FACULTAD DE DERECHO

EL TRATAMIENTO PENAL DE LOS DELITOS COMETIDOS A TRAVÉS DE INTERNET. LA PROTECCIÓN FRENTE A LAS ESTAFAS INFORMÁTICAS

Autor: María Bañón Medina

5º Derecho y Relaciones Internacionales (E-5)

Derecho Penal

Tutor: María Teresa Requejo Naveros

Madrid
Abril 2021

ABREVIATURAS UTILIZADAS

Código Penal – CP

Sentencia del Tribunal Supremo – STS

Centro Criptológico Nacional y Centro Nacional de Inteligencia – CCN-CERT

RESUMEN

El desarrollo de las nuevas tecnologías supone la creación de nuevos escenarios para las conductas delictivas. El Código Penal se ha tenido que adaptar a estas nuevas formas de comisión de los delitos, y para ello ha incorporado nuevos ilícitos en su cuerpo normativo. Entre estas nuevas conductas delictivas se encuentra la estafa informática.

Tras varias reformas, el legislador ha optado por incluir en el artículo 248.2 CP, tres conductas que encajan dentro de este tipo de estafa: la comisión a través de una manipulación informática y artificio semejante, la fabricación, introducción, posesión o facilitación de los programas informáticos como actos preparatorios, y la comisión del delitos a través de la utilización de tarjetas.

Este trabajo tiene como objetivo, en primer lugar, analizar el tipo del artículo 248.2 CP y aclarar las controversias y los conflictos de interpretación que han surgido como consecuencia del uso generalizado de los programas informáticos. Asimismo, se abordará la cuestión de si la regulación por la que ha optado el legislador es apta para abordar las nuevas fórmulas específicas que han ido apareciendo para la comisión de estos delitos. Por último, se van a proponer medidas preventivas y nuevas soluciones de acuerdo con las experiencias con las que los tribunales se han encontrado hasta ahora, la normativa europea y la regulación de otros países

PALABRAS CLAVE

Delitos informáticos, estafa informática, programa informático, perjuicio económico, *phishing.*

ABSTRACT

The development of new technologies has created new scenarios for criminal conducts to be carried out. The Criminal Code has had to adapt to these new ways of committing crimes, and to this end has incorporated new offenses in its regulatory body. Among these new criminal conducts we can find the crime of computer fraud.

After several reforms, the legislator has opted to include in Article 248.2 of the Criminal Code, three conducts that fit within this type of fraud: the commission through computer manipulation and similar artifice, the manufacture, introduction, possession or facilitation of computer programs as preparatory acts, and the commission of crimes through the use of credit cards.

This paper aims, first, to analyze the type of Article 248.2 PC and clarify the controversies and conflicts of interpretation that have arisen as a result of the widespread use of computer programs. It will also address the question of whether the regulation chosen by the legislator is suitable for dealing with the new specific formulas that have been appearing for the commission of these crimes. Finally, preventive measures and new solutions will be proposed in accordance with the experiences encountered by Spanish courts, European regulations and regulations in other countries.

KEY WORDS

Computer crimes, computer fraud, computer program, financial damage, phishing

ÍNDICE DE CONTENIDO

CAPÍTULO I.- INTRODUCCIÓN

Los conocidos como *delitos informáticos* o la *ciberdelincuencia* son producto del uso que le hemos dado a los desarrollos tecnológicos. Internet, para bien o para mal, es un ejemplo más del proceso de globalización y de la ruptura de las barreras que existen en la comunidad internacional. Se trata de un espacio social de un tamaño increíble; resulta imposible tener un control absoluto sobre lo que ocurre en la red, y como consecuencia, han ido surgiendo nuevas formas de criminalidad derivadas de su uso generalizado que hemos presenciado desde hace unos cuarenta años.

Como en cualquier otro ámbito, cuando aparecen nuevas formas de cometer delitos y se generaliza su comisión con la misma rapidez que se ha conseguido a través de Internet, surge la necesidad de tipificar estas conductas y controlar estos espacios que hasta hace unos años estaban libres de regulación. El ordenamiento jurídico español no ha sido ajeno a este proceso y ya en el Código Penal aparecen varios tipos asociados a los medios electrónicos. No todos los tipos vulneran el mismo bien jurídico ni tienen el mismo modo de proceder, pero todos tienen algún medio electrónico como elemento en común.

Parece que el mundo jurídico no puede seguir el ritmo del mundo virtual, sin embargo, tanto en 2003 como en 2010 se han modificado los delitos que ubicamos bajo la categoría de *delitos informáticos*, y se han introducido nuevos tipos, a medida que se han desarrollado novedades tecnológicas. Se está luchando frente a estas nuevas conductas a medida que van surgiendo, pero también queda latente la importancia de desarrollar un modelo de prevención de la comisión de estos delitos nuevos.

El *Estudio sobre la cibercriminalidad en España* (Gabinete de Coordinación y Estudios; Secretaría de Estado de Seguridad, 2019) analiza la información recabada por el Ministerio del Interior con la finalidad de poner de manifiesto la relevancia que está adquiriendo este fenómeno penal. Entre los datos que ofrece la publicación, destaca el total de 218.302 hechos que constituyen delitos informáticos de diferente índole, lo que supone un 35,8% más con respecto del año anterior. Entre los hechos delictivos, una gran mayoría (el 88,1%) constituyen estafas informáticas (Gabinete de Coordinación y Estudios; Secretaría de Estado de Seguridad, 2019). Teniendo estos datos en cuenta, primero vamos a realizar una aproximación al concepto de *delito informático* en

general, para situarnos en la dirección en la que el legislador ha decidido regular esta clase de conductas delictivas. No obstante, nos vamos a centrar en este último delito de estafa informática que está más generalizado y cuyo tratamiento y prevención ha generado debates a nivel jurisprudencial y doctrinal, por su regulación paralela a la estafa, y las distintas formas de comisión que han ido surgiendo rápidamente de la mano de los diferentes desarrollos tecnológicos.

CAPÍTULO II.- ORIGEN Y EVOLUCIÓN DE LOS DELITOS COMETIDOS A TRAVÉS DE INTERNET: CONCEPTO Y CLASIFICACIÓN

A medida que aumenta el número de usuarios de Internet, mayor es la importancia que se le debe dar a la cibercriminalidad, pues van apareciendo nuevas formas de operar en la red a las que hay que hacer frente. Cuando comenzaron a detectarse movimientos delictivos en la red, el derecho penal se adaptó a los cambios en la forma en la que se cometen los delitos. Surgió una necesidad de regulación en la sociedad; en este caso fue el derecho el que tuvo que amoldarse a la realidad, y no al revés. Aunque uno de los fines del derecho sea organizar la sociedad, vemos que la sociedad civil, cuando crea nuevas necesidades, es la que determina la forma de ser y actuar del Estado (Barrio Andrés, 2011, pág. 275).

En un primer momento, pudo parecer que la red operaba bajo el principio de libre disposición, pues fue creada por la sociedad para sus necesidades específicas, y los Poderes Públicos no fueron los que la pusieron a disposición de la sociedad con una regulación y unos límites. Sin embargo, no tardaron mucho las autoridades en darse cuenta de la importancia que tenía todo lo que ocurría en ese espacio social, que aunque no sea visible, es muy poderoso. Se rechazó, por lo tanto, la categorización del mundo virtual como un supuesto de *no-derecho* como explicaba Carbonnier en su *L'hypothese de non-droit*, en el que se discutía la práctica de *laissez faire* aplicada a aquellos ámbitos de la sociedad que debían regularse por sí mismos (entre ellos se encontraba Internet) (Barrio Andrés, 2011, pág. 275).

Como con todos los hechos que se convierten en ilícitos penales, el legislador tuvo en cuenta la importancia tanto del principio de proporcionalidad como del principio de intervención mínima. Es decir, el derecho penal debe limitarse a responder solo a las agresiones más graves que se produzcan contra los bienes jurídicos más importantes (Lascuraín Sánchez, 2019). Como veremos a lo largo de este trabajo, cuando hablamos de *ciberdelincuencia* no está claro el bien jurídico que se protege de forma general, ni tampoco la magnitud de las agresiones en muchos de los casos. Esta doble limitación de la intervención penal en los delitos informáticos, por lo tanto, es objeto de discusión por muchos autores, pero está claro que se debió tener en cuenta al introducir la regulación.

Se evitó una ordenación extensa en un primer momento, pues el uso de la tecnología no estaba tan generalizado en 1995 como lo está ahora, no obstante, el legislador pretendió en todo momento cubrir las lagunas de punibilidad que se descubrieron en la jurisprudencia que trataba la comisión de delitos mediante medios electrónicos. Como consecuencia de esa falta de bien jurídico protegido común en los diferentes delitos informáticos que se buscaba penalizar, el Código Penal no incluyó ningún apartado único para esta clase de ilícitos. El resultado fue una ordenación dispersa: diferentes delitos en los que Internet jugaba una parte importante distribuidos en los distintos apartados del Código Penal, ya fuera como tipos equivalentes a figuras tradicionales (que incluían algún elemento informático), o como nuevas figuras delictivas[1]. A pesar de las reformas que ha sufrido nuestro Código Penal, y de los distintos autores que han defendido la creación de un título específico sobre la *ciberdelincuencia*, actualmente la regulación sigue estando diseminada por el cuerpo normativo.

> La doctrina no ha llegado todavía a un consenso sobre lo que se entiende por *delito informático*. De hecho, usamos este término, igual que el de *ciberdelincuencia*, con un sentido impropio, pues realmente la legislación no alude a *delitos informáticos* en ningún momento; no existe ningún delito tipificado como tal (Gómez Perals, 1994, pág. 482). Se empezó a tener en consideración esta clase de delitos por su característica común, y acogiendo en cierto modo el concepto inglés de *computer crimes* (Barrio Andrés, 2011, pág. 277), pero el Código Penal de 1995 no introdujo el *delito informático* ni admitió su existencia. Tampoco hay ninguna Ley Especial que trate este tema de forma autónoma, pero se sigue usando.

A pesar de conocer una serie de definiciones generalizadas por autores especialistas en la materia y usadas en documentos oficiales, para poder llevar a cabo un análisis de lo que a lo largo de este trabajo se debe entender por *delitos informáticos* vamos a centrarnos en el uso que el Convenio sobre la Ciberdelincuencia de 2001 hace del concepto. Siendo el documento más importante sobre la materia, el Convenio de

[1] Debemos tener en cuenta, tal y como indica Ignacio Flores Prada, que el hecho de que *los sistemas informáticos no han creado nuevos bienes jurídicos, no significa que su utilización sea penalmente irrelevante. El derecho penal no regula bienes jurídicos sino conductas de lesión (…) lo relevante es saber de qué modo el uso de los sistemas informáticos puede llegar a lesionar los bienes jurídicos protegidos por el sistema penal*. (Prada, 2012)

Budapest fue redactado por el Consejo de Europa en 2001, pero en España no se ratificó hasta 2010. Aunque no haya en él ningún precepto que establezca formalmente una definición del delito informático, se intuye el significado que le está dando, y realmente se trata de una de las definiciones más aceptadas por el carácter transnacional de su origen y por ser uno de los primeros cuerpos normativos internacionales que se ocupa de esta cuestión.

El Convenio de Budapest trata el *delito informático* como un tipo de delito, ya sea tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta. El concepto que ofrece se basa en la utilización de determinadas técnicas y modos de proceder informáticos, (como por ejemplo el acceso ilícito a un sistema informático o fraude informático) pero también se refiere a ciertos contenidos cuya vulneración se ve facilitada por el medio internet (como ocurre con los delitos de pornografía infantil) (Urbano Castrillo, 2011, pág. 2). Por lo tanto, además de proponer un concepto de delito informático con el fin de facilitar la cooperación en el ámbito penal, también ofrece una clasificación de los distintos delitos informáticos que existen.

El Convenio agrupa en un mismo apartado una serie de conductas que denomina *Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*, y aquí incluye el acceso ilícito a los sistemas informáticos, la interceptación de datos informáticos y actos dirigidos a dañar o borrar datos informáticos. Es decir, delitos que afectan directamente a los sistemas informáticos y ponen en peligro su funcionamiento y contenido.

En el siguiente apartado el Convenio describe dos delitos a los que clasifica como *delitos informáticos*. El primero es la falsificación informática (en concreto, la alteración de datos informáticos que generen información falsa), y el segundo es el fraude informático, caracterizado por el perjuicio patrimonial que causa. En general no se ha interpretado esta categoría de forma restrictiva. Por mucho que se califique estos dos delitos como delitos informáticos distinguiéndolos de los demás, no significa que no debamos incluir dentro de este concepto al resto de ilícitos descritos en los demás preceptos.

