LA RESPUESTA PENAL AL CIBERFRAUDE

Especial atención a la responsabilidad de los muleros del *phishing*

Fernando Miró Llinares

Profesor Titular de Derecho Penal. Universidad Miguel Hernández de Elche

MIRÓ LLINARES, Fernando. La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del *phishing*. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2013, núm. 15-12, p. 12:1-12:56. Disponible en internet: http://criminet.ugr.es/recpc/15/recpc15-12.pdf
ISSN 1695-0194 [RECPC 15-12 (2013), 17 sep]

RESUMEN: El ciberfraude sigue siendo el crimen prevalente en el ciberespacio, especialmente si tenemos en cuenta que otros ciberataques como el hacking, el envío de spam, o las infecciones de malware suelen realizarse instrumentalmente para la posterior defraudación. El trabajo aborda el análisis de la respuesta penal a las diversas formas de fraude en Internet, entre ellas el fraude de subastas o el tipo scam. Se centra, por la prevalencia de esta modalidad, en el análisis de la punición del phishing y, aún más en concreto, en la responsabilidad penal de los muleros, cuestión controvertida que ha dado lugar a una prolija y a la vez confusa jurisprudencia de audiencias provinciales que el Tribunal Supremo no ha llegado a resolver. La posible aplicación de los tipos penales del blanqueo de capitales, en su nueva redacción tras la reforma de 2010, y de la propia estafa informática considerando cooperador necesario al mulero, obligan al intérprete a plantear temáticas de "parte general" tan interesantes y complejas como la del contenido del dolo de participación o el auténtico sentido de la doctrina de la ignorancia deliberada.

PALABRAS CLAVE: Cibercrimen, cibercrímenes económicos, ciberfraude, hacking, phishing, pharming, spoofing, scam, responsabilidad del mulero, ignorancia deliberada, dolo de participación, teoría de la integración en el injusto.

Fecha de publicación: 17 septiembre 2013

SUMARIO: 1. Introducción. 1.1. El ciberfraude: "Moby Dick" de la ciberdelincuencia económica. 1.2. Tipologías de ciberfraude. Análisis particular de los fraudes de spam: scam y phishing. 2. La respuesta penal al ciberfraude. 2.1. La regulación de la estafa informática en el Ordenamiento Jurídico español y la respuesta penal a los ciberfraudes. 2.1.1. Ciberfraude y delito de estafa informática. 2.1.2. Respuesta penal a ciberfraudes tipo scam y fraudes de compras. 2.1.3. Sobre la posible punición de algunos actos previos al ciberfraude como tentativa de estafa. 2.2. Tratamiento penal del phishing. 2.2.1. La punibilidad del spoofing y otras conductas preparatorias del phishing. 2.2.2. La calificación jurídica del phishing. 3. La responsabilidad penal de los muleros del phishing. 3.1. Entre la receptación,

1. **Introducción**

1.1. ***El ciberfraude: "Moby Dick" de la ciberdelincuencia económica***

El constructo doctrinal "delitos informáticos" surgió hace más de tres décadas para referirse a todo un conjunto de infracciones penales tales como el fraude informático, el sabotaje o daños informáticos, el *hacking* o acceso ilícito a sistemas informáticos, la sustracción de servicios informáticos, el espionaje informático, o la piratería informática de obras del ingenio[1], que trataban de responder a una fenomenología de comportamientos unidos por la utilización de sistemas informáticos o

NOTA: El presente artículo ha sido realizado en el marco del Proyecto de Investigación financiado por el Ministerio de Ciencia e Innovación, DER2011-26054, titulado "Cibercriminalidad: detección de déficits en su prevención jurídica y determinación de los riesgos de victimización para una mejor prevención situacional criminológica".

[1] Conforme a la clasificación que popularizó SIEBER, U.: *Computerkriminalität und Strafrecht,* Carl Heymanns, Köln/Berlin/Bonn/München, 1980 (2ª edición), pp. 39 y ss., y que, tal y como recuerda ROMEO CASABONA, C. M.: *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las nuevas tecnologías de la información,* Fundesco, Madrid, 1988, p. 45, había sido utilizada anteriormente por LAMPE. Sistematización similar es la de TIEDEMANN, al diferenciar entre manipulaciones, hurto de tiempo, hurto de software y espionaje y sabotaje, TIEDEMANN, K.: *Poder económico y delito,* Barcelona, Ariel, 1985, pp. 122 y ss. También GUTIÉRREZ FRANCÉS, M. L.: "Delincuencia económica e informática en el nuevo Código penal", en *CDJ,* núm. 11, 1996, pp. 252 y ss., distingue entre infracciones patrimoniales por medios informáticos (incluye la estafa informática y la utilización ilícita de tarjetas electromagnéticas a los efectos del delito de robo con fuerza) y atentados contra la información como bien de contenido económico, entre los que incluye el espionaje informático, el sabotaje informático y el intrusismo informático, y los delitos relativos a la propiedad intelectual, si bien no entra en su estudio porque, a su parecer, estos delitos "no sufren modificaciones de interés en el nuevo Código". ROMEO CASABONA, aceptando las bases de la clasificación de SIEBER, distingue en su estudio entre el fraude informático, las manipulaciones en cajeros automáticos mediante tarjetas provistas de banda magnética, y las agresiones a los sistemas o elementos informáticos, dentro de las cuales incluye el sabotaje informático y las agresiones al soporte material, y la sustracción o copia de bases de datos o de programas, cuyos principales tipos son el espionaje informático y la piratería de programas. ROMEO CASABONA, C. M.: *Poder informático y seguridad..., ob. cit.,* pp. 46 y ss., y CORCOY BIDASOLO, M. /JOSHI, U.: "Delitos contra el patrimonio cometidos por medios informáticos", en *RJC,* núm. 3, Barcelona, 1988, pp. 133 y ss., incluyen entre la delincuencia económica patrimonial la falsificación de datos, las estafas por computador, el descubrimiento y revelación de secretos, el hurto de software, la destrucción de datos y la utilización de sistemas informáticos sin costo. Véanse también enumeraciones similares de ALONSO ROYANO, F.: "¿Estado de Derecho o derecho del Estado? El delito informático", en *RGD,* núm. 498, marzo, 1986, pp. 602 y ss., y GONZÁLEZ RUS, J. J.: "Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en *PJ,* Número especial IX, 1989, p. 40. Sobre las clasificaciones de delitos informáticos llevadas a cabo por los principales autores del ámbito anglosajón y continental, nos remitimos al completo estudio de ROMEO CASABONA, C. M.: *Poder informático y seguridad..., ob. cit.,* pp. 43 y ss.

por realizarse sobre los mismos. La preocupación jurídico penal de incardinar tales conductas en los tipos penales tradicionales, de reformar los mismos o de crear tipos nuevos para proteger mejor los intereses dignos de tutela, se centraba en conductas cuyo nexo de unión era el sistema informático, como medio u objeto, y todo lo que venía unido a él: su valor económico, en relación con la intimidad, etc. Podría decirse que ésta fue una primera generación de la delincuencia relacionada con el uso de las TIC en la que lo característico era la utilización de ordenadores para la comisión de delitos, y a ella le ha precedido una segunda época, ya enmarcada más claramente en el concepto cibercriminalidad, en la que la característica central es que el delito se comete a través de Internet[2]. Lo relevante hoy no es tanto el sistema como el hecho de que el mismo permita la interconexión entre millones de ellos en el ciberespacio, de modo tal que sean múltiples los potenciales agresores que puedan utilizar este nuevo ámbito para seleccionar objetivos potenciales sobre los que atacar[3]. La tercera generación también ha comenzado ya, y se relaciona con el desarrollo de la web 2.0 y la aparición a su albor de las redes sociales, sistemas de mensajería instantánea y demás instrumentos, que permiten la construcción de una vida social paralela en el ciberespacio a la existente en el espacio físico y que conllevan que los crímenes en Internet ya no afecten esencialmente a lo patrimonial sino que pueden hacerlo también sobre otros intereses más personales como la libertad sexual, el honor, o la propia dignidad personal[4].

Pese a esta evolución que hace que hoy no pueda, ni deba, identificarse completamente la cibercriminalidad con una delincuencia patrimonial o económica, une a todas las épocas analizadas de evolución de la delincuencia relacionada con el uso de las TIC el protagonismo absoluto, en términos de prevalencia, del fraude, no tanto en cuanto a delito consumado pero sí en lo relativo a la finalidad última de las infracciones. Así sucedía con las primeras formas de delincuencia informática, en las que junto a las formas propias de estafa informática aparecían comportamientos como los de *hacking* que generalmente buscaban acceder a información sensible para poder realizar posteriores fraudes. Y así sigue sucediendo en la actualidad, incluso pese a la irrupción de las redes sociales y la consiguiente aparición de otras formas de cibercriminalidad no económica.

Esto es hasta tal punto así que podría decirse, y de ahí la titulación del presente apartado, que el ciberfraude es la ballena blanca de la mayor parte de los cibercrímenes. El cibercriminal económico utiliza la Red, los sistemas conectados a ella, la información en ellos contenida, los servicios y cualquier otro elemento de las TIC

[2] WALL, D.: *Cybercrime: the transformation of crime in the information age*, Polity Press, Cambridge, 2007, pp. 44 y ss.

[3] MIRÓ LLINARES, F.: "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", en *RECPC,* núm. 13-07, 2011. También *El cibercrimen,* Marcial Pons, Madrid/Barcelona/Buenos Aires/ São Paulo, 2012.

[4] CLOUGH, J.: *Principles of Cybercrime,* Cambridge University Press, Cambridge, 2010, p. 4.

como medio u objeto para el lucro económico ilícito realizado en perjuicio de tercero. Puede hablarse, incluso, de una simbiosis entre gran parte de los comportamientos ilícitos realizados en el ciberespacio: unos y otros no sólo se entremezclan, sino que generalmente forman parte de una misma dinámica comisiva cuyo objetivo final es la obtención de lucro por parte de las organizaciones cibercriminales. El envío de correos *spam*, por ejemplo, como forma de ataque a innumerables terminales informáticas, es en muchos casos, el primer paso para la posterior infección con *malware*, bien con intención destructiva de información de usuarios o de empresas (a veces con propósito de extorsión), bien con intención de incorporar una *backdoor* que permita el acceso ilícito al sistema para el apoderamiento de información privada o para convertir el sistema informático en un *bot* que permita, posteriormente, su uso como *botnet* para un ataque de denegación de servicios a otra web o para el envío de cantidades ingentes de *spam* con la consiguiente "vuelta a empezar" de la cadena de ataque, o, en la mayoría de casos, para el envío de publicidad falsa tras la cual existe un ataque de *phishing,* cuyo propósito puede ser, de nuevo, la infección con *malware* para la consecución del fraude, o el engaño directo para que sea el usuario el que envíe la información privada bancaria. Y en tal cadena se pueden integrar otros cibercrímenes relacionados con la distribución ilícita de contenidos, como ocurre con la descarga de material protegido por derechos de autor, que puede esconder en muchos casos virus troyanos o infecciones de *botnet*, y también con la distribución de material pornográfico "ilícito"[5], e incluso detrás de la lícita distribución de pornografía "lícita" [6].

Los resultados del primer estudio nacional de cibervictimización[7] muestran esta

[5] En el caso de la distribución de material pornográfico ilícito, usualmente de menores, los cibercriminales muchas veces controlan las propias redes de difusión del citado contenido, y aprovechan la vulnerabilidad del sujeto que trata de descargarse el mismo y el hecho de que la víctima del ataque final difícilmente denunciará unos hechos que le convertirían a él mismo en autor de un delito, para incluir entre los objetos descargados algún tipo de *malware* que permita posteriormente el acceso a las cuentas corrientes de la víctima o para utilizar su sistema informático como parte de una *botnet* que realice posteriores ataques de *spam* o de Denegación de Servicios. Véase sobre todo ello, MIRÓ LLINARES, F.: *El cibercrimen…, ob. cit. p. 120.*

[6] Como señala Maniyara, en estos casos e aprovecha el enorme potencial de difusión de este contenido para atraer a los usuarios con ofertas de gratuidad. De nuevo la cadena comienza con un ataque de *spam,* en el que el correo electrónico reenvía a una página de *phishing* que contiene material pornográfico y en la que al registrarse el usuario con la promesa de material pornográfico gratuito de mayor impacto (contactos con otros usuarios, *videochats* pornográficos, etc.), el usuario se descarga involuntariamente un *malware* con el propósito de la posterior obtención de datos privados bancarios. MANIYARA, M.: "Post del blog Security Response de Symantec, 3 de febrero de 2010". En Internet, en http://www.symantec.com/connect/blogs/phishing-using-pornographic-content-bait. Citado el 3 de abril de 2013, p. 1.

[7] MIRÓ LLINARES, F. /GARCÍA GUILABERT, N.: "Encuesta Nacional de victimización en el ciberespacio", en el marco del Proyecto de Investigación financiado por el Ministerio de Ciencia e Innovación, DER2011-2605, titulado "Cibercriminalidad: detección de déficits en su prevención jurídica y determinación de los riesgos de victimización para una mejor prevención situacional criminológica", presentada en la conferencia *La victimización en el ciberespacio,* impartida en el *IX Congreso Español de Criminología*, Girona, 2012.

prevalencia de los cibercrímenes cuyo objetivo final es el ciberfraude. Concretamente más del 45% de la población española reconoce haber recibido correos proponiéndoles algún tipo de favor o negocio económico sospechoso de ser engañoso y un 43,6% ha recibido algún correo cuya identidad de quien lo enviaba era falsa. En cuanto a infecciones de *malware,* las cuales en la actualidad son admitidas unánimemente por la literatura como ataques de troyanos y *backdoors* destinados a obtener información sensible para un posterior fraude o para conformar una cadena de *spam*, el 72,8% de la población reconoce haberlas sufrido. Y a todo ello hay que sumar el significativo dato de que un 24,4% de la población española reconoce haber sufrido efectivamente una pérdida patrimonial víctima de un ciberfraude.

1.2. *Tipologías de ciberfraude. Análisis particular de los fraudes de* spam*:* scam *y* phishing

Desde una perspectiva criminológica, sin entrar todavía en una calificación jurídica de algún tipo de conducta en particular, hablamos de ciberfraude para denominar a toda una variedad de conductas en las cuales las redes telemáticas se convierten en instrumento esencial mediante el cual lograr un beneficio patrimonial ilícito derivado de un perjuicio patrimonial a una víctima. Son muchas las formas en las que se puede lograr acceder al patrimonio de terceros, utilizando las múltiples formas de relación comercial existentes en el ciberespacio, así como las propias debilidades de seguridad de los sistemas informáticos que dan directamente acceso al patrimonio o indirectamente a él, al contener las claves o datos bancarios de los usuarios. Así, algunas de las más conocidas son los distintos fraudes de tarjetas de crédito, los fraudes de cheques[8], las estafas de inversión[9], las estafas piramidales realizadas a través de Internet[10], las conocidas estafas de la lotería[11], las ventas *online* defraudatorias en las que no se envía el producto comprado (o se envía con otras características, como en el *auction fraud*) o no se paga el recibido o se cobran servicios no establecidos previamente, las estafas de inversión en las que se cobran gastos no previstos o no se explican pérdidas inesperadas[12], así como los ataques de

[8] Especialmente el fraude denominado en inglés, *the counteerfeit cashier's check scheme*, o esquema de falsificación de cheques de caja, destinado a defraudar a personas que venden mercancías por medio de los anuncios clasificados en Internet. Véase la explicación del procedimiento por el IC3 en Internet en http://www.ic3.gov/crimeschemes.aspx#item-3.

[9] O *invest fraud,* por medio de la cual se ofrecen productos financieros, préstamos o similares, que resultan ser falsos.

[10] También denominadas *ponzi frauds* y que son en última instancia fraudes 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.

[11] Aunque las hay de muchos tipos, el esquema del fraude de loterías suele caracterizarse por el envío de *spam* con *emails* en los que se informa a quien lo recibe de que ha ganado una lotería internacional por una cantidad altísima de dinero y que para retirarla, se solicita sin embargo, el ingreso de un dinero que es el objeto de la defraudación.

