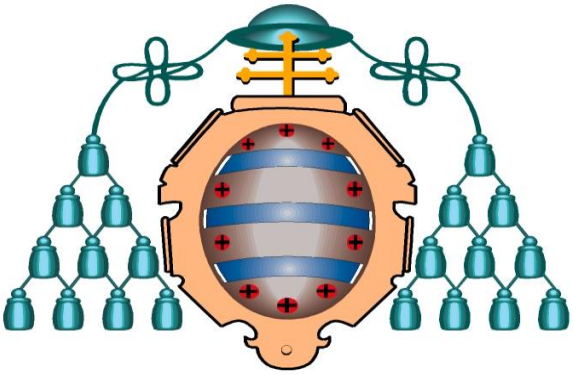
MÁSTER UNIVERSITARIO EN ABOGACÍA

CURSO 2013/2014

TRABAJO FIN DE MÁSTER



UNIVERSIDAD DE OVIEDO

"FRAUDES EN INTERNET Y ESTAFA INFORMÁTICA"

Alumno: MARCOS GONZÁLEZ SUÁREZ

Tutor: JAVIER G. FERNÁNDEZ TERUELO

MAYO 2014

INDICE

1.-Introducción:

El ciberdelito es una categoría criminológica que a raíz del imparable avance de las nuevas tecnologías se ha convertido en una realidad indiscutible. Cualquier ciudadano tiene acceso a tecnologías como puede ser un ordenador con internet o un móvil con tarifa de datos; es un medio que se ha instaurado en la sociedad actual y por sí solo no es un medio negativo, pero como casi depende del uso que se le dé.

La definición que podría hacerse de ciberdelito es cualquier actividad delictiva cometida por medio de herramientas informáticas o contra los sistemas informáticos. La característica principal de este tipo de delitos es que para ser perpetrados es necesario acceder a redes de información o medios informáticos. Se han elaborado muchas categorías y los grupos en que pueden englobarse son muy amplios; por citar los más curiosos y relevantes se pueden mencionar el phishing (robar información de alguien), el grooming (conocer a menores con fines sexuales) o el ciberbullying (acoso a través de la red)[1].

Pueden manifestarse tanto en conductas orientadas a incidir ilícitamente en el instrumental informático, como aquellas que se sirven de medios informáticos para cometer diversos tipos de delitos. En el primero, la informática es el objeto del delito, en el segundo los sistemas informáticos son el medio para acometer el delito. Pero no nos llevemos a error, los delitos serán los mismos dentro o fuera de Internet, en ambos casos se atenta contra algún bien jurídico. No es un delito informático necesariamente aquel que se comete utilizando un ordenador, sino aquel que emplea las redes informáticas u otros medios telemáticos.

Los autores de este tipo de delitos suelen ser personas con un elevado conocimiento de informática, aunque teniendo en cuenta como han avanzado las nuevas tecnologías y el modo en que se han implantado en la sociedad como un elemento común, casi cualquier persona puede acceder hoy en día a un ordenador y a internet, pudiendo

[1] LÓPEZ ORTEGA, J.J. *Internet y Derecho Penal.* Madrid: Consejo General del Poder Judicial, 2001. Pág. 314

entrar en redes sociales o mandar correos electrónicos a particulares. No obstante delitos como el fraude informático siguen requiriendo de un nivel elevado de conocimientos técnicos para llevarlas a cabo. Hay delitos como la estafa o el robo que pueden realizarse por otros medios además del informático, pero supuestos como el ataque a sistemas informáticos y la destrucción de sus archivos sólo puede realizarse mediante un ordenador.

El cibercrimen tiene una serie de características como la rapidez o la permanencia en el tiempo de sus consecuencias. Se precisan de una serie de medios para algunos delitos informáticos, como son una gran velocidad para navegar por internet y una elevada capacidad de almacenamiento de datos. El hecho de que estos datos queden guardados y se extiendan en la red supone que su recuperación o eliminación es una tarea muy complicada, puesto que en un medio tan abierto y en donde cualquier dato, información o imagen puede propagarse y extenderse de una manera rápida y directa, es casi imposible establecer unas medidas de seguridad realmente eficaces. Por otro lado su rápida expansión supone que el autor pueda acceder a un mayor número de víctimas. Otro aspecto a destacar en este tipo de delitos es que a veces conllevan el tratamiento de datos contables o fiscales muy delicados.

Se han realizado diversos estudios sobre el tipo de perfil que podemos elaborar de un cibercriminal, lo que está claro es la imposibilidad de crear un perfil único. Por ejemplo el perfil de cibercriminal económico no suele atender a un único sujeto, sino a una organización criminal compuesta por una pluralidad de individuos. En el cibercrimen político lo más destacable es su organización horizontal y no vertical, con un objetivo central, al que se unen múltiples personas que no tienen porqué tener necesariamente un elevado conocimiento tecnológico, con lo que son prescindibles; igualmente es frecuente la actuación individual, fuera de toda relación organizativa. Por último la cibercriminalidad social, es la presentada como más compleja, especialmente por la existencia de múltiples motivaciones en el sujeto activo, pero siempre con la particularidad que le da el ciberespacio[2].

[2] MIRÓ LLINARES, F. "*El Cibercrimen, fenomenología y criminología de la delincuencia en el ciberespacio*". Madrid: Editorial Marcial Pons, 2012. Pág. 237 y ss.

Al igual que en el caso del cibercriminal, es imposible desarrollar un perfil único de la víctima de ciberdelitos. Se configura además de por la motivación del criminal, por los hábitos de la víctima, como el modo en que utiliza las nuevas tecnologías e internet. Es destacable la especial vulnerabilidad de la víctima virtual frente a la víctima física, por la dificultad para delimitar a la misma.

Estamos tratando un tema cuya nota más característica es su rápida evolución, cambio y adaptación a nuevos medios, en la mayoría de las ocasiones va por delante del propio ordenamiento, superando todas las expectativas y previsiones del legislador, dada su naturaleza cambiante. Por poner un ejemplo claro, hasta hace no muchos años nadie imaginaba la repercusión de redes como Facebook o las posibilidades de los móviles a la hora de enviar datos. Todo el marco en donde nos movemos ha cambiado radicalmente y seguirá cambiando, por tanto muchas veces las leyes son superadas y pueden no regular con la profundidad necesaria algunos de estos casos. Es indiscutible que las leyes son algo vivo, no pueden existir en un vacío teórico, es la realidad social la que realmente marca las leyes y su aplicación. Por esto a mi modo de ver, es el juzgador quien debe aplicar el ordenamiento y quien debe intentar suplir la dificultad del legislador para tratar una materia en continuo cambio; debe hacerlo siendo consciente en todo momento de los nuevos medios informáticos existentes.

1.1.-Evolución de la estafa informática en nuestro Código Penal:

Antes del Código Penal de 1995 la mayoría de los delitos referentes a la informática resultaban atípicos y extraños para los Tribunales, pero nuestro actual Código Penal regula y trata los delitos en donde la informática se utiliza para ejecutarlos. Había casos como los de transferencias electrónicas de fondos que exigían dicha regulación, puesto que llegaron a aumentar considerablemente los supuestos cuyo enjuiciamiento resultaba muy difícil por la ineficacia del anterior Código Penal a la hora de tratarlos.

La principal limitación del anterior Código Penal era que sólo alcanzaba bienes o valores que se corporeizasen en objetos físicos, tangibles y visibles; por tanto aplicar la ley penal a objetos que no tuvieran dichas características no era posible. Esto llegó a suponer un problema importante en situaciones de manipulación donde se alteraban asientos contables para adquirir un derecho de crédito o suprimir un débito, situaciones donde no había dinero en efecto de por medio. Con el nuevo Código Penal de 1995 se regulan no sólo objetos físicos sino también bienes intangibles como datos, en tipos penales como el descubrimiento de secretos o espionaje industrial de los artículos 197 y 278 del Código Penal. Los activos patrimoniales se consideran bienes susceptibles de apropiación en el art. 252 CP relativo a la apropiación indebida. Quedaba patente que un cambio importante se produjo para dar cabida a nuevas situaciones, y cada vez era más evidente la necesidad de regular el fraude informático de manera específica. Al actuarse sobre una máquina, en lugar de sobre una persona, se hacía imposible aplicar el tipo básico de estafa. El elemento del engaño es el que mayores problemas plantea, puesto que no se puede engañar a una máquina, sólo se la puede manipular para que otra persona caiga en el error[3].

Pero la reforma no tenía como objeto los delitos informáticos, el principal objeto de la reforma era sancionar conductas fraudulentas en las entidades bancarias, donde empleados o terceros podían operar sobre las terminales de pago y realizar transferencias

[3] En este sentido me gustaría señalar la Sentencia del Tribunal Supremo de 19 de abril de 1991 en donde queda patente cómo los juzgadores consideraban que el tipo de estafa básico no podía contener los supuestos de fraude informático, dice la sentencia 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… La inducción a un acto de disposición patrimonial sólo es realizable frente a una persona y no frente a una máquina… 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 de 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*". Pero la jurisprudencia del Tribunal Supremo no era pacífica, de este modo la Sentencia del Tribunal Supremo del 22 de septiembre de 2000 se aplicaban los artículos 528 y 529.7 del Código Penal de 1973, decía el Tribunal que " *la incorporación del metálico a su patrimonio se logró mediante la manipulación de aparatos informáticos*", de este modo se saltaba el problema de la inexistencia del engaño en la víctima.

bancarias a su favor[4]. De hecho cuando empezó a aplicarse este artículo se utilizaba para castigar operaciones fraudulentas ejecutadas con tarjeta de crédito en cajeros automáticos[5].

No obstante la doctrina mayoritaria consideraba que el fraude informático no podía encuadrarse sin más en el tipo de estafa básico, por la inexistencia del engaño, ya que materialmente es imposible engañar a una máquina. No se podía cubrir este vacío con los tipos de hurto o apropiación indebida, era evidente que existía una necesidad de regular este tipo de delitos. Por su especial particularidad no sirve con parchear la situación como hacían los tribunales, tratando de aplicar tipos penales que a todas luces eran insuficientes y que desde luego no se crearon con el propósito de enjuiciar delitos informáticos. Se introdujo el apartado a en el art. 248.2 del actual Código Penal con la intención de paliar esa importante laguna.

Para tratar este tipo de supuestos el método a utilizar por el legislador fue el de complementar tipos legales existentes en el anterior Código Penal. En el caso de la estafa se puntualizó sobre la conducta típica del delito, englobando los casos de estafa informática. Se atendió a las advertencias de la doctrina, dando una respuesta un nuevo tipo de crimen, que utiliza las nuevas tecnologías como medio para perpetrar el delito. Estos delitos son ahora mismo una realidad, y en el futuro no pueden hacer más sino aumentar, teniendo en cuenta el rápido avance de las tecnologías. Podríamos poner como un ejemplo al alcance de todos los teléfonos móviles, hace menos de una década han pasado de ser teléfonos propiamente dichos, a constituir pequeños ordenadores desde los que poder realizar un sinfín de acciones. Ya pudimos observar que clasificar este tipo de delitos es particularmente difícil debido a su constante cambio y evolución, además sus formas de comisión son muy variadas originando un abanico de posibilidades enorme. Para ejemplificar la problemática de este tipo de delitos en el caso del fraude informático, un mismo procedimiento comisivo podría dar lugar a diversos delitos distintos entre sí[6].

