FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS DE ELCHE
GRADO EN DERECHO ||| ÁREA DE DERECHO PENAL

RESPONSABILIDAD PENAL DE LOS MULEROS DEL PHISHING

TRABAJO DE FIN DE GRADO

UNIVERSIDAD MIGUEL HERNÁNDEZ DE ELCHE
CURSO 2014/2015

PROFESORA:	**ELENA BEATRIZ FERNÁNDEZ CASTEJÓN**
ALUMNA:	**ISABEL SAPENA GILABERT**

RESUMEN

El fraude en la banca electrónica es un delito cada vez más común en nuestra sociedad. Con el desarrollo de los sistemas informáticos y con la nueva era de Internet a la vez que avanzamos en la comunicación entre las personas mundialmente y en los negocios con solo un "clic", también se crea un nuevo ámbito de actuación para los delitos. Este nuevo mundo cibernético presenta muchas dificultades legales, no sólo porque es novedoso para nuestros tribunales sino porque también en estas circunstancias la tarea de limitar las conductas de miles de usuarios y de miles de actuaciones resulta muy compleja. Este es el motivo principal que fundamenta la realización del presente trabajo. Mediante el análisis del *phishing* se pretende dar respuesta a la responsabilidad penal de este tipo de conductas. Pero sobre todo se pretende aportar una idea global de los distintos problemas que surgen en el mundo cibernético y entre estos problemas, destacar la posible responsabilidad penal de un sujeto que participa en alguna las fases de la dinámica del *phishing*.

ÍNDICE

INTRODUCCIÓN **6**

CAPÍTULO I: EL FENÓMENO DEL CIBERFRAUDE **7**

CAPÍTULO II: DEL CONCEPTO DE CIBERDELITO A CIBERFRAUDE **9**

CAPÍTULO III: MODALIDADES DE CIBERFRAUDES **10**

1.- FRAUDES TRADICIONALES QUE AMPLIAN SU ÁMBITO DE ACTUACIÓN A INTERNET. 11

1.1 Fraudes de tarjetas de crédito 11

1.2 Fraudes de cheques 13

1.3 Estafas de inversión 14

2.- FRAUDES PRODUCIDOS EXCLUSIVAMENTE POR INTERNET 16

2.1 Envíos de correos electrónicos denominados *spam* 16

2.2 *Spyware* o *malware* 17

2.3 *Phishing* y *pharming*. 18

CAPÍTULO IV: DINÁMICA DEL *PHISHING* **19**

1.- CONCEPTO Y DINÁMICA DEL *PHISHING*. 19

2.- SUJETOS INTERVINIENTES Y FUNCIONES 21

3.- TIPOS DE *PHISHING* 23

3.1*Phishing* engañoso o *Deceptive Phishing* 23

3.2*Phishing* basado en *software* malicioso o *malware based phishing* 25

3.3*Phishing* basado en el DNS o *pharming* 26

3.4 *Phishing* mediante introducción de contenidos o *Content-Injection phishing* 26

3.5 *Phishing* mediante la técnica del intermediario o *Man-in- the middle* y *phishing* de motor de búsqueda. 27

CAPÍTULO V: RESPONSABILIDAD PENAL DEL CIBERFRAUDE. ESPECIAL REFERENCIA AL *PHISHING*. 28

CAPÍTULO VI: CALIFICACIÓN JURÍDICA DEL *PHISHING*.....29

1.-SANCIÓN DE LOS ACTOS PREPARATORIOS DEL *PHISHING*.....29

1.1. *Spoofing* 30

1.2 Acceso informático ilícito 32

1.3 Fabricación, introducción, posesión o facilitación de programas de ordenador 33

2 PROBLEMÁTICA EN LA CALIFICACIÓN JURÍDICA DEL *PHISHING*. 34

2.1 La Estafa en relación con el *phishing* 35

2.2. La Estafa Informática y el *phishing* 39

CAPÍTULO VII: RESPONSABILIDAD PENAL DE LOS MULEROS DEL *PHISHING*. 46

CAPÍTULO VIII: TIPOS PENALES SUSCEPTIBLES DE SANCIONAR LA CONDUCTA DEL CIBERMULERO. 48

1.- RECEPTACIÓN.....49

2 BLANQUEO DE CAPITALES.....51

3 ESTAFA INFORMÁTICA 55

CAPÍTULO IX: LA PROBLEMÁTICA DE LA IGNORANCIA DELIBERADA Y SU DESARROLLO JURISPRUDENCIAL PARA DAR RESPUESTA A LA CONDUCTA DE LOS CIBERMULEROS..... 58

CAPÍTULO X: CONCLUSIONES FINALES.....65

ABREVIATURAS

AEAT	Agencia Estatal de Administración Tributaria
AP	Audiencia Provincial
CD	CD-ROM: Compact Disc Read-Only Memory
CP	Código Penal
CSS/ XSS	Cross-site scripting
DNS	Demain Name Server
INTECO	Instituto Nacional de Tecnologías de la Comunicación
IP	Internet Protocol
JAI	Justicia y asuntos de Interior
LO	Ley Orgánica
RJ	Repertorio de Jurisprudencia
SAP	Sentencia de la audiencia provincial
SMS	Short Message Service
SQL	StructuRed Query Language
STS	Sentencia del Tribunal Supremo
TIC	Tecnologías de la información y de la comunicación
URL	Uniform Resource Locator
VoIp	Voice over IP

INTRODUCCIÓN

Los delitos informáticos son los nuevos crímenes del siglo XXI. Las nuevas tecnologías y sobre todo Internet evolucionan y se desarrollan a pasos agigantados causando en la legislación problemas de adaptación e interpretación en el ámbito de las nuevas conductas irregulares que derivan del uso de la informática. Los problemas se ven reflejados, mayoritariamente, en los fraudes cometidos a través de Internet sobre todo en la banca electrónica. Los delitos tradicionales tienen su metodología y su respuesta en nuestro código penal. Las respuestas son claras y concisas sin lugar a dudas ni a lagunas legales. Pero las nuevas tecnologías y el uso de la informática traen consigo un nuevo ámbito de actuación, que nada que ver tiene con el mundo físico y prácticamente desconocido para el legislador: el mundo cibernético.

Es decir, que un fraude o la disposición de patrimonio ajeno puede realizarse bien físicamente cuando te ofrecen un cheque a cambio de una determinada mercancía y el cheque resulta ser falso o bien, introduciéndose en nuestro sistema informático para obtener los datos necesarios para posteriormente vía electrónica apoderarse del dinero de nuestra cuenta corriente. Parece ser que los delitos tradicionales de estafa han encontrado un nuevo hábitat en el que desarrollarse.

Hay que añadir que además del desarrollo de las TIC, la situación de crisis económica empeora la situación. Las personas pierden su trabajo y a pesar de su constante búsqueda, no encuentran. Esta circunstancia lleva a mucha gente a optar por conseguir dinero fácil por Internet, y a pesar de la extrañeza de las ofertas que se encuentran, la situación de estas personas es tan difícil que no se detienen ni por un segundo a pensar en la legalidad de estos ofrecimientos. Sancionar las nuevas conductas y responsabilizar tanto a los autores como a los partícipes de este tipo de actuaciones es, por tanto, el nuevo reto para nuestro ordenamiento jurídico.

Por consiguiente, debemos hacernos la siguiente pregunta: ¿Cómo se responde penalmente al ciberfraude? Esta es la pregunta que puede resolver el problema y que vamos a analizar en este trabajo. En el primer capítulo se realizará una breve

introducción al fenómeno del ciberfraude. Seguidamente se expondrá un estudio sobre el Phishing explicando en qué consiste, por qué elementos está formado, quienes intervienen, los tipos, etc. Y en el tercer capítulo estudiaremos afondo el problema de la sanción de este fenómeno y de la responsabilidad del cibermulero, desde la perspectiva de la jurisprudencia y desde la doctrina, para acabar haciendo referencia a la ignorancia deliberada y los partícipes del Phishing. Finalmente se realizarán unas breves conclusiones.

CAPÍTULO I: EL FENÓMENO DEL CIBERFRAUDE

Los delitos informáticos son un hecho muy reciente en nuestra historia. Son conductas antijurídicas que aparecieron hace unas tres décadas aproximadamente y de las cuales se tiene poca información. Antes de empezar a fondo con los ciberfraudes, vamos a contextualizar este concepto dentro de los delitos informáticos y más concretamente dentro de los cibercrimenes.

Los delitos informáticos se definen como cualquier acción, típica, antijurídica, culpable y punible cometida a través de sistemas informáticos o de las TIC. A modo de ejemplo podemos decir que el ciberfraude, el sabotaje o daños informáticos, el *hacking*, el *spoofing*, la piratería informática, el ciberterrorismo o el ciberacoso, entre otros, forman parte de la definición de delito informático.

Como se ha mencionado en la introducción, la llegada de la era de la informática ha dado lugar a la creación de un nuevo ámbito para la realización de delitos. No solo estamos hablando de que los delitos tradicionales amplían su campo de batalla sino que además se crean nuevos delitos. Se trata de dos mundos totalmente paralelos y que nada tienen que ver uno con el otro: el mundo físico y el mundo virtual. En el mundo físico existen las leyes que regulan los comportamientos de las personas que vivimos en él, pero en el mundo virtual la legislación es escasa y limitar los comportamientos que en este mundo se den resulta una tarea complicada.

Con este razonamiento nos podemos plantear si en este nuevo mundo, en el que se crean nuevos delitos, se deberían proteger bienes jurídicos distintos de los vistos hasta ahora. ¿Qué hay de la llamada Seguridad Informática? Cuando hablamos de ciberdelitos, hacemos referencia a bienes jurídicos como el patrimonio, la intimidad, la propiedad intelectual, etc. Todos ellos son conocidos y se protegen de igual forma con los delitos tradicionales. Pero teniendo en cuenta la gran revolución de Internet el legislador se tendría que preguntar si la seguridad informática podría ser un nuevo bien jurídico a proteger. Internet y el mundo de la informática tienen unas características muy particulares, que hacen que la tarea de delimitar que conductas son o no sancionables, qué criterios se deben seguir para ello y los instrumentos para llevarlo a cabo sean muy complejos. Además de las grandes Redes de transmisión de datos, la multitud de usuarios de Internet, hacen más difícil esta tarea.

Por ello hay autores que discuten si la seguridad informática debería ser un nuevo bien jurídico protegido adaptado a estas nuevas conductas delictivas. "La seguridad informática se concibe como un bien jurídico colectivo que viene a dar protección anticipada a otros de naturaleza personal como la intimidad, el honor, el patrimonio, la libertad de información, el secreto y la inviolabilidad de las comunicaciones; aunque no siempre queda claro cuáles son efectivamente los derechos relacionados con ella"[1].

Extrayendo algunas ideas del autor J.G FERNÁNDEZ TERUELO[2], podemos observar desde otro punto de vista los problemas derivados del desarrollo de las TIC. La primera idea es: la aparición de Internet ha trastocado de forma muy importante el esquema tradicional de los delitos. Y la segunda idea (resaltamos esta idea como más importante en relación al estudio del *phishing*): la comisión delitos por Internet dificultan y traen mayores problemas a la hora de la detección y la persecución. El

[1] GONZÁLEZ RUS, Juan José, "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", en los Cuadernos Penales de José María Lidón, núm. 4, (2007), Págs. 13-40. También se pronuncia sobre el delito informático: ALONSO ROYANO, Fernando: "¿Estado de Derecho o derecho del Estado? El delito informático, en RGD, núm. 498, marzo, (1986), Págs. 602 y ss.

[2] FERNÁNDEZ TERUELO, Javier Gustavo, *Derecho Penal e Internet. Especial consideración a delitos que afectan a jóvenes y adolescentes*, Valladolid, Lex Nova, 2011, págs. 16-17.

anonimato, la escasa protección de los usuarios y el carácter transnacional de algunas conductas delictivas, hacen de los ciberfraudes, delitos en los que cada vez más se dificulta la atribución de responsabilidad penal a los verdaderos defraudadores.

Una vez contextualizado y visto qué problemas surgen del uso de la informática y de Internet, podemos hablar del término de ciberfraude como todos aquellos fraudes cometidos por Internet que mediante las Redes telemáticas consiguen un beneficio patrimonial a costa del perjuicio patrimonial de un tercero. El ejemplo más común de ciberfraude es el de la subasta por Internet. Se trata de subastas, normalmente por eBay, en las que se paga por un producto que resulta ser defectuoso o no llega nunca a su comprador. A pesar de ser el más común, en este trabajo nos vamos a centrar en los problemas del fraude en la banca electrónica, más comúnmente conocido como *phishing.*

CAPÍTULO II: DEL CONCEPTO DE CIBERDELITO A CIBERFRAUDE

Los delitos informáticos como bien hemos explicado en párrafos anteriores pueden afectar a todo tipo de bienes jurídicos como la intimidad, el honor, la indemnidad, la libertad sexual, el patrimonio, etc. Sin embargo, en el presente trabajo, nos vamos a centrar en los ciberdelitos que afectan al patrimonio, que se cometen en el ciberespacio y conllevan un perjuicio patrimonial para las víctimas: los Ciberfraudes.

Según el Instituto Nacional de Tecnologías de la Comunicación (INTECO)[3] el concepto de delito informático o ciberdelito sería el siguiente: cualquier tipo de conducta tipificada como delictiva para cuya comisión se utilizan tecnologías de información y /o comunicaciones. Como elementos de este tipo de delitos podemos

[3] INTECO: "Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como Phishing", en Internet: www.inteco.es, Octubre (2007).

señalar la transnacionalidad y la complejidad derivada de la profesionalización de las Redes organizadas de ciberdelincuentes.

Dentro de estas conductas delictivas nos encontramos con los delitos informáticos que atentan contra la propiedad entre los cuales se encuentra el fraude informático del que INTECO define según lo hace el Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia recoge en su artículo 8 el fraude informático, considerando dentro del mismo: *"* los actos deliberados e ilegítimos que causen un perjuicio patrimonial mediante una amplia gama de procedimientos (…) con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona*"*. Otra definición de cibercrimen económico o ciberfraude[4] podría ser la siguiente: cualquier ataque delictivo que afecte al patrimonio de las personas individuales o al sistema económico en relación con las transacciones comerciales en Internet. El mismo concepto hace referencia a cualquier ciberataque cuyo objetivo final sea la consecución de un beneficio económico, aunque afecte a otros bienes jurídicos como la intimidad, la seguridad de los sistemas y Redes, etc.

Nos vamos a centrar exclusivamente en los cibercrimenes económicos que afecten al patrimonio como bien jurídico protegido, y en aquellos cibercriminales que utilizan la Red y los sistemas conectados a ella para realizar las diferentes actividades delictivas, que principalmente tienen como fin el lucro económico en perjuicio siempre de un tercero. Más concretamente diremos, que nos vamos a centrar en el denominado *phishing*. Se trata de un ciberfraude que cada día afecta a más personas, y que en epígrafes posteriores procederemos a desarrollar detenidamente, tanto su definición como su responsabilidad penal.

CAPÍTULO III: MODALIDADES DE CIBERFRAUDES

[4] MIRÓ LLINARES, FERNANDO: "Cibercrímenes económicos y patrimoniales" en Ortiz de Urbina (COORD): *Memento Práctico Francis Lefebvre. Penal Económico y de la Empresa 2011-2012,* Santiago de Compostela, Francis Lefebvre 2011, pág. 469.

El Código Penal de 1995, en su artículo 248 indica que *"*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 párrafo 2 del mismo artículo se incluye una novedosa modalidad de estafa al entender que "también se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".

Existen numerosos tipos de ciberfraudes y son muy diversas sus clasificaciones. En este apartado vamos a explicar brevemente algunos de los más importantes clasificándolos en dos grandes grupos: por una parte aquellos que en su origen empezaron siendo fraudes tradicionales y que han evolucionado ampliando su ámbito de actuación a Internet, y por otra parte aquellos que única y exclusivamente se realizan por medio o sobre Internet

1.- FRAUDES TRADICIONALES QUE AMPLIAN SU ÁMBITO DE ACTUACIÓN A INTERNET.

