TRABAJO FINAL DE GRADO EN DERECHO

LA ESTAFA INFORMÁTICA: ESTUDIO DEL MARCO NORMATIVO Y ANÁLISIS DE LA CONDUCTA TÍPICA TRAS LA REFORMA OPERADA POR LA LEY 5/2010

Universitat de les Illes Balears

Álvaro Tarek Tomás Marín
GDRET M02

ÍNDICE

LA ESTAFA INFORMÁTICA: ESTUDIO NORMATIVO Y ANÁLISIS DE LA CONDUCTA TÍPICA TRAS LA REFORMA OPERADA POR LA LEY 5/2010

I. INTRODUCCIÓN

La red interconectada nació el día 21 de noviembre de 1969, cuando se lograron conectar los nodos de los diversos ordenadores de cuatro universidades norteamericanas. Poco a poco esta red fue creciendo, y en 1973 se verificó la primera conexión internacional, cuyo uso se mantuvo hasta los 90 en el ámbito militar, universitario y científico. Fue a principios de esta década cuando se produjo el verdadero auge de Internet, una auténtica revolución, un instrumento fascinante de progreso al alcance ya de todo el mundo, de las personas más comunes, pero también con un lado oscuro, al ser el espacio virtual un espacio sin fronteras ideal para el delito, dada la facilidad que ofrece para su comisión y las grandes dificultades para su persecución.

Desde entonces, en la denominada "era digital" los legisladores han intentado adaptar sus sistemas jurídicos al vertiginoso ritmo del crecimiento de la red de redes, intentando ganarle la carrera a quien hace un mal uso de ella, lesionando bienes jurídicos fundamentales. Un reto difícil, ya que basta un ordenador y una conexión telefónica para cometer los peores abusos no solo contra la intimidad o la dignidad de las personas, empresa privada, la economía de un país, sino también para la sociedad global internacional, extremo que ha conducido a la celebración de convenios y acuerdos internacionales sobre esta nueva amenaza del llamado delito informático.

Este trabajo es un breve recorrido por esa novedosa materia del denominado delito informático, reflejando someramente las disquisiciones conceptuales, las iniciativas supranacionales para crear un marco común legislativo y de acción, el derecho comparado y nuestro Código Penal, con especial referencia a la estafa informática tras la reforma del 2010, sin olvidar sus azarosos y discutidos antecedentes legislativos, doctrinales y jurisprudenciales.

II. CONCEPTUALIZACIÓN DE LA DELINCUENCIA RELACIONADA CON LA INFORMÁTICA

Ríos de tinta se han derramado a propósito del término jurídico adecuado para referirse a estas nuevas formas de criminalidad y su contenido. Al respecto, SNEYERS destacó ya en 1990 que "*La falta de un acuerdo amplio y general, tanto a nivel nacional como internacional, sobre las definiciones de los fraudes y otros delitos informáticos, sus características, distintos tipos, elementos principales y nuevas formas que adoptan según se desarrolla la tecnología informática, dificulta la prevención, la detección y la investigación, introduce escollos en las conferencias internacionales, provoca conflictos de leyes e impide una acción rápida y eficaz de los organismos nacionales e internacionales en la lucha contra dichos delitos y en la protección de los activos públicos y privados*"[1].

Con carácter general, se ha generalizado la denominación de "delito informático", aduciendo algunos autores, sin embargo, que es un concepto de naturaleza claramente doctrinal y que carece de respaldo legal, habiéndose desarrollado para dar respuesta a las mismas definiciones de una enorme amplitud y con la única pretensión de dar cabida a todas las posibles figuras delictivas que pudieran tener una conexión con el uso de sistemas de tratamiento electrónico de datos. Así, GALÁN MUÑOZ lo conceptúa como "*un término de referencia no estrictamente jurídico, que si bien aludiría a una pluralidad de delitos protectores de bienes jurídicos de naturaleza diversa, dejaría al margen de tal denominación a todas aquellas conductas en las que la utilización de un sistema informático no representase problema alguno a la hora de calificar el hecho efectuado como constitutivo de alguno de los delitos tradicionales*"[2]. En igual sentido, DAVARA RODRIGUEZ cree necesario aceptar la expresión delito informático que define como: "*la realización de una acción, que reuniendo las características que delimita el concepto de delito, sea llevada a cabo utilizando un elemento informático o*

[1] SNEYERS, Alfredo, *El fraude y otros delitos informáticos*, Madrid, Tecnologías de Gerencia y Producción, S.A, 1990, págs. 35 y 36.
[2] GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 C.P*, Valencia, Tirant lo Blanch, 2005, págs. 30 y 36.

telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"[3].

A diferencia de los anteriores autores, GUTIÉRREZ FRANCÉS se inclina por una fórmula menos rígida que permite abarcar no solo las conductas ya tipificadas, sino también a las merecedoras de pena y surgidas en conexión con la informática y utiliza el término "criminalidad o delincuencia informática", remarcando que nunca debe hablarse de delito informático[4]; e igual senda sigue un sector minoritario de la doctrina[5]. Todos estos juristas ponen de manifiesto como elemento común la comisión de acciones a través de elementos informáticos o con vulneración de los mismos, pero no elementos privativos que puedan sustentar una categoría penal. Para ellos, ni el bien jurídico protegido es de igual naturaleza, ni la forma de comisión del hecho punible presenta características similares.

En definitiva, el delito informático no constituye hoy una categoría autónoma, sino solo una categoría criminológica, que agrupa una pluralidad de manifestaciones delictivas que tienen que ver con las funciones propias de un ordenador y por ello, en España la regulación del delito informático se encuentra dispersa en la parte especial del Código Penal[6].

Pese a que actualmente como he dicho se ha generalizado tal denominación, personalmente me parece muy importante utilizar el término ciberdelincuencia, porque es el que da nombre al importante Convenio de Budapest del 2001[7], instrumento que hace una referencia más específica a los delitos cometidos en o a través de las redes

[3]DAVARA RODRÍGUEZ, Miguel Ángel, *Manual de derecho informático,* Thomson Aranzadi, 5º edición, págs. 350 y 361.
[4]GUTIÉRREZ FRANCÉS, Mª Luz, *Fraude informático y estafa (Aptitud del tipo de estafa en el Derecho español ante las defraudaciones por medios informáticos),* Madrid, Ministerio de Justicia, Secretaria General Técnica, Centro de Publicaciones, págs. 53 y 62.
[5]ESPARZA LEIBAR, Iñaki et. al; SAN JUAN GUILLÉN, César; PÉREZ MACHIO, Ana Isabel; SAIZ GARITAONANDÍA, Alberto; PÉREZ ESTRADA, Miren Josune; HERNÁNDEZ DÍAZ, Leyre, *Derecho penal informático,* CUESTA ARZAMENDI (dir.); DE LA MATA BARRANCO, Norberto (coord.). Thomson Reuters, pág. 147.
[6]CHOCLÁN MONTALVO, José Antonio et. al; GARCÍA GONZÁLEZ, Javier; GONZÁLEZ RUUS, Juan José; GUTIÉRREZ FRANCÉS, Mariluz; HAMM, Rainer; MATA Y MARTÍN, Ricardo; MORALES PRATS, Fermín; PICOTTI, Lorenzo; PIÑAR MAÑAS, José Luis; SANCHÍS CRESPO, Carolina, *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* ROMEO CASABONA, Carlos María (Coord).Granada, Editorial Comares, pág. 69.
[7] BOE 17-9-2010, Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

informáticas. Y ello no porque suene mejor, sino porque refleja un acuerdo de la comunidad internacional en ese afán de uniformizar al que se refería ya en 1990 SNEYERS, fruto de los trabajos que al respecto realizaron 56 expertos nombrados por el Consejo de Europa, de 1997 al 2001 y que no solamente fue signado por los países miembros sino por otros como Estados Unidos, Japón y Canadá. Debe agradecerse ese esfuerzo para conseguir un consenso internacional de mínimos, incluida la denominación: Ciberdelincuencia.

