En

15 Cfr. Álvarez García et al (2011, p. 252); Choclán Montalvo (2006, pp. 74 y ss.) indica que se trata de "*operaciones realizadas autónomamente por la máquina sin necesidad de la contribución de la persona que realice un desplazamiento patrimonial voluntario*"; Corcoy Bisadolo et al (2004, p. 588 y ss.); Faraldo Cabana (2009, p. 85 y ss.); González Rus (en Morillas Cueva (Coord.) et al); Cobo del Rosal (2011, p. 495); Mantovani, (2009, p. 200); Matellanes Rodríguez (2000, p. 139); Muñoz Conde (2007, p. 422); Polaino Navarrete et al, (2011, p. 98); Suárez Sánchez (2010, p. 259); Suárez-Mira et al (2004, p. 245); Serrano Gómez et al (2009, p. 435 y ss.); Tiedemann K. (1985, p. 226).

el último caso, el legislador decidió imponer también como sanción principal la pena privativa de derechos consistente en la *inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos informáticos,* por el mismo tiempo que dure la pena privativa de la libertad.

Este tipo penal admite la coautoría y otras formas de autoría, y las diversas formas de participación criminal: (i) determinación, (ii) complicidad e (iii) intervención (CP/arts. 29 y 30). En nuestro medio, suele pasar con frecuencia que el sujeto activo organiza una verdadera empresa criminal, de tal manera que intermedia, por ejemplo, el pago en dinero de servicios públicos a cargo de personas que no tienen fácil acceso a terminales de pago o que no cuentan con los conocimientos adecuados para hacer este tipo de transacciones. En estas hipótesis, el sujeto activo manipula el sistema o usa códigos y datos personales previamente obtenidos (CP/art. 269F), componiendo créditos a cargo de cuentas bancarias corrientes o de ahorros de terceros, cuyos fondos o activos emplea a su vez para abonar los pagos mediante transferencias no autorizadas de activos, luego de lo cual, los autores se apoderan del dinero en efectivo y crean un perjuicio para la empresa prestadora del servicio, el verdadero titular de la cuenta y el abonado. Naturalmente, es usual que quien acude al criminal actúe como un tercero de buena fe, a quien, de todas maneras, estafan en términos tradicionales.

En la práctica el asunto no es fácil, pues también sucede que las personas "prestan" su cuenta bancaria para la realización de transferencias no consentidas de activos dolosas, que luego, al ser obtenido el dinero, quedan formalmente subsumidas por el tipo de *hurto por medios informáticos* (CP/art. 269I), como una hipótesis especial de hurto calificado (CP/art. 240) que tiene una pena "más grave". La dificultad consiste en saber si, en el caso concreto, estas personas actúan como verdaderos coautores o como cómplices del sujeto activo, o sí en verdad son terceros que actúan de buena fe en la realización del cibercrimen. Un asunto de mucha complejidad que depende, fundamentalmente, de la evidencia/prueba de los elementos objetivos y subjetivos del tipo; y, en particular, de la clase de acuerdo previo, la distribución de funciones y la importancia del aporte doloso efectuado para la realización del "fraude". En estos casos también se discute si quien presta la cuenta de destino para la transferencia ilícita, que no necesariamente es el destino final de los activos o los fondos ajenos, tiene dominio funcional del hecho respecto de la transferencia ilícita o del hurto.

2. Sujeto Pasivo

Monosubjetivo y común: solo pueden ser sujetos pasivos de este tipo penal las personas que, por una parte, sean titulares del bien jurídico patrimonio económico perjudicado y de los datos informatizados con valor contable y, por la otra, aquella persona que sea el titular del medio informático que resulta objeto de manipulación por parte del autor, que incluso puede ser una persona jurídica[16].

16 Sigue un concepto amplio de autor: Rovira del Canto (2002, p. 570): "[…] sujetos pasivos del delito son además del titular del derecho patrimonial objeto de afectación, los titulares individuales de la información, de los datos o programas objeto de la acción delictual,

Otros sujetos no serán sujetos pasivos del tipo, así resulte perjudicado su patrimonio económico con la acción del sujeto activo.

3. Bien Jurídico

El tipo penal exige la afectación, tanto del patrimonio económico (activos) del sujeto pasivo, como la puesta en peligro de la seguridad de la información informatizada y de las funciones informáticas en sentido estricto. Por esto, se trata de un delito *pluriofensivo* (Rovira del Canto, 2002, 187).

4. Objeto Jurídico

Consiste en la facultad personalísima del titular de la información (en su condición de sujeto pasivo) para acceder, disponer, transferir y conocer, de manera libre, acerca de sus datos e información informatizada de carácter económico que represente activos patrimoniales; además de su propia seguridad, sin la intervención abusiva, violenta o no consentida por parte de terceros. También, se trata de proteger la confiabilidad, disponibilidad y control de las funciones informáticas que permitan el almacenamiento de la información de contenido económico y la seguridad propia de los sistemas y redes informáticas y telemáticas; ello es, "la regularidad del funcionamiento de los sistemas informáticos y la reserva que debe acompañar su utilización" (Fiandaca/Musco, 2007, p. 199).

y de los equipos y sistemas afectados, aunque no sufran perjuicio económico patrimonial efectivo, así como la sociedad en general en cuanto titular de la información informatizada y de los sistemas por los que se procesa y transfiere".

5. Objeto sobre el cual recae la acción

Inmaterial determinable: en primer lugar, el objeto de la transferencia serían *los datos o la información informatizada* que representan un activo patrimonial de cualquier naturaleza, esto es *bienes y derechos con valor monetario positivo que se reflejan en la contabilidad de una empresa, institución o individuo* (RAE, 2012), como dinero escritural o contable, de giro, bancario o documental, derechos de crédito, asientos o datos contables que supongan reconocer ingresos o egresos, y créditos bancarios[17]. Por dato se debe entender la unidad básica de información, ello es, "cualquier representación de información, conocimiento, hechos, conceptos o instrucciones que pueden ser procesadas u operadas por sistemas automáticos de computadores, y cuya unión con otros datos conforma la información en sentido estricto" (Convención de Budapest, Ch. I, art. 1°).

En segundo lugar, además de otro tipo de datos e información también son objetos-medio sobre los que recae la manipulación informática previa: i) los sistemas informáticos y ii) los programas de computación o *software* (objetos intangibles). Por sistema informático se entiende un dispositivo (PC, tableta, Smartphone, cajero automático, P.A.C. electrónico, etc.) o grupo de dispositivos interconectados o conexos que, con arreglo a un programa, realizan el procesamiento automático de datos[18].

17 Suárez Sánchez (2012, p. 271), habla de una concepción restringida de los activos patrimoniales, es decir, sólo aquellos que puedan ser objeto de anotaciones informáticas y de transferencias.