1.1 Fraudes de tarjetas de crédito

En la sociedad de hoy en día es muy común (y cada vez más) utilizar como sistema de pago la tarjeta de crédito o débito por Internet. Esta forma de pago tiene numerosas ventajas como la facilidad, comodidad y rapidez en que se producen las diferentes transacciones comerciales. Pero a su vez, muchas personas son víctimas de estafas realizadas a través de estas tarjetas y se producen de muy diversas formas. Una de las formas más comunes es mediante el uso de páginas webs inseguras. Este fenómeno consiste en crear sitios webs, aparentemente auténticos, de venta de billetes inexistentes o de valor inferior al real, de entradas de conciertos falsas, espectáculos, eventos deportivos, etc. La víctima introduce los datos de su tarjeta de crédito, normalmente el número de la tarjeta y su fecha de caducidad, en la página web y seguidamente, o se produce un error en la página o el servicio solicitado nunca es

recibido por la víctima. Se trata entones de obtener una información específica de la tarjeta mientras se ofrecen bienes y servicios inexistentes[5]

Además de este tipo de fraude, existen numerosas conductas vinculadas con las tarjetas bancarias: falsificación de tarjeta bancaria, colocación de instrumentos electrónicos en cajeros automáticos que descifren los datos de tarjetas bancarias para su clonación, falsificación del documento que convierte al sujeto en titular de una tarjeta auténtica, falsificación de la firma que incorpora una tarjeta auténtica, uso ilícito de una tarjeta obtenida de forma legal, uso ilícito de una tarjeta falsificada, uso ilícito de una tarjeta ajena obtenida a través de un delito patrimonial, uso ilícito de una tarjeta obtenida a través de engaño realizado al emisor, etc.[6]

Para finalizar, podemos citar dos casos acontecidos en España: el primero de ellos producido entre Palma y Málaga. Una Red estafaba a sus clientes haciéndose pasar por una agencia de viajes con datos de contacto e identidades falsas. Adquirían el número de la tarjeta de crédito argumentando cualquier circunstancia y de esta forma efectuaban el fraude por Internet. *"*Los miembros de la Red, residentes en Rusia, Vietnam, Perú, Ecuador y Estados Unidos conseguían las numeraciones mediante técnicas de *phising* o *skimming*, por medio de ataques informáticos a empresas de comercio electrónico o a través de programas automáticos de generación de numeraciones. Después, revendían los productos a precios inferiores al valor de mercado. Para ello, se había instaurado una Red de contactos que asemejaban en su funcionamiento a una "auténtica agencia de viajes*". "* Esta noticia fue publicada por el periódico ABC el día 11/07/2013, en la página web del mismo.[7]

Otra noticia publicada en el periódico Cinco Días en su página web el día 13/04/2014 bajo el título de *"*1200 Estafas en fraude con tarjetas a través de Internet*".* *"*La Policía Nacional ha destapado más de 1.200 estafas mediante cargos fraudulentos en tarjetas bancarias a través de Internet. La Red usaba la página web de Loterías y

---

[5] Véase en Internet: www.muface.es/revista/P.190/report.htm.
Además en: www.consumidor.ftc.gov/articulos/s016-protejase-contra-el-fraude-con-tarjeta-decRedito.

[6] RAMÓN RUIZ, LUIS: "Uso ilícito y falsificación de tarjetas bancarias", en RIDP, Núm. 3 (2006)

[7] Véase el procedimiento en Internet: http://www.abc.es/espana/20130711/abci-estafas-tarjetas-cRedito-201307101717.html

Apuestas del Estado para cargar, a través de internet desde Redes wifi 'pirateadas', sin autorización de los titulares de las tarjetas, entre 90 y 180 euros que después desviaban a cuentas bancarias abiertas del grupo.*"*[8] Este caso parecido al anterior, se descubre que creaban "monederos virtuales" en la página web de Loterías y Apuestas del Estado. El dinero realmente se destinaba a una cuenta corriente creada por los estafadores y posteriormente retiraban el dinero en cajeros automáticos. Esta noticia sirve de ejemplo también para el caso de las estafas de loterías que se expondrán en párrafos posteriores

1.2 Fraudes de cheques[9]

Al igual que las tarjetas de crédito, los cheques bancarios o de caja son un medio de pago. Aunque no son tan comunes entre la población, también aquí se producen situaciones fraudulentas. Algunos ejemplos de estafas son: las estafas del cheque con sobrepago, estafas de subastas en Internet, las del comprador secreto o encubierto y las estafas de loterías y sorteos.[10]En este apartado nos vamos a prestar especial atención a aquellos fraudes que se relacionan con Internet como son: el cheque con sobre pago y las subastas en Internet.

El fraude se desarrolla de la siguiente manera: el estafador contacta con el vendedor respondiendo a un anuncio clasificado u oferta de subasta en la Web. Este último se compromete a pagarle en cheque de caja, empresa o personal por un precio por encima del precio de mercado del producto ofertado (los defraudadores argumentan cualquier excusa para utilizar este medio de pago, como por ejemplo que se trata de gastos de envío), de tal forma que el vendedor confía en su comprador y sigue las instrucciones de este último depositando la diferencia en el banco, como así le pidió el estafador. Pero una vez ha realizado esta transacción y cobrado el cheque, el banco tarda un par de días en darse cuenta de que el cheque está falsificado. Como consecuencia, el banco pide responsabilidades al vendedor, debiendo pagar este último

---

[8] En Internet: http://cincodias.com/cincodias/2014/04/13/mercados/1397383926_973859.html

[9] Un cheque de caja responde a la definición siguiente: "título-valor emitido por una entidad de crédito contra su cuenta corriente en otra entidad o en otra sucursal del mismo librador". Regulado en la Ley Cambiaria y del Cheque en su artículo 12.

[10] Véase el procedimiento en Internet: http://www.ic3.gov/crimeschemes.aspx#item-3

el valor total del cheque (el precio de mercado del producto más la suma adicional de dinero que el estafador propuso con cualquier excusa).

De manera adicional vamos a proceder a explicar sucintamente cómo funciona la estafa de loterías y sorteos y a que nos referimos con el comprador secreto o encubierto. La primera hace referencia a aquellos casos en los que la víctima recibe una carta anunciándole que ha sido la premiada de una lotería o sorteo extranjero. En la misma carta se acompaña un cheque. La supuesta ganadora o ganador se dispone a depositar el dinero en su banco y a cobrarlo. Cuando el banco al paso de los días se da cuenta de que es falso, la víctima será la responsable de devolver todo el dinero supuestamente ganado. En cambio el comprador encubierto o secreto es aquel que contratan para que evalúe la efectividad de un servicio de transferencia de dinero. A la víctima se le entrega un cheque que debe depositar en su cuenta corriente y seguidamente retirar el dinero en efectivo. Tras esta operación le indican que debe transferir ese dinero a otra cuenta (normalmente procedente de Canadá). Finalmente el consumidor debe evaluar la experiencia con este servicio, pero es algo que nunca llega a su fin porque el dinero ha sido transferido a los estafadores haciendo responsable a la víctima del engaño del cheque, que resulta ser falso. Como último dato, podemos decir que en las transferencia de dinero aparecen como empresas más comunes: MoneyGram y Western Union. [11]

1.3 Estafas de inversión

Denominadas en inglés ***invest fraud*** son aquellas mediante las cuales se ofrecen productos financieros, préstamos o similares, que resultan ser falsos. Son aquellas inversiones en las que el engaño recae sobre las características (riesgo y rentabilidad) de un producto de inversión, de manera que el inversor-víctima realiza la inversión sobre la base de informaciones falsas. [12] Otras estafas como los **fraudes de subastas** (*Auction Fraud*) son aquellas que consisten en la tergiversación de un producto o su no entrega conforme a lo pactado en los sistemas de subasta online tipo eBay. En general, la actividad relacionada con las subastas en Internet comprende una serie de acciones que requieren de la participación de los usuarios, así es necesario el registro de una cuenta,

[11] En Internet: http://www.consumidor.ftc.gov/articulos/s0159-cheques-falsos

[12] MIRÓ LLINARES, Fernando: "La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing", en RECPC 15-12 (2013)

la búsqueda de productos, la puja, ganar la puja, la transacción y finalmente informar sobre la reputación de los vendedores, cada una de las cuales puede ser objeto de fraude.[13]

Otra modalidad de estafa es la **estafa piramidal** o *ponzi frauds*. Son aquellas estafas de inversión en los que a los inversores se les prometen beneficios anormales que, en realidad, no son (cuando se cobran) más que las inversiones, falsas en realidad, de otros sujetos idénticamente engañados. Este tipo de mecanismo defraudatorio consiste en reclutar al mayor número de personas para conseguir unos beneficios que realmente provienen de otras personas igualmente engañadas. Existe en primer lugar un alto cargo directivo que se encuentra en la cúspide de la pirámide, con unos conocimientos de economía y finanzas elevados. Este sujeto pretende que el resto de gente que se encuentra en los niveles inferiores de este entramad, hagan publicidad de un producto o de la misma empresa a cambio de una suma importante de dinero. Se trata de publicitar por Internet la web de la supuesta empresa. Un trabajo muy fácil y que no requiere, en estos casos, ningún tipo de conocimientos en informática o finanzas.

Es necesario tener en cuenta que toda la gente que cae en las Redes de este tipo de empresas quedan condicionadas por dos elementos: el primero es una inversión inicial que puede variar entre los 211 y los 759 €, y el segundo elemento es que la persona contratada debe reclutar a más gente, es decir, debe ofrecer este tipo de trabajo a personas de su entorno, ya pueden ser familiares o amigos de confianza. Este tipo de empresas puede durar años e incluso épocas. Ya que se basan en un círculo vicioso que es muy poco probable que pare en algún momento. El reclutamiento de personas es constante en todo momento, por tanto aquellas personas que invirtieron en un principio pueden recuperar su dinero gracias a esas nuevas personas que se incorporan en este entramado. Siempre el creador de la empresa conseguirá beneficios de las aportaciones iniciales.

Existen tres grandes casos en el mundo que reflejan este tipo de estafas piramidales: el Caso Madoff, Caso Ponzi y TelexFree. Nosotros nos vamos a centrar en este último que es el que se realizó haciendo publicidad falsa por Internet. En el caso Telexfree, una empresa americana de publicidad llega en Julio de 2012 a España. Se

[13] Ibíd.

trata de un organismo multinivel que llegó a defraudar masivamente a alRededor de un millón de personas en todo el mundo. Esta empresa ofrecía a personas, normalmente desempleadas o inmigrantes, un trabajo consistente en hacer publicidad sobre un producto en Internet, de forma que apareciera en los términos más buscados en Google. A cambio de una suma de dinero elevada. Simplemente estas personas estaban condicionadas por dos aspectos: en primer lugar debían de realizar una primera inversión que oscilaba entre los 1400 y 1500 dólares, y posteriormente debían invertir más. En segundo lugar debían de reclutar a más gente para este trabajo. Para ello esta gente engañada sin saberlo difundía este tipo de trabajos entre sus más allegados, bien amigos de confianza bien familiares. Finalmente: La investigación sacó a la luz una impostura que había durado dos años. Los orígenes de Merrill conducían a una pequeña firma de limpieza de oficinas en la ciudad estadounidense de Ashland. El fundador de la pirámide carecía del título de Económicas por la Westfield State University del que presumía. Y el flamante edificio de la publicidad resultó ser un espacio de trabajo compartido con otras 28 sociedades. Merrill, de 52 años, fue detenido. Su socio Wanzeler, de 45, declarado prófugo. Publicado en el País, el 6 de Julio de 2014.[14]

2.- FRAUDES PRODUCIDOS EXCLUSIVAMENTE POR INTERNET

2.1 Envíos de correos electrónicos denominados *spam*

Con el desarrollo de las nuevas tecnologías y el acceso mundial a Internet los denominados correos *spam* son ahora el medio mediante el cual se cometen las tradicionales estafas: la de inversión, de tarjetas de crédito, el robo de identidad, la de cheques, entre otros. La persona que recibe este conjunto masivo de correos electrónicos de manera simultánea no ha solicitado su envío en ningún momento. El fin que pretenden conseguir estos correos es poder acceder a cualquier sistema informático consiguiendo todo tipo de información como: cuentas bancarias, números de tarjetas de

[14] Véase: http://politica.elpais.com/politica/2014/07/04/actualidad/1404498398_556596.html

crédito, etc., o bien pretenden introducir en el sistema informático que abordan virus o *botnets*.[15]

En este apartado hay que hacer una breve referencia a las Cartas Nigerianas: se trata de una combinación entre el robo de identidad y las estafas de las transmisiones de dinero por adelantado. Las víctimas reciben la suculenta oferta, que consiste en ganar una gran fortuna realizando una pequeña inversión, por email, fax o carta. El estafador se hace pasar por un funcionario de un gobierno extranjero, o bien un alto cargo bancario o una autoridad petrolera importante proveniente de África, que promete a su víctima unas elevadas ganancias realizando una transacción de dinero fuera del país en el que se encuentre. El estafador le promete que todo lo que haya invertido a causa de impuestos o de alguna tasa le será reembolsado, cosa que jamás ocurre.

2.2 *Spyware* o *malware*

Se trata de un software malicioso que tiene como fin robar información personal de los sistemas informáticos o realizar fraudes consiguiendo pérdidas patrimoniales muy importantes. Por un lado nos encontramos con el *spyware* a los archivos o aplicaciones de *software* que son instalados en los sistemas, algunas veces sin conocimiento u autorización de los usuarios o después que los mismos acepten las "Condiciones de Uso". Los *spyware* monitorizan y capturan información de las actividades de los usuarios, hacia servidores donde almacenarán los datos recolectados. Seguidamente esta información se usa en robos de identidad o para enviar publicidad personalizada. Estos programas pueden instalarse en el equipo de muchas maneras, pero normalmente se encuentran ocultos en otros como: protectores de pantalla, juegos gratuitos, etc. Los *spyware* pueden contener rutinas que capturan las teclas digitadas por el usuario denominadas *keyloggers*, tales como nombres de usuario, contraseñas, números de tarjetas de crédito, fecha de expiración y hasta sus códigos secretos las

[15] MIRÓ LLINARES, FERNANDO: "Cibercrímenes económicos y patrimoniales" en Ortiz de Urbina (COORD): *Memento…." ob. cit.*, pág. 469. Además en Internet: http://www.ic3.gov/crimeschemes.aspx#item-3

cuales son almacenadas en archivos de tipo "log" para posteriormente ser enviadas al intruso vía cualquier servicio de Internet.[16]

En el caso del *malware* se trata de un programa o archivo, que mediante la infección de un virus trata de dañar, alterar o suprimir la información que se encuentra almacenada en el sistema informático en el que se introduce. Se encarga de destruir elementos básicos del *hardware*, que puede suponer en la mayoría de ocasiones pérdidas de archivos con valor económico o incluso sentimental. Este tipo de virus se propaga de un sistema informático a otro incidiendo en la información en ellos contenida.

Dos tipos comunes de malware son los virus y los gusanos informáticos, este tipo de programas tienen en común la capacidad para auto replicarse, es decir, pueden contaminar con copias de sí mismo que en algunas ocasiones ya han mutado, la diferencia entre un gusano y un virus informático radica en que el gusano opera de forma más o menos independiente a otros archivos, mientras que el virus depende de un portador para poderse replicar.[17]

2.3 *Phishing* y *Pharming*.

Según el Memento Práctico, Penal Económico y de la empresa[18] un concepto de *phishing* y *pharming* sería el siguiente: "mecanismo criminal que emplea tanto ingeniería social, como subterfugios técnicos para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias. El uso de la ingeniería social se produce en el momento en el que se utiliza la identidad personal de otro (*spoofing*), mediante la falsificación de sitios web, para conducir a los consumidores a que confíen en la veracidad del mensaje y divulguen los dato objeto". En cambio el *pharming* es una modalidad del *phishing* en el cual: "se utilizan artificios

[16] Véase en Internet: http://windows.microsoft.com/es-es/windows/is-computer-infected-spyware#1TC=windows-7

[17] MIRÓ LLINARES, FERNANDO, *El Cibercrimen*, Madrid, Marcial Pons, 2011, págs.: 59-62. Concretamente en la página 59 se encuentran los distintos tipos de malware que explica el autor.

[18] MIRÓ LLINARES, FERNANDO: "Cibercrímenes económicos y patrimoniales" en Ortiz de Urbina (COORD): *Memento…" ob.cit.,* pág. 480

técnicos, como, por ejemplo, cuando se redirecciona un nombre de dominio de una página web verdadera situada en la memoria caché del sujeto o de otro modo, a una página web falsa, o se monitoriza la intervención del sujeto en la verdadera*".*

CAPÍTULO IV: DINÁMICA DEL *PHISHING*

En este apartado vamos a desarrollar todos los aspectos relacionados con el *phishing.* De esta forma, podremos estudiar con mejor claridad las responsabilidades penales de los muleros.

1.- CONCEPTO Y DINÁMICA DEL *PHISHING.*

El *phisihing* o "la pesca de incautos" es una modalidad de fraude que opera en Internet. Emplea la ingeniería social y todo tipo de falsedades y evasivas técnicas para conseguir lograr su objetivo: robar los datos de identidad personales de los consumidores y el número de tarjetas de créditos o de cuentas bancarias. Los atacantes inducen a la víctima en un engaño bastante, de esta forma consiguen que ella misma les proporcione los datos necesarios, con el objetivo final de conseguir unos beneficios económicos a costa del perjuicio patrimonial de la víctima. Con el uso de la ingeniería social nos referimos a la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. En el caso del *phishing*, este uso se ve reflejado en el momento en el que simulando ser una entidad legítima (bien sea una entidad bancaria, una Red social o una organización pública, entre otros) mediante imágenes y logotipos extraídos de las páginas webs oficiales y reales, consiguen que la víctima confíe en la veracidad de esta web falsa y por tanto divulgue sus datos bancarios. Cabe añadir que en este tipo de conductas el cibercriminal se acerca a la víctima mediante el envío masivo de correos electrónicos. De esta forma tiene más probabilidades de "pescar" a su víctima. Aunque este sea la metodología más seguida existen otros métodos como los SMS, mensajes en las Redes sociales, aplicaciones de mensajería instantánea o VoIP.

El modus operandi de este ciberdelito se encuentra integrado por tres elementos: el mensaje, la interacción y el robo[19] y cualquier actuación típica de *phishing* se desarrolla de la siguiente manera: el ciberdelincuente procede al envío masivo de correos electrónicos. Los destinatarios más comunes a los que van dirigidos los correos electrónicos son clientes del banco (el cual pretenden suplantar su identidad). Pero este dato resulta difícil de saber por los atacantes. Esta desventaja se ve compensada por el envío de miles y miles de correos electrónicos. El mensaje en la mayoría de los casos suele ser un correo electrónico, pero como hemos dicho anteriormente el ataque puede iniciarse también mediante SMS, mensajes en las redes sociales, aplicaciones de mensajería instantánea o VoIP.

