El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico

Autora: Dra. Josefina García García-Cervigón
Profesora Asociada del Departamento de Derecho Penal.
Universidad Nacional de Educación a Distancia.

Resumen

Este artículo pretende dar una perspectiva jurídico penal y criminológica general de los aspectos más relevantes del fraude informático en España e Italia. Se destacan las diferencias y similitudes de ambas legislaciones. Y se describen los aspectos criminológicos de forma general y simultánea al darse los mismos aspectos en ambos países.

Palabras clave: estafa, fraude informático, derecho penal, criminología, España, Italia.

Abstract

This article aspires to give a general penal and criminological legal perspective of the most relevant aspects of the computer fraud in Spain and Italy. It emphasizes the differences and similarities between both legislations. And it describes the criminological aspects in a general and simultaneous approach as the same aspects exist in both countries.

Key words: Swindling, computer fraud, criminal law, criminology, Spain, Italy.

Recibido: 01.12.2007
Aceptado: 18.01.2008

I. El delito informático

Abordar el estudio del tipo descrito en el art. 248.2º[1] del Código Penal español, fraude informático, y del tipo descrito en el art. 248.3º[2] (actos preparatorios de futuro y de participación), así como la tipología de la legislación italiana[3], requiere un breve análisis del delito informático[4]. Pues informática e Internet constituyen un medio por el que pueden lesionarse diferentes bienes jurídicos[5].

Internet nace en EE.UU en la Guerra Fría, desarrollándose en los años ochenta y extendiéndose hasta la actualidad a todo el mundo. Esta generalización de la red conlleva ciertos problemas entre los que se encuentra la carencia de mecanismos efectivos de autocontrol y la proliferación de actividades delictivas. Pero Internet se ha convertido en el centro de las nuevas tecnologías de la información y las telecomunicaciones rompiendo con todas las barreras geográficas y políticas.

Por ello, el Derecho penal ha de adaptarse a las novedades sociales y los riesgos que suponen[6]. A veces, estos riesgos no permitidos tienen una magnitud desconocida.

[1] Art. 248.2º del CP: "También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".

[2] Art. 248.3º del CP: "La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a al comisión de las estafas previstas en este artículo".

[3] El fraude informático se regula en el art. 640ter del Codice Penale sancionando al que de cualquier modo altere el funcionamiento de un sistema informático o telemático o interviniendo sin derecho con cualquier modalidad sobre los datos, informaciones o programas contenidos en un sistema informático o telemático o a ellos concernientes, procurando para sí o a otro un injusto provecho con daño para otro, siendo castigado con reclusión de seis meses a tres años y con multa de 51 euros a 1.032 euros. La pena se eleva si concurre alguna de las circunstancias del 640.2º. 1 o bien si el hecho es cometido con abuso de la cualidad de operador del sistema. El delito es punible por querella de la parte ofendida, salvo que concurra alguna de las circunstancias del 2º o alguna otra circunstancia agravante.

Y el 640quatre observa la aplicabilidad del art. 322ter (comiso de bienes).

[4] Un sector doctrinal prefiere la denominación 'delitos informáticos' definiéndolos como "todos aquellos delitos que se relacionan directa o indirectamente con el medio informático (ordenadores, miniordenadores, microordenadores, equipos de tratamiento de textos, redes de telecomunicaciones y otros equipos informáticos, software, ficheros de datos y bases de datos)"; véase, SNEYERS, Alfredo, *El fraude y otros delitos informáticos*. Madrid: Tecnologías de gerencia y producción, S.A, 1990, 15.

[5] Para Ruggiero el desarrollo en el ámbito de las actividades realizadas en el entorno telemático determinará una tendencia a la disminución de los delitos convencionales y a un incremento exponencial de los delitos conexos al ciberespacio; véase, RUGGIERO, Francescopaolo, "Ciberspazio e diritto penale: il problema del bene giuridico", en *Revista Penale,* (2001), 213.

[6] "Es inevitable que la difusión de la tecnología informática influya en el Derecho"; véase, ZENO-ZENCOVICH, Vincenzo, "Informatica ed evoluzione del Diritto", en *Il Diritto dell'informazione e dell'informatica*, (gennaio-febbraio, 2003), 89.

En este sentido, la delincuencia informática y las nuevas formas de criminalidad unidas a la misma implican una cierta incertidumbre sobre todas las posibilidades criminales que conlleva. De ahí la necesidad de un cierto control en la red para prevenir posibles daños y de ahí que los diferentes gobiernos de la Unión Europea hayan trabajado en la Convención del Consejo de Europa sobre delincuencia informática de 23-11-2003 en Budapest con la finalidad de unificar legislaciones[7]. En el ámbito del fraude informático se dice que no ha estado acertada dicha Convención pues no hay una definición de estafa, no hay respuesta clara a la utilización abusiva de tarjetas[8].

No obstante, la rapidez de cambios en la red hace que la legislación adoptada por los diferentes países se muestre lenta.

Estamos ante un delito que trasciende fronteras con el consiguiente problema que ello supone[9]. A pesar de esta forma de delincuencia hay quien se cuestiona la necesidad o no de intervenir penalmente en la red. Discusión planteada máxime cuando actualmente se está viviendo una expansión del Derecho penal[10]. A pesar de dicha expansión se dice que no cabe la intromisión estatal en la regulación del mundo virtual pues podría vulnerarse la libertad.

El legislador español partió de la base de regular el problema informático específicamente y optó por la modificación de los tipos tradicionales completándolos con las necesidades requeridas para adaptarlos a las peculiaridades del delito informático[11]. Éste se concreta en tipologías cuyos bienes jurídicos afectan a las personas[12] y aquellos otros que afectan al patrimonio[13]. Estamos ante una categoría penal autónoma,

---

[7] De ahí que se trabaje sobre una Convención y no sobre una Recomendación. Dicha unificación se concreta en: derecho penal, procesal, coordinación policial, etc.

[8] Opinión manifestada por Morales García; véase, MORALES GARCÍA, Óscar, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre cyber-crime", en *Delincuencia informática, problemas de responsabilidad*, Cuadernos de Derecho Judicial, (2002), 31.

El art. 8 de la Convención hace referencia a "(…) la causación intencionada y antijurídica de una lesión de la propiedad mediante: a. la introducción, alteración, borrado o eliminación de datos informáticos; b. cualquier forma de atentar contra el funcionamiento de un sistema informático con la intención de obtener, sin derecho a ello, un beneficio económico para sí mismo o para otro"

[9] "El ciberdelito constituye hoy un problema sustancialmente referido a optimizar los mecanismos procesales de lucha contra este tipo de criminalidad y, fundamentalmente, estrechar las relaciones internacionales de cooperación judicial"; véase, CHOCLÁN MONTALVO, José Antonio, "Fraude informático y estafa por computación", en *Internet y Derecho penal*, Cuadernos de Derecho Judicial, (X-2001), 311.

[10] Tal expansión se concreta en el derecho penal simbólico. Aunque frente a esta posición amplia está la que aboga por un derecho penal mínimo; véase, ÁLVAREZ VIZCAYA, Maite, "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red", en *Internet y Derecho penal*, Cuadernos de Derecho Judicial, (2001), 260 y 261.

[11] Las posibilidades de actuación del Derecho penal son dos: establecer tipos de equivalencia, esto es, cláusulas que complementen los tipos ya existentes o por el contrario establecer nuevos tipos penales. Para Álvarez Vizcaya ambos sistemas tienen ventajas e inconvenientes, debiendo entender que ambos sistemas no son incompatibles sino que pueden llegar a complementarse; véase, ÁLVAREZ VIZCAYA, "Consideraciones político criminales…", cit., 2001, 269 y 270.

[12] Descubrimiento y revelación de secretos, art. 197.2 en relación con el art. 200 del CP.