El tercer Título lo dedica a los *delitos relacionados con el contenido*, entre los que encontramos los diferentes usos de los sistemas informáticos relacionados con la

pornografía. Por último, propone una serie de medidas para los *delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.*

Se trata de una ordenación clara y lógica, de acuerdo con los bienes jurídicos protegidos en cada caso. No obstante, no debemos olvidar que esta enumeración de delitos informáticos existentes y punibles se realizó hace veinte años. Quizás en otros ámbitos del Derecho Penal la delincuencia y los hechos ilícitos no aumentan de manera acelerada en un periodo de tiempo como este, pero cuando hablamos de Internet, cada vez se descubren nuevas formas de cometer infracciones asociadas a las novedades tecnológicas más actuales.

Por consiguiente, pese a la importancia de lo establecido en el Convenio de Budapest, resulta igualmente relevante tener en mente alguna definición y clasificación más reciente. A nivel de investigación y análisis, la Estrategia Nacional de Ciberseguridad 2019 aprobada por el Consejo de Seguridad Nacional incluye dentro del término de cibercriminalidad todas las *actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas* (Gabinete de Coordinación y Estudios; Secretaría de Estado de Seguridad, 2019). El elemento clave sigue siendo la intervención de medios informáticos, sin embargo, abarca más supuestos, y en vez de centrarse en tipos delictivos específicos como el Convenio de 2001, las clasificación la hace en atención a los distintos ámbitos en los que se pueden desarrollar los hechos y la forma en la que el *ciberespacio* se ve afectado por ellos (puede ser como objetivo directo de los hechos, como medio clave para la comisión del ilícito, o como objeto de investigación para cualquier hecho).

El Informe que nos ofrece el Consejo de Seguridad Nacionalda un paso más allá en la lucha contra esta clase de ilícitos penales, configurando un sistema más amplio y genérico con el objetivo tanto de poder incluir nuevos supuestos que vayan apareciendo, como de darle importancia a la concienciación, prevención e investigación de la cibercriminalidad.

Por último, cabe destacar la labor realizada por Eloy Velasco en su libro *Delincuencia informática*, en el que desmenuza los diferentes ilícitos penales con los que nos encontramos en Internet, basándose tanto en los tipos fijados en el Código

Penal, como en la clásica clasificación ofrecida por el profesor y especialista en el ámbito, Ulrich Sieber (Velasco Nuñez & Sanchís Crespo, 2019). Es posible que esta sea la diferenciación que más encaje con la legislación penal actual; primero tenemos la *ciberdelincuencia económica*, que se caracteriza por el perjuicio a un patrimonio ajeno a través de la informática, en segundo lugar *ciberdelincuencia "*intrusiva", con la que se daña la privacidad y la intimidad a través de estos medios, y por último el *ciberespionaje y ciberterrorismo*, que tiene un alcance más nacional y con objetivos de mayor escala (Velasco Nuñez & Sanchís Crespo, 2019, pág. 12).

En suma, la legislación penal española, a pesar de los esfuerzos de diferentes autores e instituciones, no ha logrado introducir un concepto genérico de lo que estudiamos como delitos informáticos. Tampoco podemos oficialmente decir que hay distintas categorías en las que se pueden dividir las diferentes formas de cometer un delito informático, de forma que solo nos queda identificar los diferentes tipos que aparecen en el Código Penal en los que los medios informáticos juegan un rol esencial en cualquier fase de su comisión.

CAPÍTULO III.- LA ESTRATEGIA DEL LEGISLADOR ESPAÑOL ANTE EL DELITO DE ESTAFA INFORMÁTICA COMO PARTE DE LOS DELITOS DE CARÁCTER INFORMÁTICO

Antes de delimitar cronológicamente la evolución legislativa del delito de estafa informática, sería bueno tratar de precisar si puede o no advertirse, en el modo en que viene actuando el legislador, un sentido programático concreto, una política legislativa específicamente destinada a la regulación de los delitos informáticos, de los que el delito de estafa informática sería una manifestación más.

Hasta la reforma de 2010, en un listado aproximativo, los distintos lugares en los que se regulaban los tipos relacionados con la delincuencia informática se encontraban dispersos en una serie de preceptos:

1. Los artículos 186 a 189 CP, relativos a la pornografía infantil.
2. El artículo 197.2 CP, sobre espionaje informático.
3. El artículo 238.5 CP, referido al robo que se lleva a cabo inutilizando los sistemas de guarda criptográfica.
4. "Nuestro" artículo 248.2 CP sobre la estafa informática.
5. El 256 CP relativo a la ubicación abusiva de equipos de terminales de telecomunicación.
6. El 264.2 CP sobre sabotaje o daños informáticos.
7. El artículo 270 CP referente a la propiedad intelectual.
8. Los artículos 273, 274 y 275 CP, sobre propiedad industrial.
9. El artículo 278.1 CP en lo que concierne a los secretos de empresa.
10. El artículo 286 CP sobre el uso ilegal de equipos, programas y servicios informáticos.
11. el artículo 402 CP que regula la usurpación de funciones públicas por correo electrónico.
12. Los artículos 417 y 418 CP sobre infidelidad en la custodia de documentos y violación de secretos.
13. El artículo 560.1 CP, que regula los ataques a líneas o instalaciones de telecomunicaciones o correspondencia postal.
14. Y, en fin, los artículos 598 y 603 CP sobre descubrimiento y revelación de secretos relativos a la defensa nacional.

La normativa existente en el Código Penal podría caracterizarse por las siguientes notas; en primer lugar, no contiene ningún título o rúbrica específica, ni en su redacción original ni en sus reformas se ha dedicado un capítulo a los delitos informáticos que contenga alguna norma común que facilite su tratamiento y sanción (Urbano Castrillo, 2011, pág. 3); en segundo lugar, aunque no haya ningún título que formalmente junte todas las conductas delictivas de la misma índole, tampoco están al menos situadas en una misma parte del texto normativo. Por lo tanto, la otra característica de la redacción es la dispersión normativa, el único orden que podemos encontrar es que los delitos se distribuyen de acuerdo con el bien jurídico que se protege en cada caso concreto. No se considera que exista ningún vínculo entre ellos, salvo el que se ha generado académicamente al hablar de delitos informáticos.

La reforma de 2010 no supuso ningún cambio en lo que respecta a esta percepción de falta de regulación general y sistemática de los delitos informáticos, en tanto se limitó a introducir nuevos tipos y a reformar los ya existentes. Es evidente la falta de intención sistematizadora del legislador pues no hay nada más, sobre política criminal, salvo lo que podamos deducir del documento articulado a través de lo que nos han dejado: más delitos y más penas (Urbano Castrillo, 2011, pág. 4).

Las razones de esta dispersión pueden encontrarse en la explicación que da Patricia Faraldo-Cabana (Faraldo-Cabana, 2015) al tratar de exponer las estrategias legislativas de las reformas de los delitos informáticos. Según esta autora, en el derecho español pueden advertirse tres caminos para enfrentarse a tales delitos: en primer lugar, mediante la construcción de figuras paralelas a los tipos clásicos, recogiendo conductas equivalentes a las tradicionalmente desarrolladas, pero mediante el uso de nuevas tecnologías o, al menos, de objetos materiales que utilizan tecnología avanzada; en segundo lugar, a través de la creación de nuevas figuras delictivas, aunque un examen más detenido de ellas conduzca a interpretar que se trata más bien de *"actos preparatorios de otros delitos clásicos, con un elevado grado de adelantamiento de la tutela de bienes jurídicos individuales"*; y, en tercer lugar, mediante la regulación de delitos de nuevo cuño que *"aparentando proteger bienes jurídicos supraindividuales, en realidad tutelan enérgicamente el patrimonio de grandes empresas multinacionales de los sectores del entretenimiento y las telecomunicaciones"* (Faraldo-Cabana, 2015, pág. 1).

Dando por buena esta clasificación sobre la regulación de los delitos informáticos, tras las modificaciones sufridas en las reformas del Código Penal que veremos a continuación, el delito de estafa informática ahora se mostraría, fundamentalmente, como una manifestación más del primero de esos caminos: una figura paralela a otro tipo clásico, el de la estafa, en la que lo esencial es el uso de nuevas tecnologías o de objetos materiales que las utilizan. Bajo esta visión, y con esta perspectiva, se irán abordado a lo largo de este trabajo los problemas suscitados para la calificación de los hechos enjuiciados, o en relación con los sujetos afectados, con el bien jurídico protegido o con las modalidades de ejecución y relación con otros delitos, aun cuando con ello se pongan de manifiesto las dificultades para aceptar este esquema o presupuesto de valoración.

CAPÍTULO IV.- EL DELITO DE ESTAFA INFORMÁTICA EN LA LEGISLACIÓN ESPAÑOLA.

4.1 LA REDACCIÓN INICIAL DEL CÓDIGO PENAL DE 1995

En su redacción inicial, fruto de la Ley Orgánica 10/1995, de 23 de noviembre, el Código Penal, el artículo 248 tenía el siguiente texto: *"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 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".* Incardinado en la regulación de la figura del delito de estafa, podemos observar como son hoy idénticas tanto la redacción dada a ese tipo genérico, como la dedicada al específico de estafa informática. Hoy se contiene ese mismo texto en el artículo 248.1 y en el apartado 248.2 letra a). Se trataba, con la introducción de este último apartado, de dar cobertura a una necesidad sentida con carácter general en la doctrina y en la jurisprudencia: la de regular de forma concreta una conducta delictiva que, superando la opinión de que "no se puede engañar a una máquina", encontrara una sanción penal directa como delito de estafa, aunque lo fuera bajo el calificativo de "informática".

En efecto, el problema al que se enfrentaba el legislador era, entre otros, una posición jurisprudencial según la cual el fraude ejecutado a través de medios informáticos no podía castigarse a través de la figura de la estafa, precisamente porque, siendo el engaño uno de los elementos definitorios de aquélla, sólo pueden ser las personas, y no las máquinas, objeto de aquél. Pueden examinarse tales argumentos en la Sentencia 4025/1991 del Tribunal Supremo, de 19 de abril, en su análisis respecto de si la conducta de un empleado de una sucursal bancaria que *"manipulando las cuentas corrientes de diversos clientes haciendo apuntes inexistentes por vía del ordenador, consiguió incorporar a su peculio las cantidades que se enumeran"*, se insertaba en el tipo de la estafa o en el de apropiación indebida. El Tribunal Supremo rechazó lo primero argumentando 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 personas, sugiriendo en el afectado un vicio de voluntad por mor de la alteración psicológica provocada. La "inducción "a un acto de disposición patrimonial sólo es realizable frente a una persona y no frente a*

una máquina, implica una dinámica comisiva con acusado sustrato ideológico. Con razón se ha destacado que a las máquinas no se las puede engañar, a los ordenadores tampoco, por lo que 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 necesarios para el delito de estafa. Sin engaño, elemento cardinal de la estafa, no puede entenderse producida esta" (EDJ 1991/4025)

4.2 LEY ORGÁNICA 15/2003, DE 25 DE NOVIEMBRE, POR LA QUE SE MODIFICA LA LEY ORGÁNICA 10/1995, DE 23 DE NOVIEMBRE, DEL CÓDIGO PENAL

Con posterioridad, el citado precepto sería objeto de una primera reforma legal a través de la Ley Orgánica 15/2003 de 25 de noviembre. Se añadiría por ella lo que entonces sería un apartado 3 que quedaría redactado como sigue: *"3. La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo".* En la Exposición de Motivos de la ley de reforma, de modo muy genérico e indirecto que nada permite interpretar sobre la definición de una estrategia concreta en la regulación de los delitos informáticos, el legislador se limitaba a anunciar que *"se incorporan las figuras delictivas relacionadas con el acceso a los servicios de radiodifusión sonora o televisiva o servicios interactivos prestados a distancia por vía electrónica, haciendo una minuciosa regulación de las conductas que atentan directa y gravemente contra la prestación de estos servicios, y castigando la manipulación de los equipos de telecomunicación, como en el caso de los teléfonos móviles."* Con ello, explica, que se intenta dar solución a los hechos delictivos que van surgiendo a medida que vamos incorporando en los diferentes sectores sociales de forma masiva las tecnologías de la información y de la comunicación.

4.3 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

Por último, la Ley Orgánica 5/2010, de 22 de junio, además de reunir en el apartado 2, letra b), lo que era antes el apartado 3, introdujo una letra c) a dicho apartado: *"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." En su preámbulo justificaba la reforma con las siguientes palabras: *"entre las estafas descritas en el artículo 248 del Código Penal, cuyo catálogo en su momento ya se había acrecentado con los fraudes informáticos, ha sido preciso incorporar la cada vez más extendida modalidad consistente en defraudar utilizando las tarjetas ajenas o los datos obrantes en ellas, realizando con ello operaciones de cualquier clase en perjuicio de su titular o de un tercero".*

A pesar de las esperanzas que pudieron albergarse, la Ley Orgánica de 5/2010, de 22 de junio no alteraría en lo esencial un estado de cosas caracterizado por la falta de regulación sistemática de los delitos informáticos; y es que no fue mucho más allá de incardinar algunas conductas punibles nuevas *"en el marco de los denominados delitos informáticos, para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información",* según podemos leer en el preámbulo de la propia ley.