El remitente del correo electrónico es la entidad bancaria que junto a su supuesta dirección de correo-e, el logotipo de la entidad y el asunto (que puede ser cualquier tipo de notificación tal como: el renueve del sistema de seguridad de la entidad bancaria, la actualización de la cuenta de la banca on-line, completar los datos de la banca on-line para el mantenimiento de la cuenta) aparece o bien una dirección de la supuesta página web del banco o un formulario. El inicio de la pesca de incautos no es muy sofisticado, pero el uso de la ingeniería social[20] para llegar al engaño bastante, hace que la víctima, muerda el anzuelo.

El segundo componente de la estrategia del engaño es: la Interacción. La víctima proporciona los datos que se le requieren siguiendo el enlace de la URL inserta en el correo, bien respondiendo al correo o instalando *malware*. Los *phishers* utilizan todo tipo de falsedades y subterfugios técnicos para conseguir el engaño bastante en la víctima: utilizan nombres de dominio similares a los de las entidades bancarias o de los organismos públicos, así como logos e imágenes extraídas de los sitios webs verdaderos. Mediante la suplantación de identidad de estos organismos (*spoofing*) crean

---

[19] MIRÓ LLINARES, FERNANDO: "La Respuesta Penal al Ciberfraude. Especial atención a la responsabilidad de los muleros del Phishing", en RECPC 15-12 (2013), págs.8-9

[20] Ingeniería Social: se trata de la manipulación inteligente de la tendencia natural de la gente a confiar. El *phishing* aprovecha las debilidades de los individuos para engañarles y hacer que actúen en contra de sus propios intereses. Hay que añadir, que en muchas ocasiones aparece en el mensaje una advertencia en la cual se indica que de no seguir las instrucciones proporcionadas en el mensaje, el banco puede proceder a cancelar o bloquear sus cuentas corrientes.

en la víctima una falsa seguridad que da lugar a resultados realmente perjudiciales. El *spoofing* es el robo o suplantación de la personalidad de una persona física o, más usualmente, jurídica, con intención maliciosa. Este acto es esencial en el *phishing* ya que se trata del primer paso de la dinámica comisiva en unión con el mensaje (o también denominado *spam*)[21]. Además de la suplantación de identidad, en la interacción, los delincuentes utilizan distintas técnicas para ocultar la dirección web en la que están navegando. Estas técnicas pueden ser: el uso de dirección IP numérica en lugar de utilizar el nombre de dominio, el uso de pequeñas rutinas realizadas mediante lenguaje de programación que esconden la barra de direcciones del navegador o bien registrar un nombre de dominio similar al de la organización a la que se está suplantando para realizar la estafa[22], utilizan "ebay-login.com" en vez de eBay.

En tercer lugar y como último elemento: el robo. Con los datos obtenidos mediante la suplantación de identidad, el *phisher* hace un uso efectivo por sí mismo de los datos o los vende a terceros (por ejemplo en los casos: de los juegos on-line o la venta de tarjetas de crédito). En este punto debemos mencionar a los llamados muleros. Son intermediarios contratados por el *phisher*, que engañados o no, se les ofrece un trabajo consistente en el traspaso de dinero de una cuenta corriente a otra. Se trata de transferir el dinero desde la cuenta corriente de la víctima a la del delincuente. El mulero o también denominado cibermulero debe realizar esa transacción de dinero a cambio de una comisión. La transacción del dinero se produce de forma fraccionada en diversas cuentas repartidas por varios lugares del mundo pero de una zona geográfica relativamente cercana. De esta forma el *phisher* logra extraer el dinero de las cuentas y al ser de terceros países e incluso de países transoceánicos, se hace más difícil la tarea de encontrar al verdadero responsable de estas conductas delictivas.

2.- SUJETOS INTERVINIENTES Y FUNCIONES

[21] MIRÓ LLINARES, FERNANDO: "Cibercrímenes económicos y patrimoniales" en Ortiz de Urbina (COORD): *Memento…" ob. cit.,* pág. 483.

[22] INTECO:"Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como Phishing", en www.inteco.es, Octubre 2007, págs. 42-43.

Siempre en este tipo de conductas delictivas nos encontramos con un sujeto pasivo o víctima y con el Phisher o atacante. El resto de sujetos, como la entidad bancaria o el cibermulero, son posibles intervinientes según el caso de *phishing* en el que nos encontremos.

En este contexto, el **sujeto pasivo** será la persona a la que el ciberfraude afecta directamente. Cualquier usuario o consumidor puede ser víctima de este fraude. En el caso concreto del *phishing*, el usuario deberá realizar sus gestiones bancarias de forma on-line y estar utilizando un sistema informático. De estos sujetos podemos decir que su grado de conocimientos, educación o estudios pueden ser más o menos sofisticados, pero el elemento principal de estas conductas es el engaño bastante, que afecta a todas las personas por igual. Y como norma general, el atacante suele buscar a clientes de la entidad bancaria la cual pretende suplantar. La **entidad bancaria u organismo público** no es el más afectado por las acciones del *phisher*. Estas entidades u organismos pueden ser tanto víctima como responsable. En primer lugar es víctima del que *spoofing*, es decir, víctima de un robo de identidad. Pero por otra parte, este organismo representa a un grupo de personas que depositan su confianza y ahorros en él. Como consecuencia de esto último es lógico que se les pida responsabilidad civil a causa de los perjuicios que les pueda ocasionar a sus clientes. En varios casos los bancos indemnizan a sus clientes y de esta forma no dañan su imagen empresarial, que como es obvio, puede verse perjudicada por este tipo de conductas delictivas.

El encargado de realizar todo tipo de estrategias y engaños para conseguir su objetivo de lucrarse económicamente es el ***phisher***. Se hace valer para ello de la ingeniería social y los diversos subterfugios técnicos. Cabe destacar que la mayoría de casos de *phishing* no se suele captar al verdadero responsable porque utilizan unos mecanismos tan complejos que es casi imposible saber quién es la persona que manipula el sistema informático para obtener la información sensible. Como bien hemos expuesto anteriormente, las transacciones de dinero suelen ser a terceros países de muy difícil acceso a informaciones bancarias. Es por ello que existe una gran preocupación a la hora de captar al verdadero responsable del delito. Otro tipo de

delincuentes según el autor FERNANDO MIRÓ[23] son aquellos que se asocian para realizar el fraude: los mensajeros, los recolectores y los cajeros.

Por último, en todo el entramado del *phishing* existen numerosos participantes como los que empiezan planeando el ataque, los que redactan el *spam*, aquellos que envían los correos, quienes diseñan las webs falsas, los que se ocupan de llevar a cabo la transferencia económica, y por último nos encontramos con los **cibermuleros**, que son aquellos que reciben en sus cuentas el dinero y se encargan de transmitirlo por canales seguros a los jefes de la organización. Es importante destacar que no actúan como muleros propiamente dichos quienes realizan las transferencias de dinero por Internet, porque puede darse el caso de que el ordenador se encuentre infectado por algún tipo de malware. Hay que añadir el hecho de que para lograr el beneficio patrimonial en el *phishing*, hay que realizar la transacción de dinero de forma personal. El cibermulero lo recibe en su cuenta y tras una transacción económica por sistemas no electrónicos le hace llegar el dinero al *phisher*.

3.- TIPOS DE *PHISHING*[24]

En el mundo cibernético existen numerosas modalidades de *phishing*. Cada uno de ellos afecta a un grupo diferente de personas y además no siempre intervienen los mismos sujetos. En este apartado vamos a hacer referencia a seis de las modalidades más conocidas y usuales.

3.1 *Phishing* engañoso o Deceptive *Phishing*

También denominado *phishing* tradicional, es el tipo de ciberfraude más común en nuestros días. El modus operandi que utiliza es igual al que hemos explicado en el apartado anterior llamado Dinámica del *phishing*. Se trata de un envío masivo de correos electrónicos en los cuales se suplanta la identidad de las entidades bancarias copiando las imágenes y logotipos de la página web real. En este mensaje se inserta un

[23] Véase para más información: MIRÓ LLINARES, Fernando: *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Prólogo de Marcus Felson, Madrid, Marcial Pons 2012, págs.76-79

[24] Véase: Ididem. Además: INTECO:"Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como *phishing*", en www.inteco.es, Octubre 2007, págs. 36-48.

enlace, si el destinatario "pincha" sobre él que le redireccionarán hacia una web falsa en la que de forma inconsciente revelará sus datos bancarios. En el mismo mensaje se advierte que de no seguir las instrucciones sus cuentas pueden verse bloqueadas o canceladas. Normalmente el mensaje se envía por alguna de las siguientes razones: porque existe algún tipo de problema en la cuenta corriente del destinatario, porque necesita actualizaciones, para la comunicación de algún tipo de riesgo de fraude, para la comunicación de un cambio no autorizado de la cuenta corriente, entre otras razones. El *phisher* tan solo intenta que la víctima acceda a esa web falsa con la excusa de subsanar aquello que se le comunica en el mensaje. A partir de aquí se comete la acción fraudulenta.

Dentro de este tipo de *phishing* existen subtipos. Empezando por el *spear phishing* en el que los destinatarios no son cualquier persona, sino que los mensajes van destinados a clientes de entidades bancarias u otro tipo de organizaciones concretas. En el *Business Services Phishing* también los destinatarios son personas concretas, pero en este caso se trata de empleados de entidades bancarias que utilizan servicios como Google AdWords o Yahoo! De forma similar que ocurre en el *Business Services Phishing*, en el *Whaling* el atacante se centra en un grupo reducido de personas que trabajan en organizaciones o empresas de alto nivel o en el gobierno. Además en este último caso el *phisher* no se limita a enviar los correos sino que utiliza todo tipo de técnicas como CDs o instalar *hardware* del tipo *keylogger*. Se trata de robar las credenciales de estos altos cargos instalando malware en sus sistemas informáticos.

Otros subtipos de esta modalidad de *phishing* son: el *vishing* y el *smishing*. En el primer caso se utiliza el teléfono como herramienta. Se basa en el uso de un tipo de *software* denominado "war dialers" cuya función es realizar la marcación de teléfonos desde un ordenador, utilizando la tecnología de telefonía sobre IP. Una vez que el usuario atacado descuelga se activa una grabación que trata de convencerle o bien de que visite un sitio web para dar sus datos personales o bien de que directamente confirme sus datos en la misma llamada. En el caso del *smishing* se trata de embaucar a los usuarios, pero esta vez a través de mensajes de texto a móviles. El mensaje (SMS) que recibe la víctima le informa que alguien le ha dado de alta en algún servicio de pago para recibir, por ejemplo, determinados contenidos. Si la víctima desea darse de baja,

deberá hacerlo a través de una web, en la cual una vez haya accedido, se le instalará un *software* de captura de datos.

3.2 *Phishing* basado en *software* malicioso o *Malware Based Phishing*

Esta modalidad de *phishing* se basa en la ejecución de un *software* malicioso en el ordenador de la víctima. Las conductas que se siguen en este tipo de *phishing* son la ejecución de archivos adjuntos a mensajes de correo electrónico o la descarga de *software* desde una web relacionada con pornografía o cotilleos sobre famosos, o también visitar páginas web en las que se descargue el programa.

Cabe añadir que en este modalidad se utilizan diferentes tipos de programas para robar la información confidencial: *keyloggers y screenloggers*: los primeros son programas que registran la información de las pulsaciones que se realizan en el teclado. En el momento en que la víctima accede a la página web deseada el programa graba toda la información que se teclea en el ordenador y la envía al delincuente. El *screenlogger* realiza la misma función que los programas de *keyloggers*, pero la diferencia radica en que en este caso se capturan imágenes de la pantalla del ordenador que son remitidas al atacante; los Secuestradores de Sesión actúan una vez el usuario accede a la web registrada en el *software*. No se roban los datos sino que actúa directamente en el momento en que la víctima accede a su cuenta corriente bancaria en su sesión. Los Troyanos Web (Web *Trojans*) son aquellos programas que contienen malware y aparecen de forma inesperada en formas de ventanas emergentes dentro de la página web legítima con el objetivo de conseguir datos confidenciales.

En estos casos el *phishing* actúa en su forma natural, ya que engaña al usuario haciéndole introducir datos confidenciales en la página web aparentemente real; los ataques de reconfiguración del Sistema o *System Reconfiguration Attacks* son los ataques que se realizan a través de la modificación de los parámetros de configuración del ordenador del usuario. Existen dos formas de realizar este ataque: bien modificando el sistema de nombre de dominio o bien realizando una instalación de *proxy* (mediante este servidor se canaliza toda la información que entra y sale del ordenador) y el robo de datos (*Data Theft*) que trata de instalar códigos maliciosos que tienen como fin

obtener información confidencial almacenada en el sistema informático para posteriormente remitirla al atacante. Estos tipos de programas son los más utilizados en la Red.

3.3*Phishing* basado en el DNS o *Pharming*

Esta variante de *phishing* es en la que se incluyen todas las formas que se basan en la interferencia del proceso de búsqueda del nombre de dominio (se trata de la traducción de la dirección introducida en el navegador de la dirección IP).
Se trata de manipular las direcciones DNS (Demain Name Server) que utiliza el usuario. El delincuente consigue que las páginas web visitadas no se correspondan con las auténticas, sino con otras creadas para recabar datos confidenciales, sobre todo los datos bancarios. La forma de actuar es modificando el archivo denominado *hosts* (fichero incluido en el sistema operativo, almacena la información de las páginas que el usuario ha visitado con el fin de evitar la consulta al servidor DNS y acelerar el proceso) siempre que se utilice el sistema operativo de Windows y el navegador de Internet Explorer. Este tipo de conducta opera en el momento en que el usuario quiere acceder a la dirección de la página en su navegador, es reenviado a otra creada por el hacker que tiene el mismo aspecto que la original. En este preciso momento el usuario de manera inconsciente y confiada está revelando datos confidenciales al defraudador[25].

3.4 *Phishing* mediante introducción de contenidos o *Content-Injection phishing*

Modalidad que consiste en introducir contenido malicioso dentro de la web legítima. La introducción puede realizarse de diversas formas: asaltando al servidor legítimo por parte de los *hackers* que se aprovechan de cualquier vulnerabilidad del sistema. Otras formas son mediante *cross-site scripting*, también conocido como XSS y mediante la incorporación de contenido malicioso SQL. El *cross-site scripting* conocido también por las siglas CSS o XSS consiste en un engaño mediante el cual se introduce un código o URL falsas en una web real. Por ello, la mayor parte del contenido es real

[25] FERNÁNDEZ TERUELO, Javier Gustavo: *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, Valladolid, Lex Nova, 2011, pág. 38.

pero existe una parte, la de la información sensible que no lo es. Esta última parte se construye para conseguir su objetivo: obtener los datos objetivos sin que el usuario pueda detectar anomalías. En cambio el SQL son acciones maliciosas que mediante las vulnerabilidades del ordenador del usuario el atacante introduce SQL: es una forma de provocar que sean ejecutados comandos de bases de datos en un servidor remoto que conlleven la filtración de bases de datos confidenciales.

3.5 *Phishing* mediante la técnica del intermediario o *Man-in- the middle* y *phishing* de motor de búsqueda.

Man-in-the middle consiste en el posicionamiento del *phisher* entre el ordenador del usuario y el servidor web legítimo. El atacante consigue filtrar, leer y modificar la información que se transfiere desde el ordenador del usuario al servidor y viceversa. Todo ello sin que las partes sean conscientes de que se les está violando su seguridad, aquí radica el éxito o no de este tipo de acciones. Tienen la finalidad de robar información confidencial que la usan ellos mismos o la venden a terceros. Existen diferentes técnicas para realizar esta modalidad: los *proxies* transparentes, que se sitúan en la misma Red o ruta que el servidor real; *DNS Cache Poisoning* que permite el enrutamiento de IP falsas; la ofuscación de URL, que permite redirigir el tráfico de datos a su servidor; o configurando el proxy en el navegador. En el caso del *phishing* motor de búsqueda el delincuente crea una página de web falsa para productos o servicios falsos. Introduce estas webs en los motores de búsqueda y espera a que los usuarios las visiten para realizar compras o realizan transferencias bancarias o revelen información confidencial. Normalmente las ofertas de estas webs son más tentadoras y mejores que las ofertas en las webs reales, ocurre en las webs de las entidades bancarias que el interés es superior en las falsas que en las legítimas.

CAPÍTULO V: RESPONSABILIDAD PENAL DEL CIBERFRAUDE. ESPECIAL REFERENCIA AL PHISHING.

Delitos tales como el de apoderamiento o el de apropiación indebida no parecen ser los más adecuados para definir las conductas delictivas de los ciberfraudes. Por la simple razón de que en estos dos delitos el hecho de tomar o apoderarse se interpreta en un sentido físico o material de la disposición patrimonial. Es bien sabido que en la mayoría de casos la disposición patrimonial en los ciberfraudes se suele realizar mediante la manipulación informática y por la misma víctima. En el caso del delito de estafa nos acercamos más a la tipología delictiva de los fraudes producidos por Internet. Pero aun así cabe hacer precisiones. Según en el tipo de ciberfraude en el que nos encontremos lo podremos encaminar hacia la Estafa Común o Tradicional o hacia la Estafa Informática (arts. 248.1 y 2 CP, respectivamente).

Se crean muchas dificultades a la hora de englobar a ciertos ciberfraudes dentro de la estafa común porque el elemento definitorio de este delito es el engaño bastante junto con una transacción autorizada del patrimonio realizada por el sujeto activo y estos hechos no siempre son así en todos los ciberfraudes. En cambio si hablamos de estafa informática podemos hablar de manipulación informática y de una transacción patrimonial no autorizada realizada por el sujeto pasivo en los cuales no existe ni engaño ni error en los elementos del tipo. Por lo tanto, debemos atender a las principales diferencias para poder decidir si nos encontramos ante un delito de estafa común o informática, siempre teniendo en cuenta las circunstancias de los hechos y a la doctrina.