18 Mantovani (2009, p. 200); Quintero Olivares et al (2011, p. 668): "[…] todo aquello que tiene valor de marcado medible en dinero (…)".

Es precisamente el objeto sobre el cual recae la acción delictiva, de naturaleza *inmaterial*, lo que permite distinguir en Colombia este delito de los punibles de *hurto por medios informáticos* (CP/art. 269I) y *estafa* (CP/art. 246), pues, estos requieren que la acción delictiva patrimonial recaiga, en el primer caso, sobre cosas corporales muebles y, en el segundo, sobre cosas corporales muebles o inmuebles (Quintero Olivares, 2011, 647). Así, por ejemplo, si el sujeto manipula el sistema informático (cfr. *infra* 6), para obtener directamente bienes muebles de un almacén o para sacar dinero de un cajero electrónico, entonces, el delito sería inicialmente el de hurto por medios informáticos y no el punible de transferencia no consentida de activos. Por el contrario, si la manipulación se hace para pagar una factura propia o de un tercero a cargo de los activos del titular de los datos, sería una transferencia no consentida.

Finalmente, debe tenerse en cuenta que el art. 269H num. 1, ordena agravar de la mitad a las tres cuartas partes la pena consagrada para los artículos previstos en el título, cuando la acción recaiga "1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros". Se trata de una protección sobre consideraciones de política-criminal, dada la importancia de este tipo de objetos medio y su significado para la convivencia social. Asimismo, en algunos eventos en los que se vulneran otros bienes jurídicos colectivos como la seguridad y defensa del Estado, se advierte un mayor desvalor de resultado. Sin embargo, recuérdese que los delitos de transferencia no consentida de activos deben tener lugar de manera obligada en redes o sistemas informáticos o de comunicaciones financieros (nacionales o extranjeros), lo que implica afirmar que este tipo de delitos patrimoniales informáticos, en razón del principio de prohibición de la doble valoración, no podrían ser agravados por la misma causa.

6. Verbo rector simple

"*Consiga*" la transferencia no consentida de cualquier activo (bienes, derechos, activos u otros objetos de valor inmateriales) en los términos vistos (*supra* 5), para el sujeto activo o para un tercero (Corcoy Bidasolo, 2004, p. 589). Conseguir significa, en lenguaje usual: "Alcanzar, obtener, lograr lo que se pretende o desea"[19], en este caso, con independencia de la voluntad del sujeto pasivo.

El tipo penal puede ser realizado por acción en cualquier clase de terminal pública o privada, y resulta muy discutible su realización "equivalente" por omisión impropia (CP/art. 25), pues los medios, como se verá, son particularmente comisivos[20], indeterminados y muy técnicos.

Además, el supuesto de hecho requiere que el sujeto activo "*se valga*" o se sirva para la oca-

19 De otro lado, Rovira del Canto (2002, p. 562) señala que "será fruto de una actividad automatizada independientemente de la propia voluntad del sujeto activo y sin intervención activa de tercera persona física alguna, aunque también en algunos casos excepcionalmente sea factible que derive de la propia y efectiva acción o conducta previa de un tercero cuyo consentimiento esté viciado".

20 Cfr. Rovira del Canto (2002, pp. 267 y 275). En contra: Polaino Navarrete et al (2011, pp. 99); Suárez Sánchez (2009, p. 283 y ss.), quien señala que es posible el delito por comisión por omisión cuando el sujeto tiene previamente un deber formal de custodia o haber actuado previa injerencia antijurídica. El último caso no es posible en Colombia, según el CP/art. 25, par.

sión de una "*manipulación*[21] *informática*" o de un "*artificio semejante*" sobre un sistema informático, cuya configuración técnica resulte idónea o capaz de lograr el resultado típico (la transferencia). Puede suceder que el sujeto activo ejecute de manera personal la manipulación o el artificio "semejante", o bien que se valga de alguno previamente ejecutado por un tercero (Rovira del Canto, 2002, p. 571). De todas maneras, se trata de una forma de ataque a la cadena de seguridad informática que resulta común a la *transferencia no consentida de activos* y al delito de *hurto por medios informáticos*, pero que no es equivalente al engaño de la estafa o del *phishing*, que recaen directamente sobre las personas naturales.

a) La primera modalidad consiste en una "manipulación informática", acción que ha sido definida en dos sentidos diversos (amplio o indirecto y estricto o directo), sin que exista un acuerdo sobre el asunto en la doctrina.

aa) En sentido estricto, la *manipulación informática* es entendida como una acción preparatoria ilegítima dirigida a introducir o almacenar datos incorrectos e incompletos, o a adulterar los almacenados en un sistema informático o telemático; y ii) a la manipulación o pre-ordenación de los resultados de un proceso de elaboración o transmisión de datos almacenados, mediante la configuración, alteración o modificación de las instrucciones originales de los programas que tratan los datos o la información de entrada (*input*) o salida (*output*) auténtica de los programas o *software* que, al "representar" activos (incluso dinero escritural o contable) son tratados de manera automática. En realidad, son actos que implican comportamientos de falsedad informática en sentido estricto (*Computer-related forgery* (Posada Maya, 2006, 46)).

En esta modalidad, la trasferencia incorrecta de activos no tiene lugar fundamentalmente porque se haya alterado el tratamiento de los datos, sino por la inexactitud o incorrección de los datos espurios que soportan las transacciones económicas realizadas de manera automática, y el funcionamiento incorrecto del sistema[22]. Por tal motivo, para la doctrina mayoritaria estas hipótesis no cubren los casos en los que, si bien solo se transfiere dinero escritural, el autor realiza sin estar facultado para ello los mismos comportamientos que haría el titular legítimo de un sistema informático que funciona de modo correcto, ello es, introducir datos o códigos personales verdaderos del titular legítimo, que se hayan obtenido ilegalmente (Suárez Sánchez, 2010, p. 245)[23].

21 *Manipular*: "3. tr. Intervenir con medios hábiles y, a veces, arteros, en la política, en el mercado, en la información, etc., con distorsión de la verdad o la justicia, y al servicio de intereses particulares".

22 Choclán Montalvo (2006, p. 85) afirma: "En suma, manipular el sistema informático (…) es algo más que actuar en él, equivale a la introducción de datos falsos o alteración de programas perturbando el funcionamiento debido del procesamiento, sin que resulte equivalente la acción de quien proporciona al ordenador datos correctos que son tratados adecuadamente por el programa. Es decir, cuando el funcionamiento del *software* no sufre alteración, sino sólo la persona que no debe autorizarlo, no es posible hablar de manipulación informática en el sentido del tipo penal". Suárez Sánchez (2010, p. 254).