[12] De hecho, uno de los más comunes y que se mantiene como usual en los últimos años es el denomi-

scam en los que se prometen cantidades importantes de dinero a cambio de pequeñas transferencias relacionadas con ofertas de trabajo, loterías, premios u otros[13], entre una variedad de fraudes que van transformándose constantemente[14].

De todas estas modalidades las más populares, por la total generalización del uso del correo electrónico, son las que podríamos denominar *spam-frauds o email frauds,* y son todos aquellos fraudes en los que la comunicación inicial se realiza por medio de un correo electrónico que, generalmente, ha sido enviado a miles de usuarios al mismo tiempo. Entre ellas conviene diferenciar dos tipos generales, el de los fraudes *scam* y el de los fraudes tipo *phishing.* Los ciberfraudes burdos o *scam* no son más que las tradicionales estafas en las que, en este caso, la forma de comunicación entre las personas para la realización del engaño bastante es Internet, bien el correo electrónico o bien el uso de las redes sociales[15]. Es ésta más bien una

nado *auction fraud*, o fraude en las subastas, consistente 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, 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 CHIU, C./KU, Y./LIE, T./CHEN, Y.: "Internet Auction Fraud Detection Using Social Network Analysis and Classification Tree Approaches", en *IJEC*, vol. 15, núm. 3, 2011, p. 124. ASÍ, CHUA, C.E.H./WAREHAM, J.: "Fighting Internet Auction Fraud: An Assessment and Proposal Computer", en *IEEE Computer,* núm. 10, 2004, p. 32, han tratado de pormenorizar y categorizar las distintas formas de fraude de subastas refiriéndose a las siguientes modalidades: *Shilling* (los vendedores participan en la puja subastando sus propios artículos intentando subir el precio de la puja compitiendo con otros compradores, quienes por lo tanto, deben pujar con cantidades más altas para adquirir los productos); *Bid shielding* (dos personas se confabulan para pujar en la misma subasta, una de ellas realiza pujas bajas mientras que la otra hace pujas muy altas para disuadir a otros compradores. Después, el comprador que ha ganado la puja renuncia al artículo, por lo que la otra persona puede adquirir el producto); *Tergiversación (*los vendedores proporcionan descripciones falsas de sus productos; *Ampliar la factura (*los vendedores ocultan costes extra, como gastos post-subasta por preparación del artículo); *Envío suspendido (*los vendedores no envían los artículos adquiridos por los compradores); *Pago suspendido (*los compradores no pagan después de adquirir un producto); *Reproducción y falsificación (*los vendedores envían productos de imitación de otros auténticos); *Triangulación/custodia (*los vendedores venden productos robados); *Comprar y cambiar (*los compradores reciben los productos, sin embargo, rechazan la transacción y devuelven a los vendedores otros productos similares o de inferior calidad); *Reclamación de pérdida o daños* (los compradores reclaman falsos daños en los productos y piden el reembolso al vendedor); *Auto-subasta (*los vendedores organizan falsas subastas con la intención de obtener nombres de compradores e información de tarjetas de crédito).

[13] Entre otros muchos citados por STADLER, W. A.: "Internet Fraud", en FISHER, B. S./LAB, S. P.: *Encyclopedia of Victimology and Crime Prevention,* vol. 1, Sage Publications, California/London, 2010, pp. 492 y 493.

[14] Así, y tomando como referencia la página web del IC3, que hace una importante labor de recogida de denuncias para la sistematización de los diferentes ciberfraudes existentes, deberían tomarse en cuenta además de los citados, otros como el *debt elimination fraud,* o fraude en los planes de eliminación de deudas, llevado a cabo por falsas empresas que solicitan el ingreso de un dinero al cliente para refinanciar sus deudas hipotecarias y de tarjetas de crédito pero que nunca devuelven; el *scrow services fraud,* o estafa por servicios de custodia en la que se persuade a quien participa en subastas por Internet para que contrate un servicio de custodia que asegure el éxito de la llegada de la mercancía de modo tal que el comprador acaba pagando el dinero y perdiendo el envío.

[15] Véase, extensamente, YAR, M.: *Cybercrime and society,* London, Sage, 2006, pp. 81 y ss. En la actualidad, este tipo de ataques también se conocen en el mundo anglosajón como *cons,* abreviatura del término general *confidence trick*, también denominado *bunko*. Consiste en el comportamiento de tratar de

categoría genérica que podría englobar a casi todos los fraudes, si bien se suele utilizar como referencia de los más burdos de ellos, aquellos en los que el engaño es poco elaborado y en los que el error de la víctima puede ir más allá de lo común. En este caso podríamos integrar el conocido caso de las "cartas nigerianas", estafa clásica semejante al famoso "timo de la estampita" en el que el engaño se logra explotando el ánimo de lucro de la víctima, así como muchas otras que han surgido posteriormente como la de la lotería, la del trabajo desde casa, etc., siempre caracterizadas por tratar de interesar a la víctima o ganarse su confianza para que sea él quien finalmente realice el acto de disposición patrimonial que le perjudica.

Por su parte el *phishing*[16], o pesca de incautos, ha sido definido como el 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[17]. El uso de la ingeniería social se produce cuando 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 datos objetivos. Cuando se utilizan otros artificios técnicos, como por ejemplo, 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, se utiliza el término de *pharming*.

Aunque en las primeras manifestaciones de este tipo de ciberfraude apenas se diferenciaba el mismo de los *scam* dado que los ataques consistían en el intento de obtención de las claves o contraseñas del propio usuario por medio de un engaño realizado a través del correo electrónico, con el paso de los años ha ido incrementando el refinamiento tanto del engaño, como de la calidad técnica de los ataques[18].

defraudar a una persona a partir de ganarse previamente su confianza. En el fondo, no existe apenas diferencia entre los ataques de *scam* y los *cons*.

[16] La palabra *phishing* es una evolución de *fishing*, en alusión al intento de hacer que las potenciales víctimas "muerdan el anzuelo". Los *hackers* frecuentemente reemplazan la letra "f" con las letras "ph", como raíz de la antigua forma de *hacking* telefónico conocida como *phreaking* por lo que lo más probable es que éste sea el motivo por el que se escribe de este modo. No obstante, el término también se ha atribuido a la contracción de *password harversting fishing*, es decir, cosecha y pesca de contraseñas. El origen de esta denominación puede verse más extensamente en JAKOBSSON, M.: *Phishing and Countermesasures: Understanding the Increasing Problem of Electronic Identity Theft,* John Willey & Sons, 2005. FLOR define el *phishing* como "una metodología de ingeniería social dirigida a obtener informaciones personales, costumbres o estilos de vida de otras personas, con el fin de acceder a servicios financieros o bancarios *on line*, asumiendo virtualmente la identidad del titular de los datos de identificación" y añade posteriormente que a través del mismo "puede realizarse un hurto de datos, un abuso de información personal o un fraude de identidad"; FLOR, R.: "*Phishing* y delitos relacionados con el fraude de identidad: un World Wide Problem en el World Wide", en V.V.A.A.: *Robo de identidad y protección de datos,* Aranzadi, Pamplona, 2010, pp. 83 y 84.

[17] Véase JAISHANKAR, K.: "Identity related Crime in the Cyberspace: Examining Phishing and its impact", en *IJCC*, vol. 2, enero-junio, 2008, p. 12.

[18] El número y sofisticación de los ataques de *phishing* se ha incrementado a pesar de los ingentes esfuerzos en desarrollar contramedidas. El número de webs que informaron ser objetivo de *phishing* registró un incremento de 10.047 a 55.643 en diez meses en el período comprendido entre junio de 2006 y abril de

Así por ejemplo, en el año 2000 se comenzaron a utilizar los *key loggers,* esto es, un tipo de software que registra y memoriza en un fichero las pulsaciones que se realizan en un teclado; en 2001 los *phishers* iniciaron el uso de URL ofuscadas; en 2003 llevaron a cabo las primeras grabaciones de contenidos en pantalla o s*creen loggers*; en 2004 utilizaron por primera vez una web falsa y desde 2006 es habitual el *phishing* por VoIP[19].

En la actualidad no hay un único *phishing,* sino múltiples modalidades de este tipo de fraude[20]. Del mismo modo que no hay un único tipo de *hackers* que realizan *phishing*, sino que en esta actividad delictiva participan sujetos con actividades encomendadas de muy distinta naturaleza[21]. Sin embargo, es posible identificar tanto los componentes intrínsecos esenciales del *phishing* como las modalidades más habituales hoy existentes.

En cuanto a lo primero, el *phishing* suele estar formado por tres componentes, el mensaje, la interacción y el robo. En la mayoría de las ocasiones se trata de un correo electrónico remitido por el delincuente, pero también puede ser un SMS, VoIP, mensaje en una red social e incluso en videojuegos con múltiples participantes[22]. Este señuelo no suele ser muy sofisticado desde el punto de vista técnico, sino que a través de la ingeniería social aprovecha las debilidades de las potenciales víctimas[23]. Poniendo en práctica diferentes estrategias de engaño, se consigue que

2007. Véase DONG, X. /CLARK, J.A./JACOB, J.L.: *"Defending the weakest link: phishing websites detection by analysing user behaviours",* en *Telecommun Syst,* núm. 45, 2010, p. 215. Por su parte, el *Anti-Phishing Working Group* (APWG) informó que durante la primera mitad de 2011 una media de 32.650 webs fueron objeto de *phishing,* véase "Phishing Activity Trends Report" 1st Half/2011 consultado en línea el 3 de abril de 2013 en http://apwg.org/reports/apwg_trends_report_h1_2011.pdf.

[19] OLLMAN, G.: *The Phishing Guide: Understanding and Preventing Phishing Attacks. Informe Técnico,* NGSS, 2009, p. 4

[20] Véase con más profundidad MIRÓ LLINARES, F.: *El cibercrimen…, ob. cit.*, pp. 72 y ss.

[21] Se ha producido una especialización en los delincuentes que realizan este tipo de estafas, así, no es extraño encontrar grupos de ciberdelincuentes que se organizan diferenciando entre mensajeros, recolectores y cajeros MYERS, S.: "Introduction to Phishing" en JAKOBSSON, M. /MYERS, S.: *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft,* John Wiley and Sons, 2006, p. 3 Los primeros, bien sean *spammers* o *hackers*, remiten un gran número de correos, generalmente a través de *bot-nets*, es decir, redes de ordenadores comprometidos y controlados por el mensajero. El segundo grupo, el de los recolectores, son *hackers* que construyen o alteran las webs a las que se dirigen los usuarios víctimas de *spam* y de las que se obtiene información confidencial como nombres de usuario, contraseñas o tarjetas de crédito. Un tercer grupo es el de los cajeros, los cuales obtienen información confidencial de los recolectores y hacen uso de ella, creando tarjetas de crédito para obtener dinero en cajeros, comprar productos en línea, hacer transferencias y en definitiva, cualquier actividad que permita el lucro esperado.

[22] HONG, J.: "The State of Phishing Attacks", en *Communications of the ACM,* vol. 55, núm. 1, 2012, p. 74. En relación con los juegos masivos *online,* HILVEN y WOODWARD señalan que el valor de una cuenta robada de *War of Warcraft* es superior al de una tarjeta de crédito, lo que puede ayudar a comprender las complejas consecuencias de esta modalidad de fraude.

[23] Algunos ejemplos de la aplicación de estos principios, son los mensajes en los que se requieren actualizaciones de seguridad, se insta a completar información de cuentas para su mantenimiento, incentivos financieros o falsas actualizaciones. Así, podemos encontrar mensajes del supuesto administrador de un sistema advirtiendo sobre un ataque, que debe evitarse instalando urgentemente un "parche", o la notificación de problemas con la autenticación de usuario, cuya solución consiste en la remisión de una nueva contraseña. En otros casos, el mensaje contiene una proposición relacionada con futuras ganancias o benefi-

el usuario aporte el segundo componente, la interacción; es decir, que la víctima siga un enlace a una URL inserta en un correo electrónico, proporcione determinada información sensible respondiendo a un correo o instale *malware*. Lo más usual es que se requiera a la propia víctima a que acuda a la web que se ha construido de manera idéntica a la de una organización de confianza, como un banco o una popular web de subastas, que instale el *malware* o que remita la información sensible. Para conseguir su objetivo, los *phishers* registran nombres de dominio parecidos a los de la entidad elegida, de este modo, podemos encontrar *ebay-login.com* en lugar de *eBay*, también es posible encontrar imitaciones más burdas tales como *ebay.com.phishsite.com*. Por supuesto utilizan logos e imágenes de las empresas u organismos a los que suplantan, generando una falsa seguridad en la víctima[24]. El tercer y último elemento es la utilización efectiva de la información robada. En algunos casos el delincuente usa directamente los datos de la víctima suplantando su identidad, no obstante, normalmente el *phisher* no explota por sí mismo la información obtenida, sino que la vende a terceros. Tal es el caso visto de las cuentas de usuario para juegos masivos *online* o la venta de números de tarjetas de crédito, de este modo, se ha generado un mercado negro de compraventa de información robada.

Aunque hay tantas variaciones de phishing como formas posibles en las que pueden aparecer los componentes comentados, algunas son más conocidas. La más popular de ellas sería el *phishing* en sentido estricto o *phishing* tradicional, en el que se utiliza la imagen corporativa de una entidad bancaria o de una institución, para solicitar a la víctima por medio de correo electrónico que envíe a una dirección de correo que simula ser de tal entidad, los datos bancarios requeridos. Esta forma de *phishing* ha comenzado a ser sustituida por otras más elaboradas como el *spear phishing* o "pesca con arpón", en la que en lugar de dirigirse a objetivos indiscriminados, se buscan clientes de entidades bancarias u otro tipo de organizaciones concretas. Una variante de este tipo de *phishing* es el *business services phishing*, en el que el objetivo ya no es si quiera un cliente de un banco, sino los empleados de entidades que utilizan servicios como Google AdWords o Yahoo! De manera similar en la modalidad conocida como *whaling*, se ataca a los empleados de alto nivel de grandes empresas o gobiernos. En un ataque de *whaling* el *phisher* se centra en un pequeño grupo de personas de alto nivel de una organización concreta e intenta robar sus credenciales, preferiblemente a través de la instalación de *malware* que proporciona funcionalidades de puerta atrás y *keylogging*. En estos

cios, que finalmente busca aprovechar el ánimo de lucro de la víctima para provocar ingresos de dinero en cuentas. Las ofertas, premios, promociones o regalos constituyen otro de los reclamos utilizados, junto con la solicitud de ayuda humanitaria para víctimas de desastres o situaciones desesperadas.

[24] Para completar el engaño, emplean todo tipo de subterfugios técnicos, como la ofuscación de URL o la utilización de supuestas webs seguras de terceras partes o autoridades de validación, las cuales disponen de medidas de seguridad suplementaria como URL https, o certificados SSL; estas entidades utilizan gráficos e imágenes que son igualmente replicadas por los diseñadores de las falsas webs.

casos, los señuelos no se limitan a la remisión de mensajes, puesto que lo que tratan es de infectar con *malware* el equipo informático, por lo tanto, utilizan todo tipo de medios como CD que contienen software de evaluación o instalan *hardware* del tipo *keylogger* que permite el registro de teclados y ratones.

Otra de las formas de *phishing* más común en la práctica es el basado en *malware*, es decir, cualquier tipo de *phishing* en el que se hace uso de software malicioso en el ordenador del usuario[25]. El ejemplo más común de este tipo de *phishing* es 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. Este *malware* puede presentarse de diferentes formas, que por lo general explotan vulnerabilidades de los sistemas informáticos. De este modo podemos encontrar *keyloggers* o *screenlogers*, es decir, programas diseñados para monitorizar el teclado y el ratón o las entradas en pantalla. En estos casos el sujeto ni siquiera será conocedor de que está enviando las claves, ya que el correo electrónico enviado lleva un archivo que utiliza o bien *spyware*[26], del estilo de los programas *keylogger* o *sniffer,* para localizar los datos bancarios, o bien *malware* para lograr un acceso ilícito y descubrir los datos queridos; similar a éstas, los *hosts file poisoning* o alteración de los archivos de DNS, son defraudaciones que entran dentro de la denominación de *pharming.* Se trata de una táctica fraudulenta que consiste en cambiar los contenidos del DNS (*Domain Name Server* -Servidor de Nombres de Dominio-) ya sea a través de la configuración del protocolo TCP/IP o del archivo *imhost* (que actúa como una caché local de nombres de servidores), para que el usuario, cuando teclea la dirección web de su entidad bancaria en su navegador entre, en realidad, a una web falsa muy parecida o igual a la original, en la que acaba desvelando sus datos bancarios. Además, en caso de que el usuario afectado por el *pharming* navegue a través de un *proxy* para garantizar su anonimato, la resolución de nombres del DNS del *proxy* puede verse afectada de forma que todos los usuarios que lo utilicen sean conducidos al servidor falso en lugar del legítimo; igualmente los *session hijackers* o secuestro de sesiones, lo que permiten es el acceso a los archivos del equipo o a los servicios del sistema; los troyanos web o programas maliciosos que mediante ventanas emergentes recogen claves; y en general cualquier otra técnica que, utilizando software, permite perfeccionar el engaño haciendo creer a la víctima que está fuera de peligro.