[13] Fraude informático (art. 248.2º en relación con art. 248.3º), daños informáticos (art. 264.2), propiedad intelectual (art. 270 in fine), descubrimiento de secreto de empresa (art. 278).

siendo coincidente el objeto de protección con el de los tipos tradicionales adaptados a las nuevas formas de comisión[14].

Nos podemos referir al fraude informático como una de las categorías de delitos económicos vinculados a la informática. Estamos ante atentados contra el patrimonio, tutelando un bien jurídico individual[15].

Esta clase de criminalidad informática se divide en: atentados patrimoniales contra elementos informáticos y atentados patrimoniales realizados por medio del sistema informático entre los que se encontraría el fraude informático en el que lo más característico es el modus operandis[16].

En la legislación italiana el carácter asistemático y desorganizado es la característica propia del delito informático[17]. Y se hace alusión a un Derecho penal de la informática en un doble sentido: a) como derecho que prevé y reprime específicamente las violaciones típicas de este particular sector, b) en un sentido amplio, como aquella especie del derecho de la informática que mira los ilícitos de carácter penal unidos al uso del ordenador[18].

II. Fraude informático. Aspectos penales

II.1. El fraude informático en España

El fraude informático o estafa por medios informáticos es una de las tipologías del cibercrimen en el que se da la defraudación por medios informáticos, es decir, la utilización del sistema informático como medio para transferir los activos patrimoniales a favor del autor (el desplazamiento es siempre virtual, es inaprensible[19]). Las denominaciones han sido diversas: estafa telemática, estafa por computación, fraude informático.

El fraude informático se regula en el art. 248.2[20] del CP español de 1995 siendo considerado por el legislador como una modalidad de la estafa aplicándosele los pre-

[14] CHOCLÁN MONTALVO, "Fraude informático…", cit., 2001, 314.

[15] Sólo mediatamente puede verse en la tutela del bien jurídico individual una dimensión de carácter socioeconómico, tesis seguida por Choclán Montalvo; ibid., 315.

[16] En palabras de Choclán Montalvo "(…) sólo se necesita poseer habilidades en el manejo de la informática (…)"; ibid., 318.

Se distingue, pues, entre patrimonio y propiedad siendo la estafa un delito contra el patrimonio en el que el sistema informático es un medio comisivo.

[17] Características destacadas por Militello; véase, MILITELLO, Vincenzo, "Iniziative sovranazionali di lotta alla criminalità organizzata ed al riciclagio nell'ambito delle nuove tecnologie", en *Diritto e informatica*, Pascuzzi(dir). Milano: Giuffrè Editore, 2002, pág. 93.

[18] SARZANA, Carlo, "Note sul diritto penale dell'informatica", en *La Giustizia Penale*, (prima parte, gennaio, 1984), 22.

[19] El carácter de inaprensibilidad lo destaca Álvarez Vizcaya, para quien esta característica hace que se vaya modificando poco a poco el perfil de los diferentes delitos; véase, ÁLVAREZ VIZCAYA, "Consideraciones político criminales…", cit., 2001, 274.

[20] Art. 248.2º del CP español: "2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".

ceptos relativos a la penalidad de la estafa y agravaciones, si bien las afinidades que presenta con la estafa genérica del art. 248.1º son mínimas. SUÁREZ GONZÁLEZ, estima que "lo correcto hubiera sido crear una figura autónoma no incardinada en la estafa"[21]. Lo cierto es que su regulación de una u otra manera ha sido bienvenida pues elimina la laguna legal existente hasta entonces.

Esta nueva tipología se introduce por razones político-criminales al existir una laguna legal en el caso de mediar manipulación informática ya que la defraudación de este tipo no era subsumible en la estafa y tampoco podía tipificarse en el hurto o la apropiación indebida. Además la L.O. 15/2003 de 25 de noviembre introduce un párrafo 3 vinculado directamente al fraude informático regulando actos preparatorios.

Centrándonos en el fraude informático es excesivo reconducir al mismo todo perjuicio patrimonial mediante manipulación informática[22], reduciéndose el ámbito a las defraudaciones patrimoniales por medios informáticos. Y éstas se manifiestan en la casuística de dos formas: las estafas mediante manipulaciones informáticas y las conductas ilícitas o abusivas mediante tarjetas magnéticas y su empleo en cajeros automáticos.

II.1.1. Elementos del fraude informático

El legislador establece al principio del art. 248.2 "también se consideran reos de estafa", expresión que a juicio de la doctrina cierra cualquier polémica y ello conlleva tres cosas: el sujeto activo menoscaba el patrimonio ajeno, la conducta fraudulenta consiste en manipulación informática o artificio semejante y la posibilidad de aplicar la pena de estafa y agravaciones al tipo del art. 248.2[23].

El delito de estafa en un delito de relación pero si la conducta se realiza frente a una máquina mediante las formas establecidas en el 248.2 entonces estamos frente a la estafa informática[24].

En consecuencia, el fraude informático tiene como elemento común con la estafa genérica el ánimo de lucro, no tiene los elementos del error y el engaño como ésta y difiere en otros como es la concurrencia de la manipulación informática o artificio semejante y la transferencia no consentida de activos patrimoniales en perjuicio de tercero. Si bien SUÁREZ GONZÁLEZ estima que la estructura se aproxima más a la del hurto que a la de estafa[25].

---

[21] SUÁREZ GONZÁLEZ, Carlos., en Rodríguez Mourullo (dir.)/Jorge Barreiro (coord.), *Comentarios al Código Penal*. Madrid: Editorial Civitas, 1997, 710.

[22] "La regulación del fraude informático como modalidad de la estafa, de corte individualista, deja al margen la eventual aplicación de tipos que protegen intereses supraindividuales como los delitos contra la Hacienda Pública o la intervención punible en el mercado bursátil"; véase, CHOCLÁN MONTALVO, "Fraude informático…", cit., 2001, 322.

[23] CÓRDOBA RODA, Juan y GARCÍA ARÁN, Mercedes, *Comentarios al Código Penal*, *parte especial*, Tomo I, Madrid-Barcelona: Aranzadi, 2004, 770.

[24] Así se recoge por Rodríguez Ramos y otros; véase, RODRÍGUEZ RAMOS, Luis (coord.) y otros, *Código Penal*, Madrid: La Ley, 2005, 549.

[25] SUÁREZ GONZÁLEZ, en Rodríguez Mourullo (dir)/Jorge Barreiro(coord.), *Comentarios…*, cit., 1997, 710.

De todo lo expuesto se deduce que el bien jurídico protegido es el patrimonio. El sujeto activo puede ser cualquier persona tanto las legitimadas para acceder al sistema como terceros no autorizados siempre y cuando utilicen manipulación informática o artificio semejante. Y sujeto pasivo es el titular del patrimonio, aunque muchas veces aparece por medio alguna entidad bancaria la cual podrá ser perjudicado desde el punto de vista de la responsabilidad civil.

a) La manipulación informática y artificio semejante[26]:

Manipular tiene una gran amplitud. De ahí que se[27] considere que no es una expresión adecuada al principio de legalidad[28] pues la acción típica podría englobar toda intervención autorizada o no en el sistema informático.

Por ello, doctrinalmente la manipulación informática se define como "toda acción que suponga intervenir en el sistema informático alterando, modificando u ocultando los datos que deban ser tratados automáticamente o modificando las instrucciones del programa, con el fin de alterar el resultado debido de un tratamiento informático y con el ánimo de obtener una ventaja patrimonial".

Además de este supuesto se contempla otro supuesto, el artificio semejante, lo cual lleva a dificultar más el panorama interpretativo pues también estos términos denotan imprecisión unido a la dificultad de establecer la semejanza entre manipulación informática y artificio semejante.

La manipulación informática supone una intervención sobre el software, no requiriendo un contacto inmediato con el ordenador que contiene los datos pues ahora es cada vez más frecuente el procesamiento de datos a distancia (a través de red telefónica)[29].