III. NORMATIVA EN MATERIA DE DELINCUENCIA INFORMÁTICA: ENCUADRE DE LA ESTAFA INFORMÁTICA

El carácter transfronterizo de la delincuencia informática exige una respuesta adecuada y rápida, siendo necesaria una armonización de la legislación y de la práctica policial y judicial entre los países, principal obstáculo para combatirlo y perseguirlo en esta aldea global y tal directriz se ha reflejado a nivel supranacional y en la legislación específica de cada país, resaltando que el mayor esfuerzo hasta el momento ha sido el tan citado Convenio de Budapest, al que prestaré especial atención.

A) MARCO SUPRANACIONAL

En el ámbito de la ONU hay que resaltar el Manual de las Naciones Unidas para la prevención y control de delitos informáticos de 1994. Dicho Manual establece una clasificación en la cual se incluye el objetivo central de este trabajo, la "estafa informática", destacada por su especial peligrosidad y denominada "fraude por manipulación informática", reseñándose tanto el hecho de que tal conducta vendría a efectuarse sobre fondos intangibles representados en forma de datos informáticos, como el de que se vendría a cometer por manipulaciones en la entrada de los datos, en el programa destinado a procesarlos o en las salidas de los resultados obtenidos con tal procesamiento, siendo también frecuente que dichas conductas vinieran a aprovecharse de la repetición automática de tales procesos informáticos.

En el ámbito del Consejo de Europa destaca el citado Convenio sobre el Cibercrimen aprobado en Budapest el 21-11-2001, tras cuatro años de trabajo de juristas de los 45

Estados miembros y algunos de países no miembros como Estados Unidos, Canadá y Japón. Curiosamente, la ratificación de este instrumento -que puede calificarse de universal- por España se ha producido nueve años más tarde, el 20-5-2010, publicándose en el BOE del 17-9-2010, coincidiendo así con el periodo de *vacatio legis* de la vigésimo cuarta reforma del Código penal de 1995, por contracción y en adelante CP.

Este Convenio ordena a cada parte adoptar las medidas legislativas tendentes a la tipificación del catálogo de delitos que enumera de los arts. 2 a 10, así como el establecimiento de un ámbito de cooperación internacional, dado su carácter transfronterizo. Además, ofrece una definición de delitos informáticos -así como otros conceptos como "sistemas informáticos", "datos informáticos" o "proveedor de servicios"-, y los clasifica en cuatro grupos:

-contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos incluyendo como tales: acceso ilícito a sistemas informáticos, interceptación ilícita de datos informáticos, interferencia en el sistema mediante la introducción, transmisión, provocación de daños, borrado, alteración o supresión de estos y abuso de dispositivos que faciliten la comisión de delitos;

-delitos asociados a la informática incluyendo como tales: falsificación informática que produzca la alteración, borrado o supresión de datos informáticos que ocasionen daños y los fraudes informáticos, "Computer Fraud", que centrando otra vez la atención en la estafa informática engloba "aquellas conductas con las que se ocasione intencionadamente y sin derecho, la pérdida de la propiedad de otro mediante: cualquier entrada, alteración, borrado o supresión de datos informáticos o cualquier interferencia en el funcionamiento de un sistema informático con la intención deshonesta o fraudulenta de procurarse sin derecho un beneficio económico para sí mismo o un tercero";

- delitos relacionados con contenidos considerando como tales, los delitos relacionados con la pornografía infantil;

- delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Este catálogo de conductas delictivas no es cerrado tal y como se desprende del art. 14, que señala "que cada parte aplicará los poderes y procedimientos regulados en el Convenio, no solo en los delitos previstos en los arts. 2-10, sino también a cualquiera otros que pudiera cometerse por medio de un sistema informático". El convenio persigue: establecer una tipificación común, establecer unas facultades y técnica común de investigación y establecer nuevas formas de cooperación internacional, con adaptación en la lucha contra tal tipo de delincuencia.

En el ámbito comunitario, el esfuerzo u objetivo de las instituciones internacionales tendente a la armonización del Derecho Penal en el seno de la Unión Europea, condujo a la aprobación de la Decisión Marco de 28 de mayo del 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, que impone a los Estados Miembros la tipificación de tales conductas, así como el deber de garantizar la adopción de penas efectivas, proporcionadas y disuasorias para lograr un nivel de contención adecuado contra la delincuencia informática.

Limitada a los ataques contra los sistemas de información, nos encontramos con la Decisión Marco 2005/222/JAI de 24 de febrero del 2005. Tal normativa también ofrece definiciones sobre el significado de "sistema de información", "datos informáticos", "persona jurídica o sin autorización" y en su Preámbulo se pone de manifiesto la preocupación por los frecuentes y continuos ataques contra los sistemas de información, sobre todo por parte de una delincuencia organizada de carácter transnacional que pone en peligro la sociedad de la información segura en el espacio de libertad, seguridad y justicia que la Unión Europea reconoce como propios.

La exposición de Motivos de la LO 5/2010 de Reforma de nuestro Código Penal[8], si bien no se refiere directamente al Convenio de Budapest puede entenderse que de forma indirecta lo alude cuando indica "*por un lado España tiene contraídas obligaciones internacionales*", pero sí específicamente se refiere a la Decisión Marco 2005 afirmando: "*en el marco de los denominados delitos informáticos para cumplimentar la Decisión Marco 2005/222/SAI de 24-2-2005, relativo a ataques contra Sistemas de*

[8] BOE 23 de junio de 2010, Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Información se ha resuelto incardinar las conductas punibles en los apartados diferentes al tratarse de bienes jurídicos diversos…". En su disposición final sexta, incorpora entre otras esta Decisión Marco.

En definitiva es necesario un marco de cooperación de carácter internacional, un espacio común al que tiende la normativa antes citada y que tiene como base un tratamiento jurídico penal de carácter uniforme del cibercrimen, que reclaman con urgencia esos instrumentos antes citados de carácter supranacional.

B) MARCO DE DERECHO COMPARADO

Pese a que España ha sido uno de los últimos países de Europa que ha tipificado conductas delictivas relacionadas con las nuevas tecnologías iniciando tal camino con el Código Penal de 1995, muchos otros países de nuestro entorno se adelantaron en tal reto, lo que nos lleva a hacer una breve referencia al marco del derecho comparado.

En Europa sobresalieron Alemania, con su Ley contra la Criminalidad Económica de 1986; Francia, que en 1988 contaba con una ley relativa al fraude informático; y Gran Bretaña, donde en 1991 se promulgó la Compute Misuse Act. Muchos otros países como Portugal, Austria, Italia optaron por esas fechas por la tipificación de las nuevas conductas en sus Códigos Penales, al igual que lo hizo España en 1995. En América, Estados Unidos adoptó en 1994 el Acta Federal de Abuso Computacional, que modificó el Acta de Fraude y Abuso Computacional de 1986 **y,** en Iberoamérica**,** puede resaltarse la Ley chilena contra los delitos informáticos de 1993.

Mención especial merece la citada Ley de Represión de la Criminalidad Económica alemana, que es un referente para la regulación que al cabo de nueve años tuvo lugar en España en relación al objeto central de este trabajo, la estafa informática. GALÁN MUÑOZ[9] y GUTIÉRREZ FRANCÉS[10] analizan el párrafo a) del art. 263 que la regula y que dice "*El que con intención de obtener un beneficio patrimonial ilícito para sí o por un tercero, lesiona el patrimonio de otro interfiriendo en el resultado de un tratamiento de datos, mediante una estructuración incorrecta del programa, la*

[9] GALÁN MUÑOZ, Alfonso, op.cit. (2), págs. 109 y ss.
[10] GUTIÉRREZ FRANCÉS, Mª Luz, op. cit. (4), págs. 170 y ss.

utilización incorrecta o incompleta de datos, la utilización de datos sin autorización o la intervención de cualquier modo no autorizado en el proceso, será castigado con la pena de prisión de libertad de hasta 5 años o con multa". En síntesis señalan dichos autores que, con tal regulación, el legislador alemán salva las dificultades que entrañaba la aplicación del delito de estafa tradicional, prescindiendo de sus tradicionales elementos del engaño a una persona, creando un tipo de gran amplitud con la pretensión de que diera cabida a todas las conductas que interfieren en los procesos de tratamiento de datos y determinan la producción dolosa de un perjuicio patrimonial.