[4] FERNÁNDEZ TERUELO, J.G. Cibercrimen, los delitos cometidos a través de Internet. Oviedo: Editorial Constitutio Criminalis Carolina, 2007. pág. 46

[5] Vid. Sobre la cuestión, MATA Y MARTÍN, R.-JAVATO MARTÍN, A. "Tratamiento jurídico-penal de los fraudes efectuados con tarjetas de pago: Doctrina y jurisprudencia", en Revista Aranzadi de Derecho y Nuevas Tecnologías, año 2009-2, núm. 20, pp. 37 y ss.

[6] CONDE PUMPIDO FERREIRO, C. *Estafas*. Valencia: Editorial Tirant Lo Blanch, 1997, pág. 19 y ss.

En el Código Penal de 1995 el delito de estafa informática queda regulado como ya expliqué previamente, en el art. 248.2.a). Se complementa el tipo penal diciendo que será fraude utilizar la manipulación informática o artificio semejante, además de señalar los elementos del tipo penal de estafa como ánimo de lucro o perjuicio de la víctima.

1.2-Futura Reforma del Código Penal:

La futura reforma que parece contemplar el Legislador pretende luchar contra el fraude fiscal y la Seguridad Social entre otras cosas, pero debemos preguntarnos en qué medida afectará al fraude y la estafa común, si se endurecerán las penas o no.

Ya se reformó el artículo referente a la estafa en nuestro Código Penal en la Ley Orgánica 5/2010 del 22 de junio. El objetivo de esta reforma que fue mínima, era controlar casos en donde se empleara el uso de cheques de viaje, tarjetas de crédito o débito, y en general de cualquier tipo de documento o medio informático que pudiera utilizarse para realizar lo que nuestro Código Penal entiende por estafa. La finalidad de la reforma era poder delimitar de manera clara los casos de estafa con los de falsedad documental, puesto que en muchas ocasiones debido a los elementos empleados, podrían superponer dobles valoraciones jurídicas y dar lugar a interpretaciones discordantes.

Pasando a hablar de la reforma sobre el Código Penal que tiene pensado sacar adelante el actual gobierno, ésta va en la línea de endurecer las penas y de atacar muy duramente (quizás demasiado en opinión del que escribe) algunos delitos informáticos. Se endurecen en alto grado las penas referentes a delitos contra la propiedad intelectual. El poner en una página web un enlace que permita descargar material protegido en materia de propiedad intelectual, como pueden ser películas o canciones, podría castigarse con penas de hasta seis años de prisión. En lo que respecta al tipo de estafa se endurece la pena, de este modo se reformarían los artículos 249, 250 y 251 bis. Pero con respecto a la estafa informática nos interesa especialmente el primero y en menor medida el segundo.

Actualmente la pena del delito de estafa es pena de prisión de seis meses a tres años, si la cuantía de lo defraudado excediere de 400 euros. Si no superase esa cantidad estaríamos ante una falta de estafa, con pena de localización permanente de cuatro a doce días o multa de uno a dos meses, de acuerdo al art. 623 CP.

Con la pretendida reforma quedaría de la siguiente manera, teniendo presente que se suprimen las faltas: "*Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.*

Si en atención a estas circunstancias, el hecho fuera de escasa gravedad, se impondrá la pena de multa de uno a tres meses. En ningún caso se considerarán de escasa gravedad los casos en los que el valor de la cantidad defraudada fuera superior a 1.000 euros". Por tanto la pena final sería de prisión de seis meses a tres años, si el hecho fuera de escasa gravedad la pena sería menor, multa de uno a tres meses. Realmente no parece que vaya a variar demasiado, puesto que la pena es igual en delitos de notable gravedad. La mayor diferencia la encontramos en casos de estafa de baja gravedad. Hasta ahora este tipo de delitos pasaban a faltas, pero al suprimirlas en la pretendida reforma sería otro delito más, aunque con una pena muy baja, similar a la de una falta. Es más que discutible querer suprimir de raíz esta figura, puesto que se obliga al ciudadano a una serie de gastos como es el propio abogado defensor, o un aumento en las multas impuestas por el juzgador. No obstante esto es otra discusión con distintos puntos de vista.

2.-Fraudes informáticos:

El fraude en nuestro derecho penal engloba una serie de conductas encaminadas a llevar al engaño a la víctima, para que posteriormente el estafador pueda beneficiarse patrimonialmente, causando un perjuicio al sujeto pasivo. Este tipo de delitos se ha visto

potenciado con el auge de las nuevas tecnologías, principalmente las relacionadas con Internet. El problema que tiene el fraude informático está en la propia definición de fraude, ya que se da por supuesto que debe producirse un engaño, pero a un ordenador, como máquina que es, no se le puede engañar. Por tanto hay un problema de base, y es que sin engaño no puede haber fraude ni estafa[7]. Por eso el legislador introdujo la figura de fraude informático en el art. 248.2.a) en el Código Penal de 1995[8] , porque se requería de una figura que se ajustara a la realidad social y a casos donde no podía darse un elemento esencial en el tipo básico de la estafa como es el engaño. La estafa informática tiene lugar frente a un sistema informático, en la mayoría de los supuestos al perjudicado ni podría darle tiempo a ser engañado puesto que el fraude se produce cuando el autor manipula el sistema y no después. Es decir; el momento de perpetración es cuando la manipulación del sistema es efectivo, en ese momento no existe ningún engaño, no puede haberlo ante un ordenador.

2.1-Spyware (sustracción sin el conocimiento de la víctima):

Los programas Spyware sirven para que el sujeto activo pueda sustraer datos del ordenador de la víctima con diversos fines, normalmente son datos sensibles y podrían utilizarse para acceder a cuentas bancarias y códigos de tarjetas de crédito, con el riesgo que ello supone. En líneas generales la estafa mediante estos programas consiste en sustraer unos datos que permitan la suplantación de personalidad de la víctima, con esos datos el estafador puede beneficiarse económicamente y disponer de varias ventajas de índole patrimonial, obtenidas de modo ilícito.

Además de estos programas existen otros cuyos fines son los mismos pero utilizan diferentes mecanismos; los más relevantes son los troyanos, scareware o keylogger.

[7] ARROYO DE LAS HERAS, A. *Los delitos de estafa y falsedad documental*. Barcelona: Editorial Bosch, 2005, pág. 67 y ss..

[8] GONZÁLEZ RUS, J.J. Protección penal de sistemas, elementos, datos, documentos y programas informáticos. En la Revista electrónica de ciencia penal y criminología. Nº1, 1999, sin paginación.

Mediante el scareware aparece en la pantalla de la víctima un mensaje para acceder a diversos enlaces. El engaño está en que pulse el enlace para, por ejemplo, evitar un virus informático u obtener algún premio. Pero dicho enlace sirve para que dentro del sistema se ejecute un malware, que es otro programa cuyo objetivo puede ser robar información del usuario.

El keylogger es un sistema menos habitual y más sofisticado, se pretende que la víctima pulse una serie de teclas, para de ese modo descubrir cual es la contraseña de diversos servicios. Pero también existen otros programas aún más modernos y complejos que consiguen acceder a esta información sin necesidad de observar lo que teclea.

Los troyanos son probablemente los más conocidos por todos nosotros y los que mayor temor suelen despertar, aunque no tienen porqué ser necesariamente los más dañinos. Este tipo de programas se hacen pasar por un programa inofensivo que el usuario activa sin sospechar la verdadera naturaleza del mismo, para luego ponerse en marcha la verdadera función. Con sus efectos dañinos para el sistema y los datos del sistema de la víctima.

Otros programas muy parecidos a los troyanos son las bombas lógicas, pero esta variante permanece en estado latente hasta que se activa. Cuando llega una determinada fecha, se escribe un comando concreto o se ejecuta un programa determinado número de veces.

2.2-Obtención fraudulenta de las claves (phising y pharming):

Phising es un término informático, no jurídico, y se refiere al fenómeno según el cual el sujeto activo trata de engañar a la víctima para obtener datos sensibles, haciéndole creer que está teniendo lugar una comunicación oficial con otra parte libre de toda sospecha. Cuando la realidad es un ataque contra su seguridad para obtener datos sensibles

como códigos de tarjetas de crédito y acceso a cuenta bancaria. La definición del término phising podemos encontrarla en variada jurisprudencia[9].

Un caso bastante habitual de phising[10] es aquel mediante el cual a la víctima le aparece un correo con el enlace de una página aparentemente oficial, normalmente una entidad bancaria que sea muy conocida, en donde dicen que le ha tocado un premio y que para recibirlo es necesario que de una serie de datos[11]. Realmente esos datos los está dando al sujeto activo, no al banco, pero el engaño está muy elaborado puesto que la página del banco parece totalmente real, con publicidad y todo tipo de detalles[12].

Pharming es una variante del phising, y en la jurisprudencia se trata con menos detalle, lo que se hace aquí es modificar el DNS (Domain Name Server), cuya utilidad es dirigir al usuario a las páginas que desea ver. Al modificar el DNS cuando la víctima pretende ir a una página concreta, realmente está siendo dirigido a donde quiere el estafador. Puede ser una copia de la página original y una vez aquí introducirá sus datos personales, pudiendo de ese modo apropiarse de ellos el sujeto activo. Es muy parecido al phising y la diferencia es más bien técnica. Se basa en el tipo de programas utilizados para apropiarse de esos datos. El pharming es más peligroso, al ser mucho más complicado

[9] Dice la Audiencia Provincial de la Rioja en su sentencia de 21 de diciembre de 2011, nº de sentencia 213/2011, en su fundamento de derecho primero que "*es un concepto informático que denomina el uso de un tipo de fraude caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como "phisher", envía a numerosas personas correos electrónicos masivos en los que se hace pasar por una empresa de confianza (por ejemplo, una entidad bancaria, o una compañía telefónica, etc); otras veces lo hace mediante la creación de páginas "web" que imitan la página original de esa entidad bancaria o empresa de reconocido prestigio en el mercado; en ocasiones también se realiza por medio de llamadas telefónicas masivas realizadas a numerosos usuarios en las que se simula ser un empleado u operador de esa empresa de confianza. En todo caso, siempre se trata de una aparente comunicación "oficial" que pretende engañar al receptor o destinatario a fin de que éste le facilite datos bancarios o de tarjeta de crédito, en la creencia de que es a su entidad bancaria o a otra empresa igualmente solvente y conocida a quien está suministrando dichos datos. Finalmente, en otras ocasiones el sistema consiste simplemente en remitir correos electrónicos que inducen a confianza (simulando ser de entidades bancarias, etc) que cuando son abiertos introducen "troyanos" en el ordenador del usuario, susceptibles de captar datos bancarios cuando este realiza pagos en línea*".

[10] TS, Sala Segunda, de lo Penal, S de 16 de Marzo de 2009.