La intervención sobre el software para obtención de transferencia de fondos, cancelación de deuda o reconocimiento de crédito se manifiesta de tres formas:

- Introducción de datos falsos o alteración, supresión u ocultación de los ya introducidos, sin manipulación del programa (fase input):

Es decir, en este caso los datos tratados automáticamente son incorrectos no alterándose el programa y siendo correcto el tratamiento de datos. En la casuística este supuesto es el más frecuente.

---

[26] La SAP de Barcelona de 6-10-2003, lleva a cabo un estudio doctrinal del fraude informático y destaca el equívoco respecto de aquella doctrina inicial que preconizaba "(…) la comprensión en el concepto de manipulación informática, acudiendo a la expresión artificio semejante, de aquellos casos en los que el tratamiento electrónico de datos es puesto en funcionamiento de modo no autorizado (…)".

[27] CHOCLÁN MONTALVO, "Fraude informático…", cit., 2001, 328 y 329.

[28] Tesis seguida por Choclán Montalvo; ibid., 328.

[29] De forma minoritaria Choclán Montalvo estima una acción en el caso de que el ordenador autónomamente realice sucesivas transferencia de activos patrimoniales sin una nueva intervención del sujeto en el programa salvo la intervención inicial; ibid., 329.

- Manipulación en el programa (fase de tratamiento):

Es una alteración del programa en su concepción originaria consiguiendo el autor una desfiguración de los datos que se han introducido correctamente y obtener de esta manera un beneficio[30].

- Manipulaciones en el sistema de salida de datos (fase output):

Estamos ante una manipulación del sistema de salida de datos, no hay una manipulación previa del programa.

Estas tres conductas de manipulación informática son reducidas a dos por un sector doctrinal: a) las fases input y output constituirían un único grupo de conductas que no inciden directamente en el programa modificándolo; b) aquellas que exigen operar la configuración originaria del programa[31]. Y otro sector prefiere clasificar las conductas en: dentro del sistema y fuera del sistema[32].

La manipulación informática, en general, puede entrar en concurso con el delito de daños del art. 264.2 del CP español en el caso de destrucción o alteración de los datos contenidos en el sistema informático. Y en el caso de falsedad documental el fraude informático puede entrar en concurso ideal con el fraude informático pues el art. 26 del CP equipara soporte material que incorpora datos y documento[33].

Respecto al artificio semejante se considera una "fórmula de cierre"[34] con la que cubrir todas las posibilidades de fraude informático; pero en realidad nos encontramos una fórmula que se caracteriza por su indeterminación[35]. Se sancionarían conductas de manipulación de máquinas automáticas que proporcionan servicios o mercancías sin que se establezca que la manipulación para llevarse la mercancía u obtener el servicio sea informática[36]. Ahora bien, la doctrina se muestra contraria a esta solución, y las conductas dada la cuantía podrían reconducirse a la falta de estafa o hay quien entiende de hurto o robo con fuerza si se emplea alguna de las modalidades de fuerza del robo[37].

---

[30] El Caballo de Troya , se introducen una serie de instrucciones en un programa normal para actuar de forma diferente en beneficio del autor. O la técnica del salami donde las instrucciones dadas al programa hacen que éste redondee por defecto los céntimos en transferencias bancarias o nóminas obteniendo el autor un gran beneficio.

[31] CÓRDOBA RODA/GARCÍA ARÁN, *Comentarios…*, cit., 2004, 771.

[32] Clasificación realizada por Orts Berenguer y Roig Torres; véase, ORTS BERENGUER, Enrique, y ROIG TORRES, Margarita, *Delitos informáticos y delitos comunes cometidos a través de la informática*. Valencia: Tirant lo Blanch, 2001, 64.

[33] Para ampliar el tema de concursos véase, OTRS BERENGUER y ROIG TORRES, *Delitos informáticos…*, cit., 2001, 70 y 71.

[34] CÓRDOBA RODA/GARCÍA ARÁN, *Comentarios…*, cit., 2004, 771.

[35] SUÁREZ GONZÁLEZ, en Rodríguez Mourullo (dir.)/Jorge Barreiro (coord.), *Comentarios…*, cit., 1997, 711, considera que los artificios semejantes se refieren a supuestos en los que se manipulan soportes electrónicos o telemáticos.

[36] Esta situación ha sido bastante criticada doctrinalmente; véase, CHOCLÁN MONTALVO, "Fraude informático…", cit., 2001, 334-337.

[37] En este sentido se manifiesta Córdoba Roda/García Arán; véase, CÓRDOBA RODA y GARCÍA ARÁN, *Comentarios…*, cit, 2004, 772.

No obstante, hay alguna sentencia que considera artificio semejante a la manipulación informática los supuestos en los que se aparenta ser titular de una tarjeta cuya posesión se detenta ilegítimamente y actúa en connivencia con quien introduce los datos en la máquina dando posibilidad a que actúe mecánicamente (emplea un artificio para aparecer como titular ante el terminal bancario quien suministra los datos)[38]. O aquellos casos en los que se han manipulado datos de la banda magnética volcándose a un soporte de plástico en la que aparece como titular el manipulador o persona concertada[39]. O el apoderamiento a través de Internet de códigos y programas de una empresa de Telecomunicaciones para elaboración de tarjetas que posibilitan el acceso a una empresa operadora de TV[40].

b) Transferencia no consentida de activos patrimoniales

Puesto que se hace referencia a transferencia y no a disposición (actividad humana) es perfectamente realizable por una máquina sin intervención humana. El concepto activo patrimonial es amplio pues se admiten tanto bienes muebles como bienes inmuebles. Y cabe cuestionarse si se exige la cuantía establecida para la estafa que ha de ser superior a 400 euros. Indudablemente también es exigible para el fraude informático pues en los delitos patrimoniales como la estafa la cuantía tiene relevancia y aquél ha de interpretarse en conexión con el art. 248.1º, como se ha dicho anteriormente en relación con la pena.

Especial relevancia tiene en el ámbito del fraude informático, por su complejidad, el tema de la utilización de tarjetas de crédito[41]: Utilización abusiva o irregular no consentida de tarjetas de crédito en cajeros automáticos[42].

La manipulación en cajeros automáticos no encuentra solución más o menos satisfactoria en el CP español y se relaciona con la delincuencia informática patrimonial. A diferencia de la regulación española, en Italia se regula un tipo específico, la utilización de tarjeta de pago[43], eliminando la problemática existente en España.

La doctrina española distingue los siguientes supuestos:

---

[38] STS de 20-11-2001.

[39] STS de 16-9-2005.

[40] SAP de las Islas Baleares de 18-1-2006.

[41] La jurisprudencia también estima fraude informático del art. 248.2 del CP en el caso de tarjetas con puntos regalo que pueden ser canjeados con cargo a la empresa por diversos bienes y servicios; en este sentido la SAP de las Islas Baleares de 12-9-2006.

Sin embargo, es la tarjeta de crédito la que ocupa la mayoría de las manifestaciones de nuestros Tribunales sancionando como fraude informático en el ámbito de operaciones mercantiles inexistentes utilizando terminales de venta y tarjetas de crédito fraudulentas, STS de 26-6-2006. En ocasiones absuelve, como en el supuesto de mal funcionamiento del cajero automático, SAP de Toledo de 14-7-2005.

[42] Cassazione, sentenze V, 26-3-1996; véase, *Revista trimestrale di Diritto Penale dell'Economia,* (nº 1-2, gennaio-giugno, 1997), 575 y 576. Para ampliar el tema véase: PICOTTI, Lorenzo, "Reati informatici", en *Enciclopedia Giuridica Treccani,* (Volume XXVI, 1999), 8 y 9.

[43] Si la tarjeta es legítima no es factible la subsunción en el tipo de hurto o robo; véase, CHOCLÁN MONTALVO, "Fraude informático…", cit., 2001, 341 y 342.