En Italia la introducción del art. 640 *ter* supone el castigo de las transferencias no consentidas de activos patrimoniales, sustituyendo la exigencia de engaño y artificio por la de alteración del funcionamiento del sistema o de intervención no legítima de cualquier modo en el mismo.

En conclusión, siguiendo a PEREZ MACHIO[11], a partir de las obligaciones contraídas tras la ratificación del Convenio sobre Criminalidad de 2001, tanto Alemania e Italia como Francia y Estados Unidos y el resto de países que así lo han ratificado, han reforzado la normativa para luchar contra este tipo de delincuencia. Pudiendo señalar como nota común en los ordenamientos jurídicos de nuestro entorno que pese a que todavía existen divergencias entre ellos, la tendencia es cumplimentar tales obligaciones internacionales y que en todas ellas, al modo del referente alemán y en lo que concierne a la estafa informática suelen presentar una cláusula abierta o general para evitar que los delitos informáticos queden anticuados ante la rapidez e inventiva de los ciberdelincuentes.

C) EL MARCO ESPAÑOL

España, como he dicho antes, ha sido uno de los últimos países de nuestro entorno que, pese a la existencia de esta nueva realidad criminal, ha ofrecido una respuesta punitiva a los comportamientos ilícitos en el campo de las nuevas tecnologías, pues la incriminación de las conductas integrantes de la delincuencia informática no tuvo lugar hasta el año 1995 con la aprobación del nuevo Código Penal. Además, para ello, se

[11] ESPARZA LEIBAR, Iñaki, …op. cit. (5), págs.147 y ss.

descartó la opción seguida en otros países -como los ya estudiados Francia o Gran Bretaña- de encuadrar tal tipo de delitos en una Ley especial o en un capítulo específico. A tal efecto, las distintas conductas relacionadas con la delincuencia informática se incluyeron en el nuevo Código Penal de una forma dispersa, asumiendo el legislador que se trataba de una realidad criminal compleja, situándolos en función del bien jurídico lesionado, centrándose especialmente en los atentados contra la intimidad, las falsedades y los ataques contra intereses de contenido económico (arts. 186, 197, 211, 238.5, 248.2, etc.).

En la última reforma operada por la Ley Orgánica 5/2010 se ha seguido idéntica técnica, ya que se han introducido nuevos tipos y se han reformado algunos, ubicándolos en los capítulos existentes en función del bien jurídico lesionado (libertad e indemnidad sexual, intimidad, patrimonio, etc). QUINTERO OLIVARES saluda positivamente el mantenimiento en la reforma de delitos específicos en materia informática según el bien jurídico efectivamente afectado, ya que considera que una agrupación de todas las figuras asociadas a la informática en una Ley Especial favorece interpretaciones ligadas a la seguridad y a la creación de delitos de riesgo, que deben rechazarse por su difícil convivencia con el principio de lesividad[12].

El eje central de la reforma de 2010, tal y como se desprende de su Preámbulo[13], la necesidad de cumplir con las obligaciones internacionales contraídas por España y el surgimiento de nuevas cuestiones que han de ser abordadas ha atañido como pilares esenciales al "hacking" o intrusión informática (art. 197), al "cracking" o daños informáticos (art. 264) y la estafa informática (art. 248.2). Es, concretamente, esta última conducta la que constituye el objeto de estudio del presente trabajo, cuya modificación por la reforma de 2010 ha consistido en la introducción en el art. 248 de un nuevo apartado que tipifica la utilización de tarjetas de crédito o cheques de viaje para realizar operaciones de cualquier clase en perjuicio del titular de dichos instrumentos de pago a terceros.

[12] QUINTERO OLIVARES, Gonzalo (dir.), *La Reforma Penal de 2010: Análisis y Comentarios.* Aranzadi, Thomson Reuters, págs. 182 y 183.
[13] Preámbulo de la LO 5/2010 publicada en el BOE de 23 de junio del 2010.

Ello nos lleva a un estudio más detenido del objetivo de este trabajo al ser una de las manifestaciones lesivas que con mayor frecuencia se cometen, en o a través de la red.

IV. LA ESTAFA INFORMÁTICA

A) ANTECEDENTES

En el centro de la Ciberdelincuencia, por los importantes perjuicios patrimoniales que ocasiona una cifra negra[14]de imposible cuantificación, se encuentra la denominada estafa informática. La irrupción de Internet en las esferas del comercio, la banca, la bolsa fue inmediatamente aprovechada por los amigos de lo ajeno, planteándose en España con anterioridad al Código Penal de 1995 la difícil labor, ante la falta de regulación expresa, de adaptar los tipos ya existentes a las nuevas conductas de transferencias no consentidas de activos patrimoniales por medios informáticos.

El esfuerzo para evitar la impunidad ante la laguna legislativa tuvo como objetivo determinar si los nuevos fenómenos delictivos se podían encuadrar en la estafa clásica o en figuras de apoderamiento como el hurto, la apropiación indebida o el robo con fuerza. La gran mayoría de los autores de esa época negaron tal posible subsunción en el tipo de la estafa común, aduciendo que faltaba el nuclear elemento del engaño y el error, que solo puede darse en una relación de carácter personal. No se puede engañar a una máquina, concluían. El vacío legal tampoco podía ser cubierto decían, por los tipos de apoderamiento, en cuanto requieren como objeto material una "cosa mueble" que no es equiparable al dinero o elementos intangibles o inmateriales. A tal efecto, en el año 1990, GUTIÉRREZ FRANCÉS realizó una revisión crítica de los elementos de la estafa del art. 528 del antiguo Código Penal de 1973, por contracción y en adelante ACP, con la finalidad de obviar esa laguna, llegando, a fin de cuentas, a la misma conclusión que el resto de los autores, y propugnando, en consecuencia, la necesidad de una reforma que pudiera tomar como modelo el sistema alemán anteriormente citado[15].

[14] Anti-Phishing Working Group: www.apwg.org, report 2012.

[15] GUTIÉRREZ FRANCÉS, Mª Luz, op. cit. (10, 4), págs. 409 y ss y 609 y ss

La jurisprudencia anterior a 1995, de acuerdo con la postura doctrinal mayoritaria ("no se puede engañar a una máquina"), vetaba la posibilidad de encuadrar la estafa informática en el tipo de la estafa tradicional regulada en el artículo 528 del ACP y, por consiguiente, las transferencias no consentidas que se realizaban operando sobre sistemas informáticos de la banca o cajeros automáticos fueron a veces subsumidos, forzándolos, en tipos como el hurto, la apropiación indebida, el robo con fuerza, destacándose siempre las carencias legislativas.

Un importante hito jurisprudencial fue el primer caso de estafa informática que llegó al Tribunal Supremo. Se trata de la Sentencia de fecha de 19-9-1991, cuyo ponente fue SOTO NIETO, que excluía la aplicación del tipo de la estafa en un supuesto en que el empleado de un banco efectuó apuntes contables falsos mediante el ordenador y se enriqueció, siendo condenado finalmente por un delito de apropiación indebida con base en que "*mal puede concluirse la perpetración de un delito de estafa por parte del procesado al impedirlo la concepción legal y jurisprudencial del engaño, ardid que se produce e incide por y sobre las personas…Con razón se ha destacado que a las máquinas no se les puede engañar, a los ordenadores tampoco, por lo que en los casos en los que el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se produce ni el engaño ni el error necesario para el delito de estafa*"[16].

El Código Penal de 1995 puso fin a todas las polémicas doctrinales surgidas en torno al antiguo Código Penal y aparte de las zozobras jurisprudenciales y acogiendo las peticiones de la doctrina, como la ya citada GUTIÉRREZ FRANCÉS, introdujo en la sede de los delitos patrimoniales, a continuación del tipo básico de la estafa del art. 248, un apartado 2 que decía: "*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*".