[11] Como curiosidad el término phising viene del inglés fishing que quiere decir pescar, en alusión a las víctimas de los estafadores y hackers. La sustitución de la f por ph puede ser por una forma de hacer fraude telefónico denominada phreaking.

[12] MIRÓ LLINARES, F. *La Respuesta Penal al Ciberfraude*. Revista Electrónica de Ciencia Penal y Criminología, pág. 72.

descubrir, ya que no somos nosotros quienes vamos a una página falsa pulsando un enlace, sino que nos desplaza automáticamente el propio programa. Los programas dañinos modifican el DNS o los archivos llamados hosts, si el sistema es windows, así como el navegador Internet Explorer.

Para esta forma de delitos adquiere especial importancia la figura de los muleros. De quien hablaremos con más detalle. Pero a modo de introducción; son personas que prestan sus cuentas bancarias para recibir dinero, se quedan con una parte a modo de comisión y envían el montante restante a la dirección indicada. Es muy discutido por la jurisprudencia el nivel de responsabilidad de estos "intermediarios", puesto que en muchas ocasiones pueden no saber que están cometiendo un delito.

Otra variante del phising es el scam, consiste en enviar un correo electrónico denominado scam, no es más que el típico fraude en donde se busca que el receptor del correo realice algún acto para beneficiar a quien envía el mensaje. Podemos asimilarlo al "*timo de la estampita*" o de las "*cartas nigerianas*"; se busca explotar el ánimo de lucro de la víctima. Los sistemas técnicos han evolucionado y las nuevas tecnologías son un aspecto muy importante en este tipo de delitos; pero el factor humano, concretamente su vulnerabilidad, es el punto débil del que se sirve el sujeto activo, sigue siendo el eslabón fundamental del que se sirven los estafadores. Realmente aquí no se necesitan grandes alardes informáticos ni programas especiales, simplemente es el "*timo de la estampita*" adaptado a las nuevas tecnologías, y se hace con un correo electrónico lo que podría hacerse con una carta postal. Los scammers, son los sujetos activos de este tipo de delitos. Para no venir a España y agotar su actividad delictiva, transfieren el dinero inconsentidamente apropiado a cuentas de colaboradores situados en España: los muleros.

Es importante precisar que los delitos relacionados con el scam estarían dentro de la estafa común y no del fraude informático. Ya que cumplen con todos los elementos del tipo penal, que veremos más adelante. Son casos en donde hay una trasferencia patrimonial mediante un engaño evidente, aunque la comunicación se produjera a través de medios informáticos.

2.3-Transacción de comercio electrónico fraudulento:

Estamos ante casos menos peligrosos y en la práctica realmente suelen ser pequeños fraudes. Son los típicos casos en donde la víctima pretende comprar algo por internet o puja por el artículo y luego no recibe lo prometido, ya sea total o parcialmente. Pueden darse fraudes tanto en la entrega de la cosa como en el pago del precio, las víctimas pueden ser tanto compradores como vendedores.

Podríamos englobar en este apartado el Auction Fraud. Es un fenómeno muy de moda en la actualidad, con el auge de páginas de subastas por internet como puede ser Ebay, el método empleado por los estafadores consiste en tergiversar sobre la puja de un producto en internet, o su no entrega de acuerdo a lo pactado en el sistema de subastas de Ebay u otras plataformas similares. El uso de Ebay u otras plataformas de este estilo conlleva una serie de acciones que suelen requerir la participación de los usuarios. Se necesita la utilización de una cuenta y el consiguiente registro en la plataforma, ya sea Ebay o similares. Después buscar un producto, pujar y ganar la misma. Posteriormente canjear el objeto por una cantidad de dinero. Finalmente informar acerca de la reputación de los vendedores. Cada una de estas fases puede ser objeto de fraude. Algunos ejemplos típicos son los siguientes:

-Shilling; los propios vendedores participan en la subasta haciéndose pasar por compradores para aumentar la puja y conseguir que los precios suban.

-Bid Shielding; dos personas pujan por un objeto, una de ellas pujando muy a la baja, la otra puja a la alta para disuadir a los otros posibles compradores, finalmente el que puja a la alta se retira y adquieren el producto a un precio muy reducido.

-Tergiversación; los vendedores dan falsas descripciones acerca de sus productos.

-Ampliar la factura; se ocultan costes adicionales al precio del objeto como embalaje o preparación del mismo antes de enviarlo a los compradores finales.

-Envío suspendido; no se envía el artículo al comprador una vez se ha pagado el precio acordado.

-Pago suspendido; el comprador no paga una vez adquirido el producto.

-Reproducción y falsificación; el vendedor no envía el producto original sino una imitación.

-Triangulación/custodia; el vendedor vende un producto robado.

-Comprar y cambiar; el comprador recibe el producto acorde a lo pactado, pero una vez lo tiene en su poder cancela la operación y manda otro producto que es una falsificación del original, siendo de inferior calidad.

-Reclamación de pérdida o daños; el comprador reclama falsos daños al vendedor en los productos.

-Autosubasta; son subastas falsas cuyo objetivo es conseguir nombres de compradores, o información como códigos de tarjetas de crédito u otros datos sensibles[13].

3.-Respuesta penal:

El crimen informático debería ser un objetivo prioritario para el legislador, puesto que los supuestos han dejado de ser casos de laboratorio para ser una realidad. En el caso de la estafa las consecuencias y actos del agente se interpretaban en un sentido material o físico, lo que era un error, haciéndose evidente que debía tratarse de otra manera. En el

[13] MIRÓ LLINARES, F. La Respuesta Penal al Ciberfraude. Revista Electrónica de Ciencia Penal y Criminología, pág. 70 y ss.

fraude informático no tiene importancia quien realiza la transferencia patrimonial, bastando únicamente que exista una transferencia no autorizada. Dando igual que la haga el propio perjudicado o un tercero. Además de que no existe el elemento del engaño como tal, esto supone un problema si quisiéramos utilizar la concepción que se tenía de la estafa en el anterior Código Penal. Al requerirse el elemento del engaño como requisito para el tipo penal de la estafa, se dejaban fuera todo un grupo de supuestos en donde se manipulaban los sistemas informáticos en beneficio del agente. Por eso en el Código Penal de 1995 el legislador intentó dar una protección efectiva a todos estos casos que se salían del prisma de los delitos clásicos de estafa; en el art. 248.2 CP se sancionaba, y sigue sancionándose, a los que con ánimo de lucro y en beneficio propio, manipulen informáticamente o mediante artificio semejante en perjuicio de otra persona. Con este artículo se protegen aquellos casos y conductas en donde no haya un engaño claro, porque por definición es imposible engañar a una máquina[14]. En este punto entraremos más en profundidad en posteriores capítulos, porque el término manipulación informática y lo que se entiende por él en la jurisprudencia es un aspecto complejo.

Para sancionar las conductas fuera del tipo general de la estafa el legislador dictó el actual apartado a del art. 248.2 de nuestro Código Penal. Se castigan todas aquellas conductas cuyo fin sea realizar una transferencia que beneficie al sujeto activo en perjuicio de otra persona, ya sea en una fase previa donde los datos no han sido tratados, como en fases posteriores donde sí lo han sido. La primera fase es la denominada "*Input*", la segunda es la llamada "*Output*". Acciones como modificar datos o borrarlos entrarían dentro de la primera fase, mientras que la modificación de los resultados del tratamiento automático de los datos formaría parte de la segunda fase. En cualquier caso, a la hora de castigar este tipo de delitos lo relevante es si la transferencia patrimonial se realiza por medios informáticos[15].

[14] La Sentencia del Tribunal Supremo de 20 de noviembre de 2001 * dice que la manipulación informática "*está presente cuando 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*".

[15] MIRÓ LLINARES, F. *La Respuesta Penal al Ciberfraude*. Revista Electrónica de Ciencia Penal y Criminología, pág.14.

Los fraudes de compra y de tipo scam se deberían englobar dentro de la estafa común, aunque la jurisprudencia no es pacífica en este sentido, lo cierto es que en la inmensa mayoría de los casos de scam se produce una comunicación entre el sujeto activo y la víctima, que mediante un engaño desemboca en una transmisión patrimonial a favor del primero en perjuicio del segundo. Este supuesto tiene todos los elementos de la estafa común aunque la comunicación se realice por medios informáticos[16].

La diferencia con la estafa común reside en el hecho de que la transferencia de activos patrimoniales no es realizada por la víctima del engaño, sino por el propio autor o un tercero a través del sistema. En los casos de scam se produce una comunicación, el contacto se efectúa a través del sistema informático, hay una transferencia consentida aunque viciada por el engaño[17].

3.1-Tipo Básico de estafa, definición y elementos:

En relación con el tipo penal de estafa el actual Código Penal sigue el mismo esquema que la reforma del 83, estableciendo una serie de elementos para poder determinar si existe estafa o no. La definición más clara y sencilla con respecto a la estafa la da Antón Oneca[18], pese al paso del tiempo se ajusta a la actual perspectiva que el legislador tiene de la estafa, Oneca la define como "*la conducta engañosa, con ánimo de lucro injusto, propio o ajeno, que, determinando un error en una o varias personas, les induce a realizar un acto de disposición, a consecuencia del cual se produce un perjuicio en su patrimonio o en el de un tercero*". Es muy similar a lo establecido en el art. 248.1 de nuestro Código Penal, 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. En el artículo se establecen una serie de requisitos sin los cuales no podemos entender que existe delito de estafa. Por tanto para que se produzca el tipo penal de la estafa de acuerdo a

[16] FARALDO CABANA, P. *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*. Valencia: Editorial Tirant Lo Blanch, 2009, pág. 91 y ss.
[17] FERNÁNDEZ TERUELO, J.G. *Cibercrimen, los delitos cometidos a través de Internet*. Oviedo: Editorial Constitutio Criminalis Carolina, 2007, op. cit. pág. 50.
[18] Nueva Enciclopedia Jurídica. Editorial Francisco Seix, Estafa, t. IX, 1958.

nuestro Código Penal deben de darse una serie de elementos. Son los siguientes, establecidos por el Tribunal Supremo en reiterada jurisprudencia, la más ejemplificativa es la Sentencia núm. 187/2002 de 8 Feb. de la Sala Segunda de lo Penal donde cita los elementos del tipo[19]:

1º.- Debe producirse un engaño, es el elemento nuclear de la estafa, dicho engaño debe ser bastante, y acorde a la doctrina del Tribunal Supremo sobre el engaño bastante, debe ser suficiente y proporcional para la consecución de los fines propuestos, cualquiera que sea su modalidad en la multiforme y cambiante operatividad que se manifieste, debiendo tener adecuada entidad para que en la convivencia social actúe como estímulo eficaz del traspaso patrimonial, que sea suficiente para los fines propuestos por el estafador, es decir; debe ser eficaz y hacer que el sujeto pasivo caiga en un error. 2º.- Este error en el que cae la víctima