De este modo, se introdujeron los tipos del *hacking*[2] y *cracking*[3]. Aparte de esto -y la reforma reseñada del artículo 248 sobre estafa informática- no hubo mucho más que una serie de modificaciones de detalle de otras modalidades delictivas que se realizan a través de internet, como los delitos sexuales (art. 189 bis), el llamado "robo tecnológico" (art. 239), y algunos delitos contra la propiedad intelectual e industrial (270.1 y 274.1 y 2).

Quedando de esta forma delimitado el delito de estafa informática actual, es conveniente precisar cuáles son los elementos que lo constituyen, y de esta forma explicar el porqué de su regulación paralela al delito de estafa así como las cuestiones relacionadas con su tratamiento desde el derecho internacional y las medidas preventivas que se han intentado adoptar al respecto.

[2] En el artículo 197.3 CP sobre el acceso sin autorización a datos o programas informáticos contenidos en un sistema informático.

[3] En el artículo 264 CP, sobre el borrado, daño o deterioro, alteración, supresión o provocación de inaccesibilidad da datos informáticos, o bien obstaculización o interrupción del funcionamiento de un sistema informático ajeno.

CAPÍTULO V.- ANÁLISIS DEL TIPO DEL ARTÍCULO 248.2 CP

El legislador español ha optado por ubicar sistemáticamente el delito de estafa informática en el artículo 248.2 del Código Penal, lo que constituye una manifestación clara de su decisión de configurarlo legalmente como una modalidad de estafa. Se regula precisamente a continuación del tipo básico de la estafa, resultando igualmente que serán de aplicación a la estafa informática las normas que se refieren a la estafa en la Sección 1ª del Capítulo VI del Código Penal.

Tras reconocer que las afinidades con el delito de estafa son mínimas y referirse a la opinión de Suárez González, para quien "*lo correcto hubiera sido crear una figura autónoma no incardinada en la estafa*" (Suárez González, 1997, pág. 710), García García-Cervigón (García García-Cervigón, 2008) explica que fue por razones político criminales por lo que se introdujo la regulación del delito de estafa informática, y que fue bien recibida porque colmó una laguna legal que hasta ese momento había existido: la de que la defraudación que se producía valiéndose de una manipulación informática no era subsumible en la estafa tradicional, pero tampoco podía tipificarse con una regulación paralela a la de los tipos del hurto o de la apropiación indebida (García García-Cervigón, 2008, pág. 292).

Dedica el artículo 248.2 su letra a) a la tipificación general del delito de estafa informática, al que se ha designado también con otros nombres, como el de estafa telemática, estafa por computación o fraude informático. A continuación, en las letras b) y c), se limita a establecer que serán tratados como manifestaciones del mismo delito determinados actos preparatorios (relacionados con "programas informáticos específicamente destinados a la comisión de estafas") y los casos concretos de utilización de "tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos". En una primera aproximación al delito que ella llama de "fraude informático", García García-Cervigón entiende que habría sido *"excesivo reconducir al mismo todo perjuicio patrimonial mediante manipulación informática"* (García García-Cervigón, 2008, pág. 293).

Bajo esta visión general, al tratar de delimitar los elementos del fraude informático, se pueden destacar, siguiendo a la expresada autora, los siguientes aspectos (García García-Cervigón, 2008, pág. 294):

En primer lugar, es importante tener en cuenta la expresión que usa el legislador para introducir este delito, y es que afirma que "también se consideran reos de estafa" esto acaba con las discusiones doctrinales que, antes de que se tipificase el delito, llegaron a cuestionar la configuración del tipo como una modalidad de estafa, y conlleva a admitir algunas de las similitudes que puede tener este delito con el tipificado en el primer apartado del mismo artículo. Con esta afirmación inicial, el Código Penal nos adelantar la aplicación de la pena general de la estafa y sus circunstancias agravantes al tipo del artículo248.2 CP

Por otro lado, aunque tenga como elemento común con la estafa genérica el ánimo de lucro, como veremos cuando analicemos el elemento subjetivo del tipo, no tiene los elementos del error y el engaño 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.

Con estas ideas previas podemos abordar a continuación los diversos aspectos relevantes del tipo legal, con el fin de analizar en el siguiente apartado la eficacia de estos tipos en relación con la realidad social. Esta comprensión teórica contribuye al estudio de la habilidad del legislador de abordar con estos tipos los supuestos reales con los que se encuentran los jueces en su día a día.

Para ello, vamos a dividir el análisis en las tres conductas tipificadas en cada uno de los apartados. Empezaremos analizando los elementos del tipo genérico descrito en el apartado a), y pasaremos a tratar por separado los tipos del apartado b) y luego el c), pues aunque todos tengan elementos en común, el elemento objetivo en concreto difiere del que encontramos en el tipo genérico.

5.1 MANIPULACIÓN INFORMÁTICA Y ARTIFICIO SEMEJANTE

Puede sernos útil, para una delimitación detallada de los elementos que definen el tipo de la estafa informática, la Sentencia del Tribunal Supremo (Penal) nº 2175/2001, rec. 603/2000, de 20 de noviembre, en la que podemos leer:

> *"Como en la estafa debe existir un ánimo de lucro; debe existir la manipulación informática o artificio semejante que es la modalidad comisiva mediante la que torticeramente se hace que la máquina actúe; y también* ***un acto de disposición***

económica en perjuicio de tercero *que se concreta en una transferencia no consentida. Subsiste la defraudación y el engaño, propio de la relación personal,* ***es sustituido como medio comisivo defraudatorio por la manipulación informática o artificio semejante*** *en el que 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 permite su programación, o por la introducción de datos falsos".*

De acuerdo con ello, integran el tipo:; la manipulación informática o artificio semejante que ocasiona el funcionamiento de la máquina; un acto de disposición económica a través de una transferencia no consentida; y el perjuicio de tercero (que junto a el sujeto activo, sujeto pasivo, y objeto material integran el tipo objetivo) y el ánimo de lucro (que, junto el dolo, integra el tipo subjetivo). No obstante, antes de ahondar en la conducta típica, primero debemos destacar otro elemento importante en el análisis del tipo: el bien jurídico protegido.

5.1.1 Bien jurídico protegido

Como elemento necesario y útil para poder interpretar el alcance de la norma que lo regula, debemos preguntarnos en primer lugar cuál es el bien jurídico protegido en el delito de estafa informática.

Como puede desprenderse de su ubicación concreta en el Código Penal, en el título XIII regulador de los delitos contra el patrimonio y contra el orden socioeconómico y, más concretamente, en el capítulo VI, que regula las defraudaciones, y como resulta directamente de su tipificación junto al delito de estafa, el bien jurídico protegido a través de la tipificación de la estafa informática es el patrimonio. Se confiere así un carácter esencialmente individualista al objeto de protección, lo que supone dejar al margen de la aplicación del precepto otros tipos que protegen intereses de carácter colectivo o supraindividual, como delitos contra la Hacienda Pública o los que inciden en el mercado bursátil.

5.1.2 Sujeto activo

Cualquier persona puede cometer una estafa informática, tanto las personas que están legitimadas para acceder al sistema como aquellos terceros que no están autorizados. En cualquier caso deben utilizar una manipulación informática o artificio semejante para su comisión (García García-Cervigón, 2008, pág. 294).

Velasco Núñez y Sanchís Crespo analizan el delito de estafa informática de forma paralela al delito clásico de estafa (Velasco Nuñez & Sanchís Crespo, Delincuencia Informática, 2019). Abordan el tema del sujeto activo realizando una descripción del perfil criminal con el que se identifica a los delincuentes en estos casos, y concluyen que se trata de personas que ante su propia cobardía deciden realizar los engaños sin contacto físico a través de las nuevas tecnologías. En dicho trabajo se recoge el testimonio de un sujeto detenido por un delito de estafa informática en el que ante la pregunta de porqué había optado por usar la Red para cometer el delito, dijo que *en Internet es donde se encuentra el dinero*, que es lo que prioritariamente buscan los *hackers* (Velasco Nuñez & Sanchís Crespo, 2019, pág. 26).

El sujeto activo en los delitos de esta categoría no se diferencia en gran medida de los delitos de estafa clásicos. Por ende, es aplicable a ambos tipos delictivos la excusa absolutorio del artículo 268 CP que trata los delitos patrimoniales cometidos entre parientes cercanos (exime de responsabilidad criminal y los sujeta únicamente a responsabilidad civil) (Liñán Lafuente, 2018, pág. 195).

5.1.3 Sujeto pasivo

El sujeto pasivo en los delitos de estafa informática es el titular del patrimonio que se ha atacado. En los delitos de estafa tradicionales normalmente se identifica a la víctima como a la persona engañada. Aunque, en los delitos de estafa, según como se cometa el delito, como por ejemplo en las estafas en triángulo, se distingue entre el sujeto sobre el que recae la acción (el engañado), y el titular del bien jurídico protegido (el titular del patrimonio perjudicado). Sin embargo, la mecánica de la estafa informática no usa el engaño como medio para realizar el desplazamiento patrimonial, sino que lo hace a través de las "manipulaciones informáticas o artificios semejantes".

En ocasiones, la comisión de este delito perjudica desde el punto de vista de la responsabilidad civil a entidades bancarias. Podemos considerar víctimas tanto a los propietarios de los activos económicos defraudados y titulares de la cuenta bancaria

atacada, como a la entidad bancaria que opera a través de Internet (Velasco Nuñez, 2010, pág. 3). Las entidades crediticias se ven afectadas porque con la generalización de la delincuencia informática se han ido vinculando a los problemas de seguridad a los que se exponen los servicios bancarios en la Red. Por lo tanto, hasta la fecha, el banco o sus aseguradoras han establecido un sistema de detección de estos ataques delictivos y han solido proceder reintegrando o adelantando al cliente perjudicado el importe de la cantidad defraudada (asumiendo inicialmente, de esta forma, las consecuencias económicas del importe). Esta cuestión relativa a la responsabilidad civil la anlizaremos más adelante, al tratar las fórmulas específicas del *phishing*.

5.1.4 Objeto material

En lo relativo al objeto material del delito del artículo 248.1.a) CP es perfectamente aplicable lo que se establezca con respecto al delito de estafa. El bien jurídico que protege este tipo delictivo es el patrimonio, por ende, los objetos que integran el patrimonio ajeno y son objeto de transmisión ilícita a través de estos mecanismos constituyen el objeto material en cuestión. Se trata de dinero, bienes muebles e inmuebles, y derechos, que pueden ser los elementos integrantes del patrimonio que se ataca.

5.1.5 Elemento objetivo

Una vez examinados estos elementos constitutivos del delito de estafa informática genérico, podemos centrarnos en la conducta típica que se describe en el artículo 248.1 a). Como ya se ha expuesto antes, la jurisprudencia del Tribunal Supremo ha dividido el tipo delictivo en tres elementos objetivos (y uno subjetivo) que lo integran: la manipulación informática o artificio semejante, un acto de disposición económica a través de una transferencia no consentida, y el perjuicio de tercero.

En primer lugar, es preciso realizar una delimitación de los conceptos ***manipulación informática*** **y** ***artificio semejante*****.** Debemos tener en cuenta que son estas manipulaciones informáticas o artificios semejantes los que se usan como mecánica para ocasionar el desplazamiento patrimonial no consentido (en lugar de mediante engaños a personas como ocurre en la estafa tradicional). Aquí encontramos la diferencia principal entre el tipo tradicional de estafa y la estafa informática; esta última no responde a la estructura de la estafa clásica en la que hay un engaño, un error y un acto de disposición patrimonial, pues aquí, se requiere que en la conducta típica haya

una “manipulación informática o artificio semejante”. La concurrencia del engaño como elemento básico ya no es imprescindible, pues lo sustituye este otro elemento nuevo[4] (Velasco Nuñez & Sanchís Crespo, 2019, pág. 33).

La elección del término “manipular” demuestra la voluntad del legislador de incluir diversas conductas dentro de este tipo. Se trata de un concepto quizás demasiado amplio, pues por *manipulación informática* podríamos entender cualquier intervención en un sistema informático, sin hacer alusión a qué tipos de manipulaciones se refiere ni con qué fin se llevan a cabo. Para precisar el alcance del término, García García-Cervigón, en su análisis del tipo delictivo hace alusión al estudio doctrinal llevado a cabo por la Sentencia de la Audiencia Provincial de Barcelona núm. 792/2003, de 6 de octubre. En ella, en primer lugar, se rechaza la jurisprudencia inicial en la que se interpretaba de manera extensiva el precepto, considerando que se violaba el principio de tipicidad, y, en segundo lugar, se define doctrinalmente dicha manipulación como “*las acciones que supongan 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*." (Sentencia de la Audiencia Provincial de Barcelona núm. 792/2003, de 6 de octubre).