[16] Así, CHOCLÁN MONTALVO, Jose Antonio, op. cit. (6), en el capítulo que dedica a las infracciones patrimoniales en los procesos de transferencias de datos, pág. 72; FARALDO CABANA Patricia, *Las nuevas tecnologías en los delitos contra el patrimonio*, Tirant lo Blanch, colección de delitos, 2009 pág. 84; SERRANO GÓMEZ, Alfonso; SERRANO MAÍLLO, Alfonso, *Derecho Penal: Parte Especial.* Madrid, Dykinson, 16.ª edición, 2011, pág. 430.

Como señala la STS de 26-6-2006 (ponente SÁNCHEZ MELGAR) se introdujo ese párrafo "*para tipificar como estafa los actos de acechanza al patrimonio ajeno realizados mediante manipulaciones o artificios que no se "dirigen" a otros sino a máquinas, para conseguir que estas, a consecuencia de una conducta artera, actúen, en su automatismo en perjuicio de tercero*".

Poco a poco, tanto la doctrina como la jurisprudencia encontraron gracias al cauce del 248.2 CP la adecuada ubicación de todas las nuevas conductas, bien en ese tipo si no existía relación intersubjetiva o bien en el convencional o clásico si existía, creándose cierto consenso al respecto en los últimos años, habiendo perdido fuelle la subsunción que del tema más problemático, esto es, el uso de tarjetas ajenas en cajeros se hacía en el tipo de robo con fuerza. Ello no obstante, el Legislador, tal y como se desprende de la Exposición de Motivos de la Reforma quería terminar de forma expresa con esta última polémica y así lo expresa diciendo "*ha sido preciso incorporar la cada vez más extendida modalidad consistente en defraudar utilizando tarjetas ajenas o los datos obrantes en ellas".* Pese a ello un sector de la doctrina considera innecesaria y errónea tal introducción "*toda vez que tal uso fraudulento de medios de pago desde hace tiempo no plantea ningún conflicto"*[17]

Finalmente, la reforma del 2010 ha modificado el art. 248, que actualmente tiene la siguiente redacción:

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a. Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

[17] ÁLVAREZ GARCÍA, Francisco Javier; y GONZÁLEZ CUSSAC, Jose Luís (Directores), *Comentarios a la Reforma Penal de 2010,* Valencia, Tirant lo Blanch Reformas, Trust CM, 2010, p. 278.

b. Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c. Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Con la reforma de 2010, se mantiene la figura de la estafa convencional y la equiparación que a la misma ("también") se verificaba de la estafa informática, así como la criticada criminalización de actos preparatorios que fue introducida por la reforma del CP del 2003. La novedad fundamental es la adición de ese apartado tercero, del que luego me ocuparé, por los esfuerzos que la doctrina y la jurisprudencia realizaron para subsumir la utilización ilícita de tarjetas en los tipos patrimoniales ya existentes, entre ellos la que centra mi estudio, esto es, la estafa informática, pero antes aludiré a esta, regulada como he dicho por primera vez en el CP de 1995.

B) LA ESTAFA INFORMÁTICA DEL ART. 248.2 CP

1. RELACIÓN DEL ART. 248.2 CON EL TIPO BÁSICO

Tal y como he expuesto, con la reforma de 2010, se mantiene la figura de la estafa convencional y la equiparación que a la misma ("también") se verificaba de la estafa informática**.** Como señala QUINTERO OLIVARES, el adverbio "también" marca el tácito reconocimiento de que no estamos ante conductas que pueden caber en la definición básica de la estafa que ofrece el apartado 1 del artículo, sino ante hechos que requieren una específica configuración legal si se quiere dar la debida tutela penal del patrimonio frente a ataques ejecutados aprovechando la tecnología de nuestro tiempo[18]. En igual sentido, ROVIRA DEL CANTO afirma que se trata de un tipo delictivo defraudatorio, pero no de una modalidad de la estafa genérica ni asimilable a la misma, en el que el bien jurídico protegido es única y exclusivamente el patrimonio en su

[18] QUINTERO OLIVARES, Gonzalo et. al; MORALES PRATS, Fermín; TAMARIT SUMALLA, Josep Mª; GARCÍA ALBERO, Ramón, *Comentarios al Código Penal Español, Tomo II (Artículos 234 a DF. 7ª).* QUINTERO OLIVARES, Gonzalo (dir.); MORALES PRATS, Fermín (Coord.), Aranzadi, Thomson Reuters, 6ª edición, pag.82.

vertiente microindividualista, dada su ubicación sistemática en el CP[19]. Tal consideración de delito independiente es hoy la mayoritaria en la doctrina estudiada. Igualmente, explica FARALDO CABANA que estamos ante una figura autónoma respecto de la estafa, a la que solo se equipara a efectos penológicos[20].Así pues, el tipo se configura como un delito de acción dolosa de naturaleza estrictamente patrimonial y con una estructura tradicional defraudatoria pero autónoma e independiente de la del delito de estafa general[21].

2. ELEMENTOS TÍPICOS ESPECÍFICOS DE LA ESTAFA INFORMÁTICA

En la medida en que el art. 248.2 tipifica una estafa específica pero que comparte con la estafa común el bien jurídico protegido, el patrimonio y el ánimo de lucro en el presente trabajo se obviará pues, el estudio específico de los elementos comunes, centrándose más concretamente, en los que la individualizan y distinguen de la conducta incriminada en el apartado1.Pero antes de estudiar sus elementos estructurales conviene señalar que en aquellos supuestos en los que se utilice un medio informático para realizar el engaño no estaremos ante un caso del artículo 248.2 a) del CP, sino del art. 248.1 CP, es decir, del tipo básico de la estafa y me refiero por ejemplo a los casos que continuamente se reflejan en la prensa y a los que se refieren[22], como las subastas en Internet, negocios piramidales, ofertas de cómodos y rentables trabajos en casa, prestaciones de trabajos inexistentes, estafa nigeriana, etc. No existe manipulación informática, el autor engaña al perjudicado por ejemplo, a través de una página web transmitiendo un mensaje no veraz idóneo para producir el error en la persona que la visita y el consiguiente desplazamiento patrimonial sin la contraprestación ofertada.

a) Sujetos

La estafa del 248.2 se caracteriza por ser un delito en el que no se produce una relación bilateral y personal (autor-víctima), describiendo su tipo de injusto conductas unilaterales en las que tan solo hace referencia a sus posibles víctimas a la hora de

[19] ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos.* Granada, Editorial Comares, Estudios de Derecho Penal dirigidos por Carlos Mª Romeo Casabona, 2002, pág. 563.
[20] FARALDO CABANA, Patricia, *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*. Tirant lo Blanc, "colección los delitos", 2009. pág. 85.
[21] ROVIRA DEL CANTO, Enrique, op. cit. (19), pág. 627.
[22] Unión Internacional de Comunicación, El Ciberdelito: Guía por los países en desarrollo, Ginebra 2009 www. itu.int/dmspub/ituud/otb. National, regional and international approaches in the fight against cybercrime. Computer Law Review International, 2008.

requerir que la misma no hubiese consentido la transferencia afectada[23]. El sujeto activo hoy puede ser cualquiera, siempre que despliegue la conducta típica. Atrás quedaron los perfiles trazados por la doctrina a principios de los 90. La característica fundamental del ciberdelincuente es el anonimato, puede ocultarse detrás de otras identidades, la ubicuidad, ya que puede moverse por todas las redes y acceder desde un ignoto país a las cuentas bancarias del más lejano continente con las dificultades que supone para su persecución.

El sujeto pasivo (la víctima que da la transferencia no consentida) es normalmente el titular del patrimonio afectado, defraudado, si bien también puede resultar perjudicado civil las entidades bancarias, cuando la defraudación tiene lugar a través de su sistema informático ya que asumen los perjuicios causados a sus clientes.

b) Conductas del apartado 2 del artículo 248

Tras la Reforma del 2010 el número primero del art.248 mantiene la figura de la estafa clásica, equiparándose a la misma mediante la fórmula "también", en su número segundo, tres conductas que ahora estudiaremos: la introducida en 1995, estafa informática (letra a); los criticados precursores introducidos en 2003 (letra b); y la novedad, esto es la incriminación expresa de la utilización de tarjetas de crédito o de débito o sus datos y los anticuados cheques de viaje en perjuicio de su titular u otro (letra c).