Por último y antes de pasar al estudio de la calificación jurídica del *phishing* y de sus actos preparatorios, vamos a hacer una breve clasificación para tener una visión más general, sobre aquellos ciberfraudes que podríamos englobar dentro del artículo 248.1 y 248.2 del CP. Los ciberfraudes sancionables por el artículo 248.1 CP serían por ejemplo los ataques *scam* o envío de correos electrónicos no deseados o *spam.* El defraudador envía correos electrónicos a sus víctimas de forma masiva solicitando siempre algún

tipo de actividad que conlleva una transacción económica. La consecuencia siempre en estos casos es un beneficio para el atacante y un perjuicio patrimonial para la víctima. En estos casos se puede ver claramente que existe engaño, error, y una disposición patrimonial fruto de la estrategia del sujeto activo.

Otro ejemplo que claramente se encuentra en este grupo son aquellos fraudes cometidos en operaciones de comercio electrónico en los que el defraudador puede ser tanto el comprador como el vendedor. En el caso del comprador, se adquiere un producto por Internet que una vez pagado no se llega a enviar o recibiéndolo es defectuoso o distinto de lo pactado con el vendedor quien en todo momento sabe lo ocurrido y lleva a cabo este entramado. En caso de que el vendedor sea el defraudado, lo que acontece es que el comprador no realiza el pago de la mercancía y además no la devuelve.

En el segundo grupo encontramos a los ciberfraudes sancionables por el artículo 248.2 CP. La estafa informática tiene su razón de ser en la insuficiencia del modelo clásico de estafa para hacer frente a aquellos casos de fraudes en los que no se lleva a cabo ni en- gaño ni error y que además la disposición patrimonial la realiza el propio sujeto pasivo. Responden pues a esta tipología algunos tipos de *spyware*: el defraudador introduce archivos en el sistema informático de la víctima con el fin de obtener información confidencial (claves, contraseñas, cuentas corrientes bancarias) para seguidamente usarla en su propio beneficio o venderla a terceros.

CAPÍTULO VI: CALIFICACIÓN JURÍDICA DEL *PHISHING*

1.-SANCIÓN DE LOS ACTOS PREPARATORIOS DEL *PHISHING*.

Es interesante estudiar, antes de centrarnos en la calificación jurídica del *phishing*, la posible sanción de aquellos actos como el *spoofing* o suplantación de identidad, la infección por malware, el acceso informático ilícito o la fabricación, introducción, posesión o facilitación de programas de ordenador, que se consideran preparatorios del *phishing*.

1.1. *Spoofing*

La suplantación de identidad es el primer paso para la realización no solo del *phishing*, sino de muchos otros cibercrimenes. Se trata de aquellas acciones en las que, como bien hemos explicado en párrafos anteriores, se suplanta la página web de un organismo público o de cualquier entidad financiera de renombre con el fin de dirigirse hacia los usuarios mediante el envío masivo de correos electrónicos. El contenido de estos correos son enlaces engañosos o incluso formularios para rellenar mediante los cuales se consigue acceder a los datos de identidad o los datos de cuentas corrientes de los usuarios. El sujeto pasivo entrega directamente sus datos o puede verse infectado por *malware*.

El *spoofing* como conducta delictiva específica no se encuentra recogido en el código penal y además existe mucha disparidad entre jurisprudencia y los diferentes autores. En primer lugar lo podríamos sancionar según el artículo 401 CP por usurpación de estado civil. Según el autor F. MIRÓ y acorde con la jurisprudencia, se debe rechazar esta idea porque es necesario que en la usurpación exista una continuidad en la suplantación de la personalidad[26]. En cambio P. FARALDO CABANA[27] expone que más que el estado civil, este artículo protege un bien jurídico colectivo constituido por la fe pública. Se trata de la confianza de la comunidad en la correcta identificación de las personas, que según la autora es un instrumento esencial para la vida social y para el tráfico jurídico-económico. En el sentido de esta autora podemos observar que el hecho de usurpación de la identidad no sea algo singular, sino que estemos ante unos hechos que afectan a un bien jurídico colectivo, de todos

Otro camino distinto es el del artículo 402 CP. En ocasiones, los sujetos activos de estas conductas suplantan la identidad de entidades públicas como puede ser Hacienda (AEAT), y no solo eso sino que realizan actividades propias de estas entidades y ejercen como autoridades o funcionarios públicos. En este caso sería de más gravedad porque estaríamos ante un delito de usurpación de funciones públicas.

---

[26] MIRÓ LLINARES, FERNANDO: "La Respuesta Penal al Ciberfraude. Especial atención a la responsabilidad de los muleros del Phishing", en *RCPC* 15-12 (2013), pág. 19.

[27] FARALDO CABANA, PATRICIA: "Suplantación de Identidad y uso de nombre supuesto en el Comercio Tradicional y Electrónico", en *RDPC*, Nº3 (2010), págs. 83-84.

Autores como E. VELASCO NÚÑEZ, entienden que puede constituirse un delito de falsedades en documento mercantil. El problema aquí es interpretar que o que cosas se consideran documentos. En el artículo 26 del CP[28] se establece el sentido de documento. Por tanto, tan solo con este precepto que una página web no puede considerarse un documento con relevancia jurídica[29]. No sería posible tampoco proceder a aplicar en estos casos el artículo 274 CP, aunque estemos ante marcas de corporaciones o entidades financieras. El uso al que se destinan estas falsificaciones no son para fines industriales ni comerciales, por tanto, la conducta del *spoofing* sería atípica para este tipo de delito.

En el sentido de un posible delito contra la intimidad, es la forma en que la autora FÁTIMA FLORES MENDOZA entiende esta usurpación de los datos o claves bancarias. El artículo 197.1 del CP trata el tipo básico de los delitos contra la intimidad. Se trata de garantizar un espacio privado para el desarrollo de la personalidad del individuo. Esta circunstancia nos lleva a que el propio individuo tenga la facultad de autodeterminación informativa o derecho al control de datos personales. El artículo 197.1 precisamente trata de impedir el descubrimiento de secretos ajenos y la vulneración de su intimidad. Pero debemos añadir que lo que para unos el secreto trata datos o hechos que se constituyen según la voluntad del propio individuo para otros no solo depende del individuo, sino que se debe atender también a los criterios de adecuación social. Por todo ello, la autora interpreta que los datos, claves y operaciones bancarias se pueden considerar como información personal reservada o privada y quedar al amparo de la intimidad[30]. En este sentido apunta también FERNANDO MIRÓ: se podría formar un concurso ideal medial entre el descubrimiento de secretos y el delito patrimonial en grado de tentativa en los casos en los que el sujeto descubre la clave.

Para acabar con este apartado debemos hacer referencia a la posibilidad de la tentativa. F. MIRÓ[31] explica que en los casos en los que se pudiera identificar al sujeto

---

[28] Art. 26 CP: "todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".

[29] VELASCO NÚÑEZ, E.: "Fraudes informáticos en Red: del Phishing al Pharming", en *LL*, nº37(2007), pág.61.

[30] FLORES MENDOZA, FÁTIMA: "Respuesta Penal al denominado Robo de Identidad en las conductas del Phishing Bancario", en *EPC*, Vol. XXXIV (2014), págs. 313-315.

[31] MIRÓ LLINARES,FERNANDO: " La Respuesta…", *ob. cit*., pág. 19

que envía los correos electrónicos y se pudiera probar su intención de engaño y el peligro ex ante, sí se podría considerar tentativa del ilícito principal. También en el caso de que la víctima envíe o ponga involuntariamente a disposición del defraudador los datos sensibles, pero por cualquier motivo externo al sujeto activo no se consigue realizar la transferencia, estaríamos ante una tentativa. Ahora bien, según nuestro autor, no podemos considerar el mero hecho de envíos de correos electrónicos o la infección con software espía como tentativa porque son hechos demasiado lejanos al peligro del bien jurídico que se protege.

Así como este autor considera que la infección con software espía en sí mismo no se puede considerar ni siquiera tentativa, a no ser que se den los casos del párrafo anterior, la autora FLORES MENDOZA considera que tanto algunos *spyware* como el *pharming* podrían ser conductas sancionables por el artículo 197.3 del CP por ser similares al *hacking* y al intrusismo informático ilícito. Pero la argumentación de estos hechos tiene más sentido que la expliquemos en los párrafos posteriores referentes al acceso ilícito informático.

1.2 Acceso informático ilícito

Conductas como el *phishing* o el *pharming* pueden verse sancionadas por el artículo 197.3 del CP, que se estableció con la reforma del 2010[32]. Antes de la reforma dicha conducta no era objeto de penalidad alguna. Este artículo trata el intrusismo o acceso informático ilícito a un sistema con la vulneración de medidas de seguridad. Mayoritariamente sanciona las modalidades del *phishing* que requieren *hacking.*

Según la autora FÁTIMA FLORES MENDOZA el artículo 197.3 del CP podría ser la medida para sancionar conductas como el *pharming* o el *spyware* que mediante técnicas de *hacking* proceden a realizar las conductas delictivas. Este artículo prohíbe el acceso

[32] Artículo que se introdujo con LO 5/2010, de 22 de junio, de reforma del Código Penal, trae causa de la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información y del Convenio del Consejo de Europa sobre Cibercriminalidad, firmado en Budapest el 23 de noviembre de 2001, y ratificado por España el 3 de junio de 2010. El Proyecto de Código Penal de 2009, siguiendo la propuesta de la directiva europea, incorpora al precepto el comportamiento omisivo, que no se hallaba en la Redacción original del Anteproyecto de reforma de Código Penal de 2008, ni en el Proyecto de 15 de enero de 2007.

ilícito a datos o programas de un sistema informático. Estas conductas vulneran tanto las medidas de seguridad como la permanencia no consentida en un mismo sistema informático.

1.3 Fabricación, introducción, posesión o facilitación de programas de ordenador

El artículo 248.2 b)[33] Se introduce con la reforma 15/2003 del CP de 1995[34], y su principal objetivo es anticiparse a la realización del fraude. Según el autor FERNÁNDEZ TERUELO[35], los elementos necesarios para la comisión efectiva del fraude son los diferentes programas que facilitan o resultan imprescindibles para la comisión de tales conductas fraudulentas. Concretamente hablamos de los programas *keyloggers* o *sniffers*.

Por otra parte el autor F. MIRÓ[36], explica que la doctrina critica el encuadre este tipo de conductas en el artículo 248.2 b) con dos argumentos de una excesiva anticipación de la tutela penal y una desproporcionalidad por el hecho de castigar de igual forma al delito consumado y a los actos previos. El autor expone que la cláusula del precepto en la que se especifica que el programa de ordenador debe estar destinado específicamente a la comisión de la estafa, se puede interpretas de dos formas diferentes: por un lado, tener en cuenta la intención del autor del delito aunque el programa realice diversas funciones (no solo aquellas específicas para realizar el fraude), es decir que el autor tiene que tener la intención de realizar el fraude aunque el programa tenga diferentes utilidades. Por otro lado una interpretación más restrictiva es aquella que entiende que el programa de ordenador tiene que tener la específica función y no otra, de defraudar. En el momento en que el programa tenga diversas funciones ya no se encontraría dentro del tipo penal.

---

[33] Artículo 248.2 b): Los que fabricaren, introdujeren, poseyeren o facilitaren programas de informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

[34] Reforma 15/2003 de modificación del Código Penal añadió el apartado 3 del artículo 248. En la reforma de 2010 simplemente se optó por alterar su ubicación sistemática, pasa del apartado 3 al subapartado b) del apartado 2 del mismo precepto.

[35] FERNÁNDEZ TERUELO, JAVIER GUSTAVO, *Derecho Penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, Valladolid, Lex Nova, 2011, págs. 53-54.

[36] MIRÓ LLINARES, FERNANDO: "La Respuesta…", *ob. cit.*, págs.24-27.

Por todo, el autor se decanta por la interpretación más restrictiva entendiendo que el precepto del CP cuando dice "específicamente destinados" se refiere a los programas de ordenador y no al sujeto activo. Debe realizarse una interpretación literal de los preceptos. Además F. MIRÓ expone en su artículo que de no seguir la interpretación más restrictiva se podría llegar al absurdo de igualar la pena del delito consumado con el hecho de que un sujeto utilice *software* legal para defraudar. Este hecho sería, cuanto menos, desproporcionado. Por lo tanto, no solo se restringe el ámbito de aplicación del tipo sino también los comportamientos, dejando de lado aquellos que realmente no lesionan ni ponen en peligro el bien jurídico protegido.

Finalmente explica que tanto el envío de malware que contenga troyanos, *backdoors*, cualquier *software* que permita el acceso ilícito a un sistema informático como los *spywares* que no se dedican únicamente a conseguir datos o claves bancarias, no se encontrarían dentro del tipo penal del 248.2 b). En cambio, algunos programas como los *keyloggers* o *sniffers* sí entrarían dentro del tipo penal, coincidiendo esta opinión con la de J.G FERNÁNDEZ TERUELO, pero solamente en aquellos casos en los que se pretendan apoderar de información de 20 cifras o similares. Además no solo se encontrarían estos programas, que no suelen ser los más habituales, sino que añade al *spoofing* dentro de esta tipología, por entender que esta conducta en especial se centra en crear una página web específicamente para robar información bancaria sin ninguna otra función añadida.

2.- PROBLEMÁTICA EN LA CALIFICACIÓN JURÍDICA DEL PHISHING.

Introducir la conducta del *phishing* dentro del ordenamiento jurídico español, se convierte en una tarea ardua y difícil. Sobre este tema se han pronunciado numerosos autores y existe una gran variedad de jurisprudencia. En este apartado vamos a tratar de comparar las diversas opiniones de los autores en el momento de insertar las conductas del *phishing* bien en el tipo penal del 248.1 como estafa tradicional o bien en el artículo 248.2 como estafa informática, ya que estos dos delitos son los que más nos recuerdan a dichas conductas. Las estafas son delitos en los que la violencia, intimidación o la fuerza, empleada con más menos habilidad, son sustituidas por la astucia y el ingenio;

como pasa en las conductas del *phishing* que se utiliza la manipulación informática y la ingeniería social como mecanismos para provocar un daño en la víctima.

En la introducción de esta segunda parte, hemos realizado una breve clasificación de las conductas del *phishing* para tener una idea global sobre la tipificación de estos actos. Pues bien, con el análisis que realizaremos a continuación veremos como los esquemas pueden verse modificados según la interpretación en la que nos basemos.

2.1 La Estafa en relación con el Phishing

*"*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*".* Estas dos líneas son las que definen la Estafa Tradicional en el Código Penal. El bien jurídico protegido de este delito es el patrimonio, que puede estar compuesto por bienes muebles, inmuebles o por valores inmateriales.

Es importante mencionar los elementos que conforman este delito para poder saber si nos encontramos o no ante una estafa: el engaño precedente o concurrente consiste hacer creer algo que no es, puede realizarse de forma explícita (mentir directamente) o de forma implícita (aparentar solvencia y ocultar la intención de no abonar los bienes o servicios recibidos que otro entrega confiado) activa u omisiva, además debe ser idóneo, suficiente, adecuado, hábil, para conseguir el resultado deseado. Es decir que el engaño debe ser bastante. El segundo elemento es el error. Originar error en el sujeto pasivo, hacer que se forme una representación equivocada de la realidad. Por la causa de este engaño, el sujeto pasivo actúa bajo una falsa presuposición que parte de un motivo viciado y es causa de la subsiguiente disposición patrimonial. El acto de disposición como tercer elemento, será producto de una actuación directa del propio afectado, consecuencia del error y del engaño bastante. Conlleva la producción de un daño patrimonial para sí o para un tercero. Se trata de toda acción u omisión que implique un desplazamiento patrimonial, seguidamente el perjuicio es el daño patrimonial puede afectar a la víctima o a un tercero, según de quien sea el bien. La cuantía de lo defraudado debe superar los 400€, de no ser así entrará en juego el artículo 623.4 CP. El quinto elemento es el ánimo de lucro. Se obtiene un beneficio económico para el autor y un perjuicio para la víctima o tercero ajeno. Y por

último el nexo causal: el engaño, el error, el acto de disposición y el perjuicio cada uno debe ser consecuencia del precedente[37]

2.1. 1. El problema del engaño como elemento de la estafa

Podemos decir, sin embargo, que de todos los elementos que conforman la estafa convencional el engaño es el más importante para que se dé el tipo. Se considera al engaño como el desvalor de acción concreto de la estafa. Las discusiones que rodean a este elemento son consecuencia del problema de entender que a las máquinas o a los instrumentos automáticos se les pudiera engañar. No se puede engañar o inducir a error a una máquina[38].

En la conducta típica de la estafa se exige necesariamente que interactúen dos personas físicas, es decir, que una de ellas induzca a error a otra provocándole una situación no real de los acontecimientos. Se necesitan por tanto dos personas para lograr el error y el engaño. Y tanto el engaño como el error son indispensables para una posterior disposición patrimonial por parte del defraudador, es decir que son imprescindibles para que se dé la conducta típica. Estos mismos hechos no pueden darse ante una máquina a la que no se le puede inducir a error por no tener las mismas capacidades psicológicas que las personas.

Para los autores como GUTIÉRREZ FRANCÉS o DE LA MATA[39], el camino del engaño es diferente. Es decir, que para ellos sí que existen dos personas físicas que mediante el uso un ordenador se puede llegar a la disposición patrimonial. Dichos autores están de acuerdo en que una máquina no puede ser engañada ni inducida a error. Pero entienden que realmente son personas las que interactúan una con otra: una persona la que introduce los datos erróneos dentro de la máquina y la otra persona que

---

37 ORTS BERENGUER, ENRIQUE y GONZÁLEZ CUSSAC, JOSÉ.L: *"Compendio de Derecho Penal"* (Parte General y Parte Especial), Prólogo de T.S Vives Antón, Valencia, Tirant lo Blanc 2004, págs. 567-569.