También son frecuentes aquellos otros fraudes en los que el correo electrónico

[25] Para conocer una descripción de gran variedad de *malware* véase EMIGH, A.: *Online Identity Theft: Phishing Technology, Clokepoints and Countermeasures. ITTC Report on Online Identity Theft Technology and Countermeasures*, 2005,pp. 6

[26] Que es definido por FERNÁNDEZ TERUELO, como "aplicaciones que se consiguen introducir en el PC de la víctima, y cuyo objetivo es el envío, a un lugar exterior (habitualmente al ordenador del defraudador), de datos del sistema donde están instalados (normalmente claves de acceso a determinados sistemas), sin el conocimiento del usuario"; FERNÁNDEZ TERUELO, J.G.: *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes,* Lex Nova, Valladolid, 2011, p. 36

de la supuesta entidad bancaria incluye un *link* que redirige al sujeto, aparentemente, a una página web de la entidad que en realidad no es tal y que permite al atacante conocer los datos bancarios de su víctima, ya que el sujeto piensa que está tecleando las claves en su entidad bancaria. Esto se consigue accediendo a un servidor cuya seguridad se ha visto comprometida y sustituyendo el contenido legítimo por otro malicioso o aprovechando vulnerabilidades de las bases de datos SQL que permiten ejecutar *scripts*.

2. **La respuesta penal al ciberfraude**

2.1. ***La regulación de la estafa informática en el Ordenamiento Jurídico español y la respuesta penal a los ciberfraudes***

2.1.1. *Ciberfraude y delito de estafa informática*

La preocupación por la mejor respuesta jurídico-penal posible a los ciberfraudes es, coherentemente, tan antigua como las primeras noticias de los mismos. Y pese a que, como se verá, no siempre concuerdan todas las modalidades en el constructo dogmático tradicional de la estafa, fue en el mismo en el que se intentaron encauzar desde un primer momento, especialmente por excluirse más claramente otras modalidades penales de protección patrimonial. En efecto, frente a este tipo de comportamientos en el ciberespacio los delitos tradicionales de apoderamiento, no parecen ser adecuados, dado que en ellos el elemento tomar o apoderarse siempre se ha interpretado en un sentido físico o material que no se da en la mayor parte de estas conductas en las que, además, hay muchos casos en los que es la propia víctima la que realiza el acto de disposición patrimonial que le perjudica. Tampoco la apropiación indebida concuerda en absoluto con estas tipologías de infracción al patrimonio. Los tipos defraudatorios como la estafa podían corresponder mucho mejor a la dinámica de "uso de las TIC para engañar a un tercero" en que consistían, y consisten, muchas infracciones. El problema que planteaba la estafa, por su parte, era la exigencia de engaño del sujeto activo, que dejaría fuera del ámbito típico todo un conjunto de conductas en las que la transferencia patrimonial se logra por medio de la manipulación de alguno de los procesos informáticos existentes en la actualidad.

Con esta intención de dar cobertura de protección penal a aquellas defraudaciones realizadas usando medios informáticos se incluyó en el CP de 1995 el delito de estafa informática del artículo 248.2 CP que sanciona a 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"[27]. En este delito, también denominado de fraude informático, se sustituye la

[27] Aunque, como recuerda FERNÁNDEZ TERUELO, "el tipo de la estafa informática no nació, en absoluto, con objeto de resolver situaciones fraudulentas ejecutadas a través de Internet, pues recuérdese que la

exigencia de engaño personal, por la conducta de manipulación informática, la cual ha sido definida en varias sentencias por el TS como aquella que está presente cuando la máquina, informática o mecánica, *actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquellos que permite su programación, o por la introducción de datos falsos*[28]. Sin entrar aquí en la profunda y compleja discusión sobre el alcance del concepto de manipulación informática[29], en lo que existe acuerdo doctrinal es acerca de que la descripción de la conducta típica se realizó, intencionadamente, de forma muy amplia, para englobar prácticamente cualquier modalidad de comportamiento que utilizase[30] las tecnologías de la información para conseguir el resultado de una transferencia patrimonial en perjuicio de un sujeto pasivo[31]. Este es, en realidad, el objetivo del legislador, el proteger el patrimonio frente al uso de sistemas informáticos, que es lo que en realidad se tipifica como comportamiento típico. No entiendo, pues, frente a un sector de la doctrina, que sea necesaria una equiparación de la manipulación informática al engaño de la estafa, sino que más bien la manipulación informática o el artificio semejante, se convierten en una fórmula amplia que permite integrar en el ámbito típico de la estafa informática, cualquier transferencia patrimonial que se haya obtenido mediante la utilización de técnicas o sistemas informáticos.

Hay que tener en cuenta, sin embargo, que no es la de la sustitución del engaño personal por la manipulación informática[32], la única diferencia de la estafa informáti-

introducción del tipo en el Código penal se produce en un momento (mediados de los años 90 del siglo pasado) en el que aún no se había producido un desarrollo significativo del uso de la Red en nuestro país. Realmente, el principal objetivo perseguido con su tipificación era el de sancionar situaciones fraudulentas planteadas en entidades bancarias o terminales de pago (TPV) en las que algún empleado o tercero operando sobre ellas, realizaba transferencias a su favor o a favor de tercero"; FERNÁNDEZ TERUELO, J.G.: *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes,* Lex Nova, Valladolid, 2011, p. 46.

[28] Entre otras, la STS núm. 2175/2001, de 20 de noviembre de 2001 y la STS núm. 692/2006, de 26 de junio de 2006, que confirma la SAP de Madrid núm. 92/2005 de 28 de febrero de 2005.

[29] Véase, entre otros, MATA Y MARTÍN, R. M.: *Delincuencia informática y Derecho penal,* Madrid, Edisofer, 2001, pp. 45 y ss.; HERRERA MORENO, M.: "El fraude informático en Derecho penal español", en *AP,* núm. 39, 2001, p. 952. También sobre la discusión y alcance del concepto de manipulación informática GALÁN MUÑOZ, A.: "El robo de identidad: aproximación a una nueva y difusa conducta", en V.V.A.A.: *Robo de identidad y protección de datos,* Aranzadi, Pamplona, 2010, p. 176, donde se adscribe a una concepción amplia de este concepto.

[30] Precisamente, GALÁN MUÑOZ propone reformar el vigente 248.2 CP "reemplazando el término "manipulación" por el menos problemático y general de "utilización", ya que ello permitiría excluir cualquier posible interpretación limitadora de este delito que tratase de fundamentarse en su supuesta (…) cercanía con el delito de estafa tradicional, delito del que, además, también debería diferenciarse en términos punitivos", GALÁN MUÑOZ, A.: "El robo de identidad: aproximación…", *ob. cit.*, pp. 177 y 178.

[31] Lo cual, sin embargo, ha sido criticado por algún autor por falta de taxatividad. Así, CHOCLÁN MONTALVO, J. A.: "Fraude informático y estafa por computación", en *CDJ,* núm. 10, 2001, p. 328. Precisamente por ello, el autor aporta una definición restrictiva de manipulación informática, entendiendo por ella "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".

[32] En el mismo sentido, FERNÁNDEZ TERUELO propone como elemento diferenciador entre la estafa in-

ca con la estafa tradicional y el único elemento clave definitorio del ámbito de injusto de la primera de ellas[33]. Otra diferencia importante es que en la estafa informática no se exige que sea el propio sujeto pasivo el que realice el acto de disposición patrimonial sino que, más bien a la inversa, debe ser el propio sujeto activo el que transfiera dinero a su cuenta. De este modo, al igual que para que haya estafa es necesario que sea el propio sujeto engañado el que realice el acto de disposición patrimonial, para que haya estafa informática es necesario que eso no ocurra, esto es, que haya una transferencia "no autorizada", siendo irrelevante si la transferencia la realiza el propio sujeto activo o un tercero. Y esa diferencia va a ser determinante, como hemos dicho, a la hora de concretar el régimen punitivo del delito en relación con los ataques al patrimonio que se realizan a través de Internet, pues dejará fuera del mismo a aquellos comportamientos defraudatorios que logren que sea el propio usuario el que autorice la transferencia, aunque no sepa que es en su propio perjuicio. En esos casos, y siempre que pueda probarse, además, que ha existido engaño por parte del sujeto y que ha sido éste el que ha llevado al error que, a su vez, produce el acto de disposición patrimonial en perjuicio de la víctima, habrá delito de estafa.

Parece, pues, que el legislador ha diseñado un régimen que supone una amplia tutela de la protección del patrimonio frente a las diferentes tipologías de cibercriminaliad que hemos analizado: casi cualquiera de las conductas de los cibercriminales por medio de las cuales obtienen un beneficio patrimonial directamente derivado y proporcional al perjuicio que causan a otro, puede ser sancionada penalmente. Pero hemos visto como no siempre es el delito de fraude informático el que servirá para dar respuesta penal a estas conductas, sino que las mismas deberán ser reconducidas en muchos casos al delito de estafa. Y es el momento de analizar, aunque sea someramente, la posible incardinación de las principales tipologías de fraude en Internet en los tipos penales existentes.

Pues bien, en primer lugar son sancionables penalmente, concretamente por medio del delito de estafa informática, el denominado *tampering* o *data diddling,* esto es, la modificación no autorizada de los datos o del software que los trata (que no del procesamiento), incluyendo el borrado de archivos o la modificación de éstos, y consiguiendo, de ese modo, la transferencia patrimonial. Éstas son las que se han denominado por la doctrina "alteraciones del INPUT"[34], y sobre las que existe

formática y la estafa común "la ausencia de engaño y error en la estafa informática", y por tanto la existencia en la estafa común de "una relación/interlocución entre, al menos, dos personas: la que engaña y el engañado. Si faltara ésta normalmente habrá de acudirse a la estafa informática."; FERNÁNDEZ TERUELO, J.G.: *Derecho penal e Internet…, ob. cit.* pp. 45 y 50. En el mismo sentido, FARALDO CABANA, P.: *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico,* Tirant lo Blanch, Valencia, 2009, p. 86.

[33] Sobre ellas, véase especialmente, el completo análisis de GALÁN MUÑOZ, A.: *El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 CP,* Tirant lo Blanch, Valencia, 2005, pp. 765 y ss.

[34] Véase al respecto de la distinción entre alteraciones del INPUT y del OUTPUT, GALÁN MUÑOZ, A.: *El fraude y la estafa…, ob. cit.,* pp. 560 y ss.

acuerdo doctrinal acerca de su incriminación por vía del artículo 248.2[35]. También entrarán aquellas otras transferencias logradas gracias a un uso de los tratamientos informáticos o a una modificación en los resultados del procesamiento automatizado de datos, o alteraciones de OUTPUT[36]. En realidad, y como se ha dicho, al utilizarse un concepto amplio de "manipulación", bastará con que el sujeto que consiga la transferencia patrimonial lo haga utilizando sistemas informáticos para que haya fraude del 248.2, con lo que ya estoy adelantando mi respuesta respecto a los últimos casos que vamos analizar.

2.1.2. *Respuesta penal a ciberfraudes tipo* scam *y fraudes de compras*

Nos queda por estudiar la posible incardinación dentro de los delitos patrimoniales de los que, por otra parte, son los más frecuentes casos de defraudación en el ciberespacio, los ataques *scam*, y los ataques patrimoniales realizados tras haber obtenido del propio usuario o mediante el uso de *spyware* o *malware* las claves y datos bancarios necesarios para ello. En cuanto a los primeros, los denominados *scam*, comienzan con el envío de *spam* o correo electrónico no deseado, en el que se trata de engañar al sujeto, generalmente prometiéndole la obtención de un beneficio patrimonial de forma sencilla, siempre que, previamente, el sujeto realice algún tipo de ingreso en la cuenta corriente para poder comenzar las transacciones comerciales[37]. Este comportamiento, cuyo principal exponente es el de las denominadas cartas nigerianas en las que se prometía compartir una sustanciosa fortuna de un príncipe africano a cambio de ingresar un dinero en una cuente corriente que permitiría sacar el dinero del país de procedencia, no encaja en absoluto en el delito de estafa informática del artículo 248.2, dado que en el mismo, hay una transferencia autorizada, aunque sea debida a un engaño. Por el contrario, donde encaja este comportamiento es en el delito de estafa tradicional, dado que se utiliza el correo electrónico para engañar a un sujeto llevándole al error por el que realiza posteriormente un acto de disposición patrimonial en perjuicio propio o de terceros. Así pues, se reafirma la idea de que es el elemento de la transferencia autorizada (estafa), o no autorizada (estafa informática) el que va a ser determinante para la calificación jurídica de los ciberfraudes, de forma que cuando sea el sujeto pasivo el que

[35] Así, por todos, ROVIRA DEL CANTO, E.: *Delincuencia informática y fraudes informáticos,* Comares, Granada, 2002, pp. 265 y ss. Acerca de lo que ya no existe tanto acuerdo es, en cambio, si es asimilable a las acciones relativas a la fase INPUT, la introducción de datos que no son falsos, pero por parte de un sujeto no autorizado, CHOCLÁN MONTALVO, J. A.: "Fraude informático…", *ob. cit.,* p. 330. Sobre ello, volveremos más adelante cuando analicemos el caso del *phishing*, aunque se puede adelantar nuestra opinión favorable a considerar que aquí hay manipulación informática.

[36] Así, GALÁN MUÑOZ, A.: *El fraude y la estafa…, ob. cit.,* p. 562. En sentido contrario, CORCOY BIDASOLO, M./JOSHI, U.: "Delitos contra el patrimonio…", *ob. cit.,* p. 135.

[37] FLORES PRADA describe el *scam* como "una modalidad de estafa informática compleja y estructurada en varias etapas", FLORES PRADA, I.: *Criminalidad informática. Aspectos sustantivos y procesales,* Tirant lo Blanch, Valencia, 2012, p. 210. También refiriéndose a las diversas etapas del *scam*, la SAP de Zaragoza, de 2 de noviembre de 2010.

realice la transferencia patrimonial, el hecho no podrá ser nunca calificado de estafa informática. [38]

Resta tan sólo, pues, la calificación de las conductas consistentes en la obtención, por medio de engaño, *spyware, hacking* o cualquier otra forma, de las claves y datos informáticos y su posterior utilización para obtener un lucro patrimonial en perjuicio de tercero. Pues bien, hay que distinguir en primer lugar, dentro de esta modalidad de fraude que es la que se ha acabado generalizando en Internet, entre aquella en la que se utilizan las claves para realizar una compra telefónica o electrónica, y el ya analizado *phishing*. El otro tipo de fraude es menos común, pues pese a generalizarse los sistemas de compra de bienes por medio de Internet y por vía telefónica, también los bancos están comenzando a utilizar sistemas para avisar, antes de que se produzca el envío del producto por parte del vendedor, de la venta (por ejemplo, por medio de sms). En todo caso, hay que valorar si la misma tiene incardinación en alguno de los tipos penales que protegía el patrimonio en su regulación anterior a la reforma.