1. La letra a) del segundo apartado el artículo 248 reza: *También serán considerados reos de estafa*: a) *Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.*

La primera conducta de la estafa prevista en el apartado 2 del artículo 248 del Código penal consiste en la producción dolosa de un perjuicio patrimonial valiéndose de una manipulación informática o artificio semejante.

En la formulación de la misma se utiliza una fórmula abierta, capaz de acoger todos los casos posibles, amplitud inevitable, en este campo, en que el desarrollo tecnológico es

[23] GALÁN MUÑOZ, Alfonso, op.cit. (2, 9), pág. 557.

continuo. GALÁNMUÑOZ señala que la segunda de las modalidades comisivas no sería sino una mera cláusula general del ámbito típico establecido en la primera[24]. Ello, no obstante, autores como CHOCLÁN MONTALVO[25] o GÓMEZ TOMILLO[26] reprochan tal imprecisión, puesto que ello supone una falta de respeto a las exigencias derivadas del principio de legalidad, incumpliendo el mandato de determinación. Otros, como QUINTERO OLIVARES[27], señalan que esa "vaguedad" en la descripción de la conducta típica es necesaria y que en un mundo tecnológico tan cambiante como es el de la informática reducir las acciones posibles a un listado puede ser adecuado en un momento dado pero resulta atrasado a los pocos meses y resultaría peligroso para la eficacia del sistema legal.

Todos los penalistas estudiados ofrecen una definición de lo que es la manipulación informática, aquí reseñaré la que elige FARALDOCABANA[28]y la que construye CHOCLÁN MONTALVO[29], que plantean cuestiones muy interesantes que me permitirán mencionar el azote criminal del *phishing* y el *pharming*.

Afirma la primera autora que resulta aplicable la descripción que se contiene en el art. 3 de la Decisión Marco 2001/413/JAI del Consejo de Europa citada en casi todas las Sentencias del TS y las Audiencias Provinciales cuando se han enfrentado al tema de la descripción de la conducta típica. Así, considera que debe entenderse que constituye manipulación informática la introducción, alteración, borrado o supresión indebida de datos informáticos, especialmente datos de identidad y la interferencia indebida en el funcionamiento de un programa o sistema informáticos. El segundo autor, por su parte, entiende que constituye manipulación informática toda acción que suponga intervenir en el sistema informático alterando, modificando u ocultando los datos que deben 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. Transferencia de fondos, cancelación de deuda o el reconocimiento de un crédito pueden tener lugar por las siguientes vías: introducción de datos falsos o

[24] Nota 23: Ibídem, pág. 559.
[25] CHOCLÁN MONTALVO, José Antonio…op. cit. (6 y 16), pág. 70.
[26] GÓMEZ TOMILLO, Manuel (dir.), *Comentarios al Código Penal.* Lex nova, pág. 969.
[27] QUINTERO OLIVARES, Gonzalo…op. cit. (18), pág. 83.
[28] FARALDO CABANA, Patricia, op. cit.(20), pag. 89
[29] CHOCLÁN MONTALVO, Jose Antonio…op. cit.(6, 16, 25), págs. 74 y ss.

alteración, supresión u ocultación de los ya introducidos sin manipulación al programa, manipulaciones en el programa y manipulaciones en el sistema de salida de datos.

Tanto uno como otro autor ponen de manifiesto el problema que plantea el supuesto de que los datos introducidos no son falsos, sino que se produce una intervención no autorizada de un sujeto en un sistema informático. Por ello, FARALDO CABANA descarta una comprensión estricta del término manipulación, al acoger la definición de la Decisión Marco 1811/413/JAI y comprender por tanto la introducción de datos del titular real sin su consentimiento, concepción que dice "*responde a las tendencias internacionales en esta materia y ha recibido el beneplácito de la jurisprudencia*"[30].

CHOCLÁNMONTALVO por su parte remarca la dificultad de ampliar el término de manipulación hasta comprender supuestos de simples usos no autorizados de los delitos informáticos[31]. Quien ha obtenido las claves (auténticas) y las utiliza desde su propio ordenador para realizar una transferencia a su favor o de un tercero, a través de la red no ha alterado elemento físico o de programación alguno, ni ha introducido datos falsos. No sirve el concepto estricto de manipulación informática y han sido los tribunales los que han tenido que dar una respuesta adecuada a los cada vez más abundantes casos de suplantación por persona no autorizada de la clave y contraseña ajenas, para operar en las cuentas bancarias en Internet, tanto en la modalidad del PHISHING o del PHARMING, pero antes explicaré en qué consisten.

El *phishing* es actualmente la tipología delictiva más preocupante, millones de personas han sido víctimas en todo el mundo tal y como pone de manifiesto en sus informes la agrupación Anti-Phishing Working Group (APNG) que he citado antes. FERNÁNDEZ TERUELO[32] cita dos fuentes para la obtención por los delincuentes de las claves de acceso, y contraseñas secretas de seguridad, principalmente a usuarios de la Banca *online*, una sin su conocimiento mediante el recurso de archivos espía (spyware) y otra (el *phishing* y sus variantes) en que la propia víctima hace llegar al defraudador los datos necesarios para realizar las transacciones: el *phishing* consiste normalmente en el envío masivo de correos electrónicos que aparentando provenir de fuentes fiables-normalmente entidades bancarias- adoptan su imagen corporativa. Para ello, suelen

[30] FARALDO CABANA, Patricia, op. cit.(20, 28), págs. 89 y 90.
[31] CHOCLÁN MONTALVO, Jose Antonio, op.cit. (6, 16, 25, 29), pág. 76.
[32] FERNÁNDEZ TERUELO, Javier Gustavo, *Derecho penal e internet: especial consideración de los delitos que afectan a jóvenes y adolescentes.* Lex nova, págs. 36 y ss.

incluir un enlace que lleva a páginas web falsas con aspecto casi idéntico al de la entidad y una vez allí se pide al cliente que introduzca sus contraseñas o números de tarjeta de crédito, con lo que "pescados tales datos" son utilizados para quitarles el dinero. El defraudador suplanta al Banco, suplanta la personalidad de la víctima, y, utilizando las claves secretas, opera en las cuentas y consigue las transferencias de fondos sin que pueda hablarse de manipulación informática en el sentido estricto antes citado.

Pese a las alertas, los usuarios de Internet siguen "picando" y recientemente los medios de comunicación se hicieron eco de que se estaban enviando correos de forma masiva presentándose como la Agencia Tributaria y urgiendo a los contribuyentes para que facilitasen su número de cuenta y claves para verificar la devolución de la declaración de la renta.

El *pharming*, por su parte, consiste en manipular las direcciones que utiliza el usuario y el defraudador consigue que las páginas visitadas no se correspondan con las auténticas de Banca online, sino con otras creadas para recabar datos confidenciales de forma que el usuario los introducirá sin ningún temor, sin saber que los está remitiendo al defraudador.