23 Suárez Sánchez (2010, p. 245) define el uso falso de tarjetas no es transferencia. Ello solo resulta cierto si en Colombia el sujeto activo obtiene finalmente dinero (cosas muebles), pero es absolutamente discutible si, por ejemplo, se pagan cuentas ajenas o sólo se realizan traslados de fondos. También: Álvarez García et al (2011, pp. 252-253).

bb) En sentido amplio o criminológico. Así, por ejemplo, Faraldo Cabana (2007, pp. 39, 42-47) define acertadamente la acción manipuladora informática del sujeto activo como

> la introducción, alteración, borrado o supresión indebidos de los datos informáticos, especialmente datos de identidad, y la interferencia indebida en el funcionamiento de un programa o sistema informáticos. Por tanto, se incluyen tanto la introducción de datos falsos como la introducción indebida, por no autorizada, de datos reales, auténticos en el sistema, pasando por la manipulación de los ya contenidos en cualquiera de las fases del proceso o tratamiento informático, así como las interferencias que afectan al propio sistema o programa[24]. Lo que incluye, por ejemplo, el uso no autorizado de tarjetas y claves falsas o sustraídas o de los datos ciertos del titular, en un sistema que funciona de modo correcto[25]. *Postura que es plenamente adecuada para nuestro medio jurídico*.

Por su parte, Anarte Borrallo señala: "debe quedar claro que la "manipulación" no implica una simple alteración de datos o funciones informáticas, sino que conlleva algo más, una actividad modificativa mendaz o subrepticia, una utilización "irregular" de un sistema informático, de sus presupuestos básico o de las órdenes que recibe de modo que produzca resultados no previstos o que de conocerlos no se habrían autorizado (Anarte Borrallo, 2010, pp. 233-234).

b) La segunda modalidad consiste en un "*artificio semejante"*, acción que también ha sido definida de dos maneras distintas. Por una parte, la doctrina internacional ha entendido que la expresión "artificio semejante" incluye en el tipo penal, con el propósito de asimilar la obtención de un servicio sin pagar su costo, aquellas transferencias no informáticas de un activo patrimonial, por medio de manipulaciones mecánicas. En palabras de Choclán Montalvo (2006, pp. 78-79) para "[...] poder castigar también las manipulaciones en máquinas automáticas que proporcionan servicios o mercancías sin que pueda decirse que en el caso concreto la manipulación o maquinación llevada a cabo para apoderarse del objeto o disfrutar del servicio haya de calificarse propiamente de informática". Evento que sería una verdadera hipótesis de hurto calificado o -por especialidad- una hipótesis del discutible tipo vertido en el artículo 269I, pero no una transferencia de activos no consentida. Por el otro, como una modalidad de defraudación para abarcar aquellos comportamientos que han sido definidos como manipulaciones informáticas en sentido amplio.

En cualquier caso, si bien esta fórmula ha sido criticada por vulnerar el principio de taxatividad (Faraldo Cabana, 2009, pp. 44-ss.; Suárez Sánchez, 2010, pp. 251-263) (CP/art. 10), también, ha sido justificada político-criminalmente con argumentos de *innovación tecnológica*, precisa-

24 Cfr. Faraldo Cabana (2009, pp. 89-90),

25 González Rus (2011, pp. 495 y 497), pero por la vía de los artificios semejantes; Gutiérrez Francés (1991, p. 114), también afirma que tienen cabida todos los comportamientos de manipulación, abuso o interferencia; Palazzi (2009, p. 171); Polaino Navarrete et al (2011, pp. 98-99): "La manipulación informática abarca cualquier alteración que afecte en sentido amplio el procesamiento de datos (se trate de manipulación de información o de funciones informáticas) o, en definitiva, suponga una interferencia lícita en el procesamiento de datos que obtenga un abusivo resultado transferencial". También adopta una concepción amplia de manipulación el CP italiano/art. 640-ter, pues además de la alteración por cualquier medio, castiga la intervención sin derecho con cualquier modalidad de sus datos; (Rovira del Canto, 2002, pp. 261-262 y 267, 583).

mente para evitar la inutilidad prematura de los medios a través de los cuales pueda ser obtenida la transferencia patrimonial de activos. La doctrina reclama, en consecuencia, que lo *semejante* también asuma un sentido informático[26].

Finalmente, debe tenerse en cuenta que el tipo penal implica de manera inherente que el sujeto activo que utilice datos falsos o datos correctos, pero, de manera ilegítima, también esté empleado códigos o datos personales de terceros sin facultades para ello (Violación de datos personales CP/art. 269F), y, por consiguiente, suplante en su uso al titular legítimo que tiene el derecho a usarlos. Es decir, que el medio informático semejante (que no deja de ser una manipulación informática), podría ser la suplantación.

7. El resultado

Se trata de un tipo penal de lesión y resultado que consiste en la transferencia contable y automática de cualquier clase de activos o valores (dinero escritural o contable) no autorizada y no consentida por su titular en perjuicio de un tercero (despatrimonialización efectiva por imposibilidad de disposición de los mismos). Por tal motivo, la doctrina mayoritaria considera que es un tipo penal de consumación instantánea y de efectos permanentes, en particular, cuando la manipulación de la cual se vale el sujeto activo gravita en una modalidad de falsedad informática.

Justamente, el concepto de *transferencia* es ampliamente discutido por la doctrina y la opción que se asuma pude producir diversas consecuencias dogmáticas y político-criminales, por ejemplo, en materia de consumación y tentativa. En este sentido, la doctrina expone dos planteamientos (Suárez Sánchez, 2009, 268):

a) El primero sigue directrices *comerciales* y define la transferencia como la operación automática de un equipo, terminal o sistema informático o telemático, en virtud de la cual se transfiere una cantidad de dinero de una cuenta bancaria (de ahorros o corriente) a otra cuenta. Se trata de una noción fundamentalmente *fáctica*, cuyo eje central es la manipulación de los datos o de la información, que causa o produce un cambio de adscripción de titular respecto del objeto sobre el cual recae la acción criminal (Rovira del Canto, 2002, pp. 584-588)[27]. Cambio que, *de hecho*, implica el traspaso de activos intangibles con la subsiguiente afectación patrimonial.

b) El segundo planteo asume una noción *crediticia* y afirma que la transferencia consiste en una operación que varía la adscripción formal de las partidas previstas. A diferencia de la anterior, esta es una noción de traslado contable bilateral (sujeto pasivo-beneficiado (Suárez Sánchez, 2009, p. 269), que requiere usualmente que la operación mercantil sea autorizada mediante un asiento contable que refleje la anotación del activo y la creación de un pasivo informáticos. La doctrina mayoritaria considera que esta es la

26 A lo cual, Suárez Sánchez (2010, p. 265) replica que si es informático "es difícil que el artificio no sea al mismo tiempo manipulación informática", lo que implica que sea un concepto inútil.