A raíz de esta definición, se ha planteado otra cuestión en relación con el tipo de intervención a la que se refiere la manipulación informática; si es necesario que haya un contacto directo con el dispositivo ajeno, si vale con entrar en el software de forma indirecta, o si se requiere intervenir en el programa y además alterarlo de forma permanente. Parece ser que la doctrina ha llegado a la conclusión que se admiten ambas conductas que intervienen en el Software: dentro del sistema y fuera del sistema. En decir, se considera reo de estafa informática a aquel que introduce datos falsos, suprime los ya introducidos o interviene para sacar datos del sistema, pero sin llegar a alterar el programa en sí para ello, pero también a aquel que no cambia el contenido directamente pero desfigura el programa para conseguir algún beneficio (García García-Cervigón, 2008, pág. 295).

[4] La Sentencia del Tribunal Supremo núm. 533/2007, del 12 de junio, siguiendo el patrón de jurisprudencia anterior, recuerda que no se precisa la concurrencia de engaño por el estafador en la estafa informática, pues *la asechanza a patrimonios ajenos realizados mediante manipulaciones informáticas actúa con automatismo en perjuicio de tercero, precisamente porque existe la manipulación informática y por ello no se exige el engaño personal*

Por lo que se refiere a la expresión "artificio semejante", también es una fórmula indeterminada, con todos los problemas que ello genera. El Tribunal Supremo, tras concretar en la forma más arriba expuesta el alcance que debía darse a la expresión "manipulación informática", parecía dar a las palabras "artificio semejante" un carácter de fórmula de cierre con la que pudieran quedar cubiertas todas las posibilidades de estafa informática que no entraran en la de manipulación informática. Por ejemplo, estarían cubiertas por este concepto las situaciones en las que se manipulan máquinas automáticas para obtener la mercancía o el servicio que ofrecen pero sin que la intervención sea informática, es decir, no hay manipulación informática, sino que hay algún artificio que se manipula de forma parecida.

La Sentencia de la Audiencia Provincial de Barcelona ya citada hace referencia al Código Penal alemán, en concreto al precepto en el que se tipifican conductas parecidas a las que intenta explicar, para alertar sobre la naturaleza del concepto "artificio semejante" que el legislador ha adaptado de la norma alemana. Explica cómo dicha noción *nunca puede deslindarse hermenéuticamente de la manipulación informática típica, y en ella no pueden hallar cobijo otros artificios que no sean de naturaleza tecnológica y solo mero ardid o astucia humana* (Sentencia de la Audiencia Provincial de Barcelona núm. 792/2003, de 6 de octubre).

En definitiva, la elección del legislador de los conceptos se hizo con el fin de incluir un término genérico (*"manipulación informática*") que abarcara varios supuestos en los que el ataque al patrimonio se lleve a cabo a través de la intervención en medios informáticos, pero con una alternativa (*"o artificio semejante"*) en la que se pudieran incluir aquellas otras formas de entrometerse en sistemas informáticos sin que la conducta sea informática como tal.

El precepto añade un segundo elemento objetivo; la manipulación informática ha de ser idónea para que se consiga ***una transferencia no consentida de cualquier activo patrimonial*.** Se trata de un acto de disposición económica, como indica la jurisprudencia del Tribunal Supremo, que provoca el enriquecimiento que persigue el autor a través de una transferencia no consentida. Se trata del resultado típico que, en primer lugar, se describe de esta manera en el Código Penal porque un mero "acto de disposición", exigido en el tipo del artículo 248.1 CP, tan solo entraña intervención humana, pero cuando hablamos de "transferencia" el legislador ha querido incluir

también aquellos actos de disposición que tienen lugar sin intervención humana, a través de la máquina exclusivamente (García García-Cervigón, 2008, pág. 296).

En segundo lugar, el concepto de activo patrimonial debe interpretarse en sentido amplio, y permite englobar tanto la transferencia que se hace efectiva sobre bienes muebles como sobre bienes inmuebles. Y por lo que respecta a la cuantía, el artículo 248.2 tiene que interpretarse en relación con el artículo 248.1, pues ya hemos afirmado que se trata de una modalidad de estafa. Para los reos de estafa el artículo 249 CP prevé un castigo de pena de prisión de seis meses a tres años, sin embargo, al igual para todas las formas de estafa que se incluyen en el artículo 248 CP, parece que será indudablemente exigible una cuantía mínima de 400 euros, y en caso contrario el castigo será una pena de multa de uno a tres meses.

Por lo tanto, esta transferencia está compuesta por, primero, la ausencia de consentimiento por parte del sujeto que tiene la facultad para realizarla, segundo, su objeto es el activo que sea susceptible de ser transferido, y por último, que ocasione un perjuicio a un tercero (Velasco Nuñez & Sanchís Crespo, 2019, pág. 39).

El tercer y último componente que señala la jurisprudencia del Tribunal Supremo en relación con el elemento objetivo del artículo 248.2 (a) CP es ***el perjuicio de tercero***. El efecto de la transferencia no consentida ha de causar un efecto patrimonial concreto: el de la pérdida de activos económicos por parte del propietario de éstos. En la estafa clásica la actuación engañosa provoca un error en un sujeto que le lleva a realizar un acto de disposición patrimonial en perjuicio propio o ajeno, pero en la estafa informática se prescinde del engaño y del error, y por lo tanto no es posible que el perjuicio pueda ser propio, siempre va a ser de un tercero. La víctima sufre un ataque a su patrimonio a través de una manipulación informática que hace innecesario este engaño.

Algunos autores como Suárez González (Suárez González, 1997) y Liñán Lafuente (Liñán Lafuente, 2018) discuten que las diferencias que presenta la estafa informática con la estafa clásica, aproximan más está figura nueva al delito de hurto. Ambos argumentan que, aunque no haya una obtención material como tal, se produce una sustracción en todo caso en perjuicio de tercero y en beneficio propio. No obstante, el legislador ha rechazado esta tesis y, como ya se ha expuesto, ha sido por razones

político-criminales por lo que se ha decidido incluir este tipo delictivo junto con la estafa del 248 CP.

5.1.6 Elemento subjetivo

Al ánimo de lucro como elemento subjetivo del injusto se refiere expresamente el artículo 248 del Código Penal. Se trata de un elemento que tienen en común la estafa genérica y la informática, al que el legislador hace referencia de manera explícita tanto en el apartado 1, como en el 2 letra a). El Tribunal Supremo en su Sentencia núm. 755/2016, recurso 228/2016, de 13 de octubre, define este elemento, *"como propósito por parte del infractor de obtención de una ventaja patrimonial correlativa, aunque no necesariamente equivalente, al perjuicio típico ocasionado, eliminándose, pues, la incriminación a título de imprudencia"* (Sentencia del Tribunal Supremo núm.755/2016, rec. 228/2016, de 13 de octubre).

De esta aclaración sacamos una conclusión importante en el análisis del tipo subjetivo, y es que en lo relativo a la estafa, tanto en su modalidad clásica como en la informática, solo se castiga su comisión dolosa. Se exige el ánimo del autor de perseguir un beneficio patrimonial para sí, a través del uso de la manipulación informática o artificio semejante, sin que quepa la posibilidad de llegar al resultado mediante una conducta imprudente. El elemento volitivo del dolo supone que la prueba de la "intención de estafar" sea demostrar que había una voluntad de alterar el funcionamiento del software e intervenir sobre la información o el programa.

Asimismo, se ha generalizado el criterio jurisprudencial usado por la Audiencia Provincial de Navarra, por el que no es suficiente el mero *conocimiento de la ilicitud genérica del hecho del autor* para apreciar el dolo en supuestos del art. 248.2 (a) CP. Es necesario que haya una prueba de que dicho dolo, incluso eventual, abarca los elementos objetivos del tipo de estafa que ya hemos desarrollado (Sentencia de la Audiencia Provincial de Navarra núm. 140/2013, de 26 de junio).

5.2 LA TIPIFICACIÓN DE LOS ACTOS PREPARATORIOS

Delimitada la estafa informática de forma general en el artículo 248.2 letra a) del Código Penal, y una vez relacionados los elementos definitorios del tipo general, el

legislador regularía a continuación, atribuyéndole idéntico tratamiento en la letra b) a los actos consistentes en la fabricación, introducción, posesión o facilitación de programas de ordenador "específicamente destinados a la comisión de estafas prevista en el mismo artículo". Se trata de un intento de aumentar la protección y prevención de estos ataques al patrimonio, pues lo que se castiga en este tipo son, por un lado, los actos preparatorios del futuro o posible autor, o de un tercero partícipe, y, por otro lado, los actos de participación a título de cooperador necesario o cómplice (García García-Cervigón, 2008, pág. 298).

Este precepto pretende anticipar la intervención penal antes de que se consiga el resultado típico que conocemos del delito de estafa informática. De este modo, como explica Fernández Teruelo hablando de estos precursores (Fernández Teruelo, 2007), se castigan conductas diferentes a las que hace referencia el primer apartado del art. 248.2 CP, pues son conductas que se ejecutan sobre los elementos necesarios para cometer una estafa informática genérica, por ejemplo, sobre el software mediante el cual se consigue el beneficio patrimonial (Fernández Teruelo, 2007, pág. 242). En lo relativo al bien jurídico protegido de este tipo, los sujetos activo y pasivos, nos remitimos a lo ya explicado con respecto a la estafa informática del primer apartado del artículo 248.2 CP.

El elemento objetivo, sin embargo, es diferente a esa manipulación informática o artificio semejante que se exige en el primer apartado. Las conductas que se castigan incluyen desde la fabricación de los programas que se pueden usar para llevar a cabo la estafa informática genérica, hasta la facilitación de estos medios o la simple posesión de los mismos. No obstante, debemos separar estos actos de los incluidos en el artículo 269 CP, que castigan en concreto la proposición, provocación y conspiración para cometer la estafa. Dentro de la conducta típica tampoco parece indicar el legislador que sea necesario conseguir una transferencia no consentida de un activo patrimonial, ni que se produzca un perjuicio a un tercero. La razón de esto podría ser que se trata de un tipo delictivo dirigido a evitar que se lleguen a completar estas pérdidas patrimoniales y que el estafador consiga enriquecerse injustamente.

Lo que sorprende de este tipo delictivo es que los actos preparatorios que contiene se castigan con la misma pena que la comisión de la estafa informática del primer apartado, y se puede llegar a discutir si esto puede suponer una violación del principio de proporcionalidad de las penas. Pesa al incumplimiento de este principio, los

programas o software que se fabrican, poseen o facilitan resultan imprescindibles para que se cometa el delito del primer apartado, por ende se ha decidido castigar del mismo modo estas conductas que preceden los fraudes, para darle la misma importancia a la comisión que a la prevención de la estafa informática.

En relación con el elemento subjetivo, el delito debe cometerse con el ánimo de lucro que se exige en el tipo genérico, pero también, para que la conducta sea punible, el autor del delito debe actuar con el ánimo de cometer la estafa informática. En línea con la tesis defendida por Fernández Teruelo, podemos decir que el precepto exige esta intención del autor directamente al decir que los actos estén "específicamente destinados" a la comisión de las estafas. Sin embargo, la expresión "específicamente destinados" puede estar referida tanto a la intencionalidad del autor, como a la naturaleza de los programas que se fabrican, introducen, facilitan o poseen, en cuanto a que estén destinados a la comisión de estafas, pues debemos recordar que algunos de estos programas con potencialidad fraudulenta también pueden tener un uso lícito (Fernández Teruelo, 2007, pág. 243).

Miró Llinares analiza las dos interpretaciones que se pueden realizar sobre la expresión "específicamente destinados" (Miró Llinares, 2013), señalando la importancia del sentido que toma el precepto dependiendo de la visión que defendamos. Por un lado, el enunciado puede hacer referencia a la exclusiva intención del autor de que el programa que fabrica, posee o facilita se use para cometer un delito de estafa. Esta sería la interpretación restrictiva amplia, que defiende que la importancia de la expresión radica en la intencionalidad del sujeto. Aunque el programa tenga otras finalidades, si el autor tiene la intención a la que se refiere, el tipo se convierte en aplicable al supuesto.