[19] Dice la sentencia en su fundamentación jurídica "*En los elementos configuradores del delito de estafa hay que enumerar: 1.º) Un engaño precedente o concurrente, espina dorsal, factor nuclear, alma y sustancia de la estafa, fruto del ingenio falaz y maquinador de los que tratan de aprovecharse del patrimonio ajeno. 2.º) Dicho engaño ha de ser "bastante", es decir, suficiente y proporcional para la consecución de los fines propuestos, cualquiera que sea su modalidad en la multiforme y cambiante operatividad en que se manifieste, habiendo de tener adecuada entidad para que en la convivencia social actúe como estímulo eficaz del traspaso patrimonial, debiendo valorarse aquella idoneidad tanto atendiendo a módulos objetivos como en función de las condiciones personales del sujeto afectado y de las circunstancias todas del caso concreto; la maniobra defraudatoria ha de revestir apariencia de seriedad y realidad suficientes; la idoneidad abstracta se complementa con la suficiencia en el específico supuesto contemplado, el doble módulo objetivo y subjetivo desempeñarán su función determinante. 3.º) Originación o producción de un error esencial en el sujeto pasivo, desconocedor o con conocimiento deformado o inexacto de la realidad, por causa de la insidia, mendacidad, fabulación o artificio del agente, lo que lleva a actuar bajo una falsa presuposición, y a emitir una manifestación de voluntad partiendo de un motivo viciado, por cuya virtud se produce el traspaso patrimonial. 4.º) Acto de disposición patrimonial, con el consiguiente y correlativo perjuicio para el disponente, es decir, que la lesión del bien jurídico tutelado, el daño patrimonial, sea producto de una actuación directa del propio afectado, consecuencia del error experimentado y, en definitiva, del engaño desencadenante de los diversos estadios del tipo; acto de disposición fundamental en la estructura típica de la estafa que ensambla o cohonesta la actividad engañosa y el perjuicio irrogado, y que ha de ser entendido, genéricamente como cualquier comportamiento de la persona inducida a error, que arrastre o conlleve de forma directa la producción de un daño patrimonial a sí misma o a un tercero, no siendo necesario que concurran en una misma persona la condición de engañado y de perjudicado. 5.º) Ánimo de lucro como elemento subjetivo del injusto, exigido hoy de manera explícita por el artículo 248 del CP entendido 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. 6.º) Nexo causal o relación de causalidad entre el engaño provocado y el perjuicio experimentado, ofreciéndose éste como resultancia del primero, lo que implica que el dolo del agente tiene que anteceder o ser concurrente en la dinámica defraudatoria, no valorándose penalmente, en cuanto al tipo de estafa se refiere, el "dolo subsequens", es decir, sobrevenido y no anterior a la celebración del negocio de que se trate; aquel dolo característico de la estafa supone la representación por el sujeto activo, consciente de su maquinación engañosa, de las consecuencias de su conducta, es decir, la inducción que alienta al desprendimiento patrimonial como correlato del error provocado, y el consiguiente perjuicio suscitado en el patrimonio del sujeto víctima, secundado de la correspondiente voluntad realizativa*".

es el siguiente elemento de la estafa. Debe ser un error esencial sobre la víctima, bajo su influencia debe actuar sin sospechar que sus actos traerán consecuencias negativas sobre su patrimonio. 3º.- El acto de disposición patrimonial que el sujeto pasivo llevará a cabo beneficiando al sujeto activo en perjuicio de la víctima. La jurisprudencia dice que cualquier acto que conlleve un desplazamiento patrimonial en perjuicio de la víctima estaría en este grupo, ya sea en forma de entrega o simplemente un movimiento contable aparentemente inofensivo, también podría ser la realización de algún servicio si fuera cuantificable económicamente. 4º.- Dicho perjuicio es otro elementos fundamental, a la hora de valorar la pena del tipo el Código Penal estable un criterio cuantitativo; es decir, cuanto mayor sea el perjuicio (mayor sea la cantidad defraudada), mayor será la pena y la gravedad del delito. 5º.- Ánimo de lucro, supone la motivación para que el estafador cometa el delito, además de perjudicar al sujeto pasivo beneficia al sujeto activo, normalmente desplazando el patrimonio defraudado para sí. 6º.- Nexo causal, debe existir una relación entre el engaño y el perjuicio; el engaño debe motivar el error que posteriormente causará un perjuicio patrimonial en la víctima.

3.2-Tipo específico del Fraude Informático:

Hemos señalado los elementos para el tipo básico de la estafa. Debe haber al menos dos sujetos, uno que engaña y otro que es engañado. Debido a ese acto la víctima ve perjudicados sus intereses como consecuencia del ardid elaborado por el estafador[20].

Pero no todo es tan sencillo y muchas veces la realidad supera al marco legal, debiendo hacer el juzgador un importante papel interpretativo. Los problemas vienen en supuestos donde no está claro que existan todos los elementos; por ejemplo, no siempre es evidente que haya una persona que engaña y otra que es engañada, para ese tipo de casos es cuando debemos remitirnos a la figura de la estafa informática. En este sentido hay muchas conductas que no encajan con el tipo de estafa común, al no estar presente alguno de sus elementos nucleares, en muchos casos no hay un sujeto engañado propiamente dicho. De

[20] CALLE RODRÍGUEZ, M.V. *El delito de estafa informática*. La ley penal: revista de derecho penal, procesal y penitenciario, nº37, 2007. Pág. 1 y ss.

este modo los casos típicos son los de spyware o los de phising. En ambos supuestos no se da la típica relación de engaño, en el primer caso se instala un programa malicioso en el ordenador de la víctima sin que ésta pueda ni siquiera sospechar lo sucedido, para posteriormente causarle un perjuicio. En los casos de phising sí hay un pequeño engaño inicial al incitar a la víctima a dar sus claves personales, pero una vez obtenidos los datos sensibles no es necesario más contacto entre ambos. En esa segunda fase no existe engaño ni error como tal que motive alguna variación en el patrimonio de la víctima[21].

Para este tipo de casos es para lo que se utiliza la figura de la estafa informática, para poder englobar supuestos que no eran claros ni podían enmarcarse en el tipo penal de estafa. Un elemento clave y diferenciador en el fraude informático es que la trasmisión patrimonial no la lleva a cabo la víctima siendo engañada, sino que es el propio sujeto activo quien a través de artificios tecnológicos y medios informáticos, consigue llevar a cabo tal acción. Sin que pueda llegar a existir una fase previa de engaño, como sí sucede en la estafa convencional.

A continuación analizaremos más en detalle los requisitos más relevantes para que se produzca la estafa, en su vertiente de fraude informático:

3.2.1.-Elementos del fraude informático:

Ánimo de lucro:

Es un elemento subjetivo del tipo penal del delito de estafa, no hay lugar a discusión sobre la necesidad de su existencia para que se produzca el delito, desde el Código Penal de 1973, en su artículo 528 se viene exigiendo, en nuestro Código Penal actual se reconoce el ánimo de lucro de manera expresa en el artículo 248. El sujeto activo en el delito de estafa debe tener ánimo de lucro, es el objetivo que se pretende al realizar la estafa, una

[21] ARROYO DE LAS HERAS, A. *Los delitos de estafa y falsedad documental*. Barcelona: Editorial Bosch, 2005, op. cit. pág. 66.

contrapartida que beneficia al estafador en perjuicio del estafado. Cuando hablamos de un beneficio al sujeto activo puede ser un enriquecimiento o ventaja patrimonial.

Pero no siempre está claro que exista ánimo de lucro. No son pocas las ocasiones en que la estafa no llega a fructificar en ese beneficio al sujeto activo, ya sea porque sus expectativas no pudieron prosperar o porque no hubo tiempo material. En cualquier caso como bien dice ARROYO DE LAS HERAS el propósito que persigue el sujeto "*constituye un hecho psicológico, es decir, un hecho íntimo, propio de la conciencia, nunca del todo objetivable, razón por la cual dicho ánimo o propósito deberá deducirse de los datos o circunstancias que concurren en el hecho mismo*". En consecuencia deberá tenerse en cuenta cada caso concreto, y el juzgador deberá valorar las circunstancias de cada situación, teniendo presente que a veces es difícil de cuantificar si se produjo ánimo de lucro, puesto que al depender de los propios deseos del sujeto activo puede ser un concepto muy relativo. Lo que no da lugar a dudas es que debe existir un ánimo de lucro, debe de concurrir en el momento de la acción, no tiene que prolongarse en el tiempo después de consumarse el delito. Aunque si no se hizo efectivo será mucho más difícil de demostrar la existencia del ánimo de lucro, pero para este punto deberíamos atender a la casuística. Por esto la jurisprudencia es bastante garantista con relación a ello, y suele atenderse a que se produzca algún desplazamiento patrimonial en beneficio del sujeto activo[22].

[22] En este sentido dice la Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, de 28 de noviembre de 2008 en su fundamento segundo "*en el caso enjuiciado no se cumple uno de los requisitos de la estafa constituido por el denominado "ánimo de lucro", o al menos, éste no está declarado en los hechos declarados como probados en la sentencia recurrida, ni se explicita en los fundamentos jurídicos de la misma; al contrario, se declara expresamente su inexistencia por falta probatoria. Sin tal requisito, no puede haber delito de estafa. Convenimos que es posible un escenario que puede satisfacer las exigencias del engaño bastante, tal y como esta Sala Casacional lo ha declarado reiteradamente, pero se incumple la exigencia de la obtención de un lucro personal a favor del sujeto activo del delito, o bien a favor de un tercero en connivencia con aquél, hecho éste que debe declararse como probado en la resultancia fáctica. Y aquí no se describe tal connivencia ni lucro personal. Distinto es el caso del delito de apropiación indebida (art. 252 del Código penal), en donde ha de quedar claro el acto de transmisión por alguno de los títulos aptos en poder del acusado, y en donde éste gestiona deslealmente dicho patrimonio, siendo responsable del delito aunque no se haya acreditado el destino final de la apropiación indebida, bastando la prueba de su inicial transmisión. En el delito de estafa, sin embargo, el desplazamiento patrimonial que perjudica a otro, merced al engaño desplegado por el sujeto activo, creando una situación de error a cargo de este último, tiene que ir dirigido a satisfacer las exigencias de lucro ilícito del acusado, de manera que ha de probarse el circuito de apropiación por parte de éste, o bien por parte de un tercero con el que esté conectado para tal operación jurídica, pero nunca, como aquí acontece, puede quedar esto en nebulosa, de manera que se desconozca qué clase de beneficio ha obtenido el ahora recurrente.*

Otro punto a valorar es si hay ánimo de lucro cuando el dolo es eventual. El sujeto activo asume como probable la realización del tipo penal, menoscabando el bien jurídico de la víctima, pero a pesar de ello se arriesga para alcanzar el fin deseado, dejando su producción al azar. La jurisprudencia es bastante clara en este sentido, diciendo que la existencia de ánimo de lucro no depende de que haya dolo directo[23].

Manipulación informática:

En el art. 248.2.a) CP se habla de manipulación informática o artificio semejante. La manipulación informática podría definirse como la acción consistente en alterar los elementos físicos que afectan la programación informática. Modalidades hay varias y ya citamos los más importantes supuestos. Hacerse pasar por un usuario autorizado para operar en su nombre obteniendo un beneficio, o la introducción de datos maliciosos para apropiarse de otros datos sensibles son casos típicos[24].