27 Rovira del Canto (2002, pp. 584-588), quien habla de "un cambio fáctico de adscripción patrimonial del objeto material del resultado"; De la Mata Barranco et al (2010, p. 182); Faraldo Cabana (2009, p. 105): señala que el activo patrimonial no tiene que estar representado por anotaciones o registros informáticos.

noción correcta de transferencia (González Rus, 2011, pp. 495-496)[28].

En materia bancaria, por ejemplo, la transferencia es un *medio de pago* que consiste en una orden o conjunto de instrucciones electrónicas por parte de un ordenante a una entidad de crédito (mediador), para que esta tome parte de los fondos de su cuenta (de ahorros o corriente) y los deposite en otra cuenta propia o de otra persona física o natural, que para el caso sería el beneficiario. La transferencia puede ser débito o crédito de descuento inmediato, pero de aplicación inmediata o diferida. Precisamente, en este sentido la Circular Externa 026 de junio de 2008, de la Superintendencia Financiera de Colombia, numeral 1.11, define las transferencias como

> La transacción efectuada por una persona natural o jurídica denominada ordenante, a través de una entidad autorizada en la respectiva jurisdicción para realizar transferencias nacionales y/o internacionales, mediante movimientos electrónicos o contables, con el fin de que una suma de dinero se ponga a disposición de una persona natural o jurídica denominada beneficiaria, en otra entidad autorizada para realizar este tipo de operaciones. El ordenante y el beneficiario pueden ser la misma persona.

Dicha transacción quedaría legitimada y solo existiría una vez que se hayan superado las medidas de identificación y autenticación dispuestas para la protección de los usuarios titulares de los derechos económicos protegidos. Recuérdese que la clave es, para estos efectos, la firma del titular de la cuenta (L. 527 de 1999/ art. 7°), con lo cual, se repite, la operación será exitosa a partir de la aprobación electrónica del mediador[29].

Finalmente, la discusión sobre la noción de transferencia puede llevar a situar la figura de la tentativa en dos momentos distintos (CP/art. 27). Así, de seguirse la primera postura, se podría predicar la tentativa de transferencia hasta el momento en el que se "consigue" el traspaso fáctico de los activos patrimoniales, pues, se estima que dicha obtención de fondos afecta el patrimonio económico del sujeto pasivo. Por el contrario, si se acoge la segunda posición jurídica, la obtención del traspaso de activos seguiría siendo tentativa del delito hasta que no quede perfecta la operación comercial mediante la correspondiente anotación contable informática.

La discusión no es nada fácil, pues así como no existiría una consumación típica de transferencia no consentida cuando (solo) se produzca la anotación contable de una fallida operación comercial de transferencia de activos[30], (caso en

28 González Rus (2011, pp. 495 y 496): "[…] constituye un proceso inmaterial y meramente contable que supone cargar débitos, descontar activos u ordenar ingresos con la correlativa anotación a favor de otro sujeto, al que se reconoce, de esta forma, un derecho de crédito o en favor del que se realiza una cierta prestación o servicio"; González Rus *en Cobo del Rosal* (2000, p. 446); Suárez Sánchez (2009, p. 244, 269 y 273), señala: "[…] si bien es cierto que se produce el traslado de dinero del patrimonio al del sujeto pasivo al del sujeto activo, también lo es que no se da un traslado contable, que sólo se realiza mediante la anotación de un activo con la creación de un correlativo pasivo".

29 Superintendencia Financiera de Colombia, Concepto 2006033594-001 del 29 de agosto de 2006, advierte que: "[…] si la orden de transferencia electrónica de fondos no es aceptada por el sistema por no cumplir con algunos de los procedimientos o requisitos previstos por la respectiva entidad para considerarla como tal, ésta simplemente no surte efecto alguno, es decir, no existe a efectos de determinar el cumplimiento o no de la pretendida operación".

30 Anarte Borrallo (2010, p. 236) y Suárez Sánchez (2010, p. 246), señala: "Si se registra el retiro del dinero en el sistema y en ese

el que realmente habría una tentativa de delito), también, es cuestionable sostener la *inexistencia de la consumación* cuando, en hipótesis no tan excepcionales, el momento de la operación comercial efectiva (que incluye un peligro informático, la obtención de los activos y un perjuicio patrimonial para el sujeto pasivo o un tercero) no coincida con el momento del asiento contable, que puede ocurrir días después con la fecha de la operación comercial (cuando se abona el pago de una tarjeta de crédito un día domingo). En fin, aunque la noción de transferencia contable es la correcta, no resulta por completo satisfactoria, porque puede desproteger a las víctimas.

En todo caso, si el sujeto activo tenía la finalidad original de obtener cosas muebles mediante el uso ilegítimo o abusivo de tarjetas de crédito o débito, se estará ante una conducta típica inicial de *hurto por medios informáticos* (CP/art. 269I), tipo que se amplificará en las condiciones previstas por el art. 27 del CP. Un ejemplo sería el del sujeto que intenta obtener dinero (mueble) de un cajero electrónico utilizando tarjetas clonadas, manipulando el sistema y suplantando al titular, o intenta obtener otro tipo de cosas muebles mediante tarjetas débito o crédito. Por el contrario, si desde el principio el sujeto activo tenía el propósito de orientar su acción para conseguir una transferencia no consentida de activos (inmateriales), se aplicará el CP/art. 269J. Sería el caso del sujeto que desea pagar una cuenta de servicios ajena en un punto de pago, o transferir dinero de una cuenta a otra mediante un cajero electrónico (sistema informático) usando una tarjeta sustraída o "clonada".

En términos jurídicos el asunto se complica cuando, por ejemplo, para realizar el tipo de hurto por medios informáticos, el sujeto activo decide realizar previamente, como delito medio, una transferencia no consentida de activos a una cuenta propia o de un tercero. En este caso, la tipicidad concreta dependerá de lo ocurrido:

Si el sujeto activo logra obtener el dinero físico de la cuenta corriente o de ahorros del sujeto pasivo, entonces se tendrán una *transferencia de activos* y un *hurto por medios informáticos*, ambos consumados. Sin embargo, en esta hipótesis siempre se dará aplicación al tipo de *hurto por medios informáticos* (CP/art, 269I), porque el delito de transferencia no consentida de activos es formalmente subsidiario, y su aplicación condicionada cede ante la pena "más grave" del hurto.

Pero, si el sujeto no logra obtener el dinero físico de la cuenta corriente o de ahorros del sujeto pasivo, el hurto por medios informáticos solo sería una tentativa, mientras que la transferencia de dinero escritural, comportaría un delito consumado que tendría, inicialmente, una pena mayor. En este supuesto no opera el principio de subsidiariedad formal ni material, por lo que tendría plena aplicación la transferencia de activos no consentida consumada. No parece co-

momento se presenta una falla en el mismo que impida la entrega del metálico no puede decirse que se ha consumado el delito de transferencia no consentida de activos, a pesar de haberse registrado la operación que afecta el patrimonio del titular de la respectiva cuenta, porque no obstante que se ha dado el registro de un crédito, mediante la anulación de un activo en el patrimonio de la víctima, se echa de menos la transferencia patrimonial, que se materializa cuando aquel registro tiene una cancelación en otra operación contable". En contra: Faraldo Cabana (2009, p. 40) quien advierte que a veces una mera anotación contable ya puede suponer el perjuicio.

rrecto afirmar que, en esta hipótesis, prevalezca la aplicación de la tentativa de hurto (por querer obtener un objeto mueble), bajo el amparo del principio de especialidad.