La otra interpretación que se puede llevar a cabo es la que el autor denomina la interpretación *ultra-restrictiva*. A través de esta interpretación se le otorga una importancia fundamental a la predisposición inequívoca del programa a la lesión del bien jurídico, es decir, que el programa no disponga de otras funciones distintas a las que permitan que se lesione el patrimonio. Si contara el *software* con otras utilidades, según esta posición, no sería aplicable el tipo penal. Miró Llinares apoya esta interpretación por dos razones; en primer lugar, se corresponde más con una interpretación teleológica que respeta principios como el de proporcionalidad, pues al restringir el ámbito del tipo, también reduce los comportamientos que, sin suponer una

lesión para el patrimonio, son castigados con penas iguales a aquellos que directamente dañan el bien jurídico protegido; en segundo lugar, si lo interpretamos de esta forma, aunque sea muy restrictiva, el precepto seguiría cumpliendo la función preventiva que pretende conseguir. Aunque parezca que con esta interpretación se puede dejar el precepto sin contenido, en la práctica hay programas que están dirigidos a la sola consecución de dañar el patrimonio ajeno. Especialmente en los casos de *phishing*, como veremos, en los que se usa un tipo de programa cuya única finalidad posible es la de llevar a cabo la estafa informática. En estos casos este tipo penal serviría para sancionar la fabricación, introducción, posesión o facilitación de dichos programas de ordenador, evitando sancionar otros programa que, aunque también pueden utilizarse con la misma finalidad, su uso por sí mismo no puede entenderse como una puesta en peligro del bien jurídico protegido (Miró Llinares, 2013, pág. 25). Con esta interpretación, por ende, se protegen los principios de proporcionalidad y ofensividad.

Dicho esto, la doctrina en general ha seguido criticando la creación de este precepto, y se ha discutido que aunque la intención es válida, su tipificación es problemática porque, por un lado, la excesiva anticipación de la tutela penal podría conseguir que se castiguen comportamientos lícitos, y, por otro lado, es desproporcionado considerar reo de estafa a un sujeto que no llega a consumar el delito de la misma forma que a la persona que realmente lo consigue.

No obstante, la cuestión de la conducta sancionable no es la única que ha suscitado el precepto. Como hemos explicado, las conductas tipificadas son en esencia actos preparatorios que el legislador ha decidido castigar en la misma forma que el delito consumado. Cualquier modalidad de estafa, según el artículo 249 CP se castiga con pena de prisión de seis meses a tres años siempre que la cuantía defraudada sea mayor de 400 euros, en caso contrario, la pena a imponer sería de multa. Sin embargo, en los supuestos del apartado b) del art. 248.2 CP, al no haber una lesión patrimonial no podemos determinar la pena que corresponde pues no hay una cuantía defraudada. No podemos especificar si dentro del delito de estafa le corresponde una pena de prisión o una pena de multa, y esto constituye un problema grave para la aplicación del precepto. Parece que la doctrina también ha rechazado realizar una interpretación analógica, entendiendo "cuantía de lo defraudado" como "cuantía de lo que se pretendía defraudar" (Mata Barranco, Dopico Gómez-Aller, Lascuraín Sánchez, & Nieto Martín, 2018, pág. 232).

Desde la introducción de este precepto, la jurisprudencia no parece haber llegado a un consenso sobre las penas aplicables en estos casos. De hecho, no se ha llegado a aplicar este apartado en los tribunales de manera generalizada, por lo tanto no se ofrecen alternativas y posibilidades en las sentencias. La única solución que podríamos proponer es que, de acuerdo con la tesis que defiende Miró Llinares, los programas informáticos de uso destinado a la comisión de estafas informáticas normalmente van a tener un potencial riesgo mayor de 400 euros. Son programas que en el momento de utilizarlos en la mayoría de los casos va a ser con la intención de obtener un beneficio patrimonial superior al que menciona el artículo 249 CP. Por lo tanto, parece ser que a la fabricación, introducción, posesión y facilitación de programas informáticos a la que hace referencia el precepto va a aplicarse la pena de la estafa genérica, se seis meses a tres años de prisión, porque nunca va a constituir un delito leve si el riesgo que genera puede ser mayor. Del mismo modo, no parece que vayamos a poder agravar la pena cuando se trate de la comisión de este delito, pues, como veremos a continuación, la mayoría de las circunstancias agravantes hacen referencia al resultado que se va a obtener con la estafa, lo cual no es posible determinar cuando hablamos de actos preparatorios.

En definitiva, este segundo apartado del artículo 248.2 CP no parece constituir un delito leve, porque los autores de este delito tienen la misma calificación de reo de estafa que los que realizan cualquier otro tipo de estafa. Además, estos programas informáticos a los que se refieren tiene potencial de causar el mayor de los riesgos, así que no tendría sentido sancionar ese riesgo como un delito leve.

5.3 LA REGULACIÓN ESPECÍFICA DE LA UTILIZACIÓN DE TARJETAS

En el último apartado del artículo 248.2 CP se tipifica otra conducta diferente a las dos anteriores. En el precepto se distinguen tres componentes claros; el uso de tarjetas (de crédito o débito), cheques de viaje, o datos que se incluyan en cualquiera de estos; operaciones de cualquier clase (que se realizan a través de estas tarjetas o cheques), y el perjuicio al titular de la tarjeta o cheque o a un tercero. Este precepto es el más reciente de los tres apartados y el legislador ha querido dar una solución a la creciente práctica ilícita, en concreto, de robo de datos de tarjetas (como resultado de la

generalización del uso de tarjetas de crédito en sustitución del dinero en efectivo). Los datos que se consiguen se usan para realizar las operaciones en las que se reproducen y comparten sin consentimiento y con el fin de perjudicar al verdadero titular.

Antes de la introducción en el Código Penal de la letra c) del artículo 248.2, hubo de afrontarse la penalización de las conductas relacionadas con el uso fraudulento de tarjetas sin tener una norma concreta que se refiriese a ello, debiendo ser la jurisprudencia la que llenara ese vacío mediante la interpretación de la estafa informática prevista en el artículo 248.2 CP. Este comportamiento, hasta la reforma que introdujo el tipo, se castigada como robo con fuerza en las cosas, cuando se la tarjeta se usaba para sacar dinero en un cajero, o como estafa cuando había suplantación de la identidad mediante el uso de la tarjeta (Liñán Lafuente, 2018, pág. 199)

Los problemas planteados se verían solucionados en su gran parte al introducirse la norma concreta. A pesar de referirse a la "estafa", no parece que debamos salirnos, en la exégesis y aplicación de este precepto, de la categoría de la estafa "informática". Y si con anterioridad hemos relacionado cuáles son los elementos definitorios de este delito, debemos trasladar aquí esos mismos elementos para integrar la conducta delictiva de uso fraudulento de tarjetas.

No parece ser correcto subsumir esta conducta en la figura de la estafa clásica, pues en estos supuestos de utilización de tarjetas falta el requisito del engaño bastante. Tampoco podemos tratar estos casos como estafas informáticas del apartado a). El artículo 248.2 c) va directamente destinado a regular una de sus manifestaciones del requisito de "manipulación informática o artificio semejante": la de la utilización de las tarjetas o cheques o el uso de los datos obrantes en ellos. Sin embargo, con la creación de un tipo delictivo separado, quedan expresamente solucionados muchos de los problemas que venía ocasionando la subsunción de estas conductas en el concepto de manipulación informática o de artificio semejante. Autores como Armentero León argumenta la complejidad de los supuestos que abarca el concepto de "manipulación informática o artificio semejante", en contraste con los supuestos de utilización de tarjetas que cualquiera podría cometer (Armenteros León, 2008, pág. 20).

Por lo que se refiere a la transferencia no consentida de activos patrimoniales, a pesar de que la norma aluda a la realización de *"operaciones de cualquier clase",* no debería perderse de vista el efecto patrimonial como resultado efectivo de la utilización

de la tarjeta o cheque, pues el abanico de operaciones susceptibles de ser ejecutadas a través de la tarjeta comprende en muchas ocasiones actuaciones carentes de trascendencia patrimonial directa.

Y por lo que se refiere al perjuicio de tercero, la norma alude al perjuicio del titular de la tarjeta o cheque, pero también al de un tercero. Destaca Armenteros León que en la redacción original de Anteproyecto de reforma del artículo 248.2 se preveía simplemente que el perjuicio lo fuese del titular de la tarjeta y que tanto el CGPJ como el Consejo Fiscal habían puesto de manifiesto la inconveniencia de que el perjuicio fuera sólo para el titular, sin preverse que el mismo pudiera afectar a terceras personas. Pero ya desde el Proyecto de Ley se mantuvo el texto con la redacción actual (Armenteros León, 2008, pág. 20).

En cuanto al elemento subjetivo de este tipo, ninguna particularidad ha de destacarse en relación con la exigencia de ánimo de lucro. Sigue siendo un requisito exigible el dolo, y no podrá, como ninguno de los dos tipos anteriores, castigarse la conducta imprudente.

5.4 LAS CIRCUNSTANCIAS AGRAVANTES DEL DELITO DE ESTAFA

Las penas correspondientes al delito de estafa informática (a las tres modalidades del artículo 248.2 CP) son las mismas que se prevén para el delito de estafa tradicional, con la particularidad de los supuestos del segundo apartado.

Sin embargo, la pena de prisión se agravará de uno a seis años y una multa de seis a doce meses si se dan alguna de las circunstancias enumeradas en el artículo 250 del CP. La mayoría de estas circunstancias agravantes no merecen una exposición extensa, pues se entiende su aplicación. Como, por ejemplo, cuando la estafa recae sobre cosas de primera necesidad o sobre bienes que integran el patrimonio artístico; son aplicables a los casos de fraude informático, teniendo en cuenta su objeto material, y se entiende que agravan las penas porque se trata de bienes que son objeto de especial protección por su valor, más allá del valor económico. No obstante, hay otros supuestos que merecen nuestra atención por la importancia que tienen en el ámbito de la estafa informática.

El segundo apartado del artículo 250.1 CP agrava las penas en los casos en los que la estafa se lleve a cabo mediante el abuso de firma de otro. En relación con las estafas cometidas a través de medios electrónicos, podríamos pensar que dentro de este supuesto se incluyen todos esos casos en los que el perjuicio patrimonial ajeno se logra usando las claves de la víctima para acceder por banca electrónica a las cuentas en la que los activos estaban depositados. Es decir, abusar de la firma electrónica del banco de alguien para causar el perjuicio. Sin embargo, algunos tribunales en estos casos han rechazado la aplicación de esta circunstancia agravante. Por ejemplo, la Sentencia número 47/2009 de la Audiencia Provincial de Pontevedra de 15 de julio interpreta el concepto de "abuso de firma" de manera restrictiva, impidiendo que se integren en él los actos en los que se emplean claves con las que cada entidad bancaria identifica a sus clientes. La Sentencia citada explica que *el uso por el Código únicamente del término "firma" obliga a referirlo al nombre y apellido que una persona escribe de su puño y letra en un documento para darle autenticidad o expresar que se aprueba su contenido* (Sentencia núm. 47/2009, rec. 15/2009, de la Audiencia Provincial de Pontevedra de 15 de julio).

La cuarta circunstancia agravante abarca los supuestos de especial gravedad, que se determinan atendiendo a la entidad del perjuicio y a la situación económica en que deje a la víctima o a su familia. El motivo por el que se incrementa la pena en estos casos es la situación en la que se queda la víctima estafada. Por lo tanto, no nos fijamos en el importe de la defraudación como tal, sino las circunstancias económicas del perjudicado como resultado de la estafa. Este supuesto es similar al quinto apartado del mismo artículo, que considera circunstancia agravante que el valor de la defraudación supere los 50.000 euros o afecte a un elevado número de personas. Este supuesto es muy común entre los delitos de fraude informático, por la facilidad con la que se puede alcanzar a un mayor número de personas a través de Internet.

La jurisprudencia ha detectado un problema asociado con estas dos últimas circunstancias agravantes y su relación con el delito continuado y el delito de masa del artículo 74 CP. Este artículo sanciona con la pena superior en uno o dos grados aquellos supuestos en los que se realizan una pluralidad de acciones que ofenden a uno o varios sujetos e infringen el mismo precepto penal. Si se da el caso de la comisión de varios fraudes que alcanzan la cifra de 50.000 euros, no sería posible aplicar a la vez el tipo agravado y la regla del art. 74.2 CP. Para poder aplicar ambos preceptos parece que

sería necesaria una continuidad delictiva en la que todas o por lo menos un número elevado de estafas superasen por sí solas esa cifra de 50.000 euros (Mata Barranco, Dopico Gómez-Aller, Lascuraín Sánchez, & Nieto Martín, 2018, pág. 215).

El Acuerdo del Pleno no jurisdiccional del Tribunal Supremo del 30 de octubre de 2007 al tratar este asunto establece lo siguiente:

> *Cuando esa cifra (la relevante para incrementar la pena básica) se alcanza por la suma de las diferentes infracciones, acudir a la agravación del apartado 1 del artículo 74 vulneraría la prohibición de doble valoración de una misma circunstancia o de un mismo elemento, pues de un lado se ha tenido en cuenta para acudir al artículo 250.1.6ª CP (actual artículo 250.1.5º CP), con la consiguiente elevación de la pena […] y de otro se valoraría para acudir al artículo 74.1 CP, agravándola nuevamente.*

El sexto apartado enuncia una circunstancia agravante muy relevante y frecuente en casos de estafa informática. Se trata de los supuestos en los que hay un abuso de relaciones personales con la víctima o aprovechamiento de credibilidad empresarial o profesional.