El término manipular no puede aplicarse en estos casos atendiendo a la definición dada por la Real Academia Española, el Diccionario define la acción de la siguiente manera; "*Intervenir con medios hábiles y, a veces, arteros, en la política, en el mercado, en la información, etc., con distorsión de la verdad o la justicia, y al servicio de intereses particulares*". Dicha definición es incompleta para este estudio ya que es demasiado amplia, pudiendo emplearse para todo tipo de intervención, ya sea autorizada o no. Debemos precisar esta definición; profundizando en la primera descripción podríamos ampliarla, de este modo manipulación informática sería cualquier acción que suponga una intervención en el sistema informático; alterando, modificando u ocultando los datos que

---

En suma, no puede condenarse por estafa de quien se predica que no puede conocerse si cobró o no cobró el dinero".

[23] ARROYO DE LAS HERAS, A. *Los delitos de estafa y falsedad documental*. Barcelona: Editorial Bosch, 2005, op. cit. pág. 68.

[24] La Sentencia del Tribunal Supremo del 20 de noviembre de 2010 considera que "*la manipulación informática o artificio semejante que procuran la transferencia inconsentida de activos en perjuicio de terceros admite diversas modalidades, como la creación de órdenes de pago o transferencias, o las manipulaciones de entrada o salida de datos, en virtud de las que la máquina actúa en su función mecánica propia —solo que en el sentido patrimonial no deseado por inconsentido, generador del perjuicio en tercero—.".*

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[25]. Con esta definición ya estamos precisando más correctamente el término de estafa informática. Critican algunos autores la poca precisión definitoria del art. 248.2.a) del Código Penal, siendo difícil comprender qué alcance quiso darle el legislador al término de manipulación.

Precisando un poco más sobre qué entendemos por manipulación, se puede decir que puede darse manipulación actuando sobre la introducción de datos, sobre su tratamiento o su salida, intervención sobre el software, etc. Pero la manipulación no exige un contacto directo con el ordenador que contiene los datos de interés, otro ejemplo más del modo en que avanza la tecnología y con ella la casuística son los casos en donde existen sistemas de tratamiento de datos que operan a distancia, pudiendo acceder a ellos a través de mecanismos como la red de telefonía, mediante un terminal que opera a distancia. Es algo evidente que hoy en día quien quiera perpetrar un fraude no necesita acceder físicamente al ordenador objeto de ataque, ya sea mediante internet o mediante otro tipo de redes. Las principales vías por las que el sujeto activo consigue un movimiento contable a su favor, que se la transfieran fondos o se le cancele una deuda son tres: 1-Introducción de datos falsos. 2-Manipulaciones en el programa. 3-Manipulaciones en el sistema de salida de datos u output.

1-Introducción de datos falsos. Consiste en alterar, suprimir u ocultar los datos ya introducidos. No se manipula el programa, sino los movimientos de entrada en un sistema o las operaciones. Aquí el programa hace un tratamiento correcto siguiendo un procedimiento normal, pero se han introducido unos datos falsos con lo que el resultado será incorrecto[26]. Es punible, se puede discutir si estamos ante una manipulación del sistema informático, ya que debería englobarse en la categoría de "*artificio semejante*" del art. 248.2.a) CP. Estas son acciones de la fase input, que vendría a ser la referente a la calidad de los datos

[25] CHOCLÁN MONTALVO, J. A.: Fraude informático y estafa por computación, en CDJ, núm. 10, 2001, p. 328.
[26] ROMEO CASABONA, C.M. y FLORES MENDOZ, F. Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica. Granada: Editorial Comares, 2013. Pág. 224.

tratados. Son casos muy frecuentes, un supuesto típico es el de la cartera de proveedores ficticios, se les abona las partidas que son falsas, para al final quedarse el autor el montante total.

2-Manipulaciones en el programa. Se da en la fase de tratamiento, y aquí si estamos ante una manipulación informática en todo el sentido de la palabra. Se modifican los protocolos del programa para que beneficie al autor. Las variantes y posibilidades son enormes; podemos englobar lo dicho en los apartados anteriores sobre el spyware. Casos como los troyanos son los más típicos, en donde un programa malicioso accede al sistema haciéndose pasar por un programa aparentemente inofensivo y seguro. Por citar otra técnica curiosa señalaría la llamada salami technique, mediante esta técnica se dan instrucciones para que el programa que lleva las cuentas de alguna entidad redondee los céntimos, de este modo el sujeto activo obtiene un gran beneficio con pequeñas estafas[27].

3-Manipulaciones en el sistema de salida de datos u output. Se manipula en este caso el sistema de salida de datos, como puede ser intervenir el cable telefónico o modificar la impresión final. Se requiere de un engaño posterior en el que el documento modificado es un artificio más, por lo que podría discutirse si presenta especificidad.

A la hora de manipular el sistema informático por parte del autor podría darse un concurso de delitos con el de sabotaje informático contemplado en el art. 264.2 CP. Si el sujeto activo hace desaparecer una serie de datos para beneficiarse patrimonialmente, no sólo está defraudando, sino que al estropear los datos o al sistema podríamos estar ante un delito de daños. Por un lado se engaña a la víctima para que el autor se beneficie, y por otro lado pueden destruirse datos o el propio sistema informático, pero debemos distinguir ambas figuras. El tipo penal de la estafa protege al patrimonio, el tipo penal del delito de daños protege la propiedad. Otro aspecto fundamental es que el sujeto que ha sufrido el perjuicio patrimonial no tiene porqué ser la misma persona cuyos datos fueron modificados o destruidos. Estamos ante dos situaciones distintas y deberían estudiarse como tal. Si los

[27] GUTIÉRREZ FRANCÉS, M.L., *Fraude Informático y Estafa*, Ministerio de Justicia, Centro de Publicaciones Madrid, 1991. Pág. 5 y ss.

elementos subjetivos coincidiesen creo que debería aplicarse el concurso de infracciones. Para algunos autores como CHOCLÁN MONTALVO[28], este problema de confusión de tipos penales se produce porque el legislador intentó crear figuras delictivas paralelas a las tradicionales, en lugar de tratar el tema desde una perspectiva autónoma y partiendo desde cero. Es decir; en lugar de crear unas figuras penales que solucionaran el problema desde el inicio, fue modificando las figuras existentes para solucionar estas situaciones, con los correspondientes problemas que pueden originar.

El art. 248.2.a) también recoge el término artificio semejante, dicho término se incorporó al Código Penal de 1995 para abarcar supuestos donde no se manipulaba un sistema informático como solemos entender, sino la manipulación de otro tipo de máquinas automáticas. Un ejemplo típico era el de utilizar sustitutivos de monedas para trampear máquinas automáticas que proporcionan servicios o mercancías. La intención del legislador a la hora de introducir esta expresión era abarcar los supuestos en los que el autor del delito pretende obtener de forma fraudulenta las prestaciones de un aparato automático como puede ser una máquina de tabaco, de gasolina, de refrescos, de juegos conocida coloquialmente como tragaperras, etc.. Para CHOCLÁN MONTALVO esto fue un error por parte del legislador, ya que se aleja totalmente de la estafa informática y debería ser objeto de una dura crítica. No obstante y aunque la idea inicial del legislador fuese mal dirigida, a mi modo de ver esta acepción sirve como "cajón de sastre" y aunque en origen se pensara en la manipulación de máquinas automáticas de diversa índole, al final puede abarcar cualquier supuesto que no entre dentro de la categoría manipulación informática.

Al ser un término bastante difuso es complicado darle una definición precisa, pero podemos remitirnos a la Sentencia del Tribunal Supremo del 26 de junio de 2006, en ella se indica que una de las acepciones del término artificio significa artimaña, doblez, enredo o truco y considera como tal "*la conducta de quien aparenta ser titular de una tarjeta de crédito cuya posesión detenta de forma ilegítima y actúa en connivencia con quien introduce los datos en una máquina posibilitando que esta actúe mecánicamente*", en este

[28] CHOCLÁN MONTALVO, J. A.: Fraude informático y estafa por computación, en CDJ, núm. 10, 2001, op. cit. pág. 335 y ss.

caso el juzgador emplea el término para referirse a los casos en quien aparenta ser el titular ante el cajero automático de la entidad bancaria para obtener fondos sin el consentimiento del titular de la cuenta. Sería el caso de estafas en los cajeros automáticos, un supuesto muy frecuente. La mejor manera de definir el término de artificio es como toda actuación que no entraría dentro del término manipulación informática.

Para terminar de entender a qué nos referimos con manipulación no tenemos más que observar los casos ya explicados anteriormente como el phising, pharming, Spyware, etc. Cualquier manipulación en el sistema informático o en los medios materiales del ordenador u otro tipo de máquinas se podría englobar en esta definición[29].

Transferencia de activo patrimonial:

Una vez que el afectado ha caído en el error se produce un acto de disposición patrimonial en beneficio del sujeto activo y en perjuicio de la víctima. Pero es la propia víctima quien lo realiza; esto es muy importante y lo que diferencia el delito de estafa de otros tipos penales. Si fuese el agente estaríamos ante otro delito como podría ser administración desleal. Por acto de disposición patrimonial podemos tomar la definición de MATA Y MARTÍN, sería "*en la entrega de una cosa (material o dineraria), en la realización de un acto documental con transcendencia económica (gravamen de un bien) o en la presentación de cualquier tipo de servicio, todo ello siempre cuantificable económicamente*". Lo fundamental es que sea cuantificable económicamente, para determinar si realmente podemos englobarlo dentro del delito de estafa.

Como dije antes, es fundamental que sea el propio perjudicado quien realiza el acto de disposición patrimonial. En caso contrario podríamos estar ante supuestos de administración desleal, en estos casos lo que hay es la defraudación de una relación de confianza, podríamos encuadrarlo en el art. 295 del Código Penal sobre delitos societarios. Si existe entre el poderdante y el apoderado un vínculo societario. En este sentido se

[29] ARROYO DE LAS HERAS, A. *Los delitos de estafa y falsedad documental*. Barcelona: Editorial Bosch, 2005, op. cit. pág. 69

asemeja al fraude informático; en el sentido de que no se dan todos los elementos de la estafa de manera clara, pero en la estafa informática es indudable que el acto de disposición patrimonial lo realiza de algún modo la víctima.

Otros casos que son interesantes son los de estafa triangular, pero no son como los supuestos de administración desleal citados; aquí el acto de disposición patrimonial no lo realiza el sujeto activo, pero tampoco lo realiza la víctima propiamente dicha, sino que lo llevaría a cabo otra persona que podría pasar a ser otro sujeto pasivo. El objetivo de este tipo de estafas es engañar a la víctima y a quien tiene el poder, previamente otorgado por el primer perjudicado[30].