38 STS de 21 de Diciembre de 2004 8RJ 2004/8252)

39 GUTIÉRREZ FRANCÉS, M.L., "Actualidad Informática", Aranzadi 1994, pág. 11. Además, DE LA MATA BARRANCO, N., "Utilización abusiva de cajeros automáticos: apropiación de dinero mediante la tarjeta sustraída a su titular", Poder Judicial, núm. Especial IX, Nuevas Formas de delincuencia, (1988), págs. 172 y ss.

está al otro lado, visualiza esos datos falsos y la induce a error. Significa que se llega al engaño aunque no sea de forma personal y directa. La autora GUTIÉRREZ FRANCÉS entendía que el tema del engaño era imprescindible revisarlo por el hecho de que se puede llegar a otro concepto de este elemento por los cambios sociales surgidos en el mundo contemporáneo con la aparición de los ordenadores.

Llegados a este punto en el que ya conocemos y podemos entender la estafa convencional de forma íntegra, vamos a proceder a relacionar este tipo delictivo con el *phishing*. Para ello nos haremos valer del autor J.G FERNÁNDEZ TERUELO[40] que nos guiará en la interpretación del *phishing* como estafa común. Nuestro autor interpreta de una forma clara y sin lugar a dudas que los fraudes cometidos en operaciones electrónicas y los mails o mensajes fraudulentos se encuentran incluidos dentro de la modalidad típica de la estafa. En el primer caso, ya sea el comprador o el vendedor quien estafa, nos encontramos ante dos personas: el engañado y quien engaña, es decir, que existe una persona que induce a error a otra. En el segundo caso de los mails también intervienen dos personas físicas, en la que el engañado realiza una disposición patrimonial en favor del defraudador sin percatarse de este hecho en ningún momento. Estos dos hechos encajan a la perfección con el 248.1 CP, siempre, claro está, que se den con el resto de elementos del tipo.

Pero este autor, dentro del ámbito de la estafa informática, entiende que la obtención y posterior uso de las claves a través de *spyware* u otro método que no implique la intervención de la víctima y los supuestos de *phishing* y *pharming* no podrían subsumirse dentro de este delito, a diferencia de otros autores que sí entienden que es el mejor tipo delictivo para estas conductas, que en párrafos posteriores analizaremos. Entiende así nuestro autor que para subsumir determinados hechos dentro de la estafa informática debemos estar al concepto de manipulación informático o artificio semejante que se extrae del precepto 248.2 del CP. Poniendo de relieve las sentencias: STS de 20 de noviembre de 2001 (RJ 2002/805) y la STS de 26 de junio de 2006 (RJ 2006/ 4925), en las que se explica que el concepto de manipulación

---

40 FERNÁNEZ TERUELO, JAVIER GUSTAVO, "Derecho Penal…", *ob. cit*., págs.: 44-

42 Véase además: FERNÁNDEZ TERUELO, JAVIER GUSTAVO, "Respuesta Penal Frente a Fraudes cometidos en Internet: Estafa, Estafa Informática y los nudos de la Red", *RDPC*, núm. 19 (2007), págs. 217-243.

informática debe entenderse en el sentido de que la máquina informática o mecánica *"*actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquellos que permiten su programación, o por la introducción de datos falsos*"*. FERNÁNDEZ TERUELO entiende que es necesaria la participación de dos personas físicas, y que las conductas como el *phishing* o el *pharming* no podrían subsumirse dentro de la estafa informática porque en estos casos no se alteran elementos físicos ni de programación ni de introducción de elementos falsos, necesarios para encontrarnos con el concepto de manipulación informática antes expuesto. En estas conductas, los hechos son sencillamente que quien se apropia de las claves verdaderas las utiliza para realizar una disposición patrimonial a su favor o a la de un tercero a través de la Red sin ningún tipo de alteración en su programación y no se ha podido introducir datos falsos porque las claves son las auténticas.

A modo de conclusión podemos decir que FERNÁNDEZ TERUELO entiende que para que se incluyan las conductas del *phishing* en la estafa informática, se deben de dar este tipo de alteraciones de programación o introducción de datos falsos. Además está de acuerdo con lo expuesto en lo referente al engaño por los autores GUTIÉRREZ FRANCÉS o DE LA MATA, puesto que también piensa que es necesario dos personas para cometer este delito (engañado y quien engaña), aunque el engaño no se produzca de forma personal y directa. Podríamos observar además otra interesante similitud entre estos últimos y aquél : FERNÁNDEZ TERUELO interpreta que en el *phishing* no se introducen datos falsos que puedan llevar a error a la víctima, puesto que los datos son verdaderos (porque el defraudador se ha encargado anteriormente de obtenerlos aunque de forma ilegal), y GUTIÉRREZ FRANCÉS y DE LA MATA entienden lo mismo pero en el sentido de que una máquina no puede llevar a error ni a engaño puesto que simplemente realiza la función del traspaso patrimonial ordenado y dispuesto por quien ha efectuado la programación (engaño al programador o a la institución). Es decir, que estos últimos entienden que todos los datos que se introduzcan en el sistema informático serán verdaderos puesto que a una máquina no se le puede inducir a error.

En mi opinión ambos autores se equivocan. En primer lugar porque en las conductas del *phishing* no existen dos personas una a un lado de la pantalla y la otra al otro, sino que más bien es el propio defraudador que mediante técnicas informáticas y

haciendo uso de la ingeniería social logra adentrarse en el sistema informático ajeno vulnerando la intimidad de su víctima, obtiene los datos bancarios verdaderos que necesita para su posterior fraude y seguidamente deja de tener contacto con ella. El fraude en sí, la disposición patrimonial la realiza el delincuente y nadie, más. Por tanto, al ordenador o al sistema informático no es que se le engañe o no simplemente es que se le introducen unos datos que son ciertos y a partir de aquí el fraude sigue su curso. Además cabe destacar que un ordenador o un sistema informático, a mi parecer, no puede ser capaz de decidir qué datos son falsos y cuáles no, para la máquina todos los datos son verdaderos.

2.2. La Estafa Informática y el *phishing*

El origen de este tipo delictivo se remonta a los años 90, con el objetivo de sancionar situaciones fraudulentas que se daban en las entidades bancarias o terminales de pago en las que algún empleado o tercero operando sobre ellas, realizaba transferencias a su favor o a favor de un tercero. Por lo tanto, este delito no nace por la aparición de Internet ni con la revolución de los medios informáticos puesto que en esa época la Red no estaba suficientemente desarrollada.

Se establece en el Código Penal la definición de Estafa Informática en su artículo 248.2 a)[41]. Con la reforma del Código Penal de 1995 se introduce este precepto, mediante el cual se crea un nuevo modelo de estafa. Más tarde con la reforma de 2010, la Redacción del texto se mantuvo excepto por la sustitución de "en perjuicio de tercero" por "en perjuicio de otro" y por la modificación de la pena mínima y máxima pasando de los seis meses y tres años a uno y cuatro años[42].Además, con esta reforma el legislador pretende también dar por terminado el tema de la sustitución del término engaño por el de manipulación informática. Es decir, que con la introducción de un nuevo modelo delictivo se sustituye el engaño y el error de la estafa tradicional por

[41] Artículo 248.2 a): También se consideran reos de estafa: a) los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

[42] FERNÁNDEZ TERUELO, J.G., "*Derecho Penal*…", *ob. cit*., págs.46-47.

la manipulación informática y artificio semejante. Se consigue castigar una manipulación de datos almacenados en sistemas informáticos para lograr una transferencia no consentida de activos patrimoniales.

Según R.M. MATA Y MARTÍN[43] los cambios producidos también devienen la aparición de dos alternativas en cuanto al tema de la relación de la estafa informática con la estafa genérica: por una parte aquellos que siguen manteniendo la idea de que los criterios interpretativos y la dinámica de la estafa informática sigue los mismos pasos que los de la estafa tradicional, simplemente se trata de una mera adaptación legislativa a las necesidades de la estafa informática, y por otro lado el otro grupo de personas que interpretan que la dinámica, el esquema y los elementos de la estafa informática nada tiene que ver con los de la estafa común. El autor al que hemos hecho referencia al principio de esta párrafo defiende esta última postura al considerar que no existe ni error ni engaño en la estafa informática y que atendiendo al tenor literal del precepto del Código Penal (art. 248.2 a)), los términos *"se consideran"* dan lugar a que se entienda que los supuestos de estafa informática se asemejan a los de la estafa tradicional pero no iguales, es decir que existen diferencias. Habiendo realizado estas aclaraciones, vamos a proceder a explicar al igual que hemos hecho con la estafa tradicional, los elementos de los cuales se compone la estafa informática, procediendo seguidamente a analizar el elemento más importante del delito: la manipulación informática.

Los elementos del tipo de la estafa informática son: el ánimo de lucro del autor, la manipulación informática o artificio semejante, la transferencia no consentida de activos patrimoniales que se entiende como tal toda transmisión de bienes o servicios que tienen valoración económica[44].La relación que existe entre estos elementos no es que uno precede al otro, sino que más bien se trata de una relación de causalidad entre la manipulación informática y la transferencia del patrimonio no consentida. Además se puede observar que en este precepto no se nombra ni al engaño ni al error. Siempre al hablar de este tipo de estafa se distingue entre: la estafa cometida dentro del sistema y la cometida fuera del sistema: la primera es aquella en la que la manipulación informática se produce directamente sobre el ordenador falsificando o modificando o suprimiendo

43 MATA Y MARTÍN, R., "*Delincuencia…*", *ob. cit*., págs. 44-45

44 PÉREZ MANZANO, M., en BAJO FERNÁNDEZ (Director), "*Compendio de Derecho Penal (Parte Especial)*", Volumen II, Ceura, Madrid 1998, págs. 456-457.

datos existentes. En cuanto a la segunda la manipulación se produce antes, durante o después de la elaboración del programa, y queda registrada y disponible. Ambas conductas se castigan por el 248.2 CP[45].

Para acabar con este apartado podemos observar las principales diferencias entre la estafa común y la estafa informática: en la primera el elemento esencial es el engaño bastante que conduce al error en el sujeto pasivo y en la estafa informática el error y el engaño no existen, nos encontramos con una manipulación informática o artificio semejante. Otra clara diferencia es que en el caso de la estafa informática la disposición patrimonial la lleva a cabo única y exclusivamente el autor del delito, no siendo partícipe en ningún caso la víctima a la que sin embargo perjudica patrimonialmente. En cambio en la estafa común es el sujeto pasivo quien realiza la disposición patrimonial fruto del error y el engaño bastante.

2.2.1 Manipulación Informática

Es el elemento del tipo más importante en el delito de la estafa informática y se puede equiparar al engaño bastante de la estafa convencional. Según el autor ROMEO[46] la manipulación consiste en la incorrecta modificación del resultado de un procesamiento automatizado en cualquiera de las fases de procesamiento o tratamiento informático con ánimo de lucro y perjuicio de tercero. O se puede entender como una alteración del software como así lo hace PÉREZ MANZANO[47].

Otra interpretación de este concepto nos las dan las sentencias del Tribunal Supremo: STS 20 Noviembre de 2001 (RJ 2002/805) y la STS de 26 de Junio de 2006 (RJ 2006/4925), en las que se especifica claramente en ambas lo siguiente: "Como en la

---

45 ORTS BERENGUER, ENRIQUE. y GONZÁLEZ CUSSAC, JOSÉ.L: *"Compendio de…." ob. cit.*, págs. 571-572.

46 ROMEO CASABONA, C.M., "*Poder Informático y seguridad jurídica*", Madrid 1987, pág. 47.

47 También Choclán Montalvo, J.A.: " Fraude informático y estafa por computación", en CDJ, núm. 10, (2001), pág. 328, habla de la manipulación informática en el siguiente sentido: "toda acción que suponga intervenir en el sistema informático alterando, modificando u ocultando los datos que deban ser tratados automáticamente o modificando las instrucciones del programa, con el fin de alterar el resultado debido de un tratamiento informático y con el ánimo de obtener una ventaja patrimonial"

estafa debe existir un ánimo de lucro; debe existir la manipulación informática o artificio semejante que es la modalidad comisiva mediante la que torticeramente se hace que la máquina actúe; y también un acto de disposición económica en perjuicio de tercero que se concreta en una transferencia no consentida", es más, las mismas añaden que "Subsiste la defraudación y el engaño, propio de la relación personal, es sustituido como medio comisivo defraudatorio por la **manipulación informática o artificio semejante** en el que lo relevante es que la máquina, informática o mecánica, actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquellos que permite su programación, o por la introducción de datos falsos".

Para cerrar este apartado vamos a hacer referencia a un concepto de manipulación informática que nos describe la autora P. FARALDO CABANA[48]. Esta autora se hace valer del artículo 3 de la Decisión Marco 2001/413/ JAI del Consejo mediante la cual se explica que la manipulación informática conlleva la introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, y la interferencia indebida en el funcionamiento de un programa o sistema informáticos. Por tanto y cito textualmente las palabras de la autora en su artículo: "se incluyen tanto la introducción de datos falsos como la introducción indebida, por no autorizada, de datos reales, auténticos, en el sistema, pasando por la manipulación de los ya contenidos en él en cualquiera de las fases de proceso o tratamiento informático, así como las interferencias que afectan al propio sistema o programas".

Siguiendo con el apartado en el que nos encontramos, vamos a hacer una referencia a los diferentes autores que se han pronunciado sobre la relación entre la estafa informática y el *phishing*. Según el autor F. MIRÓ[49] la estafa común no sería el delito más idóneo para describir al *phishing*, porque no es la víctima la que realiza la disposición patrimonial sino que es el propio sujeto activo quien la realiza. El autor compara estas afirmaciones con las conductas de *scam* o el de las cartas nigerianas para

[48] FARALDO CABANA, PATRICIA, "*Las Nuevas Tecnologías en los Delitos contra el Patrimonio y el Orden Socioeconómico*", Valencia, Tirant lo Blanc 2009, págs. 88-90.

[49] MIRÓ LLINARES, FERNANDO, "Responsabilidad….", *ob. cit*., págs. 28-29

explicar que en estos casos sí existe estafa común porque es la propia víctima quien realiza esa disposición patrimonial, a diferencia de los casos del *phishing* o del *pharming*, en los que la víctima ni siquiera es consciente de estos hechos. El autor entiende que la duda no se encuentra en el hecho de incluir las conductas del *phishing* dentro de la estafa común o dentro de la estafa informática puesto deja claro que esta conducta no puede ser estafa común nunca por la razón mencionada al inicio de este párrafo y por la consiguiente razón que explica que en estas conductas no existe ni error ni engaño, por lo que siempre estaremos ante una estafa informática. El problema deviene en saber si en todas las conductas del *phishing* procede la manipulación informática.

Para resolver este problema el autor realiza una interesante interpretación del concepto: entender tal manipulación como utilización de sistemas informáticos para lograr disposiciones patrimoniales no autorizadas por su titular. Se trata pues de generar un peligro típico con el hecho de usar o utilizar el sistema informático para generar un perjuicio patrimonial mediante la transferencia no autorizada. Por tanto, entiende que tanto las conductas del *phishing* como las del *pharming* se consideran estafas informáticas. El *phishing* bancario, el *phishing* que utiliza *spyware* o *malware* para conseguir la información sensible, en todas ellas se da el hecho de utilizar el sistema informático para realizar una transferencia patrimonial no consentida, en las cual el sujeto pasivo no interviene en ningún momento siendo el defraudador el personaje principal y único.

El mismo camino sigue la autora P. FARALDO CABANA respecto del *phishing*. La autora en primer lugar explica que hay que tener en cuenta las decisiones internacionales que se han realizado respecto de la estafa informática. Como bien apuntábamos anteriormente en el apartado de la manipulación informática, la autora pone de relieve la decisión marco 2001/413/JAI del consejo, de 28 de mayo de 2001 sobre la lucha contra el fraude y falsificación de medios de pago distinto del efectivo en

la que se establece un el precepto nº 3: sobre los delitos relacionados con equipos informáticos[50].

También hace referencia al Convenio del Consejo de Europa sobre criminalidad acordado en Bucarest, el 23 de Noviembre de 2001, que en sus artículos 7 y 8 del Título 2º, hace referencia a fraudes informáticos[51].

Con tales referencias internacionales la autora explica que en estos preceptos se establece de forma muy detallada aquello que podríamos entender como fraude

[50] Decisión Marco 2001/413/JAI del consejo, de 28 de Mayo de 2001, precepto nº3**:** "Cada Estado miembro adoptará las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada: realización o provocación de una transferencia de dinero o de valor monetario que cause una pérdida no autorizada de propiedad a otra persona, con el ánimo de procurar un beneficio económico no autorizado a la persona que comete el delito o a terceros, mediante:
— la introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, o
— la interferencia indebida en el funcionamiento de un programa o sistema informáticos".

[51] Artículo 7 - Falsificación informática: Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.
Artículo 8 - Fraude informático: Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a) cualquier introducción, alteración, borrado o supresión de datos informáticos;
b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

informático. Estos detalles no se pueden ver reflejados en la legislación española. Por lo que entiende que el legislador tendría que hacer valer estos preceptos para limitar de forma clara y precisa los problemas que surgen alrededor de los fraudes informáticos.