Como he dicho antes, un concepto restringido de manipulación informática impediría la subsunción en el tipo del art. 248.2 del CP de los supuestos del *phishing* y su variante el *pharming*. El delincuente con las claves de la víctima utiliza correctamente la máquina, pero lo hace sin su consentimiento, suplantando su identidad. Se puede decir vulgarmente que le roba las claves, la identidad y el dinero. Es la problemática a la que se refieren muchos autores, entre ellos los anteriormente citados CHOCLÁN y FARALDO, del tratamiento penal de uso no autorizado de los datos informatizados. Un estudio de la jurisprudencia del Tribunal Supremo y de las Audiencias Provinciales que son las que han de enfrentarse a ese problema del *phishing* y del *pharming*, ponen en evidencia la impunidad, el éxito de quienes inician la trama defraudatoria cómodamente sentados en sus casas o en un ciber-café situados normalmente en la antigua URSS o países del Este. Todas las estudiadas, referidas a la estafa informática, de los últimos 10 años, solo tienen como protagonistas a los intermediarios o muleros. Los que expolian las cuentas de las víctimas al haber obtenido vía Internet engañosamente las claves de acceso figuran en los hechos probados como "personas no identificadas". Por lo tanto,

hay que recurrir a otros supuestos, normalmente referidos a tarjetas de crédito, como la capital sentencia del TS de fecha 20-11-2001, de MARTÍNEZ ARRETIA, un hito en esta materia, que recurre al "artificio semejante a la manipulación informática", y explica: "*para hacer aplicación del art. 248.2 lo relevante es que la máquina, informática o mecánica actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos de aquellos que permiten su programación, o por la introducción de datos falsos. La conducta de quien aparente ser titular de una tarjeta de crédito cuya posesión detenta de forma ilegítima y actúa en connivencia con quien introduce los datos en una máquina posibilitando que esta actúe mecánicamente está empleando un artificio para aparecer como su titular ante el terminal bancario a quien suministra los datos requeridos para la obtención de fondos de forma no consentida por el perjudicado*". Se utiliza en consecuencia la otra modalidad comisiva, el criticado "artificio semejante", que significa artimaña, doblez enredo, o truco, "maniobra similar" a la manipulación informática y en esa línea se puede citar la STS de 21-12-2004 cuyo ponente Bacigalupo afirma "es *equivalente a los efectos del contenido de la ilicitud, que el autor modifique materialmente el programa informático indebidamente o que lo utilice sin la debida autorización o en forma contraria al deber*".

Mayor interés tiene la sentencia del TS de fecha 9-5-2007, en la que su ponente BERDUGO Y GÓMEZ DE LA TORRE citando las sentencias referidas anteriormente y la Decisión Marco del 2001 que sirve de base a la definición de FARALDO CABANA da un paso más y considera "*que la identificación a través de un número secreto o pin es una de las conductas que enuncia tal Decisión Marco como manipulación informática. La identificación a través del número secreto genera una presunción del uso del sistema por parte de su titular y por ello debe incluirse como una modalidad de manipulación informática a los efectos de aplicar el art. 248.2 el mero hecho de utilizar el número secreto de otro para identificarse ante el sistema, aunque incluso dicho número hubiese sido obtenido al margen de cualquier actividad delictiva*".

En definitiva, identificarse ante el sistema informático mendazmente, introducir datos en el sistema que no se corresponden con la realidad ha de ser considerado bajo la conducta de manipulación informática a que se refiere el tipo de la estafa del art. 248.2

CP. En esta senda jurisprudencial el auto del TS nº 1153/2012 de 28 de junio del 2012 considera correcto y por tanto sin fundamento el recurso, la calificación que de estafa informática verificó la Audiencia Provincial de Madrid en un supuesto en el que el acusado hizo uso de las claves de acceso a banca por Internet que correspondían a su pareja fallecida para acceder a su cuenta y realizar transferencias.

La constatación en ese rastreo jurisprudencial de que los únicos que responden ante los tribunales españoles, que son detenidos, son los intermediarios o muleros, obliga a hacer una breve referencia ya que aquí también existe el debate. Los muleros (argot policial), como afirma FERNÁNDEZ TERUELO son quienes prestan sus cuentas bancarias personales para recibir el dinero y tras quedarse una comisión lo remiten a donde les han indicado los autores del fraude, normalmente giras postales al extranjero que no identifica al receptor[33]. Suelen ser captados a través del teletrabajo en Internet, se les ofrece el lucrativo negocio y cobra solo por abrir una cuenta corriente en la que recibirá el dinero que han obtenido quienes iniciaron la trama, imitando páginas web falsas de entidades bancarias, que con mensajes engañosos al picar los usuarios y facilitar sus claves bancarias han accedido a la cuenta y ordenado la transferencia.

Se plantea cual es la responsabilidad penal de los muleros y como señala el autor antes citado, la jurisprudencia está ofreciendo respuestas no coincidentes y que en realidad responden al caso concreto, pudiendo distinguirse dos situaciones. En primer lugar, sentencias absolutorias al estimar que los acusados desconocían totalmente que estaban realizando un acto delictivo, numerosísimo en las Audiencias Provinciales basadas en el fundamento "*de no desprenderse que exista una certeza del conocimiento de la procedencia u origen del dinero ilícito*". Así, SAP Soria 27-2-2012, SAP León de 29-7-2011, SAP Valladolid 21-6-2010, etc. En el ámbito del TS, por todas la reciente sentencia nº 8316/2012 de 3-12-2012 (ponente Luciano Varela) que casa y absuelve a Carmelo que había sido condenado en base al art. 248.2, rechazando el recurso que hace la sentencia recurrida a la "ignorancia deliberada", al entender que no resulta adecuado a las exigencias del principio de culpabilidad.

En segundo lugar, la otra postura, cuando se considera probado que el mulero conocía y aceptaba que está participando en un hecho delictivo, la jurisprudencia menor y el TS

[33] Nota 32: Ibídem, pág. 39.

fluctúa entre considerarlo un supuesto de cooperación necesaria en el delito de estafa informática o bien de blanqueo de capitales por imprudencia. Esta última subsunción se aprecia en la SAP de la Audiencia Provincial de Palma de Mallorca de 11 de octubre de 2012 (Ponente: Ana María Cameselle Montis).

En el ámbito del TS cabe citar la sentencia nº 834-2012 de 25 de octubre de 2012 (ponente MARCHENA),que a propósito de la condena de un mulero por blanqueo realiza un análisis crítico de la controversia doctrinal y jurisprudencial sobre el encaje en dicho tipo o en la estafa del 248.2 cita STS 533/2007 de 12 de junio, STS 1548/2011 como ejemplos de condena por este último artículo y concluye que hay que atender a las circunstancias del caso concreto. "*El debate doctrinal demuestra el carácter controvertido y todo indica que lejos de formulas generales, serán las circunstancias del caso las que, a la vista de la prueba de los elementos facticos que dan vida a los elementos objetivo y subjetivo permitan formular sin error el juicio de subsunción*".

En otro orden de cosas, la acción de manipulación debe tener como consecuencia la transferencia no consentida de activos patrimoniales, con la consiguiente disminución del patrimonio de un tercero. Es un cambio de adscripción que verifica la máquina de un activo patrimonial. CHOCLÁN MONTALVO[34] dice que definida la acción como transferencia, no como disposición, cabe que aquella sea realizada por la máquina y que la referencia a activos patrimoniales tiene la clara finalidad de comprender como objeto de la acción dinero contable o escritural, valores patrimoniales sin correspondencia con un objeto material e incluso también un servicio sin abono de su importe es equivalente a la transferencia de su activo patrimonial y la supresión de los datos relativos a su pasivo. En contra de la inclusión del servicio también FARALDO CABANA[35].

La transferencia de activos patrimoniales es el resultado que debe producir o más propiamente conseguir el autor de la estafa, sin el consentimiento de la víctima, otro elemento típico de la estafa informática, que vendrá a delimitar el tipo objetivo de la estafa. Según GALÁN MUÑOZ[36], para ello se exige que dicha transferencia se realice en perjuicio de otro, elemento típico que configura a este delito como un delito de

[34] ESPAÑA. ESCUELA JUDICIAL. CONSEJO GENERAL DEL PODER JUDICIAL. *Internet y derecho penal: Fraude informático y estafa por computación.* Escrito por CHOCLÁN MONTALVO y dirigido por LÓPEZ ORTEGA, Juan José, Magistrado de la Audiencia Nacional (dir.). Madrid: Cuadernos de Derecho Judicial, 2001, pág. 337.
[35] FARALDO CABANA, Patricia, op. cit. (20, 28, 30), pág. 107.
[36] GALÁN MUÑOZ, Alfonso, op. cit. pág. (2, 9, 23) pág. 901.

resultado, tal y como lo demuestra el que se tenga en cuenta el valor del daño patrimonial efectivamente ocasionado, tanto a la hora de diferenciar el delito de la estafa como a la hora de determinar la concreta penalidad.

2.El art. 248.2 letra b) afirma que "*También se consideran reos de estafa: b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo"*.