Perjuicio:

Los efectos del engaño y el acto de disposición patrimonial se traducen en un perjuicio causado a una víctima, que puede ser el sujeto objeto del engaño o un tercero, por tanto el perjuicio puede ser propio o ajeno. Lo fundamental es que el perjuicio debe ser cuantificable económicamente. El Tribunal Supremo estudió el tema de las estafas en los siguientes supuestos; consistentes en que el agente se hace pasar por personal autorizado para revisar las instalaciones de gas, cobrándoles la correspondiente suma de dinero. El perjuicio a los supuestos clientes es claro y debería indemnizárseles como correspondiese, pero la sala entiende que las verdaderas empresas autorizadas para este tipo de revisiones no deben ser objeto de ninguna reparación y por tanto no han sufrido un verdadero perjuicio. Queda claro que el perjuicio patrimonial sería un saldo negativo en las cuentas del perjudicado. Debe ser clara la pérdida, para poder determinarse que posteriormente a la ejecución de la estafa el patrimonio de la víctima disminuyó[31].

[30] ARROYO DE LAS HERAS, A. *Los delitos de estafa y falsedad documental*. Barcelona: Editorial Bosch, 2005, op. cit. pág. 74.
[31] Sentencia del Tribunal Supremo del 31 de octubre del 2002.

Para entender la existencia del perjuicio no podemos fijarnos únicamente en el balance negativo del patrimonio del afectado, sino que el perjuicio debe ser real, efectivo y evaluable económicamente; son las notas esenciales que debemos tener en cuenta[32].

Se podría dar el siguiente problema; no poder concretar el perjuicio en el momento en que el juzgador deba pronunciarse sobre la existencia o no del delito. Pero para que pueda determinarse si hubo perjuicio es suficiente con que se fijaran las bases para su posterior determinación. Es importante señalar que no estamos hablando de un perjuicio hipotético, sino de un perjuicio cuya concreción no pudo realizarse por motivos puramente técnicos[33].

4.- Subsunción de las conductas descritas en los tipos penales analizados

En este apartado vamos a estudiar aquellos supuestos cuya inclusión en la figura de estafa informática del art. 248.2 CP, no está muy clara o puede dar lugar a dudas.

4.1-Subsunción de las conductas fraudulentas en los modelos de estafa común o estafa informática:

Un aspecto esencial es saber qué conductas pueden subsumirse en algún modelo de la estafa penal descrita en el Código Penal, ya sea la estafa común o la estafa informática[34].Ya dijimos anteriormente los elementos básicos del tipo penal de la estafa, engaño, error esencial, acto de disposición patrimonial, perjuicio, ánimo de lucro y nexo

[32] Como dice el Tribunal Supremo, Sala Segunda de lo Penal, en su sentencia de 21 de julio de 2006 "*El perjuicio en el delito de estafa no se contrae sólo a la determinación comparativa del patrimonio con anterioridad y posterioridad al hecho delictivo, sino que se hace preciso atender al acto dispositivo concretamente realizado y al aspecto patrimonial afectado en el hecho, de manera que el perjuicio debe ser real, efectivo y evaluable económicamente, esto es una disminución patrimonial lesiva al perjudicado*".

[33] ARROYO DE LAS HERAS, A. *Los delitos de estafa y falsedad documental*. Barcelona: Editorial Bosch, 2005, op. cit. pág. 75

[34] FERNÁNDEZ TERUELO, J. G., Cibercrimen, los delitos cometidos a través de Internet, Oviedo, Constitutio Criminalis Carolina, 2007. op.cit. Pág. 44.

causal. De estos el engaño y el error son los elementos nucleares de la estafa. La problemática radica en aquellos casos que no pueden englobarse dentro del tipo básico de la estafa por la inexistencia de algún requisito, especialmente alguno de estos dos elementos centrales. Casos como el envío de mensajes fraudulentos mediante mails, en donde se engaña a la víctima, entra dentro del tipo básico de estafa del art. 248.1 CP; o compraventas realizadas a través de internet, en las que el comprador no recibe lo pactado, o percibe un producto defectuoso. En estos casos si se dan todos los elementos de la estafa se englobarían en el tipo penal y no supondría mayor problema.

Pero en los supuestos donde no están presentes los elementos nucleares del engaño y error es cuando debemos estudiar y determinar si son susceptibles de subsunción. Comentamos al principio del presente trabajo casos de spyware, en supuestos en los que no hay un mensaje directo a la víctima sino que mediante un programa el defraudador puede beneficiarse patrimonialmente en perjuicio de la víctima, o hacer desaparecer deudas que previamente tuviera[35]; el engaño y error no puede producirse como tal. Otros supuestos donde no se da el engaño ni error son los casos de phising. Ya dijimos que mediante este sistema el defraudador manda un mensaje a un grupo de víctimas sin especificar, al no haber muchos de ellos identificados entra en juego la figura del "*sujeto pasivo masa*" del art. 74.2 CP.[36]. Ese correo sirve para que la víctima haga constatar datos personales, claves u otros datos sensibles, una vez el defraudador posee esa información no necesita ponerse más en contacto con su víctima. Aquí tampoco hay una comunicación al uso entre víctima y estafador, sino que más bien pretende conseguir unos datos sensibles de una generalidad de sujetos. Una vez los ha obtenido ya puede beneficiarse de ellos y la comunicación es innecesaria[37]. Tampoco hay error y engaño propiamente dichos, pero siempre existe un ánimo de lucro ya que el defraudador pretende beneficiarse patrimonialmente, aunque el error no siempre se dé en estos supuestos, el ánimo de lucro es una constante[38].

[35] AP Barcelona, Sección 10ª, S de 29 de Octubre de 2010.
[36] FARALDO CABANA, P. *Las nuevas tecnologías en los delitos contra el patrimonio*, Tirant lo Blanch, Valencia, 2009, op. cit. Pág.91.
[37] AP Valencia, Sección 3ª, S de 31 de Julio de 2012.
[38] MATA Y MARTÍN, R.M. Algunas consideraciones sobre informática y Derecho penal. El caso de la estafa informática, en Documentos Penales y Criminológicos, vol. 1, 2001, pág.48 y ss.

Por este tipo de casos es por lo que se creó la figura recogida en el art. 248.2 CP, de la denominada estafa informática, para englobar supuestos donde el error y engaño no estuvieran presentes o fuera más que discutible su presencia; no es algo que haya nacido con las nuevas tecnologías, sino que siempre hubo supuestos que se salían del modelo general del delito de estafa. Dice el art. 248.2 CP "*También serán considerados reos de estafa los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro*". El verdadero origen de este epígrafe en el art. 248 CP era el de sancionar a las entidades bancarias, en las que un tercero o empleado del banco operaba sobre ellas y realizaba transferencias a su favor en perjuicio de la víctima.

Por tanto nos encontramos con supuestos que no cumplen los requisitos de la estafa común. El engaño y error no están presentes o son de un modo indirecto, no hay una persona que sufre el engaño ni artimañas encaminadas a hacerle caer en error. La acción del defraudador se origina frente a un ordenador u otra máquina, como puede ser un cajero automático o terminal bancaria, por propia definición no se puede engañar o hacer caer en error a una máquina ya que no dispone de personalidad, como sí posee una persona[39]. Otro aspecto que lo diferencia de la estafa común es que la transferencia de los activos patrimoniales no la hace la víctima del engaño, sino el propio autor a través del sistema[40].

Los términos manipulación informática o artificio semejante del art. 248.2 CP, puede plantear alguna dificultad a la hora de contemplar cada caso. La transferencia no consentida de cualquier activo patrimonial en perjuicio de otro no supone mayor problema, siempre que exista esa transferencia se cumpliría con el requisito. La definición de manipulación informática aparece en variada jurisprudencia[41]; podría entenderse como cualquier método que consista en la alteración de los elementos físicos necesarios para la programación de la máquina, o introducción de datos falsos, con el fin de obtener la

[39] FARALDO CABANA, P. *Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática*, en Eguzkilore, núm. 21, diciembre 2007, pág. 37 y ss.
[40] FARALDO CABANA, P. *Las nuevas tecnologías en los delitos contra el patrimonio*, Tirant lo Blanch, Valencia, 2009, op. cit. Pág. 86.
[41] TS, Sala Segunda, de lo Penal, S de 30 de Mayo de 2009, TS, Sala Segunda, de lo Penal, S de 11 de Mayo de 2011.

transferencia patrimonial. Pero en los supuestos donde se obtengan claves a través de spyware u otros métodos, o los casos ya explicados de phising, pueden plantear problemas ya que no siempre existe una alteración de elementos físicos, ni una introducción de datos falsos. Si por ejemplo el sujeto activo utilizó ilícitamente las claves de la víctima, no se dio ninguna manipulación. En estos casos el Tribunal Supremo amplió el concepto de manipulación informática; dice que utilizar sin la debida autorización o en forma contraria al deber un programa informático, supondría manipulación informática o artificio semejante, y sería igualmente una conducta ilícita[42]. Si el defraudador no tiene autorización para utilizar las claves, a mi modo de ver está actuando en forma contraria al deber, y sus actos serían constitutivos del delito de estafa.

4.2.- Utilización abusiva o no consentida de tarjetas de crédito en cajeros automáticos

Un supuesto muy típico es la utilización no consentida de tarjetas de crédito en cajeros automáticos de forma fraudulenta[43] [44], podríamos establecer tres grupos: 1-Acceso al cajero mediante la utilización no consentida de la tarjeta por un tercero. 2-Utilización abusiva del cajero por el titular de la tarjeta magnética. 3-Acceso al cajero mediante una tarjeta falseada o alterada. Este último es muy típico y consiste en copiar la banda magnética de una tarjeta de crédito para que el sujeto activo pueda sacar dinero de una cuenta bancaria que no es suya, perjudicando al titular de la cuenta[45]. En estos casos tampoco hay engaño como tal, puesto que la interacción es directa con el cajero automático, no con la víctima. Antes de introducir la figura de la estafa informática del art. 248.2 CP, estos supuestos se castigaban como robo con fuerza en las cosas con uso de llave falsa, lo

[42] STS de 21 de diciembre de 2004.
[43] LÓPEZ ORTEGA, J.S. Internet y Derecho Penal. Madrid: Consejo General del Poder Judicial, 2001, op.cit. pág. 338 y ss.
[44] GONZÁLEZ RUS, J.J. Protección penal de sistemas, elementos, datos, documentos y programas informáticos. En la Revista electrónica de ciencia penal y criminología. Nº1, 1999, op, cit, sin paginación.
[45] TS, Sala Segunda, de lo Penal, S de 9 de Mayo de 2007.

que no era muy correcto jurídicamente. Pero es un requisito indispensable que el cajero haya sido manipulado mediante algún medio informático o artificio semejante[46].