Finalmente, recuérdese que el hurto por medios informáticos y la transferencia requieren de una manipulación que supone la suplantación inherente del titular legítimo de los datos o códigos personales del sujeto pasivo, aunque el tipo de hurto consagre dicha modalidad criminal, de manera expresa, como conducta alternativa a la manipulación.

c) Sobre el tema es preciso agregar dos consideraciones adicionales:

aa) La transferencia *no puede ser consentida.* Según la doctrina mayoritaria, dicho consentimiento no se debe entender como la pretensión de un acto concreto de voluntad del sujeto pasivo o del sujeto que tenga capacidad legítima para disponer de los activos patrimoniales, que demuestre la oposición a la transferencia; sino, como la ausencia de facultades jurídicas *ex ante* para realizarla o el abuso de una autorización previa. Naturalmente, el punto esencial está en la ausencia de facultades de disposición patrimonial (Anarte Borrallo, 2010, p. 236; González Rus, 2011, p. 496; Matellanes Rodríguez, 2000, pp. 139-140; Suárez Sánchez, 2009, p. 274); pero es evidente que si el sujeto activo consiente *ex ante* la realización de la transferencia, la conducta será plenamente atípica respecto de lo consentido, según lo prevé el CP/art. 32 num. 2.

Precisamente, la ausencia de facultades jurídicas puede ser total o parcial respecto del objeto inmaterial de la transferencia o frente al destinatario (Rovira del Canto, 2002, 591). Puede suceder que el titular de los datos (como dinero escritural) solo haya consentido una transferencia por determinado monto para un cierto beneficiario, pero el sujeto activo haya realizado dicha transferencia por más "dinero" de lo debido o por lo indicado para ese beneficiario y, por otro tanto, por ejemplo, para pagar una factura propia o de un tercero. También puede ocurrir que se haga la transferencia autorizada pero para un beneficiario no autorizado o, en fin, que ni la transferencia ni el beneficiario de esta hayan sido autorizados en lo absoluto. En tales casos es menester precisar, detenidamente, el objeto de la autorización, para proceder a estimar el objeto del injusto y el perjuicio causado con la transferencia de activos no consentida.

bb) El efecto correlativo de la transferencia es la *despatrimonialización efectiva* del sujeto pasivo, lo que implica un perjuicio efectivo de naturaleza patrimonial para este o un tercero[31]. En caso que el perjuicio no se presente, la doctrina discute la posibilidad de aplicar el dispositivo amplificador de la tentativa (CP/art. 27) en los términos ya señalados. Se trata, entonces, de un resultado complejo compuesto no solo por la transferencia sino por el perjuicio. Recuérdese que el verbo rector es el de "Conseguir" la transferencia y no el de "obtener" un provecho, como sucede en la estafa.

31 Álvarez, Majon-Cabeza y Ventura (2011, p. 253); Gutiérrez Francés (1991, p. 114), señala que el perjuicio no tiene que ser cuantificable.

Finalmente, se debe indicar que la norma penal no protege al sujeto pasivo frente a cualquier clase de perjuicio patrimonial, sino solo respecto de aquellos perjuicios que sean una consecuencia directa de una transferencia no consentida (autorizada o facultada) de activos. No así, por ejemplo, frente a actuaciones que resulten de una alteración o borrado de activos de titularidad del sujeto pasivo, lo que tipificará el delito de daño informático previsto en el CP/art. 269D (Faraldo Cabana, 2009, p. 38); o frente a simples fallas del sistema que, no obstante generar perjuicios, resultan atípicas.

8. Debe existir un *nexo de causalidad directo* entre la acción de manipulación *informática subrepticia* dirigida a obtener activos patrimoniales mediante una transferencia y, entre esta transferencia, la consecución de activos y el correlativo perjuicio para el titular o un tercero. De tal manera que tampoco se trata de cualquier clase de transferencia. De todas maneras, es necesario matizar este tipo de exigencias en aspectos que, como se sabe, se surten en un espacio virtual.

En este sentido, como se dijo ya, si un ser humano interviene en forma directa y de manera determinante en la producción del resultado patrimonial (obtención de activos escriturales o disminución del pasivo, etc.), en relevo del sistema informático (lo que sería una alteración mecánica, no informática), el comportamiento punible se encuadraría típicamente en el ilícito de estafa tradicional o en un hurto por medios informáticos[32]. Sin embargo, no basta que se dé cualquier intervención humana para que esto ocurra como, por ejemplo, que el dependiente de un almacén introduzca la tarjeta débito en el respectivo dispositivo de pago en la terminal (datafono), hipótesis que no deja de ser una "estafa informática".

Además, el resultado dañoso tiene que poder serle imputado objetivamente al sujeto activo (o coautores), así: en primer lugar, la transferencia debe involucrar un riesgo jurídicamente desaprobado para el patrimonio económico que, como es evidente, refuerce el riesgo también desaprobado que ha sido creado previamente por la manipulación informática respecto de la seguridad de los datos, la información o el sistema informático protegido. Es importante verificar si sujeto activo tenía el dominio del hecho sobre la introducción de las órdenes dadas al sistema informático. En segundo lugar, el riesgo creado debe traducirse en el resultado jurídico típico de carácter patrimonial e informático (lo que se discute, aunque no es muy claro, es si aquí tiene cabida aceptar las acciones a propio riesgo y las acciones negligentes como actos de suicidio informático) y, finalmente, en tercer lugar, el perjuicio causado debe quedar cubierto por los riesgos prohibidos incluidos en el diseño de la norma prohibitiva. En caso de no existir ninguna posibilidad de afectación (directa o indirecta) por la acción defraudadora, no cabe hablar de un delito informático sino de un delito patrimonial común (Quintero Olivares, 2011, p. 650; Rovira del Canto, 2002, pp. 188 y 261).

32 Sería el caso de una estafa realizada por medios informáticos (CP/art. 246, agravado por el art. 58 num. 17), a través de la cual un sujeto ofrece, sirviéndose de un medio informático, un determinado producto a otra persona, quien acepta su compra y cumple transmitiendo el pago electrónico de su valor, sin que el producto exista o el que se ha ofrecido coincida en calidad, peso o medida al producto realmente enviado. Asunto que conocía previamente el sujeto activo. Suárez Sánchez (2011, p. 270).