1. Acceso al cajero mediante la utilización de la tarjeta por un tercero

Se podría considerar dentro del tipo de robo con fuerza en las cosas del art. 239 del CP español al considerar la tarjeta como llave en el sentido del precepto mencionado[44] y al presuponer en estos casos la falta de voluntad del banco en entregar ese dinero a persona no autorizada; aunque CHOCLÁN MONTALVO se muestra contrario a esta doctrina generalizada pues entiende que el apoderamiento se produce no contra la voluntad del dueño sino contra su deseo[45]. Pero si quien utiliza la tarjeta en un cajero no lo hace para acceder al interior sino que el dinero se expide al exterior habría de plantearse, según el mencionado autor si el supuesto es subsumible en el 248.2º del CP español. Cuando el funcionamiento del software no sufre alteración sino la persona que lo utiliza no podría hablarse de manipulación informática. Pero ¿podría englobarse en artificio semejante? No, al no ser equiparable a obtención de mercancía de una máquina por cualquier artificio que altere su funcionamiento, pues el funcionamiento es correcto sólo cambia la persona que utiliza la tarjeta que no es el dueño de la misma. Al respecto, MATA Y MARTÍN va más allá al considerar la necesidad de crear un tipo específico entre las defraudaciones que recoja los supuestos de utilización ilegítima de tarjetas codificadas en cajeros automáticos pues la pulsación del número personal del titular es el momento en el que se admite la operación de traspaso y en el caso de utilización abusiva se crea una "apariencia en el ejercicio del derecho frente al banco", acercándose más esta acción a las de tipo defraudatorio[46].

Si la tarjeta es sustraída a su dueño y se sustrae dinero del cajero la STS 6-3-1989 sancionó por robo con fuerza en las cosas al estimar la tarjeta llave falsa. Pero la calificación de robo se da si la tarjeta es sustraída al propietario no si es una tarjeta extraviada por el dueño pues en ese caso se calificaría como hurto.

2. Utilización abusiva del cajero por el titular de la tarjeta magnética

No constituye tal comportamiento un comportamiento típico de estafa pues no hay engaño bastante, aunque la administración podría ser desleal por el titular de la tarjeta al obligar al banco al pago de obligaciones diferentes a las contraídas; esto no es factible pues el titular no está obligado a cuidar de los intereses del banco. De ahí que la conducta sería atípica.

3. Acceso al cajero mediante tarjeta falseada o alterada. Uso técnicamente irregular de la tarjeta magnética

Para un sector doctrinal este caso no sería subsumible dentro de la manipulación informática, ni dentro del robo con fuerza en las cosas ni del hurto[47].

---

[44] CHOCLÁN MONTALVO, "Fraude informático…", cit., 2001, 346.

[45] MATA MARTÍN, Ricardo, *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago*. Madrid: Aranzadi, 2007, 168-170.

[46] CHOCLÁN MONTALVO, "Fraude informático…", cit., 2001, 349.

[47] Supuestos recogidos por Orts Berenguer y Roig Ortiz; véase, ORTS BERENGUER y ROIG ORTIZ, *Delitos informáticos…*, cit., 2001, 67 y 68.

Se considerarían estafas mediante manipulaciones informáticas, si el sujeto activo averigua el código de la tarjeta de algún cliente del banco y lo utiliza como propio o entrando en la contabilidad bancaria anota en su cuenta una cantidad superior a su activo real, o si hace una transferencia a su cuenta u otra ajena una transferencia desde el sistema contable de cualquier banco[48].

II.1.2. Actos preparatorios

El art. 248.3 introducido en el año 2003 se encuentra vinculado directamente con el fraude informático al sancionar la fabricación, introducción, posesión o el facilitar programas de ordenador específicamente destinados a la comisión de estafas prevista en el artículo, entre las cuales se encuentra el fraude informático.

Estamos ante actos preparatorios del futuro o posible autor o de tercero partícipe y en actos de participación a título de cooperador necesario o cómplice[49].

II.2. El fraude informático en Italia: similitudes y diferencias con la legislación española

La Legge nº 57, de 23-12-1993, afronta casi todas las tipologías de agresiones informáticas en Italia de una manera más o menos adecuada[50]. Es decir, el legislador italiano aborda la regulación del delito informático de una forma similar al español: salpicando a lo largo del articulado tipos que tienen como elemento, de una u otra manera, la informática[51]. Entre estas tipologías se regula el *frode informatico* (art. 640ter del Codice Penale)[52] siendo coincidentes y diferentes en algunos aspectos ambas legislaciones.

---

[48] CÓRDOBA RODA y GARCÍA ARÁN, *Comentarios…*, cit., 2004, 772. Así describen los actos preparatorios estos autores y además exigen dolo directo y el conocimiento de que se va a cometer un delito de estafa.

[49] TOSATO, Lorenza, "Panorama di giurisprudenza sui reati informatici", en *L'Indice Penale*, (gennaio-aprile, 2001), 445. Antes de afrontarse legislativamente la reforma, los autores intuían un riesgo: que la evolución legislativa presentara un trato preferentemente criminológico o no rigurosamente penalístico; véase, PICOTTI, Lorenzo, "La criminalità informatica: profili di diritto comparado", en *Critica Penale*, (gennaio-giugno, 1989), 26.

[50] La jurisprudencia jugó su papel en la legislación italiana y de hecho la Sentenza del Tribunale di Roma del 20-6-1985 recurriendo a la estafa (truffa) en el caso de quien induciendo a error en el INPS se emite en el ordenador datos no verdaderos sobre pagos efectuados; véase, TOSATO, "Panorama…", 2001, 449. Podemos ver en ésta y otras sentencias los antecedentes de lo que sería la regulación del delito informático en el Codice Penale.

Sin embargo, en fechas en las que Italia y España adolecía de un sistema sancionatorio Francia se dota del mismo en la lucha contra la criminalidad informática en el año 1988; véase, NEDELEC, Bruno, "La criminalità informatica nel diritto penale francese", en *Diritto Penale e Proceso*, (febbraio, 2002), 241-245.

[51] Esta disposición fue adoptada en el contexto de una amplia reforma que afectó a numerosos sectores de la parte especial del Codice Penale, si bien muchos de los casos podrían reconducirse a las disposiciones existentes con anterioridad; véase, MARINI, Giuliano, "Truffa", en *Digesto delle Discipline Penalistiche*, (XIV, 1999), 395.

[52] Sentenza del Tribunale di La Spezia 23-9-2004; véase, *Giurisprudenza di Merito*, (marzo, 2005), 615.

En sentido contrario se manifiesta Manna para quien la Recomendación del Consejo de Europa R(89) 9, estableciendo líneas de intervención legislativa sobre el fraude informático , venía dado porque las tipologías tradicionales eran difícilmente aplicables al delito informático; véase, MANNA, Adelmo, "Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso dei mezzí di pagamento elettronici", en *Diritto dell'informatica*, 2002, 955.

El art. 640ter del Codice Penale establece: "el que de cualquier modo altere el funcionamiento de un sistema informático o telemático o interviniendo sin derecho con cualquier modalidad sobre los datos, informaciones o programas contenidos en un sistema informático o telemático o a ellos concernientes, procurando para sí o a otro un injusto provecho con daño para otro, será castigado con reclusión de seis meses a tres años y con multa de 51 euros a 1.032 euros". La pena se eleva si concurre alguna de las circunstancias del nº 1 del segundo párrafo del art. 640 o bien si el hecho es cometido con abuso de la cualidad de operador del sistema. El delito es punible por querella de la parte ofendida, salvo que concurra alguna de las circunstancias del 2º párrafo o alguna otra circunstancia agravante. El comiso de los bienes se contempla en el 640 quatre.