P. FARALDO CABANA, ve acertado que el legislador español diera un paso más con la reforma del Código Penal de 1995. Y a partir de la introducción del 248. 2 CP interpretó la estafa informática como un modelo autónomo y comparándolo con el tipo de la estafa común realiza la siguiente reflexión: la autora explica que existen diversos puntos que no coinciden entre la estafa informática y la común. En primer lugar establece que en la estafa informática no existe ni el engaño ni el error, elementos principales en la estafa común. La conducta típica del nuevo tipo autónomo es la disposición patrimonial del defraudador utilizando para ello la manipulación informática o cualquier artificio semejante. No es la víctima quien realiza la disposición patrimonial en su perjuicio, sino que es el autor del delito quien realiza esa disposición patrimonial por su cuenta teniendo únicamente una relación con el sistema informático. No existe en la estafa informática relación intuito personae como bien algunos atores defienden[52].Además en la estafa común no existe el hecho típico de la estafa informática como es la transferencia no consentida de activos patrimoniales. En la estafa común mediante el engaño y el error, es decir, mediante una conducta viciada de la víctima se consigue esa transmisión de activos patrimoniales.

Una vez realizado este análisis de los elementos del tipo de la estafa informática, la autora establece como hemos comentado en párrafos anteriores, un concepto de manipulación informática que extrae de la decisión marco y del convenio de Bucarest. Entiende así que la manipulación informática conlleva la introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, y la interferencia indebida en el funcionamiento de un programa o sistema informáticos. Además, nos indica que si seguimos una interpretación estricta en cuanto a la conducta de usurpar la identidad e otro en transacciones electrónicas, mediante el uso no autorizado de sus datos, se consideraría únicamente delito de falsedad en concurso, en su caso con un delito de usurpación de estado civil (401 CP).

[52] Véase FERNÁNDEZ TERUELO, J.G, "Derecho Penal…".

De acuerdo con lo anteriormente expuesto, P. FARALDO CABANA aclara que en el momento en que se utiliza la manipulación informática para introducirse en un sistema informático de una entidad bancaria mediante programas como los *spywares*, mediante los cuales se obtienen datos bancarios como números de tarjeta de crédito o claves bancarias en el ámbito del comercio electrónico, estaremos siempre ante una estafa informática. Entiende que aunque el sistema informático funcione a la perfección y los datos que se introducen en ellos son completamente veraces, la clave se encuentra en que se utilizan sin el consentimiento de su titular. A pesar de ello, algunos autores se decantan por la estafa común.

Por tanto, entiende que conductas tales como el *pharming*, el *phishing* o la web *spoofing* en las que se obtienen datos del titular de cuentas corrientes bancarias, o se obtienen números de tarjeta de crédito o cualquier dato relevante bancario, el defraudador es quien mediante estos datos consigue llevar a cabo una disposición patrimonial de datos totalmente ciertos pero mediante una utilización ilegítima de dichos datos. No existe ningún engaño idóneo para causar la obtención de esos datos, simplemente existe una manipulación informática por el delincuente y de la cual la víctima no es partícipe en ningún momento ya que ni si quiera es consciente de los hechos. En el *phishing*, el engañado se limita a proporcionar los datos que dan acceso a su patrimonio, pero no realiza ninguna disposición patrimonial, siendo necesario un acto de apoderamiento por parte del delincuente, materializado en el uso de los datos bancarios obtenidos. Y en el caso del *pharming*, ni la víctima ni el delincuente son los encargados de obtener los datos, es el propio *software* malicioso instalado sin el consentimiento de la víctima. En este último caso la autora sugiere un posible delito contra la intimidad del sujeto pasivo.

CAPÍTULO VII: RESPONSABILIDAD PENAL DE LOS MULEROS DEL *PHISHING.*

Tras el análisis del fenómeno del *phishing* y de su inclusión en alguno de los tipos penales, procedemos a realizar un estudio sobre la conducta del cibermulero. En párrafos anteriores hemos explicado que en el *phishing* intervenían varios sujetos de entre los cuales se encontraba el cibermulero, aquél que ofrece su cuenta corriente para obtener el dinero defraudado y seguidamente extraerlo para traspasarlo mediante medios no electrónicos (mediante giros postales por ejemplo) a los autores reales de la estafa. Generalmente se trata de varias cuentas distribuidas en diferentes ciudades pero dentro de la misma zona geográfica. Realmente, los intermediarios son los únicos expuestos al control legal, ya que son los que realizan el trabajo susceptible de rastreo. Es decir, que realmente la cuenta corriente en donde aparece el dinero defraudado es la del cibermulero, no la del verdadero autor, al que el dinero le llega en otras vías por las que es de gran dificultad encontrar a su receptor. Téngase en cuenta que este tipo de operaciones suelen ser internacionales pudiendo ser el autor de los delitos americano, ruso o incluso chino.

Por la complejidad de estos supuestos es por lo que resulta interesante poder descubrir de qué forma se puede sancionar o no sancionar los supuestos de estos cibermuleros o también denominados: las otras víctimas del *phishing*. Esta denominación tiene su razón de ser en que, además del control legal, el trabajo que se les ofrece es un engaño también para ellos. Con esto queremos decir que el autor del delito ofrece a este intermediario un supuesto trabajo vía internet consistente en ofrecer su cuenta corriente para traspasos de dinero cobrando por ello una comisión. Este trabajo puede ser tentador para muchas personas, sobre todo en tiempos de crisis.

A pesar del engaño que sufren estos sujetos, en inevitable pensar que con un mínimo de diligencia se puede evitar el perjuicio patrimonial que suponen estas conductas a millones de personas. Por ello surge un debate jurisprudencial y doctrinal en cuanto a la responsabilidad que deben recibir los cibermuleros. Por lo general los autores y la jurisprudencia barajan siempre tres posibilidades: receptación, blanqueo de capital y la estafa informática o común, aunque en la mayoría de los casos el tipo delictivo aplicable sea el de la estafa informática. Es de gran dificultad, por tanto, manifestar si concurren todos los elementos del tipo de la estafa, de la receptación o del blanqueo de capital pero más complejo aún es el hecho de revelar de forma exacta de

qué forma intervienen en este tipo de conductas delictivas, porque como hemos comentado en el párrafo anterior, ellos mismos pueden ser víctimas del engaño. Con ello queremos decir que el conocimiento de los cibermuleros en estos casos puede ser limitado, pudiéndonos encontrar ante casos en los que realmente sí son conocedores de los hechos delictivos y por tanto ante dolo o ante casos en los que realmente no son conocedores de los hechos pudiéndonos aferrar a la imprudencia. Cabe desatacar además un término intermedio entre el dolo y la imprudencia, como se puede dar en este tipo conductas, como sería una conducta neutral o lo que se llama: ignorancia deliberada, que explicaremos en párrafos posteriores.

CAPÍTULO VIII: TIPOS PENALES SUSCEPTIBLES DE SANCIONAR LA CONDUCTA DEL CIBERMULERO.

Antes de empezar a razonar los posibles tipos penales hay que mencionar a FERNÁNDEZ TERUELO[53] el cual explica que hay que realizar una distinción entre los diferentes cibermuleros: aquellos que desconocen totalmente que están colaborando con la realización de un acto delictivo, por lo que habría que eximirlos de cualquier responsabilidad penal, y por otro lado aquellos que conocen o se pueden imaginar que la conducta que realizan es delictiva y por tanto según este autor entraríamos en el ámbito del dolo eventual. Explica el autor que el tema realmente complicado no es sancionar la conducta en sí, sino la eventual participación del cibermulero en la actividad delictiva, afirmación de la cual F. MIRÓ está muy de acuerdo[54]. Además argumenta que al fin y al cabo el cibermulero en teoría no es el verdadero responsable de los hechos, aunque en la práctica así sea. Con esta breve introducción vamos a proceder a analizar los diferentes delitos en los que se podría encuadrar la conducta del cibermulero, que mayoritariamente son tres: receptación, blanqueo de capital y estafa (ya sea común o informática).

---

53 Véase FERNÁNDEZ TERUELO, J.G, "Derecho Penal…" *ob. cit*., pág. 39

54 En este contexto podemos citar a Cerezo Mir, J.: *Derecho Penal. Parte General*, Bdef, Buenos Aires, 2008. pág. 952. El cual argumenta la necesaria concurrencia de conocimiento y voluntad del partícipe.

1.- RECEPTACIÓN.

Es un delito que lesiona el patrimonio y a la administración de justicia, porque por un lado, supone que el sujeto hace suyo lo que es de otro o facilita que se aproveche el autor del producto de un delito patrimonial; y por otro, dificulta la actuación de los órganos judiciales, y cabría añadir, reduce para su legítimo propietario las posibilidades de recuperación de la cosa. Se trata del artículo 298.1 del CP y se compone de los siguientes elementos: comisión de un hecho tipificado como delito o falta contra el patrimonio o el orden socioeconómico, el ánimo de lucro, el conocimiento de que se ha cometido delito o falta, en este caso el sujeto no interviene ni como autor ni como cómplice y por último la conducta que realiza es de ayuda a otros para que se aprovechen de los efectos del delito, falta o en provecho propio. [55]

Las conductas del cibermulero podrían encajar dentro de este tipo delictivo, aunque hay diversas opiniones al respecto. ELOY VELASCO NÚÑEZ estaría a favor al contrario de J. G FERNÁNDEZ TERUELO. El primer autor argumenta que el cibermulero realmente ayuda a los defraudadores a cometer el delito. Explica que la acción de participar en este delito se encuentra más cercano a la receptación que a la estafa informática o del blanqueo de capitales al perjudicar al patrimonio de un tercero y aunque estemos hablando de dinero y no de objetos, entiende que el cibermulero no es autor ni cómplice del delito previo además de ser más proporcionada la pena de la receptación que la del blanqueo de capital teniendo en cuenta su tipo de intervención[56].

Por su parte FERNÁNDEZ TERUELO tiene ideas opuestas, interpretando que a pesar de que nos estemos ante un delito contra el patrimonio y que realmente el intermediario ayuda a los autores del delito, es importante explicar que la intervención en las conductas del *phishing* es el último paso para lograr la consumación del delito, por tanto hasta que no pase el dinero por las manos del cibermulero el delito no se consuma, diferente es el caso de la receptación en que el delito principal ya se ha consumado cuando el dinero defraudado llega a las manos del intermediario con pleno

---

55 PÉREZ MANZANO, M., en BAJO FERNÁNDEZ (Director), "*Compendio de Derecho Penal (Parte Especial)*", Volumen II, Ceura, Madrid 1998, págs. 621-628.

56 En este sentido encontramos la sentencia de la AP de Alicante núm. 296/2013 de 13 de Septiembre y la SAP de León (sección 3º) núm. 186/2011 de 29 de Julio.

conocimiento de ello éste último. En este mismo sentido explica F. MIRÓ que si se prueba que el sujeto ha tenido conocimiento de la comisión del delito como bien se establece en el tipo delictivo, es complicado decir que no es cómplice y que por tanto no haya participado en el delito de receptación.

Los tribunales también se han pronunciado en un sentido u otro. En la Sentencia del TS (Sala de lo Penal, Sección 1º) Sentencia núm. 834/2012 de 25 de Octubre los hechos que se juzgan son conductas del *phishing*, y en concreto se enjuicia a uno de los intervinientes que actúa como cibermulero (según podemos observar en los antecedentes de hecho de la sentencia). El juez condena las conductas por blanqueo de capitales, y en el fundamento tercero realiza una argumentación que descarta a la receptación de los hechos: *"*La Sala ha de hacer suyo el razonamiento del Fiscal. Y es que no hay razón que justifique que la acusada sólo deba responder de la parte del lucro propio. Es cierto que en los delitos de receptación, la responsabilidad civil se señala en función del lucro experimentado por el receptador. Pero en este caso, no estamos ante una receptación, en la cual la intervención del reo es independiente del alcance del tipo principal. Aquí la acusada interviene en el blanqueo de todo el dinero que es sustraído a la víctima. Por ello debe responder civilmente del total sustraído"[57].

En la misma sentencia, en su fundamento segundo se puede observar una fundamentación a favor de la receptación mencionando que algunos autores favorecen la subsunción de estas conductas penales al tipo delictivo de la receptación: "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*"*. Finalmente se acaba concluyendo que se trata de un delito de receptación: *"*De ahí que estaríamos en presencia de una participación postdelictiva o

[57] Se puede observar claramente las ideas del autor Fernández Teruelo.

postconsumativa, con un evidente contenido lucrativo, notas definitorias del delito de receptación".

2.- BLANQUEO DE CAPITALES

El artículo 301 del CP sanciona aquellas conductas dirigidas a generar cantidades masivas de dinero, fruto del incumplimiento de las obligaciones tributarias y, muy en particular, de los beneficios producidos por el tráfico de drogas y por otros delitos. Se trata de un delito pluriofensivo porque afecta tanto al patrimonio y al orden socioeconómico como a la Administración de Justicia. Se contempla pues en el mismo precepto las siguientes conductas: Adquirir, convertir o trasmitir bienes, además sabiendo que tienen su origen en un delito, y realizar cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones para eludir las consecuencias legales de sus actos.

Es importante explicar que en este caso el sujeto activo no actúa con ánimo especial, pero sí que debe conocer que los bienes no proceden de un origen lícito, aun cuando desconozca la causa de esa ilicitud. Además las conductas deben recaer sobre bienes de origen ilícito, carácter que no pierden por sufrir diferentes transformaciones. De manera que seguirá produciéndose el delito aunque se adquieran, conviertan o transmitan bienes que son fruto del blanqueo de otro bien de origen delictivo. A diferencia de la receptación, en el blanqueo no existe ánimo de lucro y no tiene lugar solo a partir de previos delitos patrimoniales. Además de que en aquella la legitimación está referida a cualquier delito, y aquí se trata de delitos de tráfico de drogas, por lo que no se trata de cualquier delito.

Antes de analizar jurisprudencialmente este asunto, tenemos que hacer una breve referencia al antes y al después de la reforma de 2010 del artículo 301 CP[58]. Así decía antes del 2010 el mencionado precepto: "El que adquiera, convierta o transmita bienes, sabiendo que éstos tienen su origen en un delito, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la

[58] Reforma del Código Penal: LO 5/2010, de 22 de Junio.

infracción o infracciones a eludir las consecuencias legales de sus actos, será castigado con la pena de prisión de seis meses a seis años y multa del tanto al triplo del valor de los bienes.*".* Podemos sacar la conclusión con palabras de F. MIRÓ: de este modo se exigía que los bienes que transmitía tuvieren origen en un delito, o bien que realizase actos para ocultar o encubrir el origen ilícito del dinero o para evitar que quien cometiese el delito sufriere las consecuencias jurídicas por ello.

Podemos decir que en realidad el cibermulero no actúa para ocultar el origen ilícito de ese dinero o para ayudar al autor del delito principal a ocultar sus actos ilícitos, sino que más bien el cibermulero actúa porque su conducta es necesaria para que se consuma el delito. Por tanto sería complicado encuadrar la conducta del cibermulero en el tipo delictivo de entonces. Pero con la nueva redacción, parece que el legislador ha querido encuadrar más conductas delictivas: *"*El que adquiera, posea, utilice, convierta o transmita bienes, sabiendo que éstos tiene su origen en una actividad delictiva, cometida por él o por cualquiera tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona*".*

F. MIRÓ entiende que la modificación de este precepto no lleva a reflexionar sobre dos puntos: el primero es que ya no se habla de delito sino de actividad delictiva, por lo que se puede llegar a entender que no es necesario que el delito se haya consumado, y en segundo lugar que el propio autor del blanqueo puede estar relacionado con el supuesto delito que no se ha llegado a consumar. Además en caso de que no quedara suficientemente probado que el delito se ha consumado, se podría sancionar al intermediario en la modalidad de imprudencia del blanqueo de capitales. Parece que no quede del todo claro cuáles son los argumentos que realmente justificarían el blanqueo de capitales como sanción contra el *phishing*. Por ello vamos a proceder a analizar algunas sentencias, que nos ayudarán en nuestro objetivo.

Las conductas del *phishing* que por la jurisprudencia se han sancionado por la vía del blanqueo de capital[59] han sido numerosas y además se han condenado tanto por

[59] Una de las sentencias del TS más citada en los trabajos de los autores sobre este tema es la número 834/2012 de 25 de Octubre de 2012 en la que se condena a la acusada a resarcir una cuantía por responsabilidad civil derivada del delito de blanqueo de capitales. Las conductas objeto de enjuiciamiento corresponden a las del Phishing.

dolo como por imprudencia grave. La sentencia de la AP de Burgos número 537/2013 del 3 de diciembre condena por blanqueo de capitales por imprudencia grave. Los hechos objeto de condena se explican en el apartado primero de los antecedentes de hecho, claras conductas del *phishing*. En este caso la condenada reconoce los hecho probados, pero teniendo en cuenta diferentes circunstancias como las personales, y las laborales así como su vago conocimiento de las conductas supuestamente ilícitas, el juzgador deja de lado el posible dolo y se centra en averiguar si hubo o no imprudencia: "En virtud de todo lo cual, dado que la recurrente no niega la comisión de los hechos, sino que su postura exculpatoria se centra en sostener que lo hizo en un contexto de la relación laboral que tenía en tales fechas con una empresa inglesa, desconociendo la procedencia ilícita del dinero, y concurriendo en la misma unas circunstancias personales (físicas y culturales), a las que se hará mención posteriormente, es por ello que la cuestión a dilucidar en el presente recurso de Apelación es, si su comportamiento se puede calificar de imprudencia grave o leve (esta última en el delito de blanqueo de capitales no tipificada penalmente)"

Por ello en esta misma sentencia se hace referencia a lo siguiente: "Dado que de todo lo actuado se desprende que la misma no adoptó las mínimas cautelas exigibles, por ello su conducta se considera correctamente encuadrada en el apartado 3 del artículo 301 del Código Penal. Puesto que como se indica por el Tribunal Supremo Sala 2ª en sentencias de fecha 23 de Diciembre de 2.003 , 16 de Marzo de 2.004 , y 14 de Septiembre de 2.005, en esta última nº 1034/2005 , rec. 1043/2004. Pte: Monterde Ferrer, Francisco se indica: " Ciertamente, el blanqueo por imprudencia no deja de presentar dificultades dogmáticas, por cuanto el blanqueo de capitales es delito esencialmente doloso que incorpora incluso el elemento subjetivo del injusto consistente en conocer la ilícita procedencia de los bienes y la intención de coadyuvar a su ocultación o transformación, y porque la distinción entre culpa grave, en este caso punible, y leve, no punible, participa de la crítica general a la distinción por su "ambigüedad e inespecificidad", y por contradecir el criterio de "taxatividad" de los tipos penales. A pesar de ello, recuerda la doctrina que el principio de legalidad, evidentemente, obliga a considerar la comisión imprudente del delito […]".Mediante esta sentencia podemos observar que se las conductas del *phishing* se plantean como un

delito de blanqueo de capitales por imprudencia grave. En esta sentencia no se pone en duda el tipo del delito, que es el que se establece en el 301. CP. Lo que sí lleva lugar a dudas es si en este caso realmente ha habido imprudencia o dolo, dejando claro que teniendo en cuenta las circunstancias descritas anteriormente, hay que decantarse por la imprudencia.