Este apartado ha sido muy criticado, empezando por su nueva ubicación sistemática (fue introducido en el 2003) tras la reforma del 2010, ya que FERNÁNDEZ TERUELO[37] la considera un sin sentido al quedar referida a ambos tipos de estafa-común e informática, pues en la práctica solo puede afectar a supuestos relativos a la segunda. Lamenta tal autor, como todos los consultados, que se mantenga lo que constituye una grave desproporción, esto es, que se castigue lo que no es sino un acto preparatorio como delito consumado, considerando también un exceso punitivo que se castigue la mera posesión de tales programas. PÉREZ MACHÍO[38] llama la atención en el sentido de que dicha regulación está yendo más allá de lo que prevé el Convenio de Budapest y GÓMEZ TOMILLO[39] pone de manifiesto que los hechos incriminados son actos preparatorios que de no haber sido incriminados expresamente carecerían de relevancia penal por encontrarse en un momento muy lejano al menoscabo de este y apunta que resulta problemática la relación con el supuesto del art. 400 CP, respecto a ciertas conductas con programas de ordenador para la realización de falsificaciones, cuestión no aclarada por la jurisprudencia en alguna ocasión que se ha planteado (STS 9-5-2006).

FARALDO CABANA[40] coincide con tales críticas y añade que la exigencia del tipo de que el programa de ordenador esté "específicamente destinado" a la comisión de la estafa debe interpretarse en el sentido de que no puede tratarse de un programa que creado para otro fin, se pueda aprovechar también para la comisión de la estafa. Y piensa que programas que solo pueden considerarse especialmente a ello son los empleados para llevar a cabo el phishing o del software malicio para llevar a cabo el pharming.

[37]ÁLVAREZ GARCÍA, Francisco Javier; y GONZÁLEZ CUSSAC, Jose Luís (Directores). *Comentarios a la Reforma Penal de 2010.* Valencia: Tirant lo Blanch Reformas, Trust CM, 2010, pág. 277.
[38] ESPARZA LEIBAR IÑAKI…op.cit.(5, 11), pág. 183.
[39] GÓMEZ TOMILLO, Manuel, op. cit. (26), pág. 970.
[40] FARALDO CABANA, Patricia, op. cit, (20, 28, 30, 35), pág. 113.

3. Por último, el art. 248.2 letra c), introducido por la reforma operada por la Ley 5/2010, afirma que también se consideran reos de estafa: *c) los que utilizando tarjetas de crédito o débito o cheques de viaje o los datos obrantes en cualquiera de ellos realicen operaciones de cualquier clase en perjuicio de su titular o un tercero.* Se equipara a efectos penológicos a la estafa común esta figura que, según una parte de la doctrina, pone fin a una intensa discusión doctrinal y jurisprudencial sobre el tratamiento penal, la subsunción, de las conductas que suponían el uso no consentido de los datos contenidos en la tarjeta en perjuicio del titular.

Antes de la reforma 2010 la jurisprudencia subsumía los supuestos de utilización de tarjetas de crédito, según los casos, en diferentes tipos penales:

. En el común (art. 248.1) cuando las tarjetas de crédito ajenas se empleaban para realizar pagos en un establecimiento, que es la conducta denominada "carding" o la conducta denominada skimming, consistente en el uso como medio de pago en el comercio tradicional de tarjetas legítimas en las que se había alterado la banda magnética. Todo ello en base a que el destinatario del engaño y quien sufre el error era la persona física, el comerciante.

. En el tipo del robo con fuerza en los casos de utilización de la tarjeta de crédito ajena en un cajero automático pues el uso de la tarjeta se consideraba como "llave falsa" de acuerdo con lo que dispone el párrafo ultimo del art. 239.

. En el tipo del art. 248.2 CP la utilización de una tarjeta perdida u obtenida por un medio constitutivo de infracción penal para realizar compras online o extraer dinero en un cajero automático, considerando que la suplantación de la identidad del titular es manipulación informática pues se utilizan datos reales del verdadero titular sin su consentimiento. Tendencia jurisprudencial que ya he citado antes, que se inició en el 2001 con la sentencia antes citada de MARTÍNEZ ARRIETA (STS 20-11-2001) y que es respaldada por la doctrina mayoritaria, así FARALDO CABANA[41], ROVIRA DEL CANTO[42], CHOCLÁN MONTALVO[43]. Se dejaba atrás, aunque aún puede verse reflejada tal postura en las Audiencias Provinciales, la subsunción de utilización de tarjetas magnéticas por tercero no autorizado en cajeros automáticos, en el tipo del robo

[41] Nota 40: Ibídem, Pag. 81.
[42] ROVIRA DEL CANTO, Enrique, op.cit.(19, 21), pág. 629.
[43] CHOCLÁN MONTALVO, Jose Antonio…op. cit. (6, 16, 25, 29, 31), pág. 84.

con fuerza en las cosas mediante el uso de llave falsa de los arts. 237, 238.4 y 239 CP y que había sido muy criticada porque no había acceso al lugar donde se encuentran las cosas. Una cuestión no baladí dada la diferente penalidad de la estafa informática y el robo con fuerza.

. Con la reforma del 2010 según señala QUINTERO OLIVARES[44] se zanja la discusión acerca de la calificación que corresponde a las extracciones de dinero de cajero utilizando tarjeta de crédito o débito y que a partir de ahora irán a parar a ese nuevo tipo, así como la conducta que hasta ese momento para él era atípica, consistente en los fraudes cometidos sin utilizar físicamente la tarjeta pero sí sus datos (número y fecha de caducidad), para comprar cosas a través de Internet.

Una visión muy crítica de la introducción de ese nuevo tipo tienen GÓMEZ TOMILLO[45], FERNÁNDEZ TERUELO[46] y MORALES GARCÍA[47] al considerar el primero que la cuestión ya estaba resuelta y ahora se diversifica en mayor medida la regulación criminal de los usos fraudulentos de los medios de pago y hace más complejo su tratamiento penal. El segundo, amén de considerar innecesario el precepto ya que existía consenso jurisprudencial, remarca la errónea selección del objeto, así al referirse el legislador solo a algunos de los posibles tarjetas (débito o crédito) omitiendo otras y en lo que respecta a los cheques de viaje son un instrumento de pago casi en desuso. En igual sentido, el tercero, al entender que puede causar confusión tal tipo ya que no le sigue una modificación del art. 239 (llave falsa) que deje clara la preferencia normativa o la circunstancia de que el legislador ha previsto la misma conducta en el art. 399 bis CP, pero reservada a casos en que las tarjetas empleadas en perjuicio del titular son falsas con pena mucho más benigna.

[44] QUINTERO OLIVARES…op.cit. (18, 27), pág. 84.
[45] GÓMEZ TOMILLO, op.cit. (26, 39), pág. 971.
[46] ÁLVAREZ GARCÍA, Francisco Javier; y GONZÁLEZ CUSSAC, Jose Luís, op.cit (37), pág. 281.
[47] MORALES GARCÍA, Oscar en "La reforma Penal de 2010", dirigida por QUINTERO OLIVARES (dir.), aranzadi, thomson reuters, Pag. 153.

V. REFLEXIÓN FINAL

Las nuevas tecnologías aplicadas a la comisión de delitos es un mundo en continuo cambio que obliga al jurista a hacer verdaderos ejercicios de funambulismo para adoptar esas nuevas conductas a los viejos delitos. Por muy rápido que quiera dar respuesta el legislador, el timador se le adelanta y es encomiable al respecto la labor que realiza la doctrina y los Tribunales en tal arduo trabajo.

Me ha llamado la atención en ese esfuerzo la obra de Gutiérrez Francés, que en el año 1990 intentó reinterpretar en un ensayo de 500 páginas el viejo tipo de la estafa del art. 528 CP, a las nuevas conductas que suponían de entrada que no había relación bilateral entre el delincuente y la víctima, entablándose la relación entre el primero y la máquina. La famosa pregunta ¿Se puede engañar a la máquina? Es llamativa pero muy interesante la división de los autores y de la jurisprudencia en el tratamiento penal de las nuevas conductas, un debate rico, pero que a veces sorprende porque sugiere un tanto de inseguridad, ya que no es lo mismo ser castigado por robo con fuerza que por estafa informática, refiriéndose a uno de los temas más candentes, se supone que hasta este momento.