En la doctrina hay quien ha considerado que el hecho es susceptible de ser sancionado como estafa común[39], y quien ha considerado que el hecho podría reputarse como estafa informática[40]. En cuanto a la consideración del hecho como una estafa común, resulta más que discutible que pueda hablarse de engaño en la conducta de obtener el número de tarjeta de crédito y demás datos necesarios (fecha de caducidad) para obtener el beneficio patrimonial[41], pero lo que desde luego no plantea ninguna duda es que no es manipulación informática, pues en este tipo de comportamientos no hay un acto de disposición patrimonial por parte del sujeto que ha sido objeto del engaño. Más bien es el propio sujeto activo el que realiza el acto que le procura a él el beneficio y a la víctima el perjuicio patrimonial[42]. Esto podría hacer pensar que entra entonces el comportamiento dentro

[38] En este mismo sentido, también menciona FERNÁNDEZ TERUELO como diferencia con la estafa común el hecho de que "la transferencia de activos patrimoniales no es realizada por la víctima del engaño, sino por el propio autor o un tercero a través del sistema", aproximándose a lo por mí apuntado; FERNÁNDEZ TERUELO, J. G.: *Derecho penal e Internet…, ob. cit.,* p. 50. En esta misma dirección explica FARALDO CABANA que "el acto de disposición patrimonial, la transferencia de activos patrimoniales, no es realizado por la víctima del engaño, como en la estafa común, pues aquí no suele haber contacto humano, sino por el propio autor a través del sistema. Consecuentemente, se exige que se trate ce una transferencia "no consentida", elemento que no está presente en la estafa común porque allí el acto de disposición lo realiza el sujeto pasivo del delito en perjuicio propio, por consentimiento viciado por el error, o el sujeto pasivo de la acción en perjuicio de tercero, siendo irrelevante que el tercero haya consentido o no"; FARALDO CABANA, P.: *Las nuevas tecnologías…, ob. cit.,* p. 86.

[39] MATA Y MARTÍN, R. M.: *Delincuencia informática…, ob. cit.,* p. 57.

[40] FARALDO CABANA, P.: *Las nuevas tecnologías…, ob. cit.,* pp. 91 y ss.

[41] Así lo advierte FARALDO CABANA, P.: *Las nuevas tecnologías…, ob. cit.,* pp. 90 y 91, quien dice que "ni se engaña a una persona física ni la transferencia del activo patrimonial es realizada por la víctima o un tercero a consecuencia del error ocasionado por el engaño, sino por el propio autor".

[42] Al fin y al cabo, el acto de disposición patrimonial no es la venta de la cosa, como luego se verá, sino el dinero que es utilizado por el sujeto activo para comprarla en perjuicio del titular de la tarjeta de crédito; por lo que no puede decirse que hay un acto de disposición patrimonial, ni del perjudicado (que no

de los parámetros de la estafa informática. Hay que distinguir, sin embargo, dos tipos de casos.

Por una parte, podríamos situar aquellos supuestos en los que el pago se realiza a través de la propia Red, utilizando algunos de los sistemas existentes en los que basta con saber el número de tarjeta, la fecha de caducidad y algún otro número de identificación que también debe haber sido espiado. Aquí, y como ha señalado Faraldo Cabana, sí hay manipulación informática "pues aunque el sistema informático funciona correctamente y los datos introducidos son reales, se utilizan sin consentimiento del titular" o, en otras palabras, simplemente porque se ha utilizado un sistema informático. Más complejo parece, por el contrario, entender que en estos casos ha habido una transferencia no autorizada. Tal consideración dependerá de cuál entendamos que es el activo patrimonial transferido: el dinero de la compra, o el objeto que se vende, lo cual a su vez dependerá de que entendamos que la compra ha sido válida y perfeccionada o de que no lo ha sido. Si entendemos que no ha habido compra legal y que, por tanto, la entidad vendedora debe devolver el dinero que ha recibido electrónicamente, estaríamos ante un hecho atípico, pues en ese supuesto la transferencia del activo patrimonial consistente en el bien que se vende, habría sido "autorizada". Por el contrario, si se entiende que sí ha habido venta y que, por tanto, el que debe cargar con la pérdida es el comprador, entonces sí podríamos hablar de una transferencia no autorizada de un activo patrimonial realizada utilizando medios informáticos y, por tanto, de una estafa informática del artículo 248.2. Evidentemente, estamos ante este último caso: la compra ya ha existido y, por tanto, el activo patrimonial que ha sido transferido es el dinero y no la cosa, y dado que no ha habido autorización por parte del titular, estaríamos ante una estafa informática punible.

Por otra, estarían aquellos en los que las claves se han obtenido utilizando sistemas informáticos pero, una vez obtenidas éstas, el pago que produce el perjuicio patrimonial, se realiza vía telefónica. En ese caso, es cierto que no puede afirmarse que la transferencia patrimonial se haya llevado a cabo gracias a una manipulación informática realizada por el sujeto, lo que nos llevaría aparentemente a la impunidad. Puede utilizarse, en cambio, la figura de la autoría mediata si entendemos que la operadora telefónica, cuando (generalmente) utiliza un sistema informático para realizar la venta, es la que está llevando a cabo la manipulación (en el sentido que le hemos dado de uso del sistema) bajo error inducido por el sujeto que se está haciendo pasar por el titular de la tarjeta de crédito. Conforme a eso, el hecho podría ser considerado punible por medio de la estafa informática, siguiendo la argumentación anterior.

Puede decirse, pues, que no hay laguna de punibilidad alguna ante este tipo de supuestos de compras llevadas a cabo utilizando los datos de la tarjeta de

interviene), ni del que realiza la venta.

crédito de otro sujeto, que siempre podrán ser sancionados como estafas informáticas.

2.1.3. *Sobre la posible punición de algunos actos previos al ciberfraude como tentativa de estafa*

Se ha señalado anteriormente que el objetivo final de la gran mayoría de los ataques en la Red es la defraudación del patrimonio de un sujeto individual que opera en el mismo y que, realice o no actividades económicas a través de Internet, utiliza servicios como el correo electrónico o la propia WWW a través de un ordenador personal o de empresa, lo cual es ya suficiente para que su patrimonio pueda verse potencialmente afectado. Los ataques de *spam*, el envío de *malware* consistente en troyanos, *backdoors,* etc., la infección por medio de *spyware*, o el uso de programas *sniffer* o *keylogger* son generalmente pasos previos destinados a localizar datos bancarios o a que sea la propia víctima quien los entregue o a que realice directamente aquello que le va a producir el perjuicio patrimonial y el beneficio patrimonial del cibercriminal. Corresponde, pues, dentro del análisis de la protección penal del patrimonio frente a las distintas modalidades de ciberfraude y su posible incardinación en la estafa común o la estafa informática, comprobar si algunos de los comportamientos preparatorios del fraude final, tales como el envío de *spam* de *phishing*, la infección de *spyware* y *malware*, y otros, que suelen servir como pasos previos para el posterior ataque patrimonial, pueden sancionarse como tentativa de estafa informática. Es éste un delito de resultado que se consuma con el perjuicio patrimonial producido por la transferencia no autorizada de activos patrimoniales, y en el que es posible, por tanto, la tentativa de quien, conociendo que su conducta puede causar la lesión del bien jurídico, la lleva a cabo sin afectarlo definitivamente, pero poniéndolo en riesgo.

No creo, conforme a ello, que el mero envío de *spam* que contenga mensajes de *phishing*, ni tampoco la infección de *malware* o *spywares*, por sí mismas, puedan reputarse tentativa del delito, excepto en aquellos casos en los que la conducta realizada ya tenga la capacidad potencial para producir el resultado, el cual no acabe por producirse por causas externas al sujeto activo[43]. Así, podremos considerar que hay tentativa de delito, por ejemplo, en los casos en los que el sujeto pasivo comienza a meter los datos en la página web falsa, pero no cuando simplemente se mandan los mensajes engañosos o se infecta con software espía el sistema informático ajeno. Quizás la duda estriba en si podrían considerarse ya tentativa, aquellos

[43] En similar sentido, se expresa MATA Y MARTÍN cuando afirma que "la creación de falsas páginas webs donde se invite a los usuarios a reproducir sus datos (*pharming)* o el envío de correos electrónicos para lograr que los propios usuarios faciliten sus datos mediante justificaciones falsas (*phishing)* no constituyen, por sí mismos, el engaño o manipulación informática requeridas como elementos típicos de estos delitos", refiriéndose a la estafa en su modalidad convencional (art. 248.1) y a la estafa informática (art. 248.2); MATA Y MARTÍN, R.: "El robo de identidad: ¿una figura necesaria?", en V.V.A.A.: *Robo de identidad y protección de datos,* Aranzadi, Pamplona, 2010, p. 211.

supuestos en los que el sujeto activo obtiene las claves bancarias que necesita, pero no ha llegado a utilizarlas en la entidad bancaria para realizar la transferencia. Como apoyo interpretativo podríamos tener en cuenta la doctrina jurisprudencial referida a los casos de sustracción de las claves de una tarjeta para posteriormente ser utilizadas en un cajero o comercio, en las que se considera que todavía no hay inicio de la tentativa ni el hecho es reconducible a ningún tipo patrimonial[44]. Aun así, esta cuestión merecería un análisis profundo que tuviera en cuenta que la tenencia de las claves de la banca electrónica, cuando con las mismas se puede realizar directamente una transferencia bancaria, es un acto con una peligrosidad idónea para la realización de tal transferencia en perjuicio de la víctima.

En todo caso, y frente a lo que se señala para las claves de las tarjetas de crédito, algunos de los comportamientos preparatorios del *phishing* y de otras formas de fraude informático, pueden ser susceptibles de ser sancionados por otros tipos penales distintos. Este es el análisis que, centrado en el *phishing,* se realizará a continuación.

2.2. ***Tratamiento penal del*** **phishing**

2.2.1. *La punibilidad del* spoofing *y otras conductas preparatorias del* phishing

Como se ha visto, la obtención de la clave y la defraudación final en el *phishing,* no es más que la punta del iceberg de un proceso complejo y variable en el que puede haber actos de suplantación de la personalidad de personas jurídicas, infección con *malware* o *spyware*, accesos ilícitos informáticos, búsqueda de claves en sistemas informáticos y actos de apoderamiento patrimonial. Antes, pues, de realizar un análisis sobre la posible calificación jurídica del *phishing* en el que ya existe el perjuicio patrimonial efectivo a la víctima, resulta de interés analizar si alguna de estas conductas que lo conforman y que se ejecutan antes del fraude propiamente dicho, puede ser sancionada penalmente.

Pues bien, el primer comportamiento ilícito cuya posible responsabilidad penal debiera analizarse, es el *spoofing* o robo o suplantación de la personalidad de una persona física o, más usualmente, jurídica, con intención maliciosa. El *spoofing* no se da únicamente en las conductas de *phishing,* sino que suele ser una técnica habitualmente utilizada por los cibercriminales, y para la realización de infracciones de muy diverso tipo[45]. En el *phishing*, el *spoofing* es esencial, y suele ser el

[44] SAP de Sevilla de 10 de marzo de 2004 (JUR 2004\12683), citada por FERNÁNDEZ TERUELO, J. G.: "Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de red", en *RDPC*, núm. 19, 2007, p. 242.

[45] No obstante, como indica FLOR, todos los informes e investigaciones realizadas por organismos nacionales e internacionales sobre el "hurto de identidad" han incluido los *phishing attacks* entre las principales técnicas empleadas para realizar el "fraude de identidad" en la sociedad de la información; FLOR, R.: "*Phishing* y delitos relacionados…", *ob. cit.,* p. 82.

primer paso de la dinámica comisiva en unión con el *spam*: en el correo que se envía a la potencial víctima, el cibercriminal suele suplantar la personalidad de, en este caso, la empresa, entidad bancaria o ente público por el que se hace pasar el sujeto activo, con la intención de que el sujeto pasivo entregue directamente las claves, o entre en una página web ficticia en la que, o bien el sujeto es infectado de un *malware* o bien es obligado por la falsa entidad bancaria a revelar sus datos. Tal suplantación de personalidad es, sin duda, un hecho ilícito que, sin embargo, tiene difícil acomodo en los tipos penales existentes. En primer lugar, si se consigue identificar a un sujeto que ha enviado correos de *phishing* y se prueba la capacidad o peligrosidad *ex ante* de su comportamiento para llevar a otro a engaño y su intención de hacerlo, podría ser posible imputarle responsabilidad por la tentativa del ilícito principal. Aunque sobre esto ya se ha adelantado algo anteriormente, vale la pena volver a argumentar que está demasiado lejano el envío del correo electrónico al peligro para el bien jurídico, como para configurar una tentativa que, sin embargo, sí puede entenderse existente cuando la víctima da por cierta la suplantación de personalidad y envía o pone involuntariamente a disposición las claves bancarias que, después, y por el motivo que sea, no dan lugar a la transferencia patrimonial o al perjuicio.

Si el *spoofing* por sí mismo no puede reputarse tentativa de estafa, hay que plantearse si puede sancionarse el mismo como delito de usurpación del estado civil. El mismo se regula en el artículo 401 que sanciona con la pena de prisión de seis meses a tres años al que "usurpare el estado civil de otro". La práctica judicial suele rechazar esta posibilidad, al entenderse implícitamente que tal usurpación exige cierta continuidad en la suplantación de personalidad. Cuestión diferente es que la suplantación lo sea de la personalidad de una institución pública (por ejemplo, la Agencia Tributaria, en el conocido *spam* en el que se insta a un sujeto a poner determinados datos, generalmente de información bancaria, en una web falsa que aparenta ser de Hacienda). En ese caso podría haber un delito de usurpación de funciones públicas si el sujeto, además de atribuirse carácter oficial, ejerce actos propios de una autoridad o funcionario público, según reza el artículo 402 CP, lo que no será habitual. Hay autores que han considerado que tal comportamiento por sí mismo puede constituir un delito de falsedades en documento mercantil[46]. Lo cierto es que tal interpretación no me parece defendible para la gran mayoría de los casos[47], especialmente para aquellos en los que lo que se falsea es una carta de

[46] Así lo entiende VELASCO NÚÑEZ, E.: "Fraudes informáticos en Red: del *phishing* al *pharming*", en *LL,* núm. 37, año IV, abril 2007, p. 61, quien dice que no existiendo en España el delito de suplantación informática de la personalidad, es necesario castigar por este tipo conductas que atacan al bien jurídico de ese delito: "la confianza en las transacciones mercantiles, en este caso, a través de la llamada banca, venta o pago on-line".

[47] Podrían excepcionarse aquellos casos en los que lo que se falsee, sí pueda considerarse lo que tradicionalmente ha entendido la jurisprudencia como un documento mercantil. Según expresan la STS núm. 35/2010, de 4 de febrero de 2010, en su fundamento quinto, la STS núm. 788/2006, de 22 de junio de 2006,

publicidad del supuesto banco, pues supondría convertir prácticamente cualquier cosa en documento mercantil (*flyers,* etc.). Otra cosa es que se pueda considerar una falsificación en documento privado del artículo 395, que castiga al que "para perjudicar a otro cometiere en documento privado alguna falsedad" tal como, por ejemplo, "la simulación de un documento en todo o en parte, de manera que induzca a error sobre su autenticidad". La clave estriba en determinar si podríamos considerar documento a tal tipo de soporte.