9. Aspecto subjetivo: a) Dolo (CP/art. 22)

Se requiere que el sujeto activo conozca y quiera la realización de una conducta dirigida: en primer lugar, a manipular en sentido informático un sistema de tratamiento, procesamiento y transmisión de datos informatizados; y, en segundo lugar, a conseguir una transferencia no facultada de activos patrimoniales de otros, con perjuicio para este o un tercero. Naturalmente, el sujeto debe querer hacerlo.

El conocimiento del dolo deberá abarcar: (i) las circunstancias de hecho que establecían la protección de la información informatizada y de los propios sistemas informáticos; (ii) la ausencia de facultades de disposición (que no es igual al conocimiento potencial de la ilicitud) y, a grandes rasgos, (iii) el plan de ataque valiéndose de una manipulación informática y la previsión del nexo de causalidad y del resultado típico. El dolo se prueba a través de los medios de prueba dispuestos en la legislación procesal vigente (CPP, L. 906 de 1994/arts. 372-ss.).

b) **Ánimo de lucro:** (*animus decipiendi* o *consilium fraudis*) se trata del elemento subjetivo especial distinto del dolo típico, que caracteriza la infracción como un delito de tendencia y, en particular, especifica el beneficio, la ventaja o la utilidad genéricos que el sujeto activo busca obtener en perjuicio de otro, a partir de la acción delictiva dolosa. Por consiguiente, resulta claro que el tipo requiere de dolo de primer grado[33].

Téngase en cuenta que si el sujeto activo no tiene ánimo de lucro genérico, si no otro propósito (como suele ocurrir entre aquellos jóvenes que buscan retos tecnológicos), el tipo aplicable no sería el de *transferencia no consentida de activos* sino el de *Obstaculización ilegítima de sistema informático o red de telecomunicación* (CP/art. 269B), por lo que atañe a la obstaculización o impedimento para acceder a los datos representativos de dinero contable o escriturales por parte de su titular (p. e. sin ánimo de lucro un sujeto trasfiere a otra cuenta el dinero, pero sin buscar beneficio de lucro u otro fin ilícito posterior), así este solo lo haya hecho para demostrar la vulnerabilidad del sistema informático o telemático atacado.

10. Agravante particular

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a doscientos salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad (6 a 15 años de prisión y multa de 300 s.m.l.m.v.). En este caso, es claro que la agravante se fundamenta en un mayor desvalor de resultado objetivo de carácter patrimonial.

Aunque no es el tema de este escrito, debe precisarse que a este artículo se le aplican de manera exclusiva las agravantes previstas en el art. 269H y no las agravantes que corresponda aplicar a los delitos patrimoniales comunes como, por ejemplo, las previstas en el CP/art. 241 (hurto agravado).

33 En contra: Suárez Sánchez, *La estafa informática*, p. 307, quien advierte que "[…] así como se admite el *dolo eventual* en la estafa común *también ha de ser aceptado en la informática*".

Fabricación, introducción, posesión y facilitación de software defraudatorio

El segundo tipo penal previsto en el artículo 269J, en el inciso segundo, consiste en la fabricación, introducción, posesión y facilitación de *software* destinado a delitos de transferencia no consentida de activos y estafas, en los siguientes términos: "La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa".

La doctrina mayoritaria critica severamente esta figura penal, pues considera excesivo castigar un simple delito de anticipación, tenencia de instrumentos "objetivamente peligrosos", mera conducta y peligro en abstracto por sospecha, como una conducta previa o preparatoria de un fraude informático (Álvarez García y Olmeda, 2011, p. 254; Corcoy Bidasolo et al, 2004, p. 589; Faraldo Cabana, 2009, p. 109 y ss.; González Rus, 2011, p. 498; Muñoz Conde, 2007, p. 423, habla de una protección reforzada al sistema informático; Polaino Navarrete et al, 2011, p. 100, señala que castiga actos previos a la tentativa de transferencia o estafa; Suárez Sánchez, 2009, pp. 302 y 303; Quintero y Morales, 2011, p. 669; Suárez-Mira et al, 2004, p. 246), con la misma penalidad imponible al delito consumado de transferencia no consentida de activos, en clara infracción al principio de proporcionalidad y ofensividad material (CP/art. 11).

1. Sujeto Activo

Monosubjetivo y común: "El que": cualquier persona natural que, por sí misma o empleando a otra persona como instrumento, realice los verbos rectores previstos en la norma jurídica. En términos nacionales, el tipo admite la coautoría y otras formas de autoría, y las diversas formas de participación criminal: (i) determinación, (ii) complicidad y (iii) intervención (CP/arts. 29 y 30).

2. Sujeto Pasivo

Monosubjetivo y colectivo. Solo puede ser sujeto pasivo de este tipo la colectividad como conjunto de sujetos protegibles en términos de la seguridad de la información informatizada de contenido económico y los sistemas informáticos y telemáticos, usualmente de naturaleza financiera.

3. Objeto Jurídico

A simple vista, se trata de un cuestionable tipo de peligro o amenaza en abstracto que anticipa la protección penal de la confiabilidad, disponibilidad y control de las funciones informáticas que permiten el almacenamiento de la información y la seguridad propia de los sistemas y redes informáticas y telemáticas, de contenido y naturaleza económicas.

4. Objeto sobre el cual recae la acción

Inmaterial e impersonal determinable, como el *software* o programa informático idóneo *desti-*

nado a la comisión de delitos de transferencia no consentida de activos o delitos de estafa. Precisamente, por *software* se entiende:

> La expresión de un conjunto de instrucciones mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador, un aparato electrónico o similar capaz de elaborar informaciones, ejecute determinada tarea u obtenga determinado resultado. El programa de ordenador comprende también la documentación técnica y los manuales de uso[34]

Desde luego, la norma utiliza una expresión en extremo equivoca, cuando señala que no se trata de cualquier clase de *software* sino de uno "*destinado a*" la realización de ciertos delitos económicos; cuando es claro que este tipo de instrucciones usualmente son de doble vía, es decir, pueden ser manipuladas, introducidas y ejecutadas para la realización de actividades lícitas o ilícitas en términos informáticos[35]. De lo que se desprende, entonces, que la destinación ilegal del programa debe ser la esencial o inherente a su programación y no aquella destinación accidental que le pueda dar el sujeto activo en ciertas circunstancias, según sus habilidades o conocimientos[36].

Si se trata de otro *software* con efectos dañinos, entonces no tendría aplicación este tipo penal, sino el vertido en el CP/art. 269E "*Uso de software malicioso*", que se aplicaría de modo preferente con base en el principio de especialidad (Orts Berenguer y González Cussac, 2009, p. 572).