En definitiva, la ciberdelincuencia, la estafa informática, sugiere la necesidad de una cooperación allende las fronteras, una serie de ideas muy interesantes en cuanto a la armonización de la legislación, los grupos policiales, las normas procesales y una cosa que nunca se me habría ocurrido antes de comenzar este trabajo, las disquisiciones doctrinales sobre las denominaciones de los delitos me parecieron farragosas y un tanto absurdas pero lo cierto es que la lectura de los tratados y la investigación en otras fuentes de Internet me ha hecho comprender la importancia de utilizar nombres comunes como pone de manifiesto Sneyers y ello porque esa deseada cooperación internacional, se encuentra de entrada con la imposibilidad de calibrar ante los diferentes nombres para una misma conducta que se utiliza en las estadísticas, la real entidad del azote criminal, lo que puede ser un obstáculo para otros muchos casos.

La ciberdelincuencia es el fenómeno más palpitante, más vivo y cambiante de nuestro Código Penal y por lo tanto me ha parecido muy interesante esta pequeña aproximación

habiendo observado que la mayoría de los penalistas consultados consideran, que la última reforma del Código Penal se ha quedado corta.

FUENTES BIBLIOGRÁFICAS

- ÁLVAREZ GARCÍA, Francisco Javier; y GONZÁLEZ CUSSAC, Jose Luís (Directores). *Comentarios a la Reforma Penal de 2010.* Valencia:Tirant lo Blanch Reformas, Trust CM, 2010. P.277-285.
- ÁLVAREZ GARCÍA, Francisco Javier (dir.); GONZÁLEZ CUSSAC, Jose Luís (dir.); MANJÓN-CABEZA OLMEDA, Araceli (coord.); VENTURA PÜSCHEL, Arturo (coord.). *Consideraciones a propósito del Proyecto de Ley de 2009 de modificación del Código Penal (Conclusiones del Seminario interuniversitario sobre la reforma del Código Penal celebrado en la Universidad Carlos III de Madrid).* Valencia: Tirant lo Blanch, 2010. P.225-231.
- ÁLVAREZ GARCÍA (dir.); MANJÓN-CABEZA OLMEDA, Araceli (coord.); VENTURA PÜSCHEL, Arturo (coord.). *Derecho Penal Español Parte Especial (II).* Valencia: Tirant lo Blanch, 2011. P. 251-259.
- BERENGUER ORTS, Enrique; ROIG TORRES, Margarita. *Delitos informáticos y delitos comunes cometidos a través de la informática.* Tirant lo Blanch, "colección los delitos", 41, 2001. P. 63-71.
- CASTIÑEIRA PALOU, Mª Teresa et. al; FELIP I SABORIT, David; BENLLOCH PETIT, Guillermo; ROBLES PLANAS, Ricardo; PASTOR MUÑOZ, Nuria; ORTIZ DE URBINA GIMENO, Íñigo; MONTANER FERNÁNDEZ, Raq uel; LLOBET ANGLÍ, Mariona. *Lecciones de derecho penal parte especial: 3.ª edición adaptada a la Ley Orgánica 5/2010 de reforma del Código Penal.* SILVA SÁNCHEZ, Jesús María (dir.); RAGUÉS I VALLÈS (coord). Barcelona: Atelier Libros Jurídicos, Iuscrimbcn. P. 239-243.
- CHOCLÁN MONTALVO, José Antonio et. al; GARCÍA GONZÁLEZ, Javier; GONZÁLEZ RUUS, Juan José; GUTIÉRREZ FRANCÉS, Mariluz; HAMM, Rainer; MATA Y MARTÍN, Ricardo; MORALES PRATS, Fermín; PICOTTI, Lorenzo; PIÑAR MAÑAS, José Luis; SANCHÍS CRESPO, Carolina*. El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales.* ROMEO CASABONA, Carlos María (Coord).Granada: Editorial Comares, 2006. P. 69-93.
- DAVARA RODRÍGUEZ, Miguel Ángel. *Manual de derecho informático.* Thomson Aranzadi, 5º edición. P.

- ESPAÑA. ESCUELA JUDICIAL. CONSEJO GENERAL DEL PODER JUDICIAL. *Internet y derecho penal: Fraude informático y estafa por computación.* LÓPEZ ORTEGA, Juan José, Magistrado de la Audiencia Nacional (dir.). Madrid: Cuadernos de Derecho Judicial, 2001. P. 307-352.
- ESPARZA LEIBAR, Iñaki et. al; SAN JUAN GUILLÉN, César; PÉREZ MACHIO, Ana Isabel; SAIZ GARITAONANDÍA, Alberto; PÉREZ ESTRADA, Miren Josune; HERNÁNDEZ DÍAZ, Leyre. *Derecho penal informático.* CUESTA ARZAMENDI (dir.); DE LA MATA BARRANCO, Norberto (coord.). Thomson Reuters, Civitas. P. 147-185.
- FARALDO CABANA, Patricia. *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico.* Tirant lo Blanc, "colección los delitos", 2009. P. 65-131.
- FERNÁNDEZ TERUELO, JavierGustavo. *Cibercrimen. Los delitos cometidos a través de internet.* Constitutio criminalis, carolina, 2010. P. 27-53.
- FERNÁNDEZ TERUELO, Javier Gustavo. *Derecho penal e internet: especial consideración de los delitos que afectan a jóvenes y adolescentes.* Lex nova. P. 35-54.
- GALÁN MUÑOZ, Alfonso. *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 C.P.* Valencia: Tirant lo Blanch, 2005. Págs. 931.
- GÓMEZ TOMILLO, Manuel (dir.). *Comentarios al Código Penal.* Lex nova. P. 969-971.
- GUTIÉRREZ FRANCÉS, Mª Luz. *Fraude informático y estafa (Aptitud del tipo de estafa en el Derecho español ante las defraudaciones por medios informáticos).* Madrid: Ministerio de Justicia, Secretaria General Técnica, Centro de Publicaciones, 1991. P. 642.
- *Memento Experto: Reforma Penal 2010.* Ediciones Francis Lefebvre. P. 197-239.
- MUÑOZ CONDE, Francisco. *Derecho Penal: Parte especial, 18ª edición, revisada y puesta al día.* Valencia: Tirant lo Blanch, 2010. P. 430-431.
- QUINTERO OLIVARES, Gonzalo (dir.). *La Reforma Penal de 2010: Análisis y Comentarios.* Aranzadi, Thomson Reuters. P. 181-194.
- QUINTERO OLIVARES, Gonzalo et. al; MORALES PRATS, Fermín; TAMARIT SUMALLA, Josep Mª; GARCÍA ALBERO, Ramón. *Comentarios al Código Penal Español, Tomo II (Artículos 234 a DF. 7ª).* QUINTERO OLIVARES, Gonzalo (dir.); MORALES PRATS, Fermín (Coord.). Aranzadi, Thomson Reuters, 6ª edición. P. 80-87.

- ROVIRA DEL CANTO, Enrique. *Delincuencia informática y fraudes informáticos.* Granada: Editorial Comares, Estudios de Derecho Penal dirigidos por Carlos Mª Romeo Casabona, 2002. P. 241-277 y 556-671.
- SNEYERS, Alfredo. *El fraude y otros delitos informáticos.* Madrid: Tecnologías de Gerencia y Producción, S.A, 1990. P. 215.
- SERRANO GÓMEZ, Alfonso; SERRANO MAÍLLO, Alfonso. *Derecho Penal: Parte Especial.* Madrid: Dykinson, 16.ª edición, 2011. P. 430-435.
- Unión Internacional de Comunicación, El Ciberdelito: Guía por los países en desarrollo, Ginebra 2009 www. itu.int/dmspub/ituud/otb. National, regional and international approaches in the fight against cybercrime. Computer Law Review International, 2008.