La complejidad de estos supuestos residía en la discusión de si es un delito de estafa, o por el contrario estamos ante un delito de robo o hurto[47] [48]. De hecho la anterior legislación al Código Penal de 1995, castigaba este tipo de delitos como robo o hurto al considerar las tarjetas de crédito como llaves falsas, en aplicación del art. 239 CP., pero posteriormente hubo discusión sobre la naturaleza de la tarjeta de crédito en este sentido. Con el Código Penal de 1995 se vino a zanjar el tema ya que la doctrina equiparó la tarjeta de crédito a la figura de llave falsa[49], aunque la doctrina científica no tiene este punto tan claro, autores como MATA Y MARTÍN considera que habrá que ver cada caso en particular, ya que no siempre pueden equipararse esas dos figuras. Es un tema complejo, pues otro punto que diferencia la jurisprudencia es cuando se han alterado los componentes de la banda magnética a cuando se ha modificado el sistema informático. En esos casos dice la jurisprudencia que la tarjeta constituye un soporte material, cuya alteración supone un acto distinto de las meras operaciones o manipulaciones informáticas para conseguir la transferencia no consentida, pudiendo considerarse incluso falsificación de moneda. Una

[46] TS, Sala Segunda, de lo Penal, S de 10 de Febrero de 2014, fundamento de derecho tercero "Por lo demás, tampoco es cierto que la conducta se pueda subsumir en una estafa ejecutada mediante artificio informático, dado que, en primer lugar, no consta en los hechos probados que esa segunda caja registradora estuviera manipulada por un procedimiento informático o artificio similar, sino que se trataba de una caja que simplemente no contaba con un mecanismo de emisión de tickets. Esto es lo que se desprende de los hechos probados de la sentencia, que no reseña nada relativo a la alteración o manipulación de un mecanismo informático o de un artificio semejante. Ni tampoco se da el supuesto que requiere el art. 249.2 a) del C. Penal de que a través de una manipulación se consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de la víctima. Pues aquí tal transferencia por medios informáticos no existió".

[47] JAVATO MARTÍN, A.M. *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago*. Artículo en la revista electrónica de ciencia penal y criminología. Edit.- Aranzadi.

[48] MATA Y MARTÍN, R.M.- JAVATO MARTÍN, A.M., Tratamiento jurídico- penal de los fraudes efectuados con tarjetas de pago: Doctrina y jurisprudencia, en Revista Aranzadi de Derecho y Nuevas Tecnologías, año 2009-2, núm. 20, pp. 37 y ss.

[49] TS, Sala Segunda, de lo Penal, S de 29 de Abril de 1999, fundamento de derecho primero "*La solución al debate suscitado en torno a la determinación jurisdiccional cuestionada toma partido por el criterio plasmado en el recurso y reforzado con la postura del Ministerio Público pues -una vez normativamente definidos conceptos (llaves falsas en el último párr. art. 239 CP 1995) y conductas (manipulación informática o artificio semejante en el art. 248.2.º de dicho Texto Legal)- consolida definitivamente su vigor la posición jurisprudencial (sentencias, entre otras, de 21 Ene. 1990, 8 May. 1992, 14 Mar. 1993, 8 Mar. 1994, 25 Abr. 1996, 29 Nov. 1997 y 22 Dic. 1998) que definía la utilización en la acción depredadora de una tarjeta magnética como un delito de robo por resultar equiparables dichas tarjetas a las llaves que, al ser ilícitamente obtenidas, se convierten en falsas y a las que se refieren los arts. 239 y 238.4.º del Texto Legal citado*".

cosa es, que se manipulen sistemas informáticos para defraudar; y otra completamente distinta, que se confeccione una tarjeta mediante la incorporación falsaria de datos de origen o producción informática; para con ella, posteriormente llevar a cabo actos fraudulentos. Diferencia que claramente ha de distinguir entre el contenido de la estafa denominada informática y la cometida mediante el empleo de una tarjeta con banda magnética previamente falsificada[50].

Pero la jurisprudencia es clara en este tema. Aunque pueda haber casos particulares que haya que estudiar en particular, el legislador ha equiparado la tarjeta de crédito con la figura de llave falsa del art. 239 CP. . Con lo que en la mayoría de estos supuestos estaremos ante un delito de robo.

4.3-Muleros:

Los muleros son personas necesarias en algunos de los presentes delitos[51]. En el phising hemos hablado que el objetivo es hacer creer a una persona que se le está mandando un correo para obtener datos sensibles, un caso típico es aquel que enlaza el phising y la figura de los muleros del siguiente modo. Se envía una oferta de trabajo aparentemente auténtica a una persona que no tiene porqué sospechar nada. Esa oferta es enviada mediante correo electrónico por una entidad supuestamente auténtica. Esta persona da sus datos y se convierten en el vehículo para realizar phising por parte de los estafadores. Una vez ha dado su número de cuenta bancaria o se ha creado una nueva cuenta con él como titular, la ficticia empresa le hace una transferencia a esa cuenta para que el mulero a su vez, envíe esa cantidad a otra cuenta, normalmente extranjera, a cambio de un porcentaje. El gran problema práctico de estos casos es saber si hubo dolo por parte del mulero, si realmente conocía lo que estaba sucediendo, demostrar la existencia de dolo por su parte es realmente complicado. Otro problema en este supuesto es distinguir si se ha

[50] TS, Sala Segunda, de lo Penal, S de 8 de Julio de 2002.
[51] VELASCO NÚÑEZ, E. Estafa informática y banda organizada, phising, pharming, smishing y "muleros". La Ley Penal, num. 49, mayo 2008. Pag. 1 y ss.

cometido un delito de estafa o de blanqueo de dinero, puesto que podríamos estar ante un concurso delictivo[52].

No hay una solución clara y desde luego es un tema controvertido en la jurisprudencia. Lo primero es delimitar dos momentos en este delito, el primero es cuando se está realizando el movimiento informático y estableciendo la red de cuentas bancarias. El segundo momento es cuando el dinero pasa de cuentas para generar beneficios fraudulentos. La primera fase sería más típica de un delito de fraude informático, mientras que la segunda correspondería al blanqueo de capitales[53].

5.-Tratamiento del Código Penal sobre los programas necesarios para cometer fraude (precursores):

Los precursores son los programas utilizados para cometer la estafa informática. Sin ellos no sería posible llevar a cabo dicha estafa. Debemos preguntarnos en qué medida se castigará a aquellos que aunque no cometan la estafa, sean quienes los diseñen, programen o faciliten. En este sentido nuestro ordenamiento se muestra bastante estricto, en el

[52] TS, Sala Segunda, de lo Penal, S de 25 de Octubre de 2012, en su fundamento de derecho segundo deja claro que no hay doctrina pacífica, y algunos juzgadores consideran que tiene mejor encaje en el Art. 298 CP. Como una modalidad de receptación "*Con carácter general, hechos de la naturaleza de los que hoy ocupan nuestra atención, en lo que tienen de operación concertada, con una estratégica distribución de roles para lograr un acto de despojo patrimonial mediante un engaño, valiéndose de terceros para poder extraer esos fondos sin suscitar sospechas en la entidad bancaria y, una vez obtenidos aquéllos, colocarlos en un país que asegure la impunidad del desapoderamiento, presentan las características que son propias del delito de estafa informática al que se refiere el art. 248.2 del CP . Así lo ha estimado la jurisprudencia de esta Sala, en sintonía con el entendimiento doctrinal mayoritario.*

3.- No faltan, sin embargo, autores que consideran que la intervención de lo que en el argot policial se denomina muleros - colaboradores como la acusada, captados mediante ofertas de teletrabajo y a los que se ofrece ganar un importante porcentaje sobre las cantidades evadidas- tiene mejor encaje en el art. 298 del CP , como una modalidad de receptación. Entienden que la colocación del dinero en países con los que no existen mecanismos jurídicos de cooperación judicial, forma parte ya de la fase de agotamiento del delito, de forma que la captación de éstos puede llegar a producirse cuando ya la estafa se habría cometido. De ahí que estaríamos en presencia de una participación postdelictiva o postconsumativa, con un evidente contenido lucrativo, notas definitorias del delito de receptación".

[53] En este sentido jurisprudencia como laAudiencia Provincial de Soria de 27 de febrero de 2012 dice en su fundamento de derecho segundo que "*la calificación jurídica de los hechos como integrantes de un delito de estafa informática, receptación o blanqueo de capitales, obligará a analizar en qué medida el dolo de ese tercero que hace posible el rendimiento del capital evadido, capta los elementos del tipo objetivo del delito de estafa*".

subapartado b) del apartado 2 del art. 248 del Código Penal, se dice que también se considerarán reos de estafa "*Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo*". De este modo se equipara a los autores de la estafa con los programadores y facilitadores de los mismos, incluso poseer uno de esos programas supone ser castigado con la correspondiente pena.

No obstante en la práctica deberemos ir caso por caso y atender a que se cumpla el ánimo de lucro del tipo básico. Lo que realmente sucede es que a la hora de la verdad, quien posee algún artificio de estas características lo ha utilizado, y su posesión sirve para reafirmar su culpabilidad.

Podemos preguntarnos si el hecho de que un programa esté colgado en la red puede suponer un atenuante o incluso un eximente, la respuesta debe ser un rotundo no[54]. Entre los programas típicos son los ya comentados anteriormente, como los keyloggers, scarewares o troyanos.

6.-Conclusiones:

El fraude informático aparece regulada en el apartado a) del art. 248.2 del Código Penal; dice que serán considerados como reos de estafa: "*Los que, con ánimo de lucro y*

[54] Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, S de 9 de Mayo de 2006 "muchos contenidos de internet son, o pueden ser, delictivos, en sus variadas formas de criminalidad por la que se accede a la red, y no por ello dejan de constituir delitos. Por ejemplo, un programa informático para fabricar billetes de curso legal, eventualmente "colgado" en la red, no produciría la impunidad de la conducta de acceder a él, y "fabricar" moneda en papel falsa. Otro ejemplo: un programa para copiar discos legales a gran escala, no dejará de ser un posible instrumento de un delito contra la propiedad intelectual, si se expenden después con ánimo de lucro los discos copiados mediante ese sistema, por más que se encuentre gratuitamente "colgado" en la red. También alega que las entidades emisoras de tarjetas de crédito, como VISA, pueden neutralizar técnicamente sus tarjetas ante la existencia de estos programas informáticos. Cierto. Pero ello no producirá la impunidad delictiva de quien, utilizándolos, fabrique tarjetas falsas para introducirlas en el tráfico jurídico y engañar así a los productores de bienes o suministradores de servicios, utilizando tales tarjetas para pagar por esos medios los productos o servicios adquiridos. El engaño típico en el delito de estafa es aquel que genera un riesgo jurídicamente desaprobado para el bien jurídico tutelado y concretamente el idóneo para provocar el error determinante del desplazamiento patrimonial que se persigue por el autor del delito. En suma, no puede desplazarse sobre el sujeto pasivo del delito de estafa la falta de resortes protectores autodefensivos, cuando el engaño es suficiente para provocar un error determinante en aquél".

valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro". Con este apartado el legislador pretende englobar aquellas conductas que no pueden enmarcarse en el tipo penal de la estafa común, por faltar alguno de sus elementos esenciales. Estos elementos son los siguientes: 1º.- Engaño. 2º.- Error. 3º.- Acto de disposición patrimonial por parte del sujeto activo. 4º.-Perjuicio en la víctima. 5º.- Ánimo de lucro. 6º.- Nexo causal.