Nuestra legislación regula en el párrafo 2º del art. 248 la estafa mediante manipulación informática o artificio semejante. La legislación italiana regula en precepto independiente, aunque conectado con la estafa, el fraude informático y así lo denomina específicamente. Sin embargo, la jurisprudencia italiana se muestra partidaria de entender que el *frode informatico* tiene los mismos elementos constitutivos de la *truffa* diferenciándose sólo porque la actividad fraudulenta del agente recae no sobre una persona sino sobre un sistema informático[53]. Un sector de la doctrina difiere al respecto, previéndose una conducta completamente diferente a la de la estafa[54], si bien otros autores estiman destacable los idénticos elementos con ésta y la diferencia vendría dada por la manipulación del sistema[55].

Ahora bien, de la lectura del precepto se observa ya una diferencia con nuestra legislación: la regulación específica de la pena, a diferencia de nuestro art. 248.2 el cual no señala pena alguna pero se aplica la pena de la estafa genérica de los arts. 249 y 250. Así pues se deduce que en el caso italiano la pena es la establecida para el fraude informático (coincidente con la estafa), y las agravaciones tendrán la misma pena que alguna de las agravaciones de la estafa excluyéndose las del punto 2. La diferencia es clara, mientras nuestro ordenamiento hace extensible al fraude informático la aplicación de todos los supuestos agravados de la estafa genérica, el derecho italiano contempla sólo alguno de los supuestos. Además la perseguibilidad varía pues si en España se actúa de oficio en Italia se requiere querella del ofendido.

Sin embargo, esto es meramente anecdótico pues las diferencias existentes también se refieren a elementos del tipo en sí.

Nuestro 248.2 únicamente alude a la estafa mediante manipulación informática o artificio semejante.

---

[53] MARINI, Giuliano, LA MONICA, Mario y MAZZA Leonardo, *Commentario al Codice Penale*, Tomo quarto, Torino: UTET, 2002, 3261.

[54] ALIBRANDI, Luigi, *Il Codice Penale*, Piacenza: Casa Editrice La Tribuna, 2001, 2109.

[55] Para Zannotti la mayoría de las agresiones a bienes jurídicos realizados mediante el ordenador representan lesiones de carácter patrimonial, si bien la criminalidad informática se desarrolla en el ámbito de la criminalidad económica; véase, ZANNOTTI, Roberto, "La truffa", en *Quaderni penali*, (6, 1993), 59 y 60.

La legislación italiana es más compleja al referirse a dos hipótesis: a) alteración del funcionamiento de un sistema informático o telemático, b) intervención sobre los datos sin derecho, expresión ésta que ha dado lugar a problemas interpretativos. Y es coincidente en el provecho para sí o para tercero así como en el ánimo de lucro.

- Siguiendo una sistemática se ha de partir del bien jurídico tutelado, el cual es el patrimonio (coincidente con nuestra legislación)[56]. Aunque se menciona la libertad negocial del perjudicado, con especial referencia a la actividad bancaria, en el sentido de que la norma tutelaría la regularidad de funcionamiento de los sistemas informáticos y la reserva que debe acompañar a su utilización[57]. La doctrina niega que estemos ante una forma especial de estafa, si bien se da una paridad en lo relativo al injusto provecho con daño para otros el art. 640 ter articula los caracteres de la conducta punible.

Se distinguen dos hipótesis de actuación:

a) Objeto de esta conducta es un sistema informático o telemático. Los italianos se decantan en dos tendencias: dar una definición restrictiva del mismo entendiendo un complejo de instalaciones dotados de un alto nivel de estructuración y complejidad y excluyendo al simple ordenador personal; dar una definición amplia de sistema informático incluyendo un ordenador personal por la cantidad de datos y programas que puede contener, tratándose entonces de evaluar la autonomía funcional del mismo. Incluso hay quien incluye todos los aparatos que ofrecen servicios o bienes (teléfono, fotocopiadora, distribuidor automático de banconote)[58]. Por sistema telemático se entiende un sistema de telecomunicaciones gestado con tecnología informática. Ahora bien, un sector doctrinal destaca que la referencia legislativa a sistema informático o telemático y a intervención sin derecho no indica dos conductas alternativas sino una especificación de la primera conducta general[59].
b) La otra hipótesis de ejecución del fraude informático italiano es la intervención sobre los datos sin derecho, expresión problemática. La mención a la intervención sobre datos, informaciones o programas hace pensar que el legislador ha querido incluir toda referencia a cualquier dato registrado informáticamente. Se interpreta en el sentido de que el legislador ha querido recalcar la relevancia del eventual consenso del sujeto titular o responsable del sistema y

[56] FANELLI, Andrea, "La truffa", en *Pratica Giuridica* (15, 1998),413.

[57] CRESPI, Alberto, STELLA, Federico y ZUCCALÂ, Giuseppe, *Comentario breve al Codice Penale*, Milano: CEDAM, 2003, 2210-2212.

Otro sector doctrinal estima que el sistema informático es un complejo o conjunto de aparatos unidos e integrados con un fin determinado y el sistema telemático es un conjunto de aparatos interactuados y coordinados unidos mediante estructuras comunicativas a distancia finalizadas en datos; MARINI, "Truffa", cit., 1999, 396.

[58] MANNA, "Artifici e raggiri…", cit., 2002,962.

[59] CRESPI, STELLA y ZUCCALÂ, *Comentario breve…*, cit., 2003, 2210-2212.

a la luz de los principios generales destacar el carácter de injusticia del provecho obtenido[60]. Nos encontramos ante una conducta activa (añadir datos en el interior del ordenador, añadir datos sobre el programa), en definitiva la intervención sin derecho "se refiere a datos, informaciones o programas contenidos en un sistema informático"[61]. La expresión *intervención* es interpretada en el sentido de alteración, pues en otro caso estaríamos ante un acto preparatorio para incidir en el lógico funcionamiento de la máquina. Esta intervención puede darse sobre el hardware (ej: acción que modifica a estructura de la máquina realizando operaciones diferentes a las programadas) o sobre el software (sobre los programas o datos registrados en la máquina).

- El elemento subjetivo se concreta en el dolo (igual que en España), es decir en la voluntad de alterar el funcionamiento de los sistemas e intervenir sobre los datos, programas, informaciones[62]. Es factible el dolo eventual[63].

Además el fraude informático no contempla el error a diferencia de la estafa genérica (similitud con nuestra legislación); de ahí que se considere doctrinalmente que el tipo admite un requisito tácito, idóneo para individualizar un nexo entre la conducta fraudulenta y el provecho, consistente en la necesidad de que el provecho injusto encuentre su origen inmediato en el resultado irregular del proceso de elaboración objeto de la indebida interferencia.

- En cuanto a la específica mención de la agravación en el caso de abuso de cualidad de operador del sistema no revela una abstracta cualificación del sujeto activo sino una legitimación por motivos de prestación de servicios[64]. Nos encontramos en una agravación cuya ratio radica en una mayor gravedad del fraude realizada violando el deber de fidelidad[65].

- La consumación se da en el caso de tener disponibilidad electrónica sobre la suma defraudada; es decir, esta tipología se consuma en el momento de la realización del provecho con daño para otro[66]. Y al igual que sucede en España son factibles los

---

[60] LATTANZI, Giorgio y LUPO Ernesto, *Codice Penale rassegna di giurisprudenza e di doctrina*, volume XI. Milano: Giuffrè, 2000, 539.,

[61] Hay que tener en cuenta un doble elemento normativo referido a la conducta y al evento; véase, MARINI, "Truffa", cit., 1999, 397.

[62] MARINI, LA MONICA y MAZZA, *Comentario…*, cit., 2002, 3262. También el dolo genérico; véase, LATTANZI y LUPO, *Codice Penale…*, tomo XI, cit., 2000, 542.