El CP define documento en el artículo 26 como "todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica". Creo que una carta de información personal, o una página web no tiene relevancia jurídica ninguna, por lo que creo que, de nuevo, tales comportamientos serían reputados atípicos por cualquier tribunal sobre la base de este único precepto[48]. Del mismo modo, y aunque en gran parte de los comportamientos de *phishing* hay una utilización de marcas y signos distintivos de entidades bancarias, tampoco creo que sea posible la condena de tales conductas por

y la STS núm. 764/2008, de 20 de noviembre de 2008, en su fundamento segundo, basándose a su vez en otras resoluciones como la STS núm. 625/1997, de 8 de mayo de 1997, y la STS núm. 1148/2004, de 18 de octubre de 2004, el concepto jurídico-penal de documento mercantil es "un concepto amplio, equivalente a todo documento que sea expresión de una operación comercial, plasmado en la creación, alteración o extinción de obligaciones de naturaleza mercantil, ya sirva para cancelarlas, ya para acreditar derechos u obligaciones de tal carácter, siendo tales no solo los expresamente regulados en el Código de Comercio o en las Leyes mercantiles, sino también todos aquellos que recojan una operación de comercio o tengan validez o eficacia para hacer constar derechos u obligaciones de tal carácter o sirvan para demostrarlas, criterio éste acompañado, además por un concepto extensivo de lo que sea aquella particular actividad. Como documentos expresamente citados en estas leyes figuran las letras de cambio, pagarés, cheques, órdenes de crédito, cartas de porte, conocimientos de embarque, resguardos de deposito y otros muchos: también son documentos mercantiles todas aquellas representaciones gráficas del pensamiento creadas con fines de preconstitución probatoria, destinadas a surtir efectos en el tráfico jurídico y que se refieran a contratos u obligaciones de naturaleza comercial, finalmente, se incluye otro tipo de representaciones gráficas del pensamiento, las destinadas a acreditar la ejecución de dichos contratos tales como facturas, albaranes de entrega u otros semejantes". Añade, sin embargo, la STS 788/2006 de 22 de junio de 2006, en su fundamento primero, que a pesar de esta consolidada jurisprudencia "la moderna jurisprudencia no se ha mostrado insensible al sentido restrictivo del concepto que impera en la praxis mercantilista, habiéndose declarado que el hoy artículo 392 del Código Penal se refiere sólo a aquellos documentos mercantiles merecedores de una especial protección, porque su materialidad incorpora una presunción de veracidad y autenticidad equivalente a un documento público, lo que es la «ratio legis» de la asimilación, de modo que «no es suficiente con que se trate de un documento utilizado en el tráfico mercantil, sino que se requiere una especial fuerza probatoria, como ocurre con las letras de cambio, que sin una protección especial difícilmente podrían ser transmisibles por endoso en la forma habitual». De este modo, pues, y frente a la falsificación de documentos privados tipificada con carácter residual en el artículo 395 del CP, al que se llega por exclusión de los restantes tipos de documentos (es decir, aquéllos que, reuniendo los requisitos del artículo 26 del CP, no sean públicos, oficiales y mercantiles) y que también recoge el artículo 324 de la LECiv, no cualquier documento, ni siquiera aunque se refiera a publicidad de una empresa, debiera reputarse documento mercantil, sino sólo aquél que pueda ofrecer una especial fuerza probatoria. Creo que generalmente no será el caso en los supuestos de *web spoofing* y de *phishing*.

[48] En sentido contrario, MATA Y MARTÍN, que considera que "La naturaleza electrónica de la página web no introduce dificultades para su calificación como documento pero lo que puede generar más incertidumbre sobre su carácter son las funciones múltiples de las mismas o si es la página web la que directamente constituye un documento o en realidad lo son aquellos que se generen como consecuencia de alguna operación realizada con ella." MATA Y MARTÍN, R.: "El robo de identidad…", *ob. cit.*, p. 216.

medio del artículo 274 CP. Al fin y al cabo, el tipo exige actuar con fines industriales o comerciales que en este tipo de conductas no están presentes, y también que se actúe para distinguir los mismos o similares servicios, y aquí no se está prestando ningún servicio realmente, por lo que creo que la aplicación del tipo no cabría aun cuando se use la marca de un banco o caja, etc.

Algo similar ocurre con lo que se ha venido en denominar acceso ilícito no autorizado a un sistema informático, que es lo que se lleva a cabo en determinadas conductas de *phishing* y *pharming* cuando el *hacker* aprovecha alguna *backdoor* con la que se ha infectado previamente el sistema para entrar en él y tratar de adquirir la información privada. Este comportamiento era atípico hasta la reforma de 2010 pero ya no lo es al haberse incluido en tal modificación del Código Penal el nuevo art. 197.3 CP que sanciona el mero intrusismo o acceso informático ilícito a un sistema con vulneración de medidas de seguridad[49]. Este precepto permitirá sancionar las modalidades de *phishing* que requieran de un *hacking,* que ciertamente son las menos, dado que bastará con que el sujeto vulnere los sistemas de seguridad y acceda a datos o programas protegidos para que su conducta sea punible por medio del artículo 197.3.

En muchos casos el *hacking* o acceso se realiza no sólo al sistema sino a los datos, especialmente cuando se intenta obtener la clave. En este sentido, podríamos plantearnos si serían punibles tales actos por medio del art. 197.1 CP por entender que habría apoderamiento (en el sentido de captación mental) de documentos o interceptación de comunicaciones realizados para descubrir un secreto o vulnerar la intimidad de otro. La cuestión, sin embargo, no es tan sencilla a mi parecer. No puede dudarse de que quien, por ejemplo, observa gracias a un troyano los movimientos bancarios que un sujeto realiza desde su correo electrónico, está interceptando las comunicaciones para descubrir un secreto, en este caso, la clave bancaria. Pero la pregunta sería ¿puede conceptuarse la clave bancaria como un secreto personal? Al fin y al cabo, el TS ha señalado que no cualquier secreto es objeto del delito del artículo 197 CP, sino sólo aquellos relacionados con la intimidad personal. ¿Es el caso de, por ejemplo, las claves bancarias? Es cierto que la jurisprudencia del TC sobre el concepto de intimidad, desarrollada especialmente en casos de divorcios donde las parejas se llevan documentos bancarios del otro, afirma que los datos personales patrimoniales "sí afectan a la intimidad personal", pero también lo es que en este caso, el objeto del que se pretende el descubrimiento es una mera clave bancaria que, por sí misma, difícilmente puede llevar una carga de información personal como sí puede hacerlo, por ejemplo, el extracto de cuenta de una persona que relata sus compras, o similares documentos bancarios. Aun así, es cierto que en muchos casos de *phishing*, el objetivo es más amplio que el descu-

[49] MIRÓ LLINARES, F.: "Cibercrímenes económicos y patrimoniales", en ORTIZ DE URBINA GIMENO, I. (Dir.): *Memento práctico penal y económico de la empresa 2011-2012,* Francis Lefebvre, Madrid, 2011.

brimiento de la clave, pues en algunos de ellos puede abarcar cualquier información personal que, a su vez, revele información de tipo económico. Estos casos de *phishing*, en los que se intercepten o apoderen de documentos o comunicaciones con la intención de descubrir un secreto, podrían sancionarse por el 197.1 CP. Entonces el problema sería otro: ¿Qué tendríamos, un único delito del artículo 197 o un concurso, y de qué tipo, con la tentativa del delito patrimonial de que se trate? A mi parecer, habría que distinguir dos casos: por una parte, aquellos supuestos en los que el sujeto intercepta la comunicación pero aún no ha descubierto la clave: habría un delito de descubrimiento consumado y nada más, pues aún no había más que un acto preparatorio del delito patrimonial y, por tanto, no sancionable; por otra parte, aquellos otros casos en los que el sujeto ya descubre la clave: habría un concurso ideal medial entre el descubrimiento de secretos y el delito patrimonial en grado de tentativa.

En todo caso, esta posible punición como descubrimiento y revelación de secretos del *phishing,* se daría en casos más bien excepcionales. Generalmente la clave se obtiene, bien mediante programas *sniffer* destinados a lograr ese tipo de información que, por tanto, no puede conceptuarse como un secreto personal relacionado con la privacidad de la persona, o bien haciendo que sea el propio sujeto el que teclee en la página web falsa la información confidencial[50]. Sólo cuando haya un apoderamiento masivo de correos electrónicos o elementos y archivos de ese tipo, podrá sancionarse el *phishing* por el artículo 197.1 CP. Asimismo, para los casos en los que los datos pertenecieren a personas jurídicas y empresas, será posible aplicar el art. 200 o arts. 278 y ss. [51]

Otra opción de incriminación de los comportamientos preparatorios de algunas de las modalidades de *phishing* parece el delito 248.2.b) del CP[52], que sanciona la fabricación, introducción, posesión o facilitación de programas de ordenador destinados a la comisión de estafas. El citado precepto fue incorporado por la LO 15/2003 de 25 de noviembre, por la que se modifica la LO 10/1995 de 23 de noviembre del CP, y respondía a la adaptación de nuestro ordenamiento a la Decisión marco 2001/413/JAI del Consejo de 28 de mayo de 2001, sobre lucha contra el fraude y falsificación de medios de pago distintos del efectivo[53], y se corresponde

[50] En este sentido, se plantea MATA Y MARTÍN, si es posible la aplicación de este tipo a los casos "en los que es el usuario el que facilita los datos reservados, entrega que realiza ante una petición fraudulenta, como sucede en el *phishing o pharming",* para posteriormente concluir que no debe aplicarse para estos casos el art. 197, pues la utilización del verbo apoderarse reafirma que "no resulta compatible con una mera conducta pasiva ni con una acción puramente fraudulenta". MATA Y MARTÍN, R.: "El robo de identidad…", *ob. cit.,* pp. 212 y 213.

[51] Como también apunta MATA Y MARTÍN, R.: "El robo de identidad…", *ob. cit.,* p. 214.

[52] Anterior art. 248.3, que fue añadido en la Reforma 15/2003, y cuya ubicación fue modificada con la Reforma 5/2010 para situarlo en el apartado b) del art. 248.2.

[53] Recuerda, sin embargo, FARALDO CABANA, P.: *Las nuevas tecnologías…, ob. cit.,* pp. 110 y ss., que en la citada Decisión Marco, el castigo de estos actos preparatorios se relaciona con la presencia de una organización delictiva, señalando concretamente la norma que "la descripción de las diversas conductas que

en propósito político criminal, contenido material (más bien formal) y técnica legislativa, con otros preceptos del CP, como el art. 270.3 CP que castiga conductas similares relacionadas en este caso con los derechos de propiedad intelectual, y el artículo 400 en relación con la comisión de delitos de falsedades documentales.

La doctrina ha criticado unánimemente estas figuras delictivas, en general, y la que estamos analizando ahora en particular, tanto por la excesiva anticipación de la tutela penal que incluso puede suponer la punición de comportamientos lícitos, como por la desproporcionalidad que conlleva que se castiguen lo que, a lo máximo, son actos preparatorios de la estafa, con la misma pena que la figura delictiva consumada[54]. Es tal el absurdo que supone esta forma de tipificación, que la misma implica que comportamientos que podamos reputar como tentativa de estafa se sancionen con pena inferior a la establecida para conductas que todavía no llegan siquiera a la tentativa y se quedan en los meros actos preparatorios. Precisamente por eso, y al igual que sostuve en su momento para el artículo 270.3[55], considero,

deben tipificarse en relación con el fraude y la falsificación por medios de pago distintos del efectivo abarque toda la gama de actividades que en conjunto constituye la amenaza del crimen organizado en este ámbito". En realidad tampoco parece que esta norma exija, como condición para su tipificación, que el hecho se lleve a cabo por una banda organizada. Lo cierto es que el legislador comunitario tampoco puede considerarse un ejemplo ni en la aplicación de políticas criminales racionales y coherentes con los principios de proporcionalidad e intervención mínima, ni en la utilización de una técnica legislativa que contribuya a definir claramente cuál debe ser el objeto de tipificación.

[54] Explica GALÁN MUÑOZ que al establecer el legislador en "ambos artículos penas tan manifiestamente desproporcionadas a los autores de sus injustos típicos, los tribunales han reducido tanto sus ámbitos de aplicación que los han convertido en preceptos prácticamente inútiles y carentes de relevancia práctica alguna, lo que debería llevar al legislador a reflexionar sobre la necesidad de proceder a su reforma; GALÁN MUÑOZ, A.: "El robo de identidad: aproximación…", *ob. cit.,* p. 179. FLORES PRADA, aunque califica como "discutible" la equiparación de penas del tipo básico con las conductas previstas en el apartado 2, justifica esta opción del legislador en "la importancia que actualmente han adquirido los programas informáticos en el tráfico económico en general, y a que de este modo se le otorga una protección especial reforzada al sistema informático como bien jurídico colectivo". FLORES PRADA, I.: *Criminalidad informática…, ob. cit.,* pp. 219 y 220.

[55] En el caso del artículo 270.3, el mismo se refería a "cualquier medio específicamente destinado a facilitar la supresión no autorizada" de los dispositivos de protección, y eso llevó a GONZÁLEZ RUS a tratar de limitar el ámbito de punición al entender que no entrarían en él aquellos programas que, junto a la posibilidad de desproteger programas, incluyeran utilidades distintas. GONZÁLEZ RUS, J. J.: "Delitos contra el patrimonio y contra el orden socioeconómico", en COBO DEL ROSAL, M. (COORD.): *Derecho penal español: parte especial,* Dykinson, Madrid, 2005, pp. 780 y 781. En el mismo sentido GONZÁLEZ GÓMEZ, A.: *El tipo básico de los delitos contra la propiedad intelectual,* Tecnos, Madrid, 1998, p. 203; y JORGE BARREIRO, A.: "Comentario al artículo 270", en RODRÍGUEZ MOURULLO, G. (DIR.)/JORGE BARREIRO, A. (COORD.): *Comentarios al Código penal,* Civitas, Cizur Menor, 1997, p. 776. Es cierto que el CP no relaciona la especificidad del destino con el medio, sino con las conductas de fabricación, puesta en circulación y tenencia, ya que utiliza el femenino (destinada) y no el masculino que sería el que permitiría relacionar "medio" con el complemento modal utilizado por el legislador, por lo que aquellos medios destinados no sólo a la supresión de la protección de programas de ordenador, sino a la realización de otras funciones relacionadas, cuando sean fabricados, puestos a disposición o poseídos específicamente para facilitar la supresión, podrían ser sancionados por el párrafo tercero del artículo 270 del CP. Es cierto, sin embargo, que esta última conclusión no casaba, como señaló GUINARTE CABADA, G.: "Algunas notas sobre la nueva regulación de la Propiedad Intelectual e Industrial en el Código Penal español de 1995", en *ADI*, núm. 16, 1994-1995, p. 889, con el artículo 102. C) del TRLPI de 1996 que sancionaba la puesta en circulación o tenencia con fines comerciales de "cualquier instrumento cuyo único uso sea facilitar la supresión...", y que una interpretación teleológica que tuviera en cuenta que lo que sanciona el párrafo tercero del artículo 270

siguiendo a la doctrina que se ha ocupado de este precepto, que es posible interpretarlo restrictivamente y reducir su ámbito punitivo apoyándonos en la exigencia de que el programa de ordenador esté "específicamente destinado" a la comisión de estafa.

Hay, sin embargo, y al igual que hemos visto que ocurría en la figura del 270.3, al menos[56] dos formas de interpretar tal cláusula restrictiva: la primera supone entender que es el autor del delito el que debe poseer la exclusiva intención de que el programa que fabrica, introduce, posee o facilita, se aplique a la comisión de estafas[57], de modo tal que aunque el programa tenga otras finalidades, si las del autor son esas, entonces el tipo penal sería aplicable. Se trata, pues, de una interpretación restrictiva amplia, en cuanto que, como se verá, hay muchos tipos de programas que pueden utilizarse para la comisión de estafas y para muchas otras modalidades de defraudación, e incluso de software que pueden servir para los mismos fines y que, por tanto, entrarían dentro del ámbito del tipo penal simplemente por el hecho de que el sujeto que los tuviera pensara utilizarlos para la comisión de la estafa. La segunda vía interpretativa consistiría en entender que conforme a la exigencia, el instrumento, en sí mismo, debe estar inequívocamente predispuesto a la lesión del bien jurídico y no disponga de otras funciones, de forma que si se trata de un programa que se puede aprovechar para distintas utilidades, como por otra parte suele ser habitual, el tipo penal no podría aplicarse.

Evidentemente, y como se ha señalado por algún autor[58], una interpretación restrictiva como ésta, supondría prácticamente la imposibilidad de entender perpetrado

del Código Penal, es la puesta en peligro abstracto que supone la realización de conductas preparatorias y necesarias, en determinados supuestos concretos, para la lesión del bien jurídico protegido, pero con la misma pena del delito consumado, nos debía llevar a reputar atípicas, conforme al TRLPI de 1996, las conductas típicas realizadas sobre un instrumento cuyo único uso no sea el citado, sino que incorpore otros como compresión/descompresión de ficheros, encriptación/desencriptación, etc. Esto, como observó GONZÁLEZ GÓMEZ, A.: *El tipo básico…, ob. cit.,* p. 204., llevaba a la inoperabilidad del tipo mismo, puesto que bastaba con incluir en el programa copiador, otra secuencia de instrucciones o indicaciones destinadas a realizar otras funciones distintas a la de supresión de la protección para convertir en atípico el comportamiento, pero la misma, dada la escasa relación con el objeto jurídico de protección que, como vimos, tiene la conducta, es casi más deseable que su aplicación estricta.