En este mismo sentido se ha proclamado la sentencia de Valladolid, AP (Sección 4º), núm. 263/2010 de 21 de Junio, en la cual se acusa a dos sujetos no por estafa informática sino por blanqueo de dinero también en su modalidad de imprudencia. En esta sentencia se fundamenta que los acusados no participan en ninguna manipulación informática ni en ninguna de las fases porque con su conducta consuman el delito, es decir, que se apoderan de cantidades que provienen de una operación de estafa anterior y por lo tanto el daño patrimonial ya está hecho. Sus actuaciones se basan únicamente en la ocultación del dinero y su posterior transferencia de forma que no se pueda recuperar. Además de estas sentencias existen muchas otras en el mismo sentido: SAP de Sevilla núm. 174/2012, de 22 de marzo de 2012, SAP de Asturias núm. 148/2012 de 11 de septiembre, SAP de León núm.186/2011 de 29 de julio de 2011 o la SAP de Valladolid de 21 de junio de 2010 (ARP 2010/766).

En otro sentido argumenta la sentencia de AP de Asturias núm. 556/2010, de 29 de noviembre de 2012 el blanqueo de capitales. Se establece en este caso la modalidad dolosa: *"*A este respecto entendemos que dicha pretensión debe ser desatendida, toda vez que existen datos objetivos que confirman, al menos la existencia de un dolo eventual frente al que no pueden prevaler las excusas invocadas en tal sentido a cerca de su nivel cultural y de escasos conocimientos de informática que como acabamos de exponer no sucede así y por otro lado resulta impensable o al menos muy sospechoso el contenido de una oferta de trabajo como la recibida por el acusado, para hacer de intermediario, moviendo el dinero de una cuenta a otra y remitirla finalmente a Ucrania, no a través de otra transferencia bancaria, sino por medio de una conocida empresa internacional de envío de dinero, que hace que la operación en si resulte más opaca, a lo que debemos añadir el coste que ello genera, máxime tratándose como se dice de obras

de carácter benéfico, en la que resulta impensable hacerlas a través de una persona interpuesta y mucho menos recibiendo una comisión en metálico por tal mediación, dándose por último la circunstancia de que el acusado desconocía por completo el nombre de esa supuesta entidad benéfica así como el campo de su actuación*"*

En un sentido diferente a las anteriores sentencias, la SAP de Asturias considera que el acusado podría haber descubierto el fondo delictivo que conllevaban sus actuaciones, puesto que en este caso no existe ningún tipo de circunstancia que justifique su no actuación. En el párrafo siguiente se expresa de manera clara que el acusado actúo con dolo eventual: "Así las cosas deducimos del conjunto de lo actuado que el acusado actuó a sabiendas de lo ilícito que podría resultar la operación en que estaba interviniendo y si bien pudiera ser el que no tuviera un completo conocimiento del alcance de la misma, resulta evidente que prefirió continuar adelante a cambio de la comisión a percibir, ignorancia que la hace responsable a título de dolo eventual, pues el delito que nos ocupa no exige la concurrencia de un dolo directo, bastando el eventual (Sentencia del Tribunal Supremo 303/2010 de 22 de marzo), siendo incluso suficiente situarse en la posición de ignorancia deliberada, inserta en el dolo eventual (sentencia del Tribunal Supremo 28/2010 de 28 de Enero), es decir, la de quien pudiendo y debiendo conocer la naturaleza del acto o colaboración que se le pide, se mantiene en situación de no querer, pero no obstante presta su colaboración y se hace participe; consiguientemente se hace acreedor a las consecuencias penales que se deriven de su antijuridicidad".

3.- ESTAFA INFORMÁTICA

Además de la receptación y el blanqueo de capitales, a los muleros del *phishing* se les castiga por cooperadores necesarios en el delito de estafa informática. Empecemos comentando la sentencia de la Audiencia Provincial de Burgos (sección 1ª) número 239/2013 de 15 de mayo en la que se condena a los sujetos por cooperadores necesarios del delito de estafa informática: los hechos enjuiciados son los típicos de la conducta de los muleros del *phishing* consistentes en ofrecer sus propias cuentas

corrientes para recibir dinero que posteriormente retiraban de los cajeros y enviaban mediante giros postales a sus destinatarios (que eran los supuestos autores de la estafa). En esta sentencia se establece lo siguiente: "En el presente caso, se considera por la Acusación Pública, como medio comisivo del delito, el previsto en el párrafo segundo del artículo 248 del Código Penal, es decir el valerse de alguna manipulación informática o artificio semejante a través del cual se consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero*".*

Para seguidamente especificar que: "No cabe duda que este alegato -que tampoco y como más razón podría ser válido en personas no dotadas de unos conocimientos económicos y bancarios específicos-, no puede ser esgrimido en el presente caso como fundamento de una sentencia absolutoria, por el simple hecho de que el acusado reconoció en las declaraciones efectuadas, y así lo refrendó el agente nº NUM020 , haber efectuado el ingreso a las personas desconocidas y que lo hizo por mediación de un amigo. Así de los indicios concurrentes no puede deducirse otra consecuencia distinta de la que determina que el acusado tenía pleno conocimiento de la ilicitud de su actividad, pues estaba compinchado con el acusado declarado rebelde, y asumió el percibo de su parte -que cifró en 100 #-, cuando, en realidad, las cantidades transmitidas superaba con creces cualquier interés o comisión bancaria por idéntica operación de intermediación, o incluso, como remuneración por el contrato de trabajo al que hace referencia, pero que no acredita".

Junto a estas pruebas indiciarias se establece en esta sentencia que el sujeto desconocía la identidad de las personas titulares de las cantidades recibidas y por ello condena al sujeto por estafa. *"*Hay que tener en cuenta, además, que desconocía la identidad de la persona/s titular/es de las cantidades recibidas en su cuenta por el acusado declarado en rebeldía, y la causa de su remisión, y que, en definitiva, desconocía la identidad del destinatario en Rusia de sus transferencias y la causa de las mismas. Todos estos indicios son más que suficientes para la emisión de sentencia condenatoria por el delito de estafa imputado*"*. Por tanto se entiende que los sujetos tenían pleno conocimiento de las conductas ilícitas que realizaban, estaban totalmente al corriente de la situación aunque fuera de forma limitada pero suficiente para entender

las partes más importantes dentro del entramado del *phishing*. Además se establece en la sentencia que su participación era tal que el hecho de que supieran o no quisieran saber sobre las conductas que realizaban, no les exime de culpabilidad.

*"*En este escenario probatorio vía prueba de indicios se puede -como le resultó al Tribunal sentenciador- concluir que ellos estaban al corriente, al menos de forma limitada de la operación, que en lo que a ellos se refería se concretaba en: a) apertura de cuenta, b) recepción de transferencias por personas desconocidas, c) origen de tales fondos de auténticas cuentas de otros titulares a los que personas desconocidas, en Estados Unidos habían accedido mediante el acceso fraudulento de las claves necesarias, hecho que ha quedado acreditado en la denuncia inicial y declaración de los representantes del banco y d) otro dato a tener en cuenta es la "explicación" dada por los otros condenados por una operativa idéntica, explicación que consistía en cobrar una cantidad por este "servicio" entregando el resto a otras personas desconocida".

*"*Se está ante un caso de delincuencia económica de tipo informático de naturaleza internacional en el que los recurrentes ocupan un nivel inferior y sólo tienen un conocimiento necesario para prestar su colaboración, la ignorancia del resto del operativo no borra ni disminuye su culpabilidad porque fueron conscientes de la antijuridicidad de su conducta, prestando su conformidad con un evidente ánimo de enriquecimiento, ya supieran, no quisieran saber -ignorancia deliberada-, o les fuera indiferente el origen del dinero que en cantidad tan relevante recibieron. Lo relevante es que se beneficiaron con todo, o, más probablemente, en parte como "pago" de sus servicios, es obvio que prestaron su colaboración eficiente y causalmente relevante en una actividad antijurídica con pleno conocimiento y cobrando por ello no pueden ignorar indefensión alguna, por su parte la "explicación" que dieron de que no pensaban que efectuaban algo ilícito es de un angelismo que se desmorona por sí sólo*".* Finalmente, se les condena por cooperadores necesarios, atendiendo a que conocían todo el entramado y sin ellos la estafa informática no hubiera llegado a buen fin. En este mismo sentido se han pronunciado numerosas audiencias provinciales: SAP de Burgos núm. 40/2007 de 14 de Diciembre de 2007, SAP de Asturias núm. 127/2012, de 9 de Julio, SAP de Barcelona núm. 727/2008 de 13 de Octubre y la de SAP de Zamora núm.

11/2008 de 22 de Diciembre. Además podemos destacar la sentencia del Tribunal supremo 556/2009 de 16 de Marzo de 2009 y la núm. 5333/2007 de 12 de Junio de 2007 en la que también se condena a los acusados por cooperadores necesarios.

Pero dentro de la línea jurisprudencial en la que condena los actos de los muleros como cooperadores necesarios de la estafa informática, existe un grupo de sentencias que entiende que los intermediarios del *phishing* deben responder como autores de la estafa como por ejemplo: SAP de Vizcaya núm. 355/2006 de 9 de mayo de 2006 o la SAP de Lugo núm. 165/2008 de 26 de Septiembre. Por otro lado la SAP de Madrid núm. 43/2009 de 22 de Enero condena a los sujetos autores del delito de estafa informática en grado de tentativa. A pesar de la gran variedad de jurisprudencia sobre el blanqueo de capitales o de la estafa informática, debemos decir que lo que realmente importa en la conducta de estos intervinientes es el grado de conocimiento de la antijuridicidad de sus actos. Esto nos lleva a plantearnos los casos de la ignorancia deliberada que abordaremos en el último apartado de este capítulo.

CAPÍTULO IX: LA PROBLEMÁTICA DE LA IGNORANCIA DELIBERADA Y SU DESARROLLO JURISPRUDENCIAL PARA DAR RESPUESTA A LA CONDUCTA DE LOS CIBERMULEROS.

Una vez realizado el análisis jurisprudencial sobre los posibles delitos mediante los cuales poder sancionar las conductas del *phishing*, en este último apartado del capítulo IV vamos a proceder a explicar qué argumentos ofrece nuestra jurisprudencia a la hora de condenar a los cibermuleros bien como blanqueo de capitales o como estafa en los casos de ignorancia deliberada[60].

La ignorancia deliberada es el contexto que se crea en el momento en que una persona se coloca en situación de poder o deber saber, pero decide no hacer nada. Es decir, que prefiere no ser conocedor de lo que ocurre a su alrededor o no ser

[60] Se pronuncia a fondo sobre la ignorancia deliberada el autor: RAGUÉS I VALLÉS, R.: *La ignorancia deliberada en Derecho Penal*, Atelier, Barcelona, 2008

mínimamente diligente, antes de hacer frente a unos posibles hechos ilícitos. En el caso de los cibermuleros, en el momento en que se les ofrece un trabajo fácil (que consiste en poner a disposición de los contratantes su propia cuenta corriente para realizar transacciones de dinero) a cambio de unas elevadas comisiones. El problema que se nos plantea en este caso es averiguar el grado de conocimiento de las conductas antijurídicas que poseen los cibermuleros. Es decir si realmente saben o no que su conducta va a tener como consecuencia el perjuicio de un tercero. Como bien hemos explicado anteriormente los cibermuleros son las otras víctimas del *phishing*, precisamente porque los verdaderos autores de este tipo de conductas también utilizan el engaño para captarlos. La cuestión no es si el engaño no es bastante porque es más burdo que el que utilizan para captar a sus víctimas principales. Existe numerosa jurisprudencia que se manifiesta o bien en el sentido de que cualquier persona siendo mínimamente diligente puede percatarse del engaño, o por el contrario que el engaño es tal que el cibermulero realmente no sabe que su trabajo es totalmente ilícito.

La teoría de la ignorancia deliberada se encuentra muy relacionada con el fenómeno que la doctrina denomina como conductas neutrales. Se trata de una serie de supuestos en los que el sujeto puede realizar una acción que en circunstancias normales no es relevante jurídicamente, pero que si esta conducta es utilizada por el autor doloso puede acabar siendo relevante y por tanto calificarse como cooperador necesario del delito principal. A modo de ejemplo podemos destacar conductas como: el taxista que lleva al pasajero a sabiendas de que éste matará a otro una vez haya llegado a su destino o el que vende alimentos a otro sabiendo que los va a envenenar para matar a otro. Estas conductas son muy similares a las de los muleros del *phishing*. Se trata pues de conductas que en principio no tiene sentido delictivo alguno pero utilizadas por el autor pueden llegar a ser sancionables penalmente.[61]

[61] MIRÓ LLINARES, Fernando, *Conocimiento e imputación en la participación delictiva. Aproximación a una teoría de la intervención como partícipe en el delito*, Prólogo de Miguel Olmedo Cardenete, Barcelona, Atelier 2009, págs. 63-67. Además véase: SUÁREZ-MIRA RODRÍGUEZ.C. (COORD). : *Manual de Derecho Penal, Tomo I: Parte General*, Civitas, Cizur Menor, 2006 (4ª edición), pág. 413.

Es difícil descubrir el grado de conocimiento de los sujetos en estos casos. Es por ello que la jurisprudencia mayoritaria condena a los muleros como cooperadores necesarios, aunque según el caso utiliza unos argumentos u otros. En la SAP de Burgos (sección 1ª) núm. 239/2013 de 15 de Mayo y en la SAP de Ciudad Real (Sección 1ª) núm. 64/2013 de 16 de Mayo, se viene a condenar a los sujetos enjuiciados por cooperadores necesarios en el delito de estafa informática. En ambas sentencias[62] se argumenta que existen los elementos objetivos de la estafa informática expuestos en el artículo 248.2 a) como consecuencia de las acciones de los sujetos consistentes en: acceder de modo fraudulento a las claves de cuentas o tarjetas de terceros perjudicados y se dispone en su perjuicio. Para dificultar la localización se emplean lo que se denomina en dicho argot como "mulas o muleros", personas que a cambio de una remuneración y comisión, facilitan mediante su cuenta corriente, el desvío del dinero propiedad de los perjudicados a la misma, y posteriormente la envían a una tercera persona indicada, mediante el envío de divisas, en este supuesto a través de Western Union. Además en estas sentencias se viene a cuestionar si existe dolo en las conductas de los muleros del *phishing*. Se trata de un elemento subjetivo en las conductas de estafa que entabla ciertas dificultades en los casos de ignorancia deliberada. En ambas sentencias los sujetos condenados afirmaban no tener conocimiento de la ilicitud de sus actuaciones declarando que no conocían ni a los titulares del dinero que recibían ni a los destinatarios, pero no negaban haber realizado dichas transacciones.

Como argumentos para explicar el conocimiento y el dolo en estos casos de ignorancia deliberada la jurisprudencia y en concreto estas dos sentencias establecen los siguientes: al ánimo de lucro, es decir, el enriquecimiento propio de los sujetos mediante las comisiones que reciben a cambio del supuesto trabajo lícito y el dolo eventual. En la SAP de Burgos se establece que estaban al corriente de la operación aunque de forma limitada: *"*En este escenario probatorio vía prueba de indicios se puede -como le resultó al Tribunal sentenciador- concluir que ellos estaban al corriente, al menos de forma limitada de la operación, que en lo que a ellos se refería se concretaba en: a) apertura de cuenta, b) recepción de transferencias por personas

[62] Véanse sentencias del TS tales como: STS 3 de Abril de 2001, STS 12 de Junio de 2007, STS 4 de Febrero de 2002 o la del 8 de Marzo del 2002 entre otras. En todas ellas se establecen los elementos configuradores del delito de estafa.

desconocidas, c) origen de tales fondos de auténticas cuentas de otros titulares a los que personas desconocidas, en Estados Unidos habían accedido mediante el acceso fraudulento de las claves necesarias, hecho que ha quedado acreditado en la denuncia inicial y declaración de los representantes del banco y d) otro dato a tener en cuenta es la "explicación" dada por los otros condenados por una operativa idéntica, explicación que consistía en cobrar una cantidad por este "servicio" entregando el resto a otras personas desconocidas". En este caso existen unos conocimientos limitados de los hechos pero suficientes para ser culpables. Además se argumenta que en situaciones de ignorancia deliberada no se excluye ni se elimina la culpabilidad: *"*Se está ante un caso de delincuencia económica de tipo informático de naturaleza internacional en el que los recurrentes ocupan un nivel inferior y sólo tienen un conocimiento necesario para prestar su colaboración, la ignorancia del resto del operativo no borra ni disminuye su culpabilidad porque fueron conscientes de la antijuridicidad de su conducta, prestando su conformidad con un evidente ánimo de enriquecimiento, ya supieran, no quisieran saber -ignorancia deliberada-, o les fuera indiferente el origen del dinero que en cantidad tan relevante recibieron. Lo relevante es que se beneficiaron con todo, o, más probablemente, en parte como "pago" de sus servicios, es obvio que prestaron su colaboración eficiente y causalmente relevante en una actividad antijurídica con pleno conocimiento y cobrando por ello no pueden ignorar indefensión alguna, por su parte la "explicación" que dieron de que no pensaban que efectuaban algo ilícito es de un angelismo que se desmorona por sí sólo". De este fragmento podemos extraer que el enriquecimiento y el conocimiento de los hechos son obvios en los casos de estafa.