[63] No es necesaria una relación de trabajo dependiente; esta agravación consiste en aprovecharse de la propia cualidad utilizando de modo incorrecto los datos conocidos, disfrutando de la posibilidad de operar sobre el sistema…; véase, MARINI, "Truffa", cit., 1999, 398.

[64] LATTANZI y LUPO, *Codice Penale…*, Volume XI, cit., 2000, 543.

[65] Ibid., 543.

[66] Es factible el concurso con la falsedad informática (art. 491 bis Codice Penale), y respecto del fraude fiscal y la estafa la relación es compleja; véase, GUERNELLI, Michele, "Frodi informatiche e responsabilità delle

concursos con otros delitos[67]. En Italia destaca el concurso con el delito de acceso abusivo a un sistema informático[68].

III. El fraude informático. Aspectos criminológicos

Los estudios criminológicos en el ámbito del cibercrimen son escasos pero se puede afirmar que el aumento ha sido considerable aunque no puedan señalarse cifras pues la llamada cifra negra es amplia y ello debido a la escasez de denuncias en este ámbito así como al anonimato del autor y al carácter transfronterizo de los hechos[69]; pensemos que el mundo en el que se desarrollan es el mundo virtual. Lo cual incide en la dificultad para determinar la legislación aplicable y a veces los distintos ordenamientos aplicables pueden no coincidir en la ilicitud de la conducta.

A esto se une el hecho de que la lenta unificación a nivel legislativo de criterios para determinar qué conductas han de ser delitos puede ocasionar un aumento de las infracciones cometidas[70].

Aún así, desde un punto de vista sistemático e interaccionista el cibercrimen "podría comprender todos los casos en los que un medio telemático se interpone entre el autor y la víctima del delito representando el instrumento principal de ejecución de la acción criminal y alterando la percepción de la gravedad del crimen mismo"[71].

Los perjuicios económicos que se alcanzan en el ámbito de la delincuencia informática son muy considerables. De ahí la necesidad de hacer estudios criminológicos serios intentando salvar todas las dificultades existentes mediante la utilización de todos los medios al alcance ya sean legislativos, policiales, judiciales.

De hecho, la criminalidad informática incide de varias formas en el ámbito criminal: modifica las formas criminales tradicionales (entre ellos estafa y fraude), nacen nuevos crímenes (entre otros, la estafa telemática vía e-mail) y se altera la percep-

---

persone giuridiche alla luce del Decreto legislativo 8.6.2001, N.231", en *Rivista trimestrale di Diritto Penale dell'Economia*, (nº 4, ottobre-dicembre, 2000), 312 y 313.

[67] La diferencia entre ambas tipologías reside en los diferentes bienes jurídicos tutelados, en el elemento subjetivo y en la previsión de la posibilidad de cometer el delito de abuso sólo en los cuidados de sistemas protegidos; véase, LATTANZI y LUPO, *Codice Penale…*, Volume X, cit., 2000, 740.

[68] Se estima que los casos descubiertos y denunciados no van más allá del 1%; véase, ÁLVAREZ VIZCAYA, "Consideraciones criminológicas…", cit., 2001, 264. "La delincuencia vinculada a la informática constituye una de las parcelas donde la cifra negra de criminalidad es superior"; véase, MORÓN LERMA, Esther. *Internet y derecho penal: hacking y otras conductas ilícitas en la red*, Pamplona: Aranzadi, 1999, 36.

[69] ÁLVAREZ VIZCAYA en "Consideraciones político criminales…", cit., 2001, 278, destaca que si no hay acuerdo se produce una impunidad de las conductas.

[70] CORRADINI, Isabella y DI FEDE, Chiara, "La criminalità informatica: un'analisi socio-criminologica", en Marotta (a cura) *Tecnologie dell'informazione e comportamenti devianti*. Milano: Edizioni Universitarie di Lettere Economia Diritto, 2004, 21 y 22.

[71] STRANO, Marco, "Nuove tecnologie e nuove forme criminali", en *Cybercrime:conferenza internazionale (La Convenzione del Consiglio d'Europa sulla criminalità informatica)*. Milano: Giuffrè Editrice, 2004, 108 y 109.

ción del crimen[72]. Estadística e históricamente la criminalidad informática tiene como primera forma de manifestación al fraude informático[73].

Se hace referencia a una categoría criminológica del delincuente informático a caballo entre el delincuente de cuello blanco y el habitual o asocial[74]. Aunque hay quien se refiere al delincuente informático como delincuente de cuello blanco[75].

El procesamiento electrónico se convierte en un factor criminógeno y se acrecientan las posibilidades de actuar ilícitamente por parte de quienes tienen especiales conocimientos en la materia y de los que manejan los sistemas informáticos[76]. De facto se dice que, en muchas ocasiones, el autor suele ser un empleado de la empresa descontento o que se siente relegado[77]. El hecho de ser empleado en la empresa hace que la comisión del delito sea más factible y además dificulte su detección.

Esto conlleva la escasez de denuncias por la empresa, pues ante todo es importante guardar una buena imagen de la misma. Una mala prensa conllevaría pérdida de ganancias y un gran perjuicio. Es evidente que una empresa y/o, más concretamente, una entidad financiera no tiene interés en manifestar la vulnerabilidad de su sistema informático. Tal situación se acompaña del medio comisivo utilizado: el ordenador y la red[78].

"Internet, en determinadas circunstancias, puede llegar a ser una red verdaderamente opaca"[79], siendo desconocidas las conductas por las víctimas debido a cuestiones de carácter técnico: se puede trabajar en tiempo real, a distancia y con la facilidad de no dejar huellas. Esto hace que la víctima no detecte la conducta ilícita o si lo hace es por casualidad o error.

A ello hay que añadir que, en muchas ocasiones, estamos ante el síndrome de Robin Hood, (la víctima suele ser una persona jurídica). Estamos ante una víctima que carece de personalidad física, y ello conlleva dos cosas: una disminución de culpabilidad en el autor[80] y que la víctima, que muchas veces actúa como colaboradora, suela ocultar las conductas en las que está involucrada[81].

---

[72] PICOTTI, "La criminalità…", cit., 1989, 31.

[73] CHOCLÁN MONTALVO, "Fraude informático…", cit., 2001, 309. El autor continúa diciendo que nos encontramos ante autores ocasionales que no necesitan conocimientos especialmente técnicos o cualificados ; e incluso, se refiere a jóvenes que por curiosidad intelectual o lúdica penetran en el sistema informático.

[74] ÁLVAREZ VIZCAYA, "Consideraciones político criminales…", cit., 2001, 265. SNEYERS, en *El fraude…*, cit., 1990, 31, citando a diferentes autores hace referencia al fraude informático como delito de cuello blanco.

[75] MATA y MARTÍN, Ricardo, *Delincuencia informática y derecho penal*. Madrid: Edisofer SL, 2001, 25.

[76] Sobre todo respecto de los hackers.

[77] Los métodos de procesamiento y almacenamiento de datos apoyan esta situación. La permanencia y el automatismo así como la gran expansión de las conductas son algunas de las características criminológicas de estos hechos delictivos.

[78] ÁLVAREZ VIZCAYA, "Consideraciones político criminales…", cit., 2001, 267.

[79] Síndrome mencionado por Álvarez Vizcaya; ibid., 268.

[80] MORÓN LERMA, *Internet…*, cit., 1999, 37. Para ampliar el tema puede verse: GALDIERI, Paolo, " Il reato informatico", en Marotta (a cura) *Tecnologie…*, cit., 2004, 53-57.