Un elemento clave y diferenciador en el fraude informático, es que la trasmisión patrimonial no la lleva a cabo la víctima siendo engañada, sino que es el propio sujeto activo quien a través de artificios tecnológicos y medios informáticos consigue llevar a cabo tal acción. Sin que pueda llegar a existir una fase previa de engaño como sí sucede en la estafa convencional. En estos supuestos que no cumplen los requisitos de la estafa común, el engaño y error no están presentes o si lo están es de un modo indirecto, no hay una persona que sufra el engaño ni artimañas encaminadas a hacerle caer en el error. La acción del defraudador se origina frente a un ordenador u otra máquina, como puede ser un cajero automático o terminal bancaria. Al no haber una persona para decidir y pensar que sea engañada; nunca pueden darse los elementos nucleares del tipo penal de estafa común. Por propia definición no se puede engañar o hacer caer en error a una máquina, ya que no dispone de personalidad. Puesto que una máquina no tiene capacidad intelectual, cognoscitiva ni volitiva

La estafa informática se engloba en el art. 248.2 CP, pero en su origen no se pensaba para nada en los ordenadores y fraudes cometidos a través de ellos. El objetivo en origen era sancionar conductas fraudulentas en las entidades bancarias, donde empleados o terceros podían operar sobre las terminales de pago y realizar transferencias bancarias a su favor. El problema es que no se producía un engaño o error como tales, como ya dijimos a una máquina no se la puede engañar. La idea para combatir los fraudes a través de cajeros pudo trasladarse a los supuestos en que se utilizaban medios informáticos para estafar. Además al perjudicado no podría darle tiempo a ser engañado, puesto que el fraude se produce cuando el autor manipula el sistema y no después. Es decir; el momento de

perpetración es cuando la manipulación del sistema es efectivo, en ese momento no existe ningún engaño, no puede haberlo ante un ordenador.

Algunos fraudes informáticos que no encajan en el tipo de estafa común son los de spyware o los de phising. En ambos supuestos no se da la típica relación de engaño; en el primer caso se instala un programa malicioso en el ordenador de la víctima, sin que ésta pueda ni siquiera sospechar lo sucedido, para posteriormente causarle un perjuicio. En los casos de phising sí hay un pequeño engaño inicial, al incitar a la persona estafada a dar sus claves personales, pero una vez obtenidos los datos sensibles no es necesario más contacto entre ambos. En esa segunda fase no existe engaño ni error como tal que motive alguna variación en el patrimonio del perjudicado.

Dentro de este tipo de delitos tienen especial relevancia los de spyware, phising, scam y Auction Fraud. Los programas Spyware sirven para que el sujeto activo pueda sustraer datos del ordenador de la víctima con diversos fines, el fin suele ser acceder a cuentas bancarias. En líneas generales, la estafa mediante estos programas consiste en sustraer unos datos que permitan la suplantación de personalidad del perjudicado, con esos datos el estafador puede beneficiarse económicamente y disponer de varias ventajas de índole patrimonial, obtenidas de modo ilícito. El término phising engloba las conductas en las que el sujeto activo trata de engañar a la víctima para obtener datos sensibles, haciéndole creer que está teniendo lugar una comunicación oficial con otra parte libre de toda sospecha; cuando realmente es un ataque contra su seguridad para obtener datos sensibles, como códigos de tarjetas de crédito y acceso a cuenta bancaria. El estafador; conocido como "*phisher*", envía a numerosas personas correos electrónicos masivos en los que se hace pasar por una empresa de confianza (por ejemplo, una entidad bancaria, o una compañía telefónica, etc). Otras veces lo hace mediante la creación de páginas "web" que imitan la página original de esa entidad bancaria o empresa de reconocido prestigio en el mercado. En ocasiones también se realiza por medio de llamadas telefónicas masivas, realizadas a numerosos usuarios en las que se simula ser un empleado u operador de esa empresa de confianza. El scam deriva del phising, consistente en enviar un correo electrónico denominado scam a la víctima. No es más que el típico fraude en donde se

busca que el receptor del correo realice algún acto para beneficiar a quien envía el mensaje, podemos asimilarlo al "*timo de la estampita*" o de las "*cartas nigerianas*"; se busca explotar el ánimo de lucro de la víctima. Los sistemas técnicos han evolucionado y las nuevas tecnologías son un aspecto muy importante en este tipo de delitos, pero el factor humano, concretamente su vulnerabilidad, sigue siendo el eslabón fundamental del que se sirven los estafadores. Realmente aquí no se necesitan grandes alardes informáticos ni programas especiales, simplemente es el "*timo de la estampita*" adaptado a las nuevas tecnologías, y se hace con un correo electrónico lo que podría hacerse con una carta postal. Los scammers, son los sujetos activos de este tipo de delitos; para no venir a España y agotar su actividad delictiva, transfieren el dinero apropiado sin consentimiento a cuentas de colaboradores situados en España: los muleros. Por último hay que mencionar los casos de Auction Fraud; es un fenómeno muy de moda en la actualidad con el auge de páginas de subastas por internet como puede ser Ebay, el método empleado por los estafadores consiste en tergiversar sobre la puja de un producto en internet, o su no entrega de acuerdo a lo pactado en el sistema de subastas de Ebay u otras plataformas similares.

Debemos mencionar aquellos elementos que son necesarios para cometer este tipo de delitos. Por un lado los programas necesarios para llevar a cabo el fraude se denominan precursores. Sin ellos no sería posible llevar a cabo la estafa. Debemos preguntarnos en qué medida se castigará a aquellos que aunque no cometan la estafa, sean quienes los diseñen, programen o faciliten. De acuerdo al subapartado b) del apartado 2 del art. 248 del Código Penal, serán considerados como reos de estafa los que programen, diseñen o faciliten ese tipo de programas. El hecho de que se encuentren disponibles en internet de manera libre no supone ningún tipo de eximente o atenuante. También debemos señalar las personas sin cuya colaboración no podría efectuarse el fraude, conocidos como muleros. El caso más claro es en el de phising; se envía una oferta de trabajo aparentemente auténtica a una persona que no tiene porqué sospechar nada, esa oferta es enviada mediante correo electrónico por una entidad aparentemente auténtica, esta persona da sus datos y se convierten en el vehículo para realizar phising por parte de los estafadores, una vez ha dado su número de cuenta bancaria o se ha creado una nueva cuenta con él como titular, la ficticia empresa le hace una transferencia a esa cuenta para que el mulero a su vez, envíe

esa cantidad a otra cuenta, normalmente extranjera, a cambio de un porcentaje. El gran problema práctico de estos casos es saber si hubo dolo por parte del mulero, si realmente conocía lo que estaba sucediendo, demostrar la existencia de dolo por su parte es realmente complicado, y habrá que atender a cada caso pues la doctrina no es pacífica.

Para terminar, mi opinión acerca de este tipo de delitos es que actualmente son una realidad incontestable. Los ordenadores se han establecido como una herramienta habitual, y es algo que también aprovechan los delincuentes. A mi modo de ver en nuestro Código Penal se solventa la inexistencia del engaño y el error de una manera satisfactoria, con el apartado a) del art. 248.2 CP. se resuelve esa ausencia. De esta forma el legislador da cabida en el ordenamiento a las estafas cometidas mediante ordenadores o a través de internet.

7.- BIBLIOGRAFÍA Y MATERIALES DE REFERENCIA:

7.1.- BIBLIOGRAFÍA:

- FARALDO CABANA, P. *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*. Valencia: Editorial Tirant Lo Blanch, 2009.

- FARALDO CABANA, P. *Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática*, en Eguzkilore, núm. 21, diciembre 2007. Pág. 33-57.

- MATA Y MARTÍN, R.M. *Delincuencia informática y derecho penal*. Nicaragua: Editorial Hispamer, 2003.

- MATA Y MARTÍN, R.M. *Algunas consideraciones sobre informática y Derecho penal. El caso de la estafa informática*, en Documentos Penales y Criminológicos, vol. 1, 2001.

- JAVATO MARTÍN, A.M. *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago*. Thomson-Aranzadi, Cizur Menor, 2007, pp. 45-49.

- MATA Y MARTÍN, R.M.- JAVATO MARTÍN, A.M., *Tratamiento jurídico- penal de los fraudes efectuados con tarjetas de pago: Doctrina y jurisprudencia*, en Revista Aranzadi de Derecho y Nuevas Tecnologías, año 2009-2, núm. 20. Pág. 37 a 53.

- FERNÁNDEZ TERUELO, J.G. *Cibercrimen, los delitos cometidos a través de Internet*. Oviedo: Editorial Constitutio Criminalis Carolina, 2007.

- ROMEO CASABONA, C.M. y FLORES MENDOZ, F. *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica.* Granada: Editorial Comares, 2013.

- LÓPEZ ORTEGA, J.J. *Internet y Derecho Penal.* Madrid: Consejo General del Poder Judicial, 2001.

- MIRÓ LLINARES, F. *El Cibercrimen, fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Editorial Marcial Pons, 2012.

- MIRÓ LLINARES, F. *La Respuesta Penal al Ciberfraude*. Revista Electrónica de Ciencia Penal y Criminología. Pág. 1-56.

- MIRÓ LLINARES, F.: *La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del*

cibercrimen, en Revista Electrónica de Ciencia Penal y Crminología, 13-07/2011. Pág. 1-55.

- PONS. M. *El Cibercrimen* Madrid/Barcelona/Buenos Aires/ São Paulo, 2012.

- ARROYO DE LAS HERAS, A. *Los delitos de estafa y falsedad documental*. Barcelona: Editorial Bosch, 2005.

- CONDE PUMPIDO FERREIRO, C. *Estafas*. Valencia: Editorial Tirant Lo Blanch, 1997.

- VELASCO NÚÑEZ, E. *Estafa informática y banda organizada. Phising, pharming, Smashing y muleros.* En La ley penal: revista de derecho penal, procesal y penitenciario, Nº49, 2008. Disponible en Westlaw.

- CALLE RODRÍGUEZ, M.V. *El delito de estafa informática*. En La ley penal: revista de derecho penal, procesal y penitenciario, nº37, 2007. Disponible en Westlaw.

- HERRERO HERRERO, C. *El concepto penal de estafa en el Código Penal vigente*. En La ley penal: revista de derecho penal, procesal y penitenciario, nº33, 2006. Disponible en Westlaw.

- GONZÁLEZ RUS, J.J. *Protección penal de sistemas, elementos, datos, documentos y programas informáticos*. En la Revista electrónica de ciencia penal y criminología. Nº1, 1999.

- GUTIÉRREZ FRANCÉS, M.L., *Fraude Informático y Estafa*, Ministerio de Justicia, Centro de Publicaciones Madrid, 1991.

- CHOCLÁN MONTALVO, J. A.: *Fraude informático y estafa por computación*, en Cuadernos de Derecho Judicial, núm. 10, 2001. Pág. 305-352.

7.2. MATERIALES DE REFERENCIA.

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

- Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, que se aprobó el 20 de septiembre de 2013.

- 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

- Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal.

- Directiva 98/84/CE del Parlamento Europeo y del Consejo de 20 de noviembre de 1998, relativa a la protección jurídica de los servicios de acceso condicional o basado en dicho acceso.

- Resolución de 28 de octubre de 2005, de la Secretaría de Estado de Justicia, por la que se dispone la publicación del Acuerdo de Consejo de Ministros de 21 de octubre de 2005, por el que se aprueba el Plan de Transparencia Judicial.

- Buscador de Jurisprudencia de Consejo General de la Abogacía (CENDOJ).

- Páginas web de Noticias Jurídicas y Westlaw.