5. Verbo rector

Se trata de un tipo mixto de conducta alternativa, mera conducta y peligro abstracto que se perfecciona con la realización de cualquiera de los cuatro verbos rectores previstos por el legislador penal en la norma jurídica. Dichos verbos son: a) *Fabricar:* "4. tr. *Hacer, disponer o inventar algo no material*"; b) *Introducir:* "6. tr. *Establecer, poner en uso*", con lo cual se trata de aplicarlos al sistema informático en sentido estricto, lo que puede poner en peligro el bien jurídico seguridad de la información; c) *Poseer*: "tr. Dicho de una persona: *Tener en su poder algo*" y d) *Facilitar*: "2. tr. *Proporcionar o entregar*" [37].

Como es apenas evidente, se trata de un delito de peligro pues el *software* está destinado a la comisión de varios de estos hechos patrimoniales, sin que sea necesario que ello haya ocurrido ni siquiera en términos del inicio de actos ejecutivos (tentativa) de otro delito. Incluso, algunos autores sostienen que el tipo penal debe concursar con el tipo patrimonial, pues la lesión o peligro-concreto para un patrimonio determinado no puede subsumir materialmente el peligro abstracto que esta clase de instrumentos comportan para la seguridad de la información

34 Según la Decisión 351 de 1993/art. 2°. (Comunidad Andina de Naciones), indica: "El soporte lógico (software) comprende uno o varios de los siguientes elementos: el programa de computador, la descripción del programa y el material auxiliar".

35 Álvarez et al (2011, p.254) señalan que las posibilidades de identificar programas destinados sólo a realizar estos delitos es muy escasa, además de ser muy difícil la prueba de la destinación. También revisar Faraldo Cabana (2009 p. 112).

36 Cfr. Polaino Navarrete et al (2011, p. 100); Quintero Olivares et al (2011, p. 651). Precisamente, González Rus (2011, p. 498).

37 Todas las referencias son tomadas de http://www.rae.es/

y los patrimonios posiblemente afectados de la colectividad (Faraldo Cabana, 2009, pp. 115-116).

6. Aspecto subjetivo

Dolo. Para el caso se requiere que el sujeto activo conozca realización de una conducta dirigida *fabricar*, *introducir* (usar), *poseer* o *facilitar* a terceros programas "destinados", de modo específico, para la comisión de delitos de transferencia no consentida de activos o delitos de estafa, y que quiera fabricarlos, ejecutarlos, poseerlos o facilitarlos para que sean empleados luego por quienes los adquieran o por él mismo para comenzar dichas consumaciones típicas, con ánimo de lucro (Faraldo Cabana, 2009, p. 114). Naturalmente, ello no admite dolo eventual (Serrano Gómez et al, 2009, p. 436). La ambigüedad del tipo solo podría ser superada si el legislador nacional introduce finalidades delictivas posteriores.

IV. CONCLUSIONES

Los delitos informáticos de naturaleza económica están a la orden del día. El legislador de 2009 los consagró con el fin de evitar transferencias o apropiaciones masivas de fondos y activos de cuentahabientes, dada la precariedad dogmática de los tipos penales tradicionales para castigar esta clase de comportamientos delictivos. Actuaciones cuya ocurrencia genera una creciente desconfianza en los sistemas legales y de seguridad vigentes para proteger el patrimonio económico en el tráfico automático de pagos o transacciones financieras. Por ello, no se trata de tipos delictivos comunes. Su naturaleza y el bien jurídico protegido permiten interpretarlos como verdaderos tipos penales autónomos que protegen la seguridad de la información informatizada (bien jurídico colectivo e intermedio) y, en particular, las funciones informáticas referidas a la protección de ciertos bienes personales o personalísimos.

El legislador penal colombiano ha empleado una técnica legislativa muy discutible al consagrar los tipos penales que buscan proteger la seguridad de la información y el patrimonio económico. Por una parte, resulta cuestionable el empleo excesivo de elementos normativos a la hora de crear los tipos penales, cuya interpretación es objeto de una viva polémica por parte de la doctrina dominante. Es justamente lo que sucede con los conceptos de "manipulación", "artificio semejante" y "transferencia", que no encuentran un sentido y unos efectos unívocos cuando se trata de acotar el alcance del tipo penal de transferencia no consentida de activos. Todo ello en franca violación del principio de taxatividad penal (CP/art. 10). Por la otra, es claro que no está justificada la implantación típica hecha por el legislador, que ha copiado sin mayores reflexiones dogmáticas y político criminales la norma penal vigente en el CP español (ref. 1999), prevista en el art. 248.2, con todos los problemas que ella tiene, que ahora quedan reflejados en nuestro ordenamiento jurídico.

Por ello, para una mejor protección de los bienes jurídicos, en el texto se opta por acoger un concepto amplio de *manipulación informática,* que permita incluir aquellos actos defraudatorios que, con claridad, no quedan cubiertos por

el alcance normativo de tipos penales ordinarios o especiales como la estafa, el hurto por medios informáticos o el hurto calificado. En el mismo sentido, se defiende una noción mercantil o contable del concepto de transferencia, sin desconocer que esta es una noción imperfecta para hipótesis límite, cuando el momento de la anotación contable no coincida con el momento de la operación comercial o financiera.

Igualmente, para el autor resulta muy difícil defender la hipótesis de *Tenencia de elementos peligrosos* prevista en el mismo CP/art. 269J, pues no solo resulta de peligro en abstracto y pura peligrosidad objetiva y presunta, lo que contradice el CP/art. 11, sino también porque su prueba es muy difícil, dada la redacción de la figura típica. Se trata, pues, de una norma expansiva e ilegítima, que contradice los principios liberales de nuestro ordenamiento jurídico penal, por lo que puede tacharse de inconstitucional (CN/art. 4°).

Bibliografía

Álvarez García, F. et al. (2011). *Derecho penal español, parte especial*. Valencia: Tirant lo Blanch.

Anarte Borrallo (2010). "Incidencias de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información", en *Derecho y conocimiento* 1. 191-257.

Borja Jiménez, E. (2003). *Curso de política criminal*. Valencia: Tirant Lo Blanch.

Campoli, G. (2005). "Pasos hacia la reforma penal en materia de delitos informáticos en México" *Revista de Derecho Informático Alfaredi Derecho y Nuevas Tecnologías* 079.

Castro Ospina, S. (2002). "Delitos Informáticos: La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano", en: *XXIII Jornadas Internacionales de Derecho penal*, Memorias, Bogotá: Universidad Externado de Colombia, Departamento de Derecho Penal.

Champaud, C. (1990). "El impacto de las nuevas tecnologías en la empresa", en *Revista del derecho industrial* 33. pp. 815 y ss.

Choclán Montalvo, J. (2006). "Infracciones patrimoniales en los procesos de transferencia de datos", en: AA.VV., *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*.