Parece ser que la jurisprudencia ha matizado lo que se debe entender por esas "relaciones personales" y es que dentro de esta categoría no se admite la inclusión de meras relaciones laborales como puede haber en supuestos en los que la estafa informática se lleva a cabo abusando de los datos que se te conceden como consecuencia de la relación entre empleado y empleador. Debe probarse que hay una relación de confianza más allá de la relación laboral, además de probar que la estafa se cometen mediando un abuso de esta confianza. Es decir, para la aplicación de esta agravación es necesario que, además del artificio engañoso, el autor aproveche las relaciones personales previamente existentes para hacerlo más eficaz debilitando los mecanismos de autoprotección de la víctima (Sentencia de la Audiencia Provincial de Madrid núm 106/2011, rec. 13/2011, de 12 de diciembre).

En cuanto al concepto de "credibilidad empresarial o profesional" se debe analizar el sujeto activo, no su relación con la víctima, para ver si su consideración en el mundo de las relaciones profesionales o empresariales haría inexplicable la prevención de la comisión del delito por la victima potencial.

Faltarían, por lo tanto, las dos últimas agravantes que incluye el art. 250.1 CP, además de la modalidad hiperagravada del artículo 250.2 CP. Las dos circunstancias agravantes que cierran el primer apartado son la estafa procesal y la multirreincidencia. La estafa procesal no parece aplicable a las estafas informáticas, pues, además de no haber jurisprudencia que trate este tipo agravado en este tipo de fraudes, desde un punto de vista teórico, parecen incompatibles. Las estafas procesales se dan cuando la víctima del engaño es el juez, pero el perjudicado sujeto pasivo es otra persona. Si recordamos lo expuesto en el análisis del tipo, entre los elementos típicos de los delitos de estafa informática no hay engaño, por lo tanto parece imposible que se pueda llevar a cabo de esta manera la estafa procesal. Los supuestos de multirreincidencias no suscitan muchas cuestiones pues concurren cuando el autor del delito al delinquir ha sido condenado al menos por tres delitos cometidos en el Capítulo VI de las defraudaciones.

5.5 SITUACIONES DE CONCURSO

El delito de estafa informática a través de manipulación informática puede entrar en concurso con el delito de daños del art. 264 bis CP. Este artículo sobre daños informáticos sanciona aquellos sujetos que obstaculizan o interrumpen el funcionamiento de un sistema informático ajeno. Ambos tipos penales entrarían en concurso en los casos en los que se borraran los datos contenidos en el programa informático para beneficiarse patrimonialmente. Sería un concurso ideal de delitos en el que un solo hecho ha constituido dos delitos.

El supuesto más común de concursos con el delito de estafa informática a través de manipulación informática es el concurso con el delito de falsedad documental del artículo 390 CP. Los casos que se suelan dar normalmente son de concurso medial, pues lo que suele pasar es que la falsificación de los documentos se realiza para hacer posible la comisión de la estafa. Este concurso medial se tendría que resolver de acuerdo con el artículo 77.3 CP.

Por otro lado, podemos encontrarnos con supuestos en los que el delito de estafa informática entra en concurso con el delito de apropiación indebida. Como ya vimos, antes de tipificarse como tal, hubo discusiones doctrinales acerca de la inclusión de la estafa informática dentro de la apropiación indebida, pues son conductas parecidas. Al final se rechazó esta clasificación y podemos diferenciar los dos tipos en que en la apropiación indebida el sujeto recibe el bien de la víctima sin devolvérselo, mientras

que en la estafa se produce un perjuicio patrimonial que se consigue a través de las manipulaciones informáticas y demás medios. No estaríamos antes un concurso real de delitos pues en ambos se vulnera el mismo bien jurídico. Estaríamos entonces frente a un concurso de normas que se resolvería acudiendo a los criterios del artículo 8 CP. Se escogería el criterio por el que la estafa, que es el precepto más complejo, absorbe la apropiación indebida.

En los casos del tercer apartado del art. 248.2 CP (utilización de tarjetas) no es raro que nos encontremos con un concurso con el delito de falsificación de tarjetas de crédito del artículo 399 bis CP. Pero dependiendo del apartado del artículo 399 bis CP en el que sea subsumible la conducta estaremos ante un tipo de concurso u otro. Si en el supuesto concreto el autor del delito usa la tarjeta sin haber participado en su fabricación, pero a sabiendas de su falsedad y en perjuicio de otro (tercer apartado del art. 399 bis CP), habría un concurso de normas, resulto por los criterios del artículo 8 CP. Sin embargo, si el sujeto lo que hace es, de cualquier modo, falsificar una tarjeta, esta conducta entraría en concurso ideal o medial (artículo 77 CP) con la estafa informática. Tal y como se establece en la Sentencia del Tribunal Supremo núm. 330/2014, rec. 1772/2013, de 23 de abril, ambas conductas podrían sancionarse acumuladamente, pues se están vulnerando bienes jurídicos distintos, y la falsificación parece ser un medio para cometer la estafa.

Por último, debemos tener en cuenta que cuando la estafa informática se comete por un sujeto que pertenece a un grupo criminal, no hay concurso medial entre los dos delitos. Son numerosas las sentencias que han considerado el concurso real la figura correcta para sancionar todos aquellos delitos que se comentan conjuntamente con el delito de pertenencia a un grupo criminal.

CAPÍTULO VI.- FÓRMULAS ESPECÍFICAS DE LA ESTAFA INFORMÁTICA

Finalizado el análisis del tipo, vamos a dedicar este apartado al estudio de diferentes técnicas que se utilizan para cometer fraudes informáticos y cuya práctica ha aumentado estos últimos años como consecuencia de la generalización de los pagos por Internet y la facilidad de la transmisión de datos a través de la Web. Estos supuestos que se van a explicar a continuación constituyen la realidad social a la que se enfrentan los tribunales normalmente. Desde un punto de vista teórico está bien que tratemos los tipos tal y como vienen en el Código Penal, sin embargo, a los Tribunales llegan casos cada vez más diferentes que se adaptan a las novedades tecnológicas que aparecen cada día. El legislador con los tres apartados que constituyen la figura de la estafa informática pretende abordar la mayoría de los supuestos que puedan ir apareciendo, sin embargo, es en este apartado en el que vamos a plantearnos si realmente estos preceptos logran abordar la realidad social a la que nos enfrentamos, o si, por la rapidez con la que evolucionan los medios informáticos, siempre van a aparecer supuestos que en cierto modo "escapan" la ley.

Dos modalidades delictivas a las que nos vamos a referir son, lo que en la jurisprudencia y la doctrina se conocen como el "*phishing*" y el "*pharming*".

Por un lado, la naturaleza etimológica del término *phishing* explica lo que se pretende conseguir con esta práctica. *Phishing* viene de la palabra inglesa "*fishing*" que significa pescar, esto hace alusión al objetivo con el que se emplea esta técnica que es lanzar varios anzuelos y ver quien "pica". Realmente el *phishing* es eso; los estafadores, o "phishers" o "scammers", realizan un envío masivo de correos electrónicos en los que suplantan la identidad o apariencia de una entidad (normalmente incluyendo enlaces a una página Web que imita la Web de una entidad financiera o bancaria), y, como explica Velasco Núñez, usan excusas relacionadas con la seguridad informática bancaria para que los usuarios urgentemente cedan sus datos bancarios y personales de acceso a servicios de este tipo. Suelen pedir datos como la clave del usuario, la contraseña, el número de la tarjeta y el número pin, y de este modo hay usuarios que se creen que realmente hay una urgencia y, como en la pesca, "pican" el azuelo y dan los datos confidenciales. Con estos datos, los estafadores proceden a realizar operaciones en Internet, como transferencias bancarias, compras a través de Internet, o incluso retirar efectivo en cajeros (Velasco Nuñez, 2010, pág. 4).

La posición unánime de los tribunales determina que la mecánica del *phishing* constituye claramente una modalidad de estafa informática en la que la imitación de las páginas Web y la suplantación de la identidad electrónica de las entidades entran dentro de la categoría de manipulación informática exigida en el primer apartado del artículo 248.2 CP. A través de esta manipulación, y siguiendo los elementos del tipo que ya hemos analizado, tendríamos también una transferencia no consentida de activos patrimoniales que se consigue accediendo a las cuentas de los usuarios que han facilitado sus datos. Se trata de una conducta en principio subsumible dentro del tipo de fraude informático del primer apartado del artículo objeto de estudio.

El *phishing* desde un punto de vista teórico no supone ningún problema a la hora de sancionar como una estafa informática. Sin embargo, el elemento que dificulta su juicio es que los autores de esta técnica suelen pertenecer a bandas organizadas de delincuentes extranjeros (Velasco Nuñez, 2010, pág. 4). Cuando hemos comenzado hablando de los delitos informáticos, hemos destacado la dificultad que supone juzgar delitos que se cometen a través de medios que carecen de fronteras. El análisis del tipo delictivo lo hemos desarrollado en un ámbito nacional, sin meternos en problemas de competencia, no obstante, a la hora de hablar del *phishing* es esencial considerar el elemento extranjero pues por éste aparece una figura conflictiva que es el "mulero".

Los autores de los delitos de *phishing* lanzan sus ataques desde su país de origen y son rápidos en eliminar su identidad y rastro para no ser descubiertos. De acuerdo con Congel Díez, en el *phishing* se pueden distinguir tres fases; en la primera fase se descubren las claves de los usuarios a través de los correos masivos u otras técnicas; la siguiente fase ocurre una vez acceden a las cuentas disponibles y se ordenan las transferencias de activos a otras cuentas; y, por último, en la tercera fase los autores se apoderan efectivamente de dicho activos (Congil Díez, 2013, pág. 2). Para los delincuentes extranjeros la estafa se complicaba en la última fase de apoderamiento de las transferencias no consentidas, pues para poder efectuarlo debían venir a España donde era más fácil ser detenidos. Como posible solución a este problema apareció la figura del "mulero", que son terceras personas, que no forman parte de las organizaciones criminales que ejecutan la estafa, que viven en España y son capaces de lograr la efectiva disponibilidad del dinero para enviarlo al extranjero.

Los autores del *phishing* consiguen captar a sujetos que desempeñen la labor del muleros enviando, también, correos electrónicos masivos e indiscriminados, en los que se realiza una oferta laboral a aquellos que estén dispuestos a abrirse una cuenta bancaria a la que se puedan hacer las transferencias no consentidas de los activos. Estas cuentas "nido" (Velasco Nuñez, 2010, pág. 5) se utilizan para juntar el dinero y retirarlo en efectivo para reenviarlo a los *phishers* en metálico mediante transferencias internacionales, a través de medios como Money Gram, que no dejan prueba de quienes son los receptores. El trabajo de los muleros está remunerado, se manera que al reenviar el dinero en efectivo estos detraen lo que les corresponda de comisión (que suele ser entre un 5% y 10% de lo que se consigue con la estafa). Se trata, en definitiva, de intermediarios, que sin formar parte de la organización que dirige la práctica, reciben una comisión y normalmente son los que acaban estando detenidos por los hechos, puesto que los *phishers* en la mayoría de los casos no pueden ser identificados porque al final su identidad es puramente informática.

Hay dos problemas relacionados con esta modalidad de *phishing* a través de los "muleros", la primera relacionada con la competencia judicial de estos delitos, y la segunda, la calificación jurídica de la conducta llevada a cabo por los "muleros". Las cuestiones de competencia que se plantean surgen por el origen extranjero de los phishers. Pues, aunque los autores del delito se encuentren fuera de España, los intermediarios, las víctimas y las cuentas bancarias a través de las cuales se realizan las transferencias, están en España. El Tribunal Supremo, para resolver esta cuestión, se ha apoyado en la "Teoría de la Ubicuidad"[5]. En los casos de estafa clásica, que es el ámbito en el que más se cita este principio, se usa cualquiera de los territorios en los que se ejecute algún elemento del tipo, como por ejemplo el lugar en el que se desarrolla el engaño o donde ocurra el desplazamiento patrimonial. Pero en casos de *phishing*, donde no hay ningún elemento de engaño, el Tribunal Supremo ha matizado este principio, considerando que el lugar desde donde actúa y reside el "mulero", al ser el lugar en el que se reciben las transferencias y se extrae el dinero en metálico para su reenvío, es el lugar que tiene importancias en temas de competencia, así como el lugar desde donde se emite la orden de transferencia (que en muchos casos no se puede determinar).

[5] El principio de ubicuidad, plasmado en el Acuerdo no jurisdiccional del Pleno del Tribunal Supremo del 3 de febrero del 2005 determina lo siguiente: *el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo.*

En otras palabras, en aquellos casos en los que es imposible saber el lugar desde donde se dirigió la estafa informática, el criterio jurisprudencial, ya consolidado, que se usa es que la competencia la tiene el Juzgado del lugar donde se ingresa el dinero en la cuenta del "mulero" y desde donde se hace la transferencia (Auto del Tribunal Supremo del recurso 20768/2013, de 19 de febrero 2014).