[56] Al fin y al cabo, también existe otra forma de interpretar la cláusula, más que en sentido restrictivo, en sentido extensivo, como hace CRUZ DE PABLO, para quien ésta es la única forma de entendimiento posible, dado que la práctica totalidad de los programas informáticos pueden cumplir múltiples y muy diferentes funciones, distintas a la de permitir la comisión de ilícitos penales. CRUZ DE PABLO, J.A.: *Derecho penal y nuevas tecnologías. Aspectos sustantivos,* Difusión Jurídica y Temas de Actualidad, Madrid, 2006, p. 47.

[57] FERNÁNDEZ TERUELO, J. G.: "Respuesta penal…", *ob. cit.,* p. 243. En el mismo sentido, FARALDO CABANA, P.: *Las nuevas tecnologías…, ob. cit.*, p. 113, quien, sin embargo, más adelante y en referencia a las aplicaciones *keylogger*, afirma que "hay que tener en cuenta que tienen múltiples aplicaciones, muchas de ellas perfectamente lícitas, lo que dificulta su inclusión como objeto material del delito que nos ocupa". Esto, como se verá, es cierto, y conlleva, a mi parecer, pero desde una interpretación distinta a la de la autora, pues no se centra como ella en la intención del sujeto, sino en la potencialidad de riesgo del software, que esos programas no se pueden entender dentro del objeto material cuando tengan otras utilidades distintas a las de facilitar la estafa.

[58] CRUZ DE PABLO, J.A.: *Derecho penal…, ob. cit.,* pp. 46 y ss.

este delito, puesto que no sería aplicable más que a programas sin ninguna otra finalidad que la tipificada, lo que no suele ser habitual. Siendo esto innegable, no me parece un argumento suficiente para rebatir, por lo menos, los tres que voy a mencionar y que hacen que me decante por esta interpretación que podríamos llamar ultra-restrictiva: En primer lugar, se corresponde mucho más con una interpretación gramatical, el entendimiento de que la concordancia de "específicamente destinados" lo es con los programas de ordenador, y no con la finalidad de los sujetos, como ocurriría si el tipo hablara de fabricación, introducción, posesión o facilitación "específicamente destinadas". En segundo lugar, también se corresponde con una interpretación teleológica que respete principios básicos del Derecho penal de un Estado Social y Democrático de Derecho, tales como el de ofensividad o el de proporcionalidad. El primero, dado que con una interpretación distinta a la defendida, podríamos llegar al absurdo de que la declaración de un sujeto de que va a utilizar un software legal para realizar una defraudación, podría llevar a la incriminación de su conducta y a su punición con la pena de la estafa consumada. El segundo, y este es aún más evidente, porque al restringir el ámbito del tipo, lo hacemos también con los comportamientos que, sin suponer una lesión ni un peligro concreto para el patrimonio, son sancionados con penas correspondientes a quienes directamente dañan tal bien jurídico protegido. En tercer lugar, y también desde una perspectiva teleológica que atienda, en este caso, a los fines preventivos del precepto que, por otra parte, nunca debieran superar los límites que acabo de mencionar, con la interpretación defendida, el tipo seguiría ejerciendo una función preventiva importante, pues, como se verá, y especialmente en el *phishing,* hay un tipo de software cuya única finalidad posible es, precisamente, la de llevar a cabo el fraude informático, y este tipo penal serviría para sancionar la fabricación, introducción, posesión o facilitación de dichos programas de ordenador, sin sancionar la de otros que, si bien es cierto que también pueden utilizarse, su realización por sí misma no puede entenderse como una puesta en peligro del bien jurídico protegido.

Es el momento de analizar, pues, qué tipo de programas, de los que se utilizan en el *phishing* y otras modalidades de ciberfraude, podrían entrar dentro de los que constituyen el objeto material del artículo 248.2.b) y dar lugar, por tanto, en el caso de tenencia, fabricación, introducción o facilitación, a la punición de los hechos con la pena de la estafa. Aunque los programas utilizados son múltiples y cada vez son distintos, voy a centrarme en los más usuales.

Descartando el *spam,* o correo electrónico enviado, que no es lógicamente un programa de ordenador, podríamos comenzar por valorar si entra dentro del ámbito típico del 248.2.b) el envío de *malware* que incorpore troyanos, *backdoors* u otras formas de software que permitan posteriormente el acceso ilícito al sistema. Conforme a la interpretación del tipo mantenida, tal conducta no resultaría típica, ni como tentativa de estafa, dado que todavía no ha existido apoderamiento de los

datos, ni por medio del 248.2.b), puesto que ese tipo de software puede servir para las funciones típicas, pero también para otras (si bien normalmente ilícitas), y no se puede afirmar entonces que su introducción suponga un riesgo de idoneidad *ex ante* para la afectación del bien jurídico protegido. Algo similar ocurriría con aquellas formas de *spyware* que se dediquen a buscar cualquier tipo de información sensible y no únicamente claves bancarias, que de ellas no podría afirmarse que están específicamente destinadas a la comisión de estafas. Así ocurrirá con algunos programas *keylogger* y *sniffer,* que, por el contrario, sí serían objeto material del delito cuando se configuren de una forma tal que, por ejemplo, sólo sirvan para apoderarse de información en forma de cifras de veinte dígitos o similares. Es cierto, en todo caso, que esto no será lo habitual.

Pero como señalé anteriormente, hay una modalidad de programa de ordenador del que sí puede afirmarse que está específicamente destinado a facilitar la realización de la estafa, concretamente la del *phishing,* y es la página web falsa o *spoofing web* a la que el sujeto suele acceder pensando que es la de su entidad bancaria en una de las modalidades de *phishing* más comunes. En efecto, en la actualidad es mayoritaria la consideración de la doctrina civilista y mercantilista de que la página web, como secuencia de instrucciones escritas en un determinado lenguaje informático, debe ser considerada como un programa de ordenador[59], con un código fuente en el que está escrita y un código objeto[60]. Y no me estoy refiriendo al conjunto de obras y elementos formales que la integran, y tampoco en su propio diseño o presentación visual en pantalla, que puede constituir una obra del ingenio si se trata de una creación original, bien en el contenido, bien en la forma de lo presentado[61], sino a la propia secuencia de datos que es la página web y que cuando esté específicamente creada como un instrumento para el engaño de la víctima y para la obtención de los datos necesarios para la causación del perjuicio patrimonial, podrá considerarse por sí misma, un programa de ordenador, objeto material del artículo 248.2.b).

Desde una perspectiva preventiva, como ya se advirtió, esto es importante, pues supone admitir que todas las formas de *phishing* en las que se utilice una página web creada para lograr el conocimiento furtivo de las claves bancarias, serán sancionables directamente con la pena de la estafa por medio del artículo 248.2.b), mientras que quedarían fuera de tal ámbito punitivo aquellas otras en las que se

[59] Véase, por todos, DE MIGUEL ASENSIO, P. A.: *Derecho privado de Internet,* Civitas, Madrid, 2000, p. 229.

[60] GARROTE FERNÁNDEZ-DÍEZ, I.: *El derecho de autor en Internet,* Comares, Granada, 2004 (2ª edición), pp. 40 y 41. No parece estar de acuerdo, sin embargo, CARBAJO GASCÓN, quien prefiere hablar de la página o sitio web como "una creación tecnológica de carácter multimedial (recopilación coordinada de texto, gráficos, imagen sonido y enlaces hipertextuales configurados armónicamente por una secuencia de instrucciones informáticas) que, si es original, puede ser protegida por medio del derecho de autor" (CARBAJO GASCÓN, F.: *Publicaciones electrónicas y Propiedad Intelectual,* Colex, Madrid, 2002, p. 66).

[61] GARROTE FERNÁNDEZ-DÍEZ, I.: *El derecho de…, ob. cit.,* p. 41.

utilice *malware* con otras funcionalidades, a menos que con el mismo se consigan las claves (ya estaríamos ante una tentativa) o el efectivo perjuicio (delito consumado). Por supuesto, tal interpretación no es totalmente coherente con los diferentes riesgos producidos (especialmente porque se sigue castigando con la pena del delito consumado lo que aún son actos preparatorios), pero es la mejor forma de cohonestar la finalidad preventiva del precepto, que abarcaría la gran mayoría de las modalidades de *phishing,* con la lógica y principios del sistema penal de un Estado Democrático de Derecho.

2.2.2. *La calificación jurídica del* phishing

Hemos comprobado que varios de los actos que acompañan al *phishing* y que tienen lugar antes de que se produzca el perjuicio económico que el mismo supone, ya pueden ser sancionados penalmente, algunos de ellos incluso con la misma pena establecida para la estafa. Es el momento de ver cuál es la calificación jurídica del *phishing* propiamente dicho, sobre lo cual ha existido cierta discusión doctrinal. Antes de revisarla, sin embargo, conviene que describamos las principales modalidades de *phishing*, diferenciándolas atendiendo a la forma en la que se obtienen los datos bancarios.

En primer lugar podríamos citar el *phishing* tradicional, en el que se utiliza la imagen corporativa de una entidad bancaria o de una institución, para solicitar a la víctima por medio de correo electrónico que envíe a una dirección de correo que simula ser de tal entidad, los datos bancarios requeridos[62]. Esta forma de *phishing* ha comenzado a ser sustituida por otras más elaboradas en las que, bien el sujeto ni siquiera sabe que está enviando las claves, o bien el sujeto piensa que está tecleando las claves en su entidad bancaria. Las primeras son aquellas en las que el correo electrónico enviado lleva un archivo que utiliza o bien *spyware,* del estilo de los programas *keylogger* o *sniffer,* para localizar los datos bancarios, o bien *malware* para lograr un acceso ilícito y descubrir los datos queridos. Las segundas son aquellas otras en las que el correo electrónico de la supuesta entidad bancaria incluye un *link* que redirige al sujeto, aparentemente, a una página web de la entidad que en realidad, no es tal y que permite al atacante conocer los datos bancarios de su víctima. Similar a éstas son las defraudaciones que entran dentro de la denominación de *pharming,* y consisten en la explotación de una vulnerabilidad en la programa-

[62] Recuerda FERNÁNDEZ TERUELO que lo habitual es suplantar la imagen corporativa y la web originaria de entidades bancarias, pero que "se han detectado otras fórmulas como las siguientes: encuestas falsas en nombre de organismos oficiales que tienen por objeto recoger datos personales de los usuarios que decidan participar en la misma; páginas falsas de recargas de móviles con tarjeta de crédito o de venta de diversos productos (a precios sospechosamente baratos), en los que, una vez obtenidos los datos personales y de la tarjeta, la página enseña algún tipo de error o indica que la operación no se ha podido realizar; presuntos compradores que le piden al vendedor datos bancarios para pagarle el producto que tiene a la venta, los cuales serán utilizados para realizar transacciones ilícitas, etc." FERNÁNDEZ TERUELO, J. G.: "Respuesta penal…", *ob. cit.*

ción de los servidores DNS, en el propio sistema de la víctima, o en el propio envío de *malware,* medios por los cuales se logra que el usuario, cuando teclea la dirección web de su entidad bancaria entre, en realidad, a una web falsa muy parecida o igual a la original, en la que acaba desvelando sus datos bancarios.

La doctrina ha tratado de encuadrar estas modalidades de *phishing,* bien en la estafa común o bien en la estafa informática, existiendo autores que niegan una posibilidad y otros que lo hacen con la otra. El problema que parece tener el tipo de estafa informática para encuadrar el *phishing* es que, según se dice, en el mismo no se lleva a cabo ningún tipo de manipulación informática que lleve a una transferencia no autorizada de activos patrimoniales, sino que en todo caso, la manipulación se realiza previamente (envío de *spam,* uso de *spyware,* infección de *malware*, etc.) para lograr la clave, pero con ésta no se lleva a cabo el perjuicio patrimonial que, en cambio, tiene lugar cuando se meten las claves en el sistema bancario, haciéndose pasar el sujeto activo por la víctima[63]. Esto lleva a quienes niegan la virtualidad de la estafa informática para dar cabida al *phishing*[64]*,* a entender que este comportamiento cabe, en cambio, en la estafa común. Así, dice Fernández Teruelo, estamos ante un supuesto en el que "un sujeto (el que engaña), hace llegar un mensaje a las posibles víctimas, consiguiendo que algunas de ellas (engañadas) hagan constar datos o claves personales, que serán posteriormente utilizados por el defraudador para realizar una transferencia en favor propio o de un tercero[65]. Debe haber olvidado el autor, sin embargo, que la dinámica comisiva de la estafa común, no concuerda con lo que él precisamente relata, pues para que se dé tal tipo penal, es necesario que sea el sujeto engañado el que realice el acto de disposición patrimonial en perjuicio propio o de tercero y, tal y como el autor relata, en el *phishing* es el defraudador el que transfiere el dinero ajeno en su propio favor o el de un tercero.

La estafa común, pues, no es el tipo penal que permite sancionar estos comportamientos. En ocasiones, como ha señalado Faraldo Cabana, porque el engaño no es idóneo para causar el error[66], pero siempre porque es el defraudador el que transfie-

[63] Así FERNÁNDEZ TERUELO, J. G.: "Respuesta penal…", *ob. cit.,* p. 238, señalando que "No se trata de alteración de elementos físicos ni de programación ni introducción de datos falsos. Quien ha obtenido las claves (auténticas) y las utiliza desde su propio ordenador, para realizar una transferencia a su favor o de un tercero (cambio de titularidad de los activos) a través de la Red, no ha alterado elemento físico o de programación alguno", lo cual le lleva a decir que sostener, entonces, que existe en tales supuestos una manipulación informática parece más bien forzar "el sentido de las palabras más allá de lo lícitamente admisible".

[64] Expresamente declara la dificultad de subsumir el *phishing* en el delito de estafa informática FERNÁNDEZ TERUELO J.G.: *Derecho penal e Internet…, ob. cit.,* pp. 50 y 51.

[65] Así FERNÁNDEZ TERUELO, J. G.: "Respuesta penal…", *ob. cit.,* p. 237.

[66] FARALDO CABANA, P.: *Las nuevas tecnologías…, ob. cit*., p. 92. También señala la autora que en los casos del *pharming,* directamente no hay engaño alguno, al producirse simplemente una manipulación informática de la que el usuario no es consciente. Lo cierto es que eso podría asimilarse al engaño si, como se hace en el *pharming,* el sujeto acaba entrando en la web que no espera pensando que está en la de su banco. El problema, de nuevo, no es la presunta ausencia de engaño, como que tanto en el *pharming* como en el *phishing,* no hay acto de disposición patrimonial llevado a cabo por el sujeto engañado.

re a su cuenta o a otras el dinero, y no el engañado el que lo hace. De hecho, esto es lo que diferencia el *phishing* de los ya mencionados ataques de *scam,* como el de las cartas nigerianas, en los que se envía un correo prometiendo generalmente el envío de importantes cantidades de dinero a cambio de que el sujeto pasivo ingrese en una cuenta corriente, una cantidad económica: aquí sí que hay una estafa común cuando es el propio engañado el que realiza el acto de disposición patrimonial que le perjudica.

Queda, por tanto, revisar de nuevo la tesis anterior de que no cabe el *phishing* en todas sus modalidades, en el tipo penal de la estafa informática del artículo 248.2. Lo que queda fuera de duda, de momento, es que la dinámica comisiva de esta modalidad de comportamiento, se acerca más a este tipo penal que más que defraudatorio es de "apoderamiento por medios informáticos". En el *phishing,* el sujeto que actúa sobre el valor patrimonial no es la víctima del engaño, sino el propio cibercriminal, que es quien realiza la transferencia "no consentida" de un valor patrimonial. En ese sentido, el tipo penal que corresponde a esta dinámica no es la estafa común, sino la estafa informática. Sin embargo, lo que un sector doctrinal duda, como hemos visto, es que pueda afirmarse que en todos los casos de *phishing* exista una manipulación informática. Esto deviene, generalmente, de la idea de que la manipulación informática debe entenderse en un sentido equiparable al engaño en la estafa. Sobre la base de este entendimiento, el comportamiento del sujeto de, una vez adquiridas las claves por el procedimiento que sea, utilizarlas en el banco electrónico haciéndose pasar por el titular, no supone una manipulación informática, pues ni se modifican los datos informáticos, ni los procesos, ni el resultado.