[81] STRANO, "Nuove tecnologie…", cit., 2004, 113. Se manifiestan en sentido similar Corradini y Galdieri haciendo alusión al hecho de que "una abstracción de la víctima facilita la acción del delincuente puesto que

Todo este conjunto de situaciones hace que el autor no sienta las consecuencias negativas de los hechos y vuelva a delinquir, cuestionándonos es estos casos el efecto preventivo general de las penas. Es más, algunos de los comportamientos ilegales en el mundo virtual pueden realizarse por sujetos que difícilmente seguirían análogas acciones en el mundo no virtual; este es el caso del estafador que no aguantaría el impacto de la víctima cara a cara[82]. En este sentido, estadísticas e investigaciones de Universidades italianas han evidenciado que el medio comisivo 'ordenador' en el binomio acción-delito altera considerablemente, en la mente del responsable, la percepción de lo que se está realizando[83].

A todo esto se une el hecho de que es muy difícil descubrir, probar y perseguir la delincuencia informática[84]. De ahí la necesidad de adopción de medidas preventivas como un medio eficaz contra este tipo de delincuencia[85]. Medidas que se caracterizarían por la autenticación, la integridad y la reserva[86]. En esta línea los italianos destacan la preocupación en el ámbito de la formación y especialización ya en materia preventiva ya en materia represiva[87].

Pensemos que Internet es un medio y vehículo de la delincuencia con carácter ilimitado y la capacidad de los Estados es mucho menor. En este sentido, la proliferación del comercio electrónico ha hecho que se dispare el fraude y falsificación de tarjetas de crédito en la Unión Europea, fraude que va unido sobre todo a la delincuencia organizada internacional[88]. Por ello se han atribuido mayores sistemas de seguridad a los sistemas de pago en Internet mediante tarjeta de crédito a través de la adhesión a cuentas mediante intermediarios o mediante instrumentos encriptados de pago[89].

Pero en general, es decir en relación a la delincuencia patrimonial no sólo al fraude informático, son muchos los factores que inciden en la misma: complejidad

---

determina una disminución de sus frenos inhibitorios"; véase, CORRADINI, Isabella y GALDIERI, Paolo, " Tecnologie dell'informazione e psicopatologie (le nuove dipendenze e ripercusioni sull'accertamento della colpevolezza informatica)", en Marotta (a cura) *Tecnologie…*, cit., 2004, 279 y 280.

[82] CARLO GUALDI, B., "Reati informatici e reati coméis con strumenti informatici", en *Cybercrime: conferenza internazionale (La Convenzione del Consiglio d'Europa sulla criminalità informatica*, Milano: Giuffrè Editrice,, 2004, pág. 135.

[83] Para ampliar el tema sobre lugar de comisión del delito en el ciberespacio véase: GARRAPA, Nadia, "Conflitti di giuridizione nel cyberspazio e locus commissi delicti", en *Critica Penale*, (aprile 2002), 31-53.

[84] MORÓN LERMA, *Internet…*, cit., 1999, 39. Se suelen hacer auditorías informáticas.

[85] GRECO, Oronzo, *Problemas de criminología informática*. Roma: Aracne Editrice Srl, 2005,123 y 124.

[86] Nos encontramos ante una cultura de la seguridad , seguridad que supone una acción común que pasa a través de procesos de formación comunes a todas las instituciones; véase, PANSA, Alessandro,"Le strategie di contrasto al crimine informatico", en *Cybercrime:conferenza internazionale (La convenzione del Consiglio d'Europa sulla criminalità informatica)*. Milano, 2004, pág. 103.

[87] En el año 2000 se ocasionaron pérdidas por valor de 600 millones de euros; véase, LÓPEZ MORENO, Juana y FERNÁNDEZ GARCÍA Emilio Manuel, "La world wide web como vehículo de la delincuencia: supuestos frecuentes", en *Internet y Derecho penal*, Cuadernos de Derecho Judicial, (2001), 409.

[88] BUFFA, Francesco, *Internet e criminalità, finanza telematica off shore*. Milano: Giuffrè Editore, 2001, 6.

[89] Enumeración llevada a cabo por LÓPEZ MORENO y FERNÁNDEZ GARCÍA, "La world…", cit., 2001, 413 y 414.

del entorno técnico, alteración de datos y programas sin dejar rastro si no se han adoptado las medidas pertinentes, facilidad para eliminar pruebas (destruyendo los ficheros o datos alterados), concentración de la información en grandes bases de datos, ausencia de registros visibles, ausencia de controles internos en las aplicaciones, dispersión territorial de los puntos de salida, fácil acceso a información centralizada, creciente uso del sistema informático por las organizaciones criminales, posibilidad de grandes ganancias con pocos riesgos, casi total informatización de los medios de pago, rapidez de los procesos informáticos que permite operaciones fraudulentas y beneficiarse de los resultados antes que sean descubiertas[90]. A ello se une la existencia de paraísos informáticos o países donde no existen leyes eficaces[91].

Todo este conjunto de factores unidos a los factores generales del delito informático (cifra negra[92], víctima sin rostro…) hacen que la delincuencia patrimonial, en general, y el fraude informático, en particular, proliferen a pasos agigantados centrándose en diversos ámbitos: ámbito bancario, ámbito público y ámbito de empresas y entidades de seguros[93].

De ahí, la adopción de medidas técnicas y preventivas en relación a la seguridad[94]. Éstas serían algunas de las manifestaciones de una política criminal contra la delincuencia informática, en general, y el fraude informático, en particular.

Ahora bien, la víctima no puede ser olvidada en lo relativo a medidas frente al cibercrimen. El CERT-IT italiano es un claro ejemplo de ello. Se trata de un organismo sin afán de lucro que realiza actividades de investigación y desarrollo en el campo de la seguridad de los sistemas informáticos y es punto de referencia de las víctimas de intrusiones informáticas en la red. Ante un incidente informático la organización identifica el incidente, sugiere acciones para solventar el problema, informa

---

[90] BUFFA, *Internet…*, cit.,2001, 21.

[91] La cifra negra no es característica de nuestro país. Los italianos también destacan ésta en el entorno del cibercrimen; véase, RUGGIERO, "Ciberspazio e Diritto Penale…", cit., 2001, 215.

De hecho, la escasez de sentencias relativas al delito informático es una clara manifestación de la cifra negra característica del mismo; véase, CORRIAS LUCENTE, Giovanna, "Diritto penale ed informatica. Le nuove fattispecie di reato a confronto con l'evoluzione tecnologica e le nuove slide della criminalità informatica", en *Il Diritto dell'informazione e dell'informatica*, (gennaio-febbraio, 2003),50.

[92] Criminólogos italianos destacan el largo uso que de las tecnologías realizan en el sector bancario, y asegurativo; véase, CORRERA, Michel M. y MARTUCCI, Pierpaolo, *Elementi di criminología*, Milano: CEDAM, 1999, 166 y 167.

[93] En Italia se destacan varias medidas: a) la represión del fraude informático por el Arma de Carabineros, tanto en lo relativo al smartcard o carta plastificada con microprocesador, como al skimming o lectura y reproducción de la tarjeta de crédito magnética con el fin de obtener un clon y venderlo fuera, b) la colaboración de los Carabineros con el ABI o Asociación Bancaria Italiana, c) colaboración con la Universidad de Pisa en relación a temas de seguridad; adiestramiento en el uso del instrumento informático; véase, CARLO GUALDI, "Reati informatici…", cit., 2004, 143-145.

Junto a estas medidas cabría mencionar el tema de la perseguibilidad. En el caso del fraude informático el derecho italiano exige querella. La perseguibilidad de este delito se manifiesta a través del secuestro preventivo de la línea telefónica, el secuestro probatorio de los programas en el ámbito de la persecución domiciliaria; véase, PASCUZZI , Giovanni, *Diritto e informatica, l'avvocato di fronte alle tecnologie digitali*. Milano: Giuffrè, 2002, 87.