Como bien hemos apuntado anteriormente el dolo en estos supuestos es también un elemento subjetivo objeto de muchos debates, pero que en la SAP de Ciudad Real se deja entrever la posible solución a esta problemática muy unida a la de la ignorancia deliberada, y puesta como argumento para condenar a los sujetos por estafa informática en este caso: *"*Sin perjuicio de las valoraciones que proceden en el caso concreto, la Jurisprudencia menor- se citan, entre otras SAP secc. 1ª A Coruña de 20 de junio de dos mil doce ; SAP Asturias secc. 8 de fecha 9 de julio de dos mil doce , entre otras- se inclina mayoritariamente por entender constitutiva de delito, como cooperación necesaria en la estafa informática, la actividad realizada por el "mulero", considerando

que la aceptación de dicha propuesta implica la concurrencia de dolo eventual, en cuanto por la remuneración, tipo de oferta y "trabajo que se propone" es deducible su alta probabilidad de ilicitud. No se desconocen, contrariamente otras- Por ejemplo SAP de 29 de Junio de dos mil once, Córdoba 4 de marzo de dos mil once, SAP Secc. 1ª Soria de 27 de febrero de dos mil once - que cuestionan la concurrencia de dicho dolo eventual e incluso, la posible participación como cooperación necesaria en el delito de estafa, al afirmarse que la intervención de dicho intermediario lo es a posterior.*''*

Como hemos visto en los casos en que las conductas de los muleros son castigadas como cooperadores necesarios (a que sin la ayuda de estos intervinientes no se puede consumar el delito arts. 27 y 28. b) CP) de un delito de estafa informática podemos concluir que la jurisprudencia mayoritaria en casos de ignorancia deliberada pone de relieve dos argumentos: en primer lugar que los sujetos tiene los conocimientos suficientes para saber de la antijuridicidad de los hechos y por ello basta el dolo eventual y la simple ignorancia deliberada para ser culpables del delito de estafa, en segundo lugar el hecho de que en todos los casos se recibe un enriquecimiento por parte del culpable, y en tercer lugar porque en estos casos se dan todos los elementos tanto subjetivos como objetivos de la estafa informática del artículo 248.2 a). En este mismo sentido se argumentan otras muchas sentencias como por ejemplo: SAP de Vizcaya (Sección 1ª) núm. 721/2010 de 1 de Octubre, SAP de Sevilla (Sección 1ª) núm. 508/2014 de 22 de Septiembre o el Juzgado de lo Penal de Pamplona (Provincia de Navarra) en su sentencia núm. 18/2013 de 24 de Enero.

Otro caso es el del blanqueo de capitales en que los argumentos para sancionar a los intermediarios son distintos. A pesar de la unanimidad de la jurisprudencia sobre la estafa informática, existen sentencias que sancionan las mismas conductas por un delito diferente. La SAP de Asturias (Sección 2ª) núm. 556/2012 de 29 de Noviembre establece un caso de *phishing* en el que se condena al sujeto autor del delito de blanqueo de capitales cometido con dolo eventual. En esta sentencia no se hace hincapié en explicar las conductas del *phishing*, sino que más bien se centra en establecer unos hechos ilícitos del que el sujeto es autor. Es decir, que al autor de los hechos se le ofreció un trabajo como mínimo sospechoso por Internet el cual consistía en abrir una

cuenta corriente y recibir un dinero que seguidamente sería retirado por ventanilla y enviado a una empresa en el extranjero a cambio de una comisión elevada. El sujeto en ningún momento dudó de la ilicitud de los hechos, a pesar de que cualquier persona con un mínimo de diligencia se hubiera percatado desde el primer instante de dicha ilicitud. En el párrafo siguiente se puede observar la argumentación a favor del dolo eventual:

*"*A este respecto entendemos que dicha pretensión debe ser desatendida, toda vez que existen datos objetivos que confirman, al menos la existencia de un dolo eventual frente al que no pueden prevaler las excusas invocadas en tal sentido a cerca de su nivel cultural y de escasos conocimientos de informática que como acabamos de exponer no sucede así y por otro lado resulta impensable o al menos muy sospechoso el contenido de una oferta de trabajo como la recibida por el acusado, para hacer de intermediario, moviendo el dinero de una cuenta a otra y remitirla finalmente a Ucrania, no a través de otra transferencia bancaria, sino por medio de una conocida empresa internacional de envío de dinero, que hace que la operación en si resulte más opaca, a lo que debemos añadir el coste que ello genera, máxime tratándose como se dice de obras de carácter benéfico, en la que resulta impensable hacerlas a través de una persona interpuesta y mucho menos recibiendo una comisión en metálico por tal mediación, dándose por último la circunstancia de que el acusado desconocía por completo el nombre de esa supuesta entidad benéfica así como el campo de su actuación."

Podemos concluir que en estos casos de blanqueo de capitales el conocimiento de los sujetos sobre a donde envían el dinero o de donde procede, no es necesario para atribuirles responsabilidades penales. Lo realmente necesario es que supieran que el dinero provenía de otras actividades ilícitas. Por tanto, en estos casos es más fácil atribuir responsabilidad a los sujetos simplemente por el hecho de conocer o de poder conocer que las actividades que realizan son ilícitas. El juzgador concluye con el siguiente párrafo que nos relaciona la falta de diligencia del sujeto con la ignorancia deliberada: "Así las cosas deducimos del conjunto de lo actuado que el acusado actuó a sabiendas de lo ilícito que podría resultar la operación en que estaba interviniendo y si bien pudiera ser el que no tuviera un completo conocimiento del alcance de la misma, resulta evidente que prefirió continuar adelante a cambio de la comisión a percibir, ignorancia que la hace responsable a título de dolo eventual, pues el delito que nos

ocupa no exige la concurrencia de un dolo directo, bastando el eventual (Sentencia del Tribunal Supremo 303/2010 de 22 de marzo), siendo incluso suficiente situarse en la posición de ignorancia deliberada, inserta en el dolo eventual (sentencia del Tribunal Supremo 28/2010 de 28 de Enero), es decir, la de quien pudiendo y debiendo conocer la naturaleza del acto o colaboración que se le pide, se mantiene en situación de no querer, pero no obstante presta su colaboración y se hace participe; consiguientemente se hace acreedor a las consecuencias penales que se deriven de su antijuricidad."

Sigue el mismo camino la SAP de Burgos (Sección 1ª) núm. 537/2013 de 3 de Diciembre en la que también se condena a la acusada autora de blanqueo de capitales por imprudencia grave: *"*En consecuencia, esta Sala de conformidad con la Juzgadora de Instancia, tras valorar las pruebas anteriormente expuestas, también llega a la conclusión que la negligente omisión de la acusada, con desprecio absoluto a cualquier norma de prudencia, sin observar la más mínima cautela, justifica su condena por un delito de blanqueo de capitales por imprudencia grave. Puesto que según se ha expuesto omitió la más mínima diligencia que cabría esperar de un ciudadano medio, sino que aceptó sin más lo que se le propuso por quien había contactado vía Internet, (sin efectuar averiguación alguna), prestándose como intermediaria en unos movimientos de dinero que tenía por destino final un lugar fuera de España, lo que evidencia una ignorancia deliberada o ceguera voluntaria, según palabras de nuestro Tribunal Supremo (SS. de 10/01/2000 , 19/01/2005 , 30/12/2009 y 28/01/2010); y en igual sentido para supuestos similares por otras Audiencias Provinciales (SSAP, Huesca de 31/05/2010 ; Valladolid de 21/06/2010 ; y Asturias de 11/09/2012 y 29/11/2012)."

Por todo ello podemos decir que la ignorancia deliberada en los casos del blanqueo de capitales se base en el conocimiento de si se está ante una actividad ilícita o no sin entrar más en el fondo del asunto y sin tener en cuenta si no se sabe a quién se envía en dinero o de quien se recibe. Basta con demostrar que conocía o que pudiera hacer conocido que la actividad que realizaba era como mínimo sospechoso e irregular.

CAPÍTULO X: CONCLUSIONES FINALES

1. En primer lugar debemos decir que no todas las conductas llevadas a cabo por los muleros del phishing tienen encaje en el mismo tipo penal, ya sea estafa informática o blanqueo de capitales. Sin embargo, a mi parecer, las conductas del *phishing* se introducen en el delito de estafa informática. En todos los casos existe la manipulación informática que se detalla en el Convenio Europeo de Bucarest y en la Decisión marco: "cualquier introducción, alteración, borrado o supresión de datos informático*"* y *"*cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona*"*. Claramente la disposición patrimonial no consentida por el titular de la cuenta corriente puede verse como una estafa informática porque se cumplen todos los elementos del tipo, según el artículo 248.2 a) CP. El *phishing* está compuesto por dos fases: la primera en la que el defraudador obtiene la información sensible mediante el uso de técnicas informáticas, y la segunda fase en la que simplemente utiliza esos datos para realizar la disposición patrimonial telemáticamente sin dejar rastro de su identidad.

2. A mi parecer las conductas de *phishing* no existe solo la estafa informática del artículo 248. 2 a), sino que además existe la conducta del 197.2 del descubrimiento y revelación de secretos. Porque como bien se establece en este último precepto*"* las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos,…". La intromisión dentro de un sistema informático ajeno para conseguir información personal como perfectamente pueden ser claves bancarias, es sancionable; por ello podría darse el caso de sancionar el *phishing* como un concurso ideal medial entre el delito de descubrimiento y revelación de secretos y la estafa informática. El primer delito es necesario realizarlo para conseguir la disposición patrimonial final.

3. A lo largo del análisis y estudio detallado llevado a cabo a lo largo del trabajo queda realmente claro que tanto la doctrina como la jurisprudencia castiga, bien por estafa informática o bien por blanqueo de capitales las conductas de los cibermuleros. El hecho de que se castigue por el 248.2 a) o por el 301 CP dependerá del dolo del sujeto. Es decir, del conocimiento que se imputa al sujeto a través de una prueba indiciaria. En la mayoría de las sentencias del *phishing* se habla del dolo eventual, de unos conocimientos mínimos o limitados que bastan para que el sujeto sea condenado. La definición de este tipo de dolo podría ser la siguiente: el sujeto que interviene no busca directamente la consecución de un resultado pero se lo plantea como probable, se representa dicha probabilidad en su mente. Por lo tanto, sí que quiere de alguna manera la consecución del resultado aunque se lo represente como probable porque a pesar de todo, actúa de igual forma. Existe conocimiento del peligro hacia un bien jurídico protegido, motivado por el enriquecimiento que es lo que busca al fin y al cabo. Otro hecho que se menciona en muchas de las sentencias sobre este asunto y que aunque pretenda suavizar la situación del mulero, no logra su objetivo puesto que llegando a este punto el sujeto ya crea una situación de riesgo. Estamos hablando de la ignorancia deliberada. El sujeto decide no conocer pudiendo conocer. Esta circunstancia nos puede dar a entender que sospecha de que este inmerso en una situación antijurídica, y que aunque no se represente los hechos como seguros, se los representa como probables, pero a pesar de ello continúa con su actividad. Además podemos decir que en algunas de las sentencias mencionadas anteriormente, el tribunal argumenta que basta con conocer mínimamente los hechos sin llegar a concretar los detalles para saber que el sujeto se encuentra en una situación antijurídica. En mi opinión el tribunal habla del dolo eventual.

4. El punto del presente trabajo en el que se desarrolla lo concerniente al conocimiento del cibermulero nos lleva a la conclusión de que es crucial este conocimiento para determinar si existe o no culpabilidad y para saber de en qué tipo delictivo nos encontramos. Es decir, que lo importante es el hecho a partir del conocimiento imputado. En el caso del blanqueo de capitales las pruebas indiciarias que

nos indicarán si el mulero tenía o no conocimiento sobre la actividad fraudulenta: el porcentaje elevado de las comisiones, el oscurantismo que rodea los hechos y el sinsentido que supone el que alguien o pueda sacar el dinero que le pertenece si no es por medio de otro. Seguidamente para saber si nos encontramos ante la conducta dolosa o imprudente debemos estar a los siguientes aspectos: en primer lugar el sujeto debe conocer la procedencia del dinero de una actividad ilícita y debe conocer que está realizando actos con dinero de procedencia ilícita para que se dé la conducta dolosa. Sin embargo, en estos casos el interviniente no conoce que está participando en un fraude, ni el concreto delito del que puede proceder el dinero, tampoco sabe el grado de intervención delictiva de los que le envían el dinero ni la procedencia del mismo. En el caso de la modalidad imprudente debemos atender a las circunstancias personales del sujeto (como por ejemplo padecer alguna discapacidad) y a la extrema apariencia de legalidad del contrato.

5. Por último, cuando hablamos de la estafa informática estamos ante pruebas indiciarias y conocimientos diferentes. Se deben de dar los elementos del tipo del artículo 248.2 a) del CP y además según nos indica la AP de Vizcaya 355/2006 los hechos no se deben agotar con el descubrimiento de las claves sino que además se debe disponer de cuentas corrientes mediantes las cuales realizar transferencias de dinero y de esta forma proceder al cobro del dinero defraudado. En cuanto al conocimiento de los hechos ilícitos debemos atender al hecho de que en estos casos los sujetos sí conocían la procedencia del dinero de fondos de cuentas de otros titulares y que para acceder a esas cuentas corrientes terceras personas habían accedido de forma ilícita[63].

[63] Sentencia SAP de Madrid núm. 71/2006 de 6 de Julio de 2006 (Citibank)

BIBLIOGRAFÍA

ALONSO ROYANO, F.: "¿Estado de Derecho o derecho de Estado? El delito informático", en RGD, núm. 498, marzo, (1986).

CEREZO MIR, J.: *Derecho Penal. Parte General*, Bdef, Buenos Aires, 2008.

CHOCLÁN MONTALVO, J.A.: "Fraude informático y estafa por computación", en CDJ, núm. 10, (2001)

DE LA MATA BARRANCO, N., "Utilización abusiva de cajeros automáticos: apropiación de dinero mediante la tarjeta sustraída a su titular", Poder Judicial, núm. Especial IX, Nuevas Formas de delincuencia, (1988).

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

FERNÁNDEZ TERUELO, JAVIER GUSTAVO, *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, Valladolid, Lex Nova, 2011.

FLORES MENDOZA, FÁTIMA: "Respuesta Penal al denominado Robo de Identidad en las conductas del Phishing Bancario", en *EPC*, Vol. XXXIV (2014).

GONZÁLEZ RUS, Juan José, "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", en los Cuadernos Penales de José María Lidón, núm. 4, (2007).

GUTIÉRREZ FRANCÉS, M.L., "Actualidad Informática", Aranzadi (1994).

INTECO: "Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como Phishing", en Internet: www.inteco.es, Octubre (2007).

MATA Y MARTÍN, RICARDO M., *Delincuencia informática y derecho penal*, Madrid, Edisofer S.L, 2001.

MIRÓ LLINARES, FERNANDO, *Conocimiento e imputación en la participación delictiva. Aproximación a una teoría de la intervención como partícipe del delito*, Barcelona, Atelier, 2009.

MIRÓ LLINARES, FERNANDO, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012.

MIRÓ LLINARES, FERNANDO, "La Respuesta Penal al Ciberfraude. Especial atención a la responsabilidad de los muleros del Phishing", RECPC 15-16 (2013)

ORTS BERENGUER, ENRIQUE Y GONZÁLEZ CUSSAC, JOSÉ L., *Compendio de derecho penal. Parte general y parte especial*, Valencia, Tirant Lo Blanch, 2004.

PÉREZ MANZANO, M., en BAJO FERNÁNDEZ (Director), "*Compendio de Derecho Penal (Parte Especial)*", Volumen II, Ceura, Madrid, 1998.

RAMÓN RUIZ, LUIS: "Uso ilícito y falsificación de tarjetas bancarias", en RIDP, Núm. 3 (2006)

RAGUÉS I VALLÉS, R.: *La ignorancia deliberada en Derecho Penal*, Atelier, Barcelona, 2008.

ROMEO CASABONA, C.M., *Poder Informático y seguridad jurídica*, Madrid, 1987

SUÁREZ-MIRA RODRÍGUEZ.C (COORD): *Manual de Derecho Penal, Tomo I: Parte General*, Civitas, Cizur Menor, 2006 (4ª edición).

VELASCO NÚÑEZ, ELOY.: "Fraudes informáticos en Red: del Phishing al Pharming", en *LL*, nº37(2007).