Corcoy Bidasolo et al. (2004). *Manual práctico de derecho penal* (2ª ed.).Valencia: Tirant lo Blanch.

De la Mata Barranco, N. y Hernández Díaz, L. (2010). "Delitos vinculados a la informática en el derecho penal español", en: *Derecho penal informático.* Universidad del País Vasco: Instituto Vasco de Criminología, Civitas-Thomson-Reuters.

Faraldo Cabana, P. (2009). *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socio-económico.* Valencia: Tirant lo Blanch.

Faraldo Cabana, P. (2007). "Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática". en: *Eguzkilore* 21. San Sebastián: Cuaderno del Instituto Vasco de Criminología.

Farjat, G. (1990). "Nuevas tecnologías y derecho económico". *Revista del Derecho Industrial* 33, pp. 530 y ss.

Fiandaca, G. y Musco, E. (2007). *Diritto penale, parte speciale* II. (2), I delitti contro il patrimonio, (5ª ed.). Bologna, Zanichelli.

González Rus, J. (2011). "Delitos contra el patrimonio y contra el orden socioeconómico (V)". *Sistema de derecho penal español*. Madrid: Dykinson, 2011.

_____. (2000). "Delitos contra el patrimonio". En *Compendio de Derecho penal español.* Barcelona-Madrid: marcial Pons.

_____. Protección penal de sistemas, elementos, datos, documentos y programas informáticos (Revista Electrónica de Ciencia Penal y Criminología RECPC, 01-14- 1999) (en línea). Granada, CRIMINET, Web de Derecho Penal y Criminología, 2004. http://criminet.ugr.es/recpc/recpc_01-14.html.

Giménez García, J. (2006). "Delito e informática: algunos aspectos de derecho penal material". *Eguzkilore* 20. San Sebastián.

Gutiérrez Francés, M. (1991). *Fraude informático y estafa.* Madrid: Ministerio de Justicia.

Hernández Díaz, L (2009). "El delito informático". *Eguzkilore* 23 San Sebastián: Cuaderno del Instituto Vasco de Criminología.

Mantovani, F. (2009). *Diritto penale*, *parte speciale*, II, Delitti contro il patrimonio. (3ª ed.) Padova: CEDAM.

Márquez Escobar, C. *El delito informático, la información y la comunicación en la esfera penal.* Bogotá: Leyer, S.F.

Mata y Martín, Ricardo M. (2006) "Perspectivas sobre la protección penal del Software". *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales* 78., 97-ss.

Matellanes Rodríguez, N. (2000). "Algunas notas sobre las formas de delincuencia informática en el Código penal", en: *Hacia un Derecho penal sin fronteras*, María Rosario Diego Díaz-Santos y Virginia Sánchez López (Coord.), XII Congreso universitario de alumnos de derecho penal, Madrid, Colex, pp. 129-147.

Möhrenschlager, M. (1992). "Tendencias de política jurídica en la lucha contra la delincuencia relacionada con la informática". *Delincuencia informática, Francisco Baldó Lavilla y Santiago Mir Puig* (trads.). Barcelona: PPU.

Morón Lerma, E. (2002). *Internet y derecho penal: "Hacking" y otras conductas ilícitas en la Red*. (2ª ed.). Navarra: Aranzadi.

Muñoz Conde F. (2007), *Derecho penal*, parte especial, 16 ed., Valencia, Tirant Lo Blanch.

Orts Berenguer, Enrique. y González Cussac, J. (2004). *Compendio de derecho penal*, Valencia: Tirant lo Blanch.

Palazzi, Pablo A. *Los delitos informáticos en el código penal.* Buenos Aires: Bogotá-México-Santiago, Abeledo Perrot, 2009.

Picotti, L. (2006). "Internet y derecho penal: ¿Un empujón únicamente tecnológico a la armonización internacional?". *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminale*s. Granada: Comares.

Del Pino, L. (2009) *Diritto penale, parte speciale*. (17ª ed.). Napoli.

Polaino Navarrete, M. et ál. (2011). *Lecciones de derecho penal, parte especial*, T. II, Madrid: Tecnos.

Posada Maya, R. (2006). "Aproximación a la criminalidad informática en Colombia". *Revista de derecho, comunicaciones y nuevas tecnologías* 2. pp. 11-60.

Quintero Olivares, G. y Morales Prats, F. (Coord.), et ál. *Comentarios a la parte especial del derecho penal*. (5ª ed.). Navarra: Thomson-Aranzadi.

Rapport explicatif del convenio, Párr. II sobre los trabajos preparatorios §§ 7-15 en: www.coe.w.int.

Reyna Alfaro, L. (2011). "El bien jurídico en el delito informático". *Revista Jurídica del Perú* LI. (21) pp. 181-190.

Romeo Casabona, C. (2006). "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal". *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales.*

_____. "Los datos de carácter personal como bienes jurídicos penalmente protegidos". *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*.

_____. *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las nuevas tecnologías de la información*. Madrid: Tudesco, 1987.

Rodríguez Gómez, C. (2003). "Criminalidad y sistemas informáticos". *El sistema penal frente a los retos de la nueva sociedad*. Madrid: Colex, 2003.

Rovira del Canto, E. (2002). *Delincuencia informática y fraudes informáticos*. Granada: Comares.

Sanz Mulas, N. (2003). "La validez del sistema penal actual frente a los retos de la nueva sociedad". *El sistema penal frente a los retos de la nueva sociedad*. Madrid: Colex.

Schwarzenegger, C. "Computer crimes in cyberspace. A comparative analysis of criminal law in Germany, Switzerland and northern Europe", en: http://www.weblaw.ch/jusletter/artrtikel.jsp?articleNr=1957.ok.2002.Jusletter 14, Oktober 2002, www.jusletter.ch

Serrano Gómez, A. y Serrano Maíllo, A. (2009). *Derecho penal, parte especial*. (14ª ed.). Madrid: Dykinson.

Sieber, U, (1992). "Criminalidad informática: peligro y prevención". *Criminalidad informática*. Barcelona: PPU.

Suárez Sánchez, A. (2010). "El hurto por medios informáticos y semejantes a través de la utilización de tarjeta magnética falsa o ajena en cajero automático". *Estudios de derecho penal*. Bogotá: Universidad de Bogotá Jorge Tadeo Lozano.

_____. (2009). "La estafa informática". *Biblioteca de tesis doctorales* 5. Bogotá: UNAB-Ibáñez.

Suárez-Mira Rodríguez, C. (Coord.) et ál. (2004). *Manual de derecho penal*. (2ª ed.). Madrid: Thomson-Civitas, Madrid.

Tiedemann, K. (1985). "Criminalidad mediante computadoras". *Nuevo Foro Penal* 30 pp. 481-492.

_____. (2007). *Derecho Penal y nuevas formas de criminalidad*. (2ª ed.).. Lima: Manuel Abanto Vásquez.