Frente a ello, en cambio, hay otra forma de interpretar la conducta típica que es la que hemos defendido aquí: la manipulación informática en el sentido de utilización de sistemas informáticos para la realización de una transferencia no autorizada de un activo patrimonial. Conforme a esto, manipular supone usar o utilizar un sistema informático, deviniendo el riesgo típico, no tanto del mero uso del sistema, como de que el mismo consista en la transferencia no autorizada de un activo patrimonial. Ésa es la conducta peligrosa e idónea para causar un perjuicio económico cuya prevención se pretende con el tipo penal del artículo 248.2. Y siendo ése el comportamiento típico sí puede afirmarse que el *phishing,* en todas sus modalidades, es una manipulación informática por la que se logra la transferencia no consentida del activo patrimonial. Hay manipulación informática en el *phishing* tradicional, cuando se teclean los datos bancarios de forma indebida, al no ser quien realiza tal acción, el titular bancario ni sujeto autorizado para hacerlo; lo hay en el *phishing* en el que se han obtenido las claves por medio de *spyware* o *malware* por el mismo motivo; y lo hay en el *pharming* también por idéntica razón. Porque la manipulación informática típica en las conductas de *phishing* y *pharming* es idéntica y no es, por tanto, la utilización de medios informáticos para lograr las claves, dado que ello

no lleva todavía a ninguna transparencia no autorizada, sino más bien, y como ya he señalado, a la utilización indebida de esas claves en el sistema informático de la banca electrónica, que supone la transferencia del activo patrimonial no consentida.

El TS ha tardado en pronunciarse sobre el *phishing,* si bien las resoluciones anteriores a hacerlo, generalmente sobre casos de utilización fraudulenta de tarjetas de crédito, ofrecen una interpretación de manipulación informática amplia y muy similar a la aquí sostenida. Así, el TS señaló que la asechanza a patrimonios ajenos realizados mediante manipulaciones informáticas "actúa con automatismo en perjuicio de tercero, precisamente porque existe la manipulación informática y por ello no se exige el engaño personal"[67], y más adelante, en una significativa resolución, afirmó que para colmar la acción típica de la estafa informática, era suficiente la presencia de dos requisitos: el primero, que el autor careciera de autorización para usar el medio informático, y el segundo, que produjera «efectos semejantes a la estafa común»; de modo que consideraba equivalente a los efectos de la ilicitud que el autor modifique materialmente el programa informático indebidamente o que lo utilice sin la debida autorización o en forma contraria al deber[68]. Estas resoluciones reflejan, cuanto menos, que el TS adopta una interpretación amplia de la conducta de manipulación informática. Y esto se confirma definitivamente, por medio de la STS núm. 533/2007, de 12 de junio de 2007, que vino a confirmar la resolución condenatoria de la SAP de Madrid núm. 71/2006, de 6 julio de 2006, en un caso de cibermulas del *phishing*.

Los hechos enjuiciados en la SAP de Madrid se refieren a dos personas que aceptaron abrir cuentas corrientes en la entidad Citibank, donde recibieron transferencias con cargo a otras cuentas de clientes auténticos del Citibank en las que terceras personas, valiéndose de un falso duplicado de la página web del Banco, habían accedido a las claves secretas. Esos hechos son calificados por la sentencia de la AP como constitutivos de un delito continuado de estafa del artículo 248.2, sin que, sin embargo, se realice argumentación alguna sobre la existencia de manipulación informática. El TS, al resolver el recurso, señala que los imputados sabían que el dinero que se les ingresaba, procedía de fondos de cuentas de otros titulares a los que personas desconocidas, en Estados Unidos, habían accedido mediante el acceso fraudulento de las claves necesarias. Desde esa base fáctica, el TS confirma la existencia de estafa informática del artículo 248.2 al existir, utilizando las palabras de la sentencia anteriormente citada, "asechanza a patrimonios ajenos realizados mediante manipulaciones informáticas"[69].

[67] STS núm. 2175/2001, de 20 de noviembre de 2001.

[68] STS núm. 1476/2004, de 21 de diciembre de 2004.

[69] Este argumento es utilizado por resoluciones posteriores, como la SAP de Burgos núm. 40/2007, de 14 de diciembre de 2007, que se remite a la STS núm. 2175/2001, de 20 de noviembre de 2.001 para señalar que "la asechanza a patrimonios ajenos realizados mediante manipulaciones informáticas actúa con automatismo en perjuicio de tercero, precisamente porque existe la manipulación informática y por ello no se exige el engaño personal".

A mi parecer, la argumentación del TS respecto a la existencia de manipulación informática en los casos de *phishing,* que es lo que en última instancia estaba admitiendo como hechos probados, es deficiente por errada en el motivo y por escasa. Pero en última instancia, la interpretación de que en estos casos hay manipulación informática y, por tanto, delito del artículo 248.2 CP, es acertada. Yerra en el motivo de la existencia de manipulación informática por la "asechanza informática", pues no es, a mi parecer, ésa la manipulación informática típica sino, como ya he señalado, la que consiste en teclear indebidamente las claves obtenidas de forma ilícita y lograr así la transferencia no autorizada; y es escasa la argumentación del TS, que ni siquiera se plantea la duda de si puede haber, en este caso, una manipulación informática. Pero lo cierto es que con su resolución viene a reconocer que la utilización de sistemas informáticos para la consecución indebida de una transferencia no autorizada, constituye el contenido esencial del injusto de la estafa informática.

Aún más discutible, y ya no acertada, es, en cambio, la argumentación que utiliza el TS para condenar como autores a los cibermuleros. Esto es lo que se analizará en el próximo punto.

3. **La responsabilidad penal de los muleros del *phishing***

3.1. ***Entre la receptación, el blanqueo y la estafa: el debate jurisprudencial sobre la calificación jurídica de los actos de los muleros del* phishing**

Ya se ha explicado que los cibermuleros son un elemento esencial del entramado defraudatorio del *phishing,* que empieza con los que definen el plan de ataque, los que redactan el *spam,* quienes envían los correos de *phishing*, quienes diseñan las webs falsas, los que se ocupan de lograr la transferencia patrimonial y, finalmente, los cibermuleros, que reciben en sus cuentas el dinero y se encargan de transmitirlo por canales seguros a los jefes de la organización[70]. Muchas de estas conductas las pueden realizar las mismas personas, pero la de los cibermuleros no: ellos no forman parte del grupo criminal porque son, al fin y al cabo, los que están expuestos a la vigilancia bancaria cuando se constata el delito y, por tanto, al control legal. De hecho, el reclutamiento del cibermulero se suele hacer por medio de falsas ofertas de trabajo, consistentes en recibir un dinero, quedarse un porcentaje, y enviar el

[70] Es importante destacar que no actúa propiamente como un mulero el sujeto que realiza las transferencias por medio de Internet, puesto que la forma de lograr el éxito del delito exige realizar la transferencia personalmente, sacando el dinero de la cuenta bancaria y enviándolo por algunos de los sistemas de transmisión económica no electrónicos. De hecho, es significativa en este sentido la SAP Madrid (Sección 15ª), núm. 400/2008 de 10 septiembre de 2008, que absuelve a los acusados por los delitos de estafa informática, por considerar que no se da la conducta de *phishing* en la realización transferencias bancarias realizadas a través de Internet desde el ordenador de los acusados, quienes carecen de los conocimientos informáticos y medios para ello, siendo muy posible que su ordenador estuviera infectado por un «troyano», a través del cual se hubiera puenteado la transferencia.

resto utilizando el sistema Money Gram u otros. Por eso hay quien denomina a estos cibermuleros como "las otras víctimas del *phishing*", dado que son los que se ven implicados en los procesos delictivos por ese tipo de defraudaciones.

Desde una perspectiva jurídica, la conducta de los cibermuleros plantea muchas dudas, tanto respecto al tipo penal aplicable, a la presencia de todos los elementos típicos (especialmente del conocimiento del hecho) exigidos, como a la concreción de su forma de intervención. En cuanto a lo primero, resulta difícil situar su conducta en el ámbito de injusto de la estafa común[71], dado que el mulero no realiza engaño alguno, o en el de la estafa informática, pues no parece haber por su parte, siguiendo una interpretación estricta de tal elemento, ninguna manipulación informática. En cuanto a lo segundo, el mulero en muchos casos desconoce gran parte de la dinámica comisiva del hecho conjunto del que forma parte, si bien conoce el origen ilícito del dinero que recibe e incluso se le puede atribuir, en algunos casos, un mayor conocimiento. En otras palabras, la realización de las transferencias de importantes cantidades de dinero sin siquiera preguntarse si tal actividad es o no legal y a cambio de importantes comisiones, parece superar los márgenes del actuar imprudente, pero no llegar al dolo si se entiende como conocimiento y voluntad del hecho típico. Por último, y como se dijo anteriormente[72], el mulero suele estar sólo en el proceso penal, en cuanto que pese a ser muchos los intervinientes en este tipo de delitos, sólo es él el finalmente detenido en la mayoría de los casos y, por tanto, será a él a quien, sin conocer con precisión la intervención de los demás, habrá que atribuir una concreta forma de intervención en el delito.

Quizás todo esto influyera en que se hayan buscado otras vías diferentes a la estafa (en sus formas común e informática), concretamente los delitos de recepta-

[71] Aunque podemos encontrar alguna sentencia en la que se condena por este tipo penal como la SAP Zaragoza núm. 208/2012, de 7 junio de 2012, en la que la acusada como autora de un delito de estafa, se puso en contacto por medio de Internet con una persona desconocida (que decía representar a la empresa inglesa de nombre WeroGroup), a la que facilitó sus datos personales y bancarios, sabiendo que recibiría una comisión cifrada en un 7% de la operación realizada, a sabiendas de que no podía determinar con quién se estaba comunicando y de que éste no le proponía un contrato de trabajo regularizado (hasta el punto de que se le ofrecía no registrarlo en el Instituto Nacional de Empleo y no ser dada de alta en la Seguridad social). Así, la acusada aceptó libre y voluntariamente emplear una cuenta corriente que estaba titularizada a su nombre a la que se transfirió un determinado dinero a través de maniobras de ingeniería informática ilícitas practicadas por personas no identificadas. La imputada alegó en su defensa error de tipo y error de prohibición, lo que no fue aceptado por la AP de Zaragoza al considerar que resultaba "inverosímil que no levantase sospecha en la recurrente una denominada oferta de trabajo cuya contenido era, simplemente, convertir dinero cartular o escriturario en dinero metálico." Añade el tribunal que con "dificultad extrema puede aceptarse que la recurrente abrigase la esperanza de conseguir un trabajo que, con tan escaso esfuerzo, produjera beneficios de tal magnitud. También es muy difícil concebir que la recurrente no relacionase su comportamiento con un hecho ilícito y la denuncia con omisiones que ella interpuso milita en sentido contrario al interesado en el recurso. Lo que resulta erróneo es suponer ingenuamente que la recurrente desconocía el alcance delictivo de su conducta. No creemos que se pueda suplir esta falta apelando a la ignorancia, sea del hecho, sea de su ilicitud. No es corriente, en modo alguno, obtener por un trabajo tan escaso un fruto tan elevado."

[72] Véase *supra*.

ción[73] o de blanqueo de capitales, para sancionar penalmente a los cibermuleros del *phishing*. La primera vía la ha defendido el magistrado Eloy Velasco, argumentando que el sujeto ayuda a los responsables a aprovecharse de los efectos del mismo[74]. El problema es que si se manifiesta que el sujeto ha tenido conocimiento de la comisión de un delito, como exige el tipo, entonces difícilmente podrá decirse que no es cómplice del mismo, y entonces no habría receptación[75].

La segunda, la del blanqueo de capitales, la han seguido algunas Audiencias Provinciales[76], partiendo precisamente de la supuesta imposibilidad de punición de los hechos como estafa. Así ocurre, por ejemplo, con la SAP de Valladolid (Sección 4ª), núm. 263/2010 de 21 de junio, que absuelve de la estafa a dos sujetos que ponen a disposición de un tercero, las cuentas corrientes propias para la realización de ingresos de dinero, que luego son transferidos a otras cuentas, percibiendo un

[73] Ejemplo de ello, es el Auto de apertura de juicio oral por un delito de receptación y apropiación indebida de la AP de Barcelona núm. 175/2010, de 2 marzo de 2010, que resuelve el recurso frente a un auto anterior en el que se había decretado el sobreseimiento de la causa por considerar que "no se acreditaba por parte del imputado ni una actuación dolosa ni el conocimiento de que estuviera llevando a cabo una actuación delictiva". También el Auto la AP de Barcelona considera que cabría aclarar hasta qué punto la conducta del acusado "se inscribe dentro de la adecuada diligencia exigible a todo ciudadano de una cultura media, al que se le ofrece un puesto de trabajo que le ofrece una alta remuneración por unas tareas en apariencia sencillas, sin ningún tipo de explicaciones complementarias." Asimismo, el Auto AP Castellón núm. 165/2012, de 20 marzo de 2012, acuerda continuar con el procedimiento abierto contra la acusada por un delito de estafa y apropiación indebida, haciendo referencia expresa a la STS de 12 de junio de 2007. Explica la AP de Castellón que en el caso de autos, algunos datos resultantes de las diligencia pueden contradecir la tesis de la ignorancia o buena fe de la imputada, "tanto en el plano objetivo (recepción de transferencias de dinero de ignorada procedencia a su propia cuenta con libertad de disposición, envío del dinero recibido a personas desconocidas extranjeras, la advertencia de los empleados del banco de lo raro de tales operaciones, el conocimiento de que se llevaba a cabo para evitar "un trámite administrativo de aduanas") como en el subjetivo (el nivel cultural y la experiencia de la vida que cabe suponer a quien, como la recurrente, administrativa/contable, como se dice en el propio contrato de trabajo y es fácilmente comprobable en Internet)."

[74] Dice VELASCO NÚÑEZ que la conducta de los muleros está más cerca de la receptación que de la intervención en el delito principal de estafa informática, y si bien señala expresamente que parecería penalmente más correcta la calificación de su conducta como blanqueo, dado que se recepta dinero y no objetos, entiende más incardinable la conducta finalmente en la receptación, al ser el previo un delito contra el patrimonio y al no ser autor ni cómplice del delito previo, y especialmente por ser la pena de este tipo penal más proporcionada que la del blanqueo a la menor gravedad del comportamiento del mulero en comparación con el autor de la estafa. VELASCO NÚÑEZ, E.: "Fraudes informáticos…, *ob. cit.,* p. 65. No hace falta valorar críticamente estos argumentos aquí, pues ya se hace implícitamente en el texto.

[75] También rechaza la subsunción de esta conducta en el tipo de receptación FERNÁNDEZ TERUELO, pues considera que "Aparentemente, cuando el mulero actúa con ánimo de lucro y, con conocimiento de la comisión de un delito contra el patrimonio, ayuda a los responsables a aprovecharse de los efectos de éste; sin embargo, el delito en cuestión no está aún consumado, sino que, precisamente, la recepción por parte del mulero es el último momento necesario para determinar la consumación (perjuicio o pérdida patrimonial derivado de la disposición patrimonial), FERNÁNDEZ TERUELO J.G.: *Derecho penal e Internet…, ob. cit.,* pp. 39 y 40.