Parece que se ha llegado a un consenso sobre este primer elemento problemático del *phishing*. Sin embargo, sigue latente la discusión doctrinal sobre la segunda cuestión que suscita esta práctica: la calificación jurídica del papel que desempeñan los "muleros". La conducta de los sujetos que envían los correos electrónicos y consiguen recoger los datos de los usuarios para poder ordenar las transferencias no consentidas entra sin problema dentro de la conducta típica que establece el artículo 248.2 a) CP. Sin embargo, no está tan claro que los intermediarios que crean las cuentas bancarias para realizar las transferencias de los activos puedan ser acusados de cometer un delito de estafa informática.

Congil Díez divide las tres posiciones diferentes que podemos encontrar en la jurisprudencia (Congil Díez, 2013). En primer lugar, en algunos casos se ha calificado la conducta de los "muleros" como cooperador necesario[6] del delito de estafa informática del artículo 248.2 a) CP. El Tribunal Supremo, en los casos en los que ha apoyado esta postura, primero de todo, declara innecesario el conocimiento del "mulero" de la red a la hora de enjuiciarle, pues al final sale con un beneficio económico de la situación, por lo tanto se discute que debió conocer la cadena de hechos de la que formaba parte. Lo relevante, por lo tanto, a la hora de calificar esta conducta dentro de la estafa informática es que el "mulero" se beneficia económicamente de la conducta delictiva, actúa con dolo (aunque sea un dolo eventual), y sin su participación, no habría una estafa informática como tal (Sentencia del Tribunal Supremo número 533/2007 de 12 de junio). Según Congíl Díez, esta postura ha tenido una acogida preferente por nuestra doctrina y jurisprudencia.

Sin embargo, otros autores como Velasco Núñez, apoyándose en numerosa jurisprudencia, defienden la clasificación de la conducta dentro del delito de receptación

[6] Artículo 28 CP: *"(…) También serán considerados autores:(…) b) Los que cooperan a su ejecución con un acto sin el cual no se habría efectuado."*

del artículo 298 CP[7]. Rechazan la inclusión de los hechos dentro de la estafa informática puesto que critican que se esté vulnerando el principio de proporcionalidad ya que al mulero se le aplicaría la misma pena que al autor del fraude cuando es sabido que ocupa el escalón más bajo dentro de toda la actividad delictiva. Los partidarios de esta doctrina discuten que la intervención de los muleros se da en una fase en la que ya se ha consumado el delito, y en cierto modo rechaza que sea autor o cómplice del delito. Este último argumento Congil Díez acusa de suponer un problema de tipicidad al considerar que los "muleros" entonces no contribuyen en la consumación del delito de estafa antecedente (Congil Díez, 2013, pág. 4). Por último, una parte de la doctrina apoya que se sancione a los muleros con un delito de blanqueo de capitales del artículo 301.1 CP, pero en su modalidad imprudente.

De forma paralela a esta discusión doctrinal, aparece otra relativa a la responsabilidad de la entidad bancaria en estos casos de *phishing*. Sin embargo, en lo relativo a este tema parece que se ha alcanzado un consenso mayor. En muchas ocasiones la entidad bancaria puede incurrir en responsabilidad civil por no haber tomado las suficientes medidas de seguridad en sus páginas Webs para evitar que sus clientes transmitan con tanta facilidad sus datos personales.

En la práctica judicial, nos encontramos varios supuestos en los que las empresas bancarias reintegran a su cliente la cantidad defrauda a través de este método delictivo, y por lo tanto, no hay duda que, en ese momento, dicha entidad pasa a tener la consideración de perjudicada en sede penal al efecto de ser resarcida por los autores del delito. Igualmente, también asistimos a otros supuestos en los que la entidad no adelanta las sumas defraudas y por lo tanto el beneficiario de la responsabilidad civil será el perjudicado directamente (Congil Díez, 2013).

Cuando las entidades bancarias y aseguradoras se subrogan en la posición y el perjuicio de sus clientes deben demostrar, caso por caso, que no hay defectos de seguridad en el sistema informático de la entidad. Es decir, esto lleva a creer que con los delitos de estafa informática se ataca el patrimonio de los usuarios de Internet pero también se genera un *ataque a la confianza depositada en estas empresas bancarias*

[7] Artículo 298 CP: 1. *El que, con ánimo de lucro y con conocimiento de la comisión de un delito contra el patrimonio o el orden socioeconómico, en el que no haya intervenido ni como autor ni como cómplice, ayude a los responsables a aprovecharse de los efectos del mismo, o reciba, adquiera u oculte tales efectos, será castigado con la pena de prisión de seis meses a dos años.*

(Velasco Nuñez, 2010, pág. 4). Las entidades bancarias en cierto modo pueden ser consideradas víctimas en estos casos de *phishing*. Debemos tener en cuenta que para conseguir esta estafa los *phishers* han copiado la página Web del banco, y esto supone una brecha a su sistema de seguridad y un problema de confianza de cara a sus clientes.

Otra modalidad de estafa informática, el *pharming*, nació en 2005 como consecuencia de unos fallos de seguridad que se detectaron en los servidores de Microsoft (Velasco Nuñez, 2010, pág. 3). A través del *pharming* primero se infectan ordenadores, de manera indiscriminada, con el fin de alterar la barra de direcciones del navegador del usuario. De esta forma, se manipulan las direcciones que introduce el usuario para, en vez de dirigirle, por ejemplo, a la Web de su banco, o de subastas o ventas de segunda mano, le dirige a una página falsa que imita la Web a la que quiere acceder el sujeto. En esta página Web, que crean los delincuentes informáticos para conseguir información confidencial, el usuario introduce sus datos personales. Con estos datos, igual que en el *phishing*, los atacantes pueden apoderarse de activos patrimoniales de sus víctimas sin su consentimiento. El *pharming* es, en definitiva, un tipo de *phishing* que cuenta con más avances tecnológicos. Se diferencian, sobre todo, en que en esta segunda modalidad se introduce un virus en el ordenador. Por lo tanto, una vez se descarga el programa infectado, tienes acceso a toda la información que el usuario introduce en el ordenador. Mientras que en el *phishing* solo obtienes los datos que se piden.

Por último, debemos mencionar la importancia que está adquiriendo la criptomoneda, en especial el *bitcoin* y, más recientemente, el *dogecoin*. Con el aumento de valor de estas criptomonedas se ha empezado a plantear la posibilidad de realizar pagos con ellas. El panorama económico está cambiando y esto significa que el mundo jurídico debe actualizarse para dar respuesta a la posible comisión de delitos a través de estos futuros sistemas de pago. Actualmente ya se han cometido estafas informáticas, en concreto *phishings*, en las que los activos patrimoniales transferidos se utilizan para convertirlos en *bitcoins*. Podría ser peligroso que se generalizaran los pagos con estas monedas virtuales para la investigación de los casos de *phishing*. Pues, si no hay necesidad de retirar el dinero en efectivo para transferirlo al extranjero, desaparecerían los muleros, y por lo tanto los activos patrimoniales pasarían directamente a la organización delictiva que dirige la estafa. Como ya hemos visto, la identidad de los

phishers no se descubre en casi ningún caso de *phishing*, los que acaban detenidos son los muleros.

En definitiva, queda patente que las estafas informáticas que se cometen hoy en día pueden no encajar completamente en las conductas descritas en el artículo 248.2 CP. En la introducción del presente estudio hemos explicado cómo el derecho penal debe enfrentarse a las novedades tecnológicas y a la inseguridad en su uso diario por los usuarios y de las empresas. El *phishing*, el *pharming* y las transacciones con monedas virtuales son tres ejemplos de cómo los tribunales han ido adaptando el tipo delictivo de la estafa informática a las nuevas modalidades que han ido surgiendo.

Pese a los esfuerzos jurisprudenciales, este artículo sigue siendo limitado para la cantidad de casos diarios que se resuelven. Según el Estudio sobre cibercriminalidad en España en 2019, se conocieron un total de 218.302 hechos, un 35,8% más que en 2020. De esta cifra, el 88,1 % corresponde a fraudes informáticos (Gabinete de Coordinación y Estudios; Secretaría de Estado de Seguridad, 2019). La mayoría de los delitos informáticos, que hemos clasificado en el Capítulo III del trabajo, tienen regulaciones similares a las de la estafa informática: una regulación paralela a otro tipo delictivo del que nacen. Sin embargo, hay otros delitos que tienen una regulación más personalizada pues se han incluido en el Código Penal como delitos nuevos, como por ejemplo el delito de facilitación del acceso ilícito a servicios de telecomunicación del artículo 286 CP. Teniendo estos datos en cuenta, parece que podría plantearse una reforma en la que se diese más protagonismo a los tipos delictivos que más se más se dan en la práctica, especialmente aquellos cuya incidencia aumenta con los años como la estafa informática.

CAPÍTULO VII.- MEDIDAS PREVENTIVAS, NUEVAS SOLUCIONES Y PROPUESTAS DE OTROS PAÍSES

La solución a la continua evolución de los delitos informáticos, en especial de la estafa informática, no puede ser una reforma periódica del CP. Entraríamos en un círculo vicioso en el que la ley va detrás de la realidad social, dejando siempre conductas nuevas libres de sanción. El legislador busca un cambio en la valoración social de las conductas que tipifica como delitos, sin embargo, en ilícitos como el ciberfraude la dificultad radica en la falta de transparencia del mundo virtual y lo difícil que es dejar por escrito en la Ley las conductas que en algún futuro pueden ser peligrosas para los ciudadanos. Faraldo-Cabana advierte la consecuencia que puede tener todo esto; la existencia de "ciberpánico" o "ciberfobia" (Faraldo-Cabana, 2015, pág. 30). Son claras las muchas ventajas que ofrecen los medios tecnológicos, pero hasta que no conozcamos y controlemos el mundo virtual, no podremos utilizar estos medios con seguridad.

Frente a estos obstáculos en la efectiva regulación de las estafas informáticas, han aparecido propuestas de prevención interesantes. Es verdad que, como hemos explicado en el apartado anterior, podría defenderse la introducción de una mayor intervención y regulación de la estafa informática. Si el legislador separase el delito de estafa informática del delito de estafa, se podrían crear circunstancias agravantes especiales para estas conductas y entre éstas circunstancias tipificar modalidades de ciberfruades más específicos, o incluso crear un tipo concreto para los actos preparatorios del apartado c) con una pena inferior.

Sin embargo, contraria a esta propuesta, hay otra postura, guiada por el principio de intervención mínima, que cuestiona la necesidad de ampliar los delitos que castiguen estas conductas, pues debería ser más importante la creación de mecanismos de protección. Sabiendo que no lograremos alcanzar la sanción de todos los hechos informáticos que causen un perjuicio, quizás la alternativa es que el legislador se centre en las medidas preventivas que se pueden tomar, tanto a nivel particular como a nivel nacional. Se ha intentado en cierto modo sancionar a través del apartado b) del artículo 248.2 CP los actos preparatorios dirigidos hacia la comisión de estafas informáticas, sin embargo, ya se ha explicado cómo apenas se ha aplicado dicho precepto, tanto por la dificultad de interpretación de la conducta tipificada, como por lo complejo que puede ser detectar la simple fabricación y tenencia de los programas informáticos.

Pese a la inaplicación de este precepto, hay otros mecanismos de prevención en los que se podría trabajar para reducir la incidencia sin aumentar la sanción. Por ejemplo, los casos de *pharming* que tanto han aumentado desde 2005 podrían evitarse con programas de antivirus que estén dirigidos hacia la protección frente a los correos maliciosos que infectan tu ordenador. Hoy en día muchos usuarios cuentan con estos programas, pero no todos. Quizás una instalación generalizada de estos antivirus podría evitar la difusión masiva de los correos infectados.

Para los demás casos de *phishing* y otras manipulaciones informáticas, una de las medidas preventivas que se puede proponer es la autoprotección de la víctima. En los casos de estafa tradicional, la defensa normalmente recurre al argumento de la obligación de autoprotección. Sin embargo, en estos supuestos de fraude informático, el Tribunal Supremo ha rechazado que se culpabilice a la víctima por "cooperar" involuntariamente al delito al dar sus datos personales, ya que el sujeto pasivo está protegido por la buena fe que tiene al introducir sus claves y datos en la Web (STS núm. 845/2014, del 2 de diciembre) (Rodríguez Caro, 2015).

Lo que parece indiscutible es que una mayor educación informática es necesaria para prevenir ataques informáticos. Así lo ha anunciado el Centro Criptológico Nacional y Centro Nacional de Inteligencia (CCN-CERT), dependientes del Ministerio de Defensa, en sus informes de buenas prácticas. En el resumen ejecutivo que el organismo redactó en 2019 sobre Ciberamenazas y Tendencias (CNN-CERT, 2019), el CNN-CERT destacó cómo: *Los seres humanos siguen siendo el eslabón débil en todos los sistemas de seguridad, por lo que, a medida que aumente la eficacia de las protecciones contra código dañino, los agentes de las amenazas modificarán su objetivo, atacando a las personas* (CNN-CERT, 2019, pág. 45).