[94] GRECO, *Criminología…*, cit., 2005, 138-140.

sobre medidas de seguridad y desarrolla programas de control y seguimiento. En el mismo sentido, el IPACRI italiano es un club dedicado a crear un patrimonio de información que pone a disposición de empresas y usuarios comprendiendo acciones delictivas perpetradas contra empresas de crédito e instituciones financieras. El NOPT es el Núcleo Operativo de Policía de las telecomunicaciones italiana que prepara instrumentos válidos para luchar contra la delincuencia informática y además realiza una labor de prevención evitando la difusión de estos delitos. En España la Guardia Civil también tiene unidades especializadas en esta clase de delincuencia.

Para concluir podría seguirse una corriente doctrinal italiana que considera llegará un momento en que el ordenador formará parte de la sociedad de tal manera que la delincuencia se realizará a través de medios telemáticos y ya no se hablará de delincuencia informática sino de delincuencia[95].

Bibliografía

ALIBRANDI, Luigi, *Il Codice Penale*, Piacenza: Casa Editrice La Tribuna, 2001

ÁLVAREZ VIZCAYA, Maite, "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red", en *Internet y Derecho penal*, Cuadernos de Derecho Judicial, 2001

BUFFA, Francesco, *Internet e criminalità, finanza telematica off shore*. Milano: Giuffrè Editore, 2001

CARLO GUALDI, B., "Reati informatici e reati coméis con strumenti informatici", en *Cybercrime: conferenza internazionale (La Convenzione del Consiglio d'Europa sulla criminalità informatica*, Milano: Giuffrè Editrice), 2004

CHOCLÁN MONTALVO, José Antonio, "Fraude informático y estafa por computación", en *Internet y Derecho penal*, Cuadernos de Derecho Judicial, (X-2001)

CORBUCCI, Silvio, "I computer crimes, con particolare riferimento alla illecita riproduzione di programmi per elaboratore elettronico di dati", en *Revista di policía*, (gennaio, 1986)

CÓRDOBA RODA/GARCÍA ARÁN, *Comentarios al Código Penal*, *parte especial*, Tomo I, Madrid-Barcelona: Aranzadi, 2004

CORRADINI/DI FEDE, "La criminalità informatica: un'analisi socio-criminologica", en Marotta (a cura) *Tecnologie dell'informazione e comportamenti devianti*. Milano: Edizioni Universitarie di Lettere Economia Diritto, 2004

CORRADINI/GALDIERI, "Tecnologie dell'informazione e psicopatologie (le

[95] STRANO, en "Nuove tecnologie…", cit., 2004, 114, sigue esta teoría.

Ya en el año 1986, cuando todavía no se había regulado penalmente el delito informático se decía que la criminalidad informática parecía destinada a ampliarse con la creciente difusión de los ordenadores y el más sofisticado uso de los mismos; véase, CORBUCCI, Silvio, "I computer crimes, con particolare riferimento alla illecita riproduzione di programmi per elaboratore elettronico di dati", en *Revista di policía*, (gennaio, 1986),74.

nuove dipendenze e ripercusioni sull'accertamento della colpevolezza informatica)", en Marotta (a cura) *Tecnologie dell'informazione e comportamenti devianti.* Milano: Edizioni Universitarie di Lettere Economia Diritto, 2004

CORRERA/MARTUCCI, *Elementi di criminología*, Milano: CEDAM, 1999

CORRIAS LUCENTE, Giovanna, "Diritto penale ed informatica. Le nuove fattispecie di reato a confronto con l'evoluzione tecnologica e le nuove slide della criminalità informatica", en *Il Diritto dell'informazione e dell'informatica*, (gennaio-febbraio, 2003)

CRESPI/STELLA/ZUCCALÂ, Giuseppe, *Comentario breve al Codice Penale*, Milano: CEDAM, 2003

FANELLI, Andrea, "La truffa", en *Pratica Giuridica* (15, 1998).

GARRAPA, Nadia, "Conflitti di giuridizione nel cyberspazio e locus commissi delicti", en *Critica Penale*, (aprile 2002)

GRECO, Oronzo, *Problemas de criminología informática*. Roma: Aracne Editrice Srl, 2005

GUERNELLI, Michele, "Frodi informatiche e responsabilità delle persone giuridiche alla luce del Decreto legislativo 8.6.2001, N.231", en *Rivista trimestrale di Diritto Penale dell'Economia*, (nº 4, ottobre-dicembre, 2000)

LATTANZI/LUPO, *Codice Penale rassegna di giurisprudenza e di doctrina*, volume XI. Milano: Giuffrè, 2000

LÓPEZ MORENO/FERNÁNDEZ GARCÍA, "La world wide web como vehículo de la delincuencia: supuestos frecuentes", en *Internet y Derecho penal*, Cuadernos de Derecho Judicial, 2001

MANNA, Adelmo, "Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso dei mezzí di pagamento elettronici", en *Diritto dell'informatica*, 2002

MARINI, Giuliano, "Truffa", en *Digesto delle Discipline Penalistiche*, (XIV, 1999)

MARINI/LA MONICA/MAZZA, *Commentario al Codice Penale*, Tomo quarto, Torino: UTET, 2002

MATA MARTÍN, Ricardo, *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago*. Madrid: Aranzadi, 2007

- Delincuencia informática y derecho penal. Madrid: Edisofer SL, 2001

MILITELLO, Vincenzo, "Iniziative sovranazionali di lotta alla criminalità organizzata ed al riciclagio nell'ambito delle nuove tecnologie", en *Diritto e informatica*, PASCUZZI (dir). Milano: Giuffrè Editore, 2002

MORALES GARCÍA, Óscar, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre cyber-crime", en *Delincuencia informática, problemas de responsabilidad*, Cuadernos de Derecho Judicial, (2002)

MORÓN LERMA, Esther. *Internet y derecho penal: hacking y otras conductas ilícitas en la red*, Pamplona: Aranzadi, 1999

NEDELEC, Bruno, "La criminalità informatica nel diritto penale francese", en *Diritto Penale e Proceso*, (febbraio, 2002)

ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*. Valencia: Tirant lo Blanch, 2001

PANSA, Alessandro,"Le strategie di contrasto al crimine informatico", en *Cybercrime:conferenza internazionale (La convenzione del Consiglio d'Europa sulla criminalità informatica)*. Milano, 2004

PASCUZZI , Giovanni, *Diritto e informatica, l'avvocato di fronte alle tecnologie digitali*. Milano: Giuffrè, 2002

PICOTTI, Lorenzo, "Reati informatici", en *Enciclopedia Giuridica Treccani*, Volume XXVI, 1999

- "La criminalità informatica: profili di diritto comparado", en *Critica Penale*, (gennaio-giugno, 1989)

RODRÍGUEZ RAMOS, Luis (coord.) y otros, *Código Penal*, Madrid: La Ley, 2005

RUGGIERO, Francescopaolo, "Ciberspazio e diritto penale: il problema del bene giuridico", en *Revista Penale*, 2001

SARZANA, Carlo, "Note sul diritto penale dell'informatica", en *La Giustizia Penale*, (prima parte, gennaio, 1984)

SNEYERS, Alfredo, *El fraude y otros delitos informáticos*. Madrid: Tecnologías de gerencia y producción, S.A, 1990

STRANO, Marco, "Nuove tecnologie e nuove forme criminali", en *Cybercrime:conferenza internazionale (La Convenzione del Consiglio d'Europa sulla criminalità informatica)*. Milano: Giuffrè Editrice, 2004

SUÁREZ GONZÁLEZ, Carlos., en RODRÍGUEZ MOURULLO (dir.)/BARREIRO (coord.), *Comentarios al Código Penal*. Madrid: Editorial Civitas, 1997

TOSATO, Lorenza, "Panorama di giurisprudenza sui reati informatici", en *L'Indice Penale*, (gennaio-aprile, 2001)

ZANNOTTI, Roberto, "La truffa", en *Quaderni penali*, (6, 1993)

ZENO-ZENCOVICH, Vincenzo, "Informatica ed evoluzione del Diritto", en *Il Diritto dell'informazione e dell'informatica*, (gennaio-febbraio, 2003)