[76] También el delito de blanqueo de capitales es el aplicado en Italia como indica FLOR, en casos "en los que han actuado sujetos distintos de los *phishers* que, al margen de los casos de concurso de delito, han desarrollado conductas orientadas a "sustituir o transferir dinero, bienes u otras ventajas provenientes del delito no culposo", o han realizado "en relación" con aquellas "otras operaciones que obstaculicen la identificación de su proveniencia delictiva", FLOR, R.: "*Phishing* y delitos relacionados…", *ob. cit.,* p. 94.

porcentaje por cada transferencia[77]. La resolución se fundamenta en que "los acusados no participan en la manipulación informática, base de dicha defraudación, en ninguna de sus fases porque los actos del mismo consuman el delito cuando se apoderan de las cantidades de dinero de la cuenta del tercero ajeno, de modo que, realmente, los acusados participan en una operación posterior que tiene como base dicho fraude o estafa que ya se ha cometido, porque el perjuicio ya que se ha causado a través del artificio informático, operación que consiste en la ocultación de dicho dinero y su transferencia a un lugar del que no se puede recuperar."[78] De ahí no deriva, sin embargo, el tribunal, impunidad, sino que los hechos son sancionables como delito de blanqueo de capitales, si bien no doloso, sino realizado por imprudencia grave, argumentando que no es aceptable que considerasen verosímil que una empresa repartiese beneficios lícitos de un modo tan poco convencional y necesitando intermediarios, por lo que la actitud de los imputados de no "querer plantearse (con deliberada ignorancia), qué trascendencia puede tener el trabajo realizado ni el origen de las sumas de dinero que van a transferir, y de hecho transfieren, a Kiev", debe considerarse una negligencia que propicia "que un dinero procedente de una estafa informática encuentre la vía para no ser recuperado, cuando, los acusados, con un mínimo de diligencias o cuidado, podrían haber evitado el daño patrimonial que se produjo." Esta línea ha sido seguida por un nutrido grupo de Audiencias Provinciales como la de Sevilla (en la SAP de Sevilla núm. 174/2012, de 22 marzo de 2012[79]), la de Asturias (en la SAP de Asturias núm. 148/2012, de 11 septiembre de 2012[80]) o la de León (en la SAP de León núm.

[77] En similar sentido, la SAP de Granada núm. 402/2008, de 27 de junio de 2008. El acusado recurrió dicha resolución en casación y el TS inadmite el recurso por Auto núm. 790/2009, de 16 de abril de 2009, argumentando que "Ha de convenirse con la Audiencia Provincial en que cualquier persona con un nivel intelectivo medio es sabedora, sin necesidad de especiales conocimientos técnicos y/o especial formación académica, de que para realizar una transferencia no es preciso valerse de la cuenta corriente de un tercero, lo que hubo de despertar sus sospechas"; así como que "en el plano subjetivo, no se exige un conocimiento preciso o exacto del delito previo (que, de ordinario, sólo se dará cuando se integren organizaciones criminales amplias con distribución de tareas delictivas), sino que basta con la conciencia de la anormalidad de la operación a realizar y la razonable inferencia de que procede de un delito grave (ahora ya de cualquier tipo, aunque no sea grave), como por ejemplo por su cuantía, medidas de protección, contraprestación ofrecida, etc."

[78] En sentido similar, la SAP de León núm. 186/2011 de 29 de julio de 2011 también decía no ser aplicable la estafa argumentando que en ese caso concreto, "la acusada no participó en la manipulación informática, base de dicha defraudación, en ninguna de sus fases porque los actos de la misma consuman el delito cuando se apoderan de las cantidades de dinero de la cuenta del tercero ajeno, de modo que, realmente, la acusada participa en una operación posterior que tienen como base dicho fraude o estafa que ya se ha cometido, porque el perjuicio ya se ha causado a través del artificio informático, operación que consiste en la ocultación de dicho dinero y su transferencia a un lugar del que no se puede recuperar".

[79] Afirma la AP que en el supuesto existían "datos objetivos y circunstancias que claramente debieron causar a la acusada extrañeza o perplejidad o dudas racionales sobre la ilícita procedencia del dinero en cuestión". Resulta curiosa, en todo caso, la argumentación de la resolución respecto a la aplicación del tipo imprudente y no del doloso cuando señala el tribunal que la propia acusada había admitido que en la segunda transferencia pensaba que se trataba de blanqueo, de lo cual infiere el tribunal que la acusada "es al menos responsable del delito descrito a título de imprudencia grave."

[80] Explica que se debe aplicar la modalidad imprudente del blanqueo de capitales porque "el acusado no

186/2011, de 29 julio de 2011) así como por el TS en una resolución, la Sentencia núm. 834/2012, de 25 octubre de 2012[81]. E incluso ha habido resoluciones condenatorias por el delito de blanqueo de capitales en su modalidad dolosa, como la reciente SAP de Asturias núm. 556/2012, de 29 noviembre de 2012[82].

Lo cierto es que pese a esta línea jurisprudencial, la regulación del blanqueo de capitales anterior a la reforma penal de 2010 hacía difícil encuadrar la conducta del cibermulero en el tipo penal del art. 301 CP. El citado precepto sancionaba a aquél 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 infracción o infracciones a eludir las consecuencias legales de sus actos". De ese modo exigía que los bienes que transmitía tuviesen 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 sufriese las consecuencias jurídicas por ello. Pues bien, lo lógico es entender el mulero no actúa "para ocultar o encubrir el origen ilícito del dinero", ni "para ayu-

fue conocedor de la procedencia ilícita del dinero, porque precisamente por ello se le condena por el tipo imprudente del apartado 3 del artículo 301 del CP, pues si hubiera tenido tal conocimiento cierto se le aplicarían los tipos dolosos más gravemente penados de los apartados 1 y 2 del mismo artículo". Añade además la AP de Asturias que procede la apreciación de la "imprudencia grave" en el caso de autos porque aun no existiendo prueba de que el acusado supiera a ciencia cierta que el dinero ingresado procedía de la sustracción fraudulenta de una cuenta, sí se daban los siguientes seis elementos: "1) el lucro ofrecido era demasiado cuantioso (nada menos que una comisión del 4 por 100 y un sueldo mensual de 2.500 euros) y fácil para no ser algo ilícito o al menos sospechoso (en expresión castiza: los duros no se venden a pesetas)"; 2) por el secretismo de la operación; 3) "porque aunque al recibir el acusado la oferta a través de Internet figuraba el nombre de una mujer (" Celia ") como oferente, resulta que quien le llama por teléfono para indicarle a dónde tenía que transferir el dinero era "una voz de hombre"; 4) "porque no es fácil de entender (lícitamente) por qué el que quería transferir ese dinero al extranjero no lo hacía él mismo directamente"; 5) "porque el que transfirió el dinero a la cuenta del acusado no coincide con quien hizo la oferta de la operación al acusado y ninguno de ellos con la titular de la cuenta de la que se sustrajo ilícitamente el dinero, discrepancia fácil de comprobar a través del Banco", y 6) porque "aunque puede que el acusado no lo supiera, este "modus operandi" ya ha sido y sigue siendo empleado para blanquear dinero de procedencia ilícita y los medios de comunicación ya han dado cuenta de ello".

[81] Entre otras que también condenan por imprudencia, como la SAP de Valladolid núm. 263/2010 de 21 junio de 2010; SAP de Granada, de 27 de junio de 2008; la SAP de Huesca, de 31 de mayo de 2010 y la SAP Valladolid, de 21 de junio de 2010.

[82] Ante la alegación del acusado de error para que, en todo caso, se le aplique el blanqueo de capitales en su modalidad imprudente, la AP de Asturias desestima por considerar que la conducta del acusado es dolosa, afirmando el tribunal que "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". Añade además, la AP de Asturias que "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 partícipe; consiguientemente se hace acreedor a las consecuencias penales que se deriven de su antijuricidad."

dar a la persona que haya participado en la infracción a eludir las consecuencias legales de sus actos", sino para favorecer la comisión del delito que, sin su intervención, no puede llevarse a cabo[83]. Al fin y al cabo, y frente a lo que señala la SAP de Valladolid núm. 263/2010, de 21 de junio, el delito de estafa se está consumando cuando se ingresa el dinero de una cuenta corriente a otra, que por tanto ya existe, y que es titularidad del mulero del *phishing* que debe, entonces, sacar el dinero y enviarlo al destinatario. En el blanqueo, como bien se advertía en alguna resolución judicial, el objeto material de la acción de encubrir o enmascarar eran los bienes que tienen su origen en el delito antecedente, mientras que en este caso, el dinero es el propio objeto material del delito en el que, por tanto, está colaborando el cibermulero[84].

Como he adelantado, sin embargo, la reforma penal de 2010 modifica el art. 301.1 CP en la línea de aumentar los márgenes punitivos del blanqueo de capitales, abriendo, así, la posibilidad de sancionar los actos que estamos analizando. El tipo penal en su nueva redacción castiga al que "adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen 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 que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos". Los cambios que más nos interesan, a los efectos de la presente investigación, son dos:

[83] Tampoco considera que sea punible esta conducta por blanqueo de capitales la AP de Madrid en su Sentencia núm. 332/2010 de 29 julio de 2010, pues determinó que no había lugar a los recursos de apelación interpuestos por la acusación particular y el Ministerio Fiscal contra la sentencia absolutoria dictada en causa seguida contra los acusados de delitos de blanqueo de capitales y estafa, por haber puesto a disposición de un tercero la cuenta corriente propia para la realización de ingresos de dinero, que luego fueron transferidos a otras cuentas, percibiendo un porcentaje por cada transferencia. La AP de Madrid además de afirmar que no se desprendía de los hechos probados que existiera "una certeza del conocimiento de procedencia u origen ilícito del dinero", por lo que descartó en primer lugar que en la conducta de los acusados fuera dolosa, señaló posteriormente en relación con la acusación por blanqueo de capitales por la que podría haber habido una posible responsabilidad por imprudencia, que "Como establece un sector de la doctrina (como Blanco Lozano y Palma Herrera), en un Estado de Derecho es inadmisible imponer a los ciudadanos un deber de investigación sobre las actividades económicas ajenas para determinar si los bienes que manejan han sido generados o no en actividades ilícitas. Por otro lado, la calificación de imprudencia grave ha de reservarse para las actuaciones de los sujetos obligados por la Ley de Prevención de Blanqueo de Capitales, sobre determinadas medidas de prevención del blanqueo de capitales que son los únicos a los que se les va a poder exigir precaución superior a lo normal."

[84] Así lo manifiesta la SAP de Madrid núm. 271/2008, de 26 de mayo de 2008, que absuelve del blanqueo de capitales a quien no había sido imputada por delito de estafa informática, argumentando que "cuando el precepto indicado (blanqueo) habla de bienes no se trata de los que constituyen el objeto material del delito antecedente, sino de aquéllos que tienen su origen en el mismo, poniendo el ejemplo del delito de tráfico de drogas, en el que el bien a blanquear no es la sustancia estupefaciente, sino el dinero o bienes entregados a cambio de aquélla. Y en el caso de autos resulta que estamos ante un tipo de estafa informática denominada phishing en el que el "bien" supuestamente blanqueado es el objeto material del delito, pues el objeto de la estafa es el dinero que recibió la acusada en su cuenta bancaria. Ello determinaría que no pudiera hablarse en el caso de autos de un delito de blanqueo de capitales, sino de un delito de estafa, tal y como estableció la sentencia del Tribunal Supremo de 12 de Junio de 2007 que confirmó una sentencia en la que se condenaba como autores de un delito de estafa a varias personas que habían desarrollado una conducta idéntica a la de la acusada en la presente causa".

el primero, que el tipo penal ya no se refiere a delito sino a actividad delictiva, de modo que podría entenderse que ya no es necesario que el dinero provenga de un delito consumado, sino que puede provenir de una actividad delictiva en la que, y este es el segundo cambio de interés, también podría estar participando el propio autor del blanqueo. Esta interpretación, que supondría una modificación de la tradicional forma de entender el objeto material del blanqueo de capitales, permitiría, por lo menos tras una primera vista que será completada más adelante en la toma de posición, sancionar como delitos de blanqueo de capitales muchos de los supuestos englobados en el tópico de los muleros del *phishing*. Al fin y al cabo, el mulero posee y transmite bienes, y aquello que habría que demostrar, para la aplicación del tipo doloso, es que el sujeto sabe que el dinero que recibe tiene su origen en una actividad delictiva indeterminada. Ya no sería necesario que el delito del que deriva el dinero estuviese consumado, sino que al referirse ahora el tipo a "actividad delictiva" podría entenderse que también hay blanqueo cuando se está transmitiendo una cantidad económica que se está generando por la propia conducta delictiva en la que, además, podría estar implicado el propio autor del blanqueo. En el caso de no imputar dicho conocimiento quedaría, además, la posibilidad de sancionar los hechos por el tipo imprudente del art. 301.3.

Lo cierto es, en todo caso, que la calificación más usual de este comportamiento por los tribunales españoles, ha sido la de estafa informática. El problema, en ese caso, estribaba en precisar la forma de intervención delictiva. Así, y como precedente de la resolución que abriría la puerta a una doctrina hoy mayoritaria en materia de muleros del *phishing,* la AP de Vizcaya en sentencia núm. 355/2006, de 9 de mayo de 2006, condenó como autor de estafa informática a quien abrió a su nombre cuatro cuentas bancarias diferentes desde las que tenía que transferir el dinero que recibía fruto del *phishing,* considerando el tribunal que "la conducta típica no se agota en el descubrimiento de las claves que identifican al cliente y en su utilización haciéndose pasar por tal, sino que también es preciso disponer de cuentas a beneficio de las cuales ordenar las transferencias, de manera que posibilite el cobro del importe defraudado" y por ello interviene "con una conducta integradora de la acción típica descrita en el art. 248.2 del Código Penal". No hace falta prolija argumentación relativa a que no se sostiene la imputación del cibermulero a título de autor y menos sobre la base de un criterio formal de autoría, ni tampoco a que no es necesario para atribuir responsabilidad en un injusto a un interviniente, utilizar el título de autor, puesto que es posible que el sujeto sea partícipe en el mismo.

La anterior premisa sí la tuvo en cuenta el Tribunal Supremo en la STS núm. 533/2007, de 12 de junio de 2007, que venía a resolver el recurso contra la resolución de la AP Madrid que enjuició una prototípica conducta de *phishing:* una serie de sujetos son convencidos por otros, no procesados en la causa, para participar en una actividad a partir de la cual se quedaban una cantidad de dinero y otra las

enviaban a sujetos indeterminados[85]. La AP Madrid condenó a los acusados como cooperadores necesarios de un delito continuado de estafa previsto y penado en los artículos 248.2, 250.6º y 74, del CP, y el TS confirmó la condena de la AP en todos sus extremos, dando lugar al inicio de una cuasi doctrina que parece haberse impuesto definitivamente en Audiencias Provinciales[86] como Burgos[87], Asturias[88], Barcelona[89], Zamora[90], Lugo[91] o Madrid[92], y que ha confirmado el propio Tribunal Supremo en Sentencia de 16 de marzo de 2009[93].

[85] Según se afirma en el relato de hechos, no consta la identidad del grupo de personas desconocidas, con excepción de un menor no procesado en la causa que se ocupaba de reclutar a los muleros, que se dedicaban a enviar diversos correos electrónicos a clientes de Citibank con un falso duplicado de su página web haciéndose pasar por empleados para conseguir las claves secretas de clientes del banco en EEUU y una vez sabidas, ordenaban las falsas transferencias a favor de las cuentas de los acusados en España. Los acusados recibieron cada uno en sus cuentas diversas transferencias por importantes cantidades de 159.559,20 euros, 73.197,77 euros y 22.374,63 euros, disponiendo posteriormente de gran parte de ese dinero.

[86] Así, en la actualidad encontramos escasas resoluciones absolutorias, como la Sentencia núm. 227/12 del Juzgado de lo Penal núm. 17 de Madrid de 19 de junio de 2012, que absuelve al acusado de un delito de estafa por considerar que si los hechos se hubieran producido en la actualidad, "no podría ser admitido conforme a la lógica y la experiencia" el desconocimiento alegado por el acusado, pues actualmente "el conocimiento de esta modalidad delictiva determina que existen razones suficientes para suponer que se colabora en un negocio presuntamente ilícito"; no obstante, la juez considera que al haber sucedido los hechos que se enjuician en el 2006 "y en esas fechas la modalidad delictiva no era todavía muy conocida", la alegación del acusado puede ser considerada. Entre otros argumentos para fundamentar la ausencia de conocimiento del imputado, destaca la juez que el acusado no aperturó una cuenta con la finalidad concreta de realizar esta operación, pues la cuenta a la que se realizó la transferencia existía desde hacía años. Añade además la juez que en los hechos probados consta que el acusado envió sus datos personales a una empresa extranjera, pensando que iba a actuar como agente comercial y aseguró que "tras enterarse de la ilegalidad de la operación él proporcionó a la policía toda la información de la que disponía" y que "Dicha aseveración fue confirmada por los agentes deponentes en el acto del Plenario". Por todo ello, concluye la sentencia que "existiendo indicios de que el acusado pudo actuar bajo los efectos de un error de tipo, procede dictar una sentencia absolutoria (…) puesto que, aunque el mismo fuera evitable, el dolo