Por último, para una mayor comprensión de las diferentes medidas que podrían plantearse para la regulación de las estafas informáticas, deberíamos fijarnos en la legislación por la que han optado otros países y la normativa propuesta por la Unión Europea. Al introducir los delitos informáticos, hemos visto como hay tres mecanismos distintos que se utilizan para regular estas conductas delictivas, y cuál ha sido el elegido por el legislador en el caso español. Por un lado, países como Francia, Gran Bretaña, Estados Unidos, Holanda y Chile abordan este fenómeno a través de una ley específica que lo regula. En Francia, por ejemplo, tienen la *Loi nº 88-19 du 5 janvier 1988 relative*

à la fraude informatique. A través de esta ley especial se regularon específicamente las penas previstas para conductas concretas que pueden considerarse fraudes informáticos, y después se pudo modificar el Código Penal de acuerdo con lo establecido en esta Ley especial. En Gran Bretaña cuentan con el "*Computer Misuse Act*" de 1990 que penaliza el acceso o modificación de datos de un sistema informático ajeno sin consentimiento. La propuesta inglesa es correcta, sin embargo, debemos tener en cuenta que se trata de un sistema de Common Law con menos similitudes con el sistema español que las que tiene el derecho penal francés. En cambio, Alemania combina los dos sistemas en su "Ley contra la criminalidad económica" que entró en vigor en 1986, en combinación con los artículos que contiene en su código punitivo relativos a los delitos informáticos (Urbano Castrillo, 2011, pág. 1).

Estados Unidos, por otro lado, cuenta con una regulación similar a la española. En cada estado federado se ha incorporado a sus estatutos conductas relativas a la delincuencia vinculada a sistemas informáticos y en casi todos los Estado entre estas normas hay una que regula el fraude informático, perfilado como una figura parecida a la estafa pero llevada a cabo mediante una manipulación informática (es decir, se regula como si fuera una estafa especial) (Suárez Sánchez, 2006, pág. 219).

En la luchas contra las estafas informáticas las diferentes fórmulas empleadas por otros países deben servir como referente para los demás, pues se trata de un delito transnacional que tiene el mismo carácter en todas las legislaciones. Sin embargo, en ningún país parece estar bajando la incidencia, por lo tanto ningún país tiene una regulación del fraude informático que pueda servir de ejemplo.

A nivel nacional no se han podido alcanzar niveles de protección y prevención eficaces, en consecuencia también se han propuesto soluciones a nivel europeo. Por ejemplo, la reciente *Directiva (UE) 2019/731 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo* resalta la importe dimensión transfronteriza del fraude informático y las recomendación de armonizar a estos efectos la legislación penal relativa al asunto. Propone definiciones comunes de conceptos como "monedas virtuales" o "sistema de información" para garantizar un *enfoque coherente a la hora de aplicar la presente Directiva en los Estados miembros y facilitar el intercambio de información y la*

cooperación entre las autoridades competentes. Se adopta esta directiva con la finalidad establecer normas mínimas que faciliten la prevención de estas infracciones, peor también la prestación de asistencia y apoyo a las víctimas.

En definitiva, la regulación española no es muy diferente a la que se ha adoptado en otros países. El uso de leyes especiales en el derecho penal español (artículo 7 CP) todavía no está generalizado, y parece más conveniente su inclusión directa en el Código Penal. Por otro lado, la creciente armonización europea en materia penal podría abrir nuevas posibilidades especialmente en lo relativo a la prevención de las estafas informáticas.

CAPÍTULO VIII.- CONCLUSIONES

En este capítulo final vamos a reunir las principales conclusiones a las que hemos llegado a lo largo de este trabajo y las posturas adoptadas en relación con el delito de estafa informática.

En primer lugar, en lo relativo a los delitos informáticos en general, el legislador ha optado por la dispersión normativa, ignorando los elementos comunes que tienen esta clase de ilícitos. El resultado ha sido encontrarnos con tipos como el delito de daños informáticos, la estafa informática, o delitos de propiedad intelectual, que se cometen con medios de la misma naturaleza, pero que el Código Penal no relaciona de ninguna forma, llevando a interpretaciones distintas sobre el tratamiento de su contenido. Si resulta que un delito como el fraude informático tiene menos elementos en común con la estafa tradicional que con otros delitos que podemos clasificar como informáticos, parece que habría sido más conveniente tipificar la estafa como un delito independiente e incorporarlo a un Título nuevo en el que pueda estar relacionado con otros *ciberdelitos*.

En segundo lugar, en cuanto al delito de estafa informática en concreto, parece que podemos admitir que el legislador ha acertado en la introducción de los tipos del apartado a) y c) del art. 248.2CP. Mediante el uso de conceptos abiertos y la interpretación de la jurisprudencia, podemos afirmar que se han podido abordar la mayoría de los supuestos que han ido surgiendo con los desarrollos tecnológicos. Sin embargo, hay dos problemas a los que se debe dar solución:

- Primero, el apartado b) debería tener un tratamiento penal separado a los otros dos apartados. Su introducción como mecanismo preventivo de la comisión de estafa es correcta, sin embargo se vulnera el principio de proporcionalidad sancionando dicha conducta con las mismas penas que las demás estafas consumadas. Este problema podría solucionarse a través de una regulación autónoma de esta conducta delictiva: por ejemplo, podría constituir una circunstancia atenuante del delito de estafa informática en general, de esta forma se seguiría sancionando la conducta y se daría más independencia a la labor de prevención de estos delitos.

- Segundo, viendo las discusiones que ha suscitado la sanción de la conducta de los muleros en los delitos de *phishing*, quizás se debería aclarar cuál es la correcta.

Parece que los tribunales usan diferentes criterios dependiendo del caso, sin embargo, con el aumento de casos este año, lo conveniente sería reunir los criterios para crear una doctrina asentada. Debemos tener en cuenta que la incidencia va a incrementar con más rapidez que antes; si hasta ahora el número de usuarios de Internet cada año incrementaba exponencialmente, desde la crisis del COVID-19 son más personas las que usan las nuevas tecnologías para su día a día. Los pagos en Internet son cada vez mayores, pues la gente ha dejado de salir a la calle para comprar por miedo al contagio. Asimismo, el teletrabajo también aumenta los datos personales y confidenciales que se encuentran en la Red. Estas prácticas son atractivas para los *phishers*, pues les resulta más fácil acceder a la información al haber un mayor número de usuarios compartiendo dichos datos. Por otro lado, ya no son sólo los jóvenes los que usan Internet, ahora las personas que menos saben sobre estos programas y que han recibido menos educación sobre su funcionamiento, se ven obligados a manejarlos, con menos conocimientos sobre *ciberseguiridad* y con más posibilidades de "picar" el anzuelo.

La tercera conclusión a la que hemos llegado guarda relación con la importancia de las medidas de prevención y cooperación entre los países para la lucha contra este delito transnacional. Si se creara un Título nuevo para el tratamiento de los delitos informáticos en general, quizás podrían incluirse las definiciones a las que se refiere la Directiva de la UE, que pretende armonizar conceptos tanto preventivos como de sanción para que los países puedan cooperar fácilmente en la persecución de estos delitos. De esta manera se daría más protagonismo a esta clase de delitos que se encuentran en auge.

En definitiva, el tratamiento penal de los delitos informáticos, y en concreto la tipificación del delito de estafa informática, es un tema que va a ganar protagonismo en los próximos años. Hasta ahora tan solo se han probado mecanismos nuevos adaptados a las conductas que han ido apareciendo con los desarrollos tecnológicos, sin embargo, con lo años, las prácticas informáticas se van generalizar mucho más, como ya está ocurriendo, y como consecuencia se van a crear nuevas formas de causar perjuicios patrimoniales a través de programas informáticos a las que el derecho penal va a tener que dar respuesta.

CAPÍTULO IX.- BIBLIOGRAFÍA

Obras doctrinales

Armenteros León, M. (2008). Algunas consideraciones sobre la utilización delictiva de tarjetas de crédito, de débito y otras que pueden utilizarse como medio de pago. *El Derecho Editores*, 19-20.

Barrio Andrés, M. (2011). La ciberdelincuencia en el Derecho español. *Revista de las Cortes Generales (83)*, 273-305.

CNN-CERT. (2019). *Ciberamenazas y Tendencias 2019.* Madrid: Ministerio de Defensa.

Congil Díez, A. (2013). Problemática relativa a la calificación jurídica de la participación de los denominados "muleros bancarios". Estado actual de nuestra doctrina y jurisprudencia. *Revista de Jurisprudencia El Derecho, nº2*, 3-7.

De Urbano Castrillo, E. (2011). Los delitos informáticos tras la reforma del CP de 2010. *Revista Aranzadi Doctrinar núm. 9*, 163-176.

Faraldo-Cabana, P. (2015). Estrategias legislativas en las reformas de los delitos informáticos contra el patrimonio. *Revista Aranzadi de Derecho y Nuevas Tecnologías núm. 38*, 29-61.

Fernández Teruelo, J. G. (2007). Respuesta penal frente a fraudes cometidos en Internet: Estafa, estafa informática y los nudos de la red. *Revista de derecho penal y criminología, 2ª Época, nº 19*, 217-243.

Gabinete de Coordinación y Estudios; Secretaría de Estado de Seguridad. (2019). *Estudio sobre la cibercriminalidad en España.* Madrid: Ministerio del Interior. Gobierno de España.

García García-Cervigón, J. (2008). El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. *ICADE. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, nº74*, 289-308.

Gómez Perals, M. (1994). Los delitos informáticos en el derecho español. *Informática y derecho: Revista iberoamericana de derecho informático, nº 4*, 481-496.

Lascuraín Sánchez, J. A. (2019). *Manual de introducción al Derecho Penal.* Madrid: Agencia Estatal Boletín Oficial del Estado.

Liñán Lafuente, A. (2018). *Trazos de Derecho penal. 2ª edición.* Madrid: Autoedición.

Mata Barranco, N. J., Dopico Gómez-Aller, J., Lascuraín Sánchez, J. A., & Nieto Martín, A. (2018). *Derecho penal económico y de la empresa.* Madrid: Dykinson.

Miró Llinares, F. (2013). La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing. *Revista Electrónica de Ciencia Penal y Criminología ISSN 1695-0194*.

Prada, I. F. (2012). *Criminalidad informática.* Valencia: Tirant Lo Blanch.

Suárez González, C. (1997). *Comentarios al Código Penal.* Madrid: Editorial Civitas.

Suárez González, C. (1997). *Comentarios al Código Penal.* Madrid: Civitas.

Urbano Castrillo, E. d. (2011). Los delitos informáticos tras la reforma del CP de 2010. *Revista Aranzadi Doctrinal num.9*, 1-12.

Velasco Nuñez, E. (2010). Los delitos informáticos: la reparación y las indemnizaciones. Especial referencia al fraude. *Revista de Jurisprudencia El Derecho, nº3*, 3.

Velasco Nuñez, E. (2010). Los delitos informáticos: la reparación y las indemnizaciones. Especial referencia al fraude. *Revista de Jurisprudencia El Derecho, nº3*, 3.

Velasco Nuñez, E., & Sanchís Crespo, C. (2019). *Delincuencia Informática.* Valencia: Tirant lo Blanch.

Recursos de Internet

Rodríguez Caro, M. V. (30 de Octubre de 2015). *Noticias Jurídicas*. Recuperado el 19 de abril de 2021, de https://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo;mulero-bancariordquo;:-categorizacion-y-doctrina-de-la-sala-segunda-del-tribunal-supremo/

CAPÍTULO X.- ANEXO

ANEXO LEGISLATIVO

Normas Internacionales

Directiva (UE) 2019/731 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo

Normas nacionales

Ley Orgánica 10/1995, de 23 de noviembre, el Código Penal

Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

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

ANEXO JURISPRUDENCIAL

Sentencia del Tribunal Supremo núm. 4025/1991, de 19 de abril

Sentencia del Tribunal Supremo núm. 2175/2001, rec. 603/2000, de 20 de noviembre

Sentencia del Tribunal Supremo número 533/2007 de 12 de junio

Sentencia del Tribunal Supremo núm. 330/2014, recurso 1772/2013, de 23 de abril

Sentencia del Tribunal Supremo núm. 755/2016, recurso 228/2016, de 13 de octubre

Sentencia de la Audiencia Provincial de Barcelona núm. 792/2003, de 6 de octubre

Sentencia de la Audiencia Provincial de Pontevedra núm. 47/2009 de 15 de julio

Sentencia de la Audiencia Provincial de Madrid núm 106/2011, recurso 13/2011, de 12 de diciembre

Sentencia de la Audiencia Provincial de Navarra núm. 140/2013, de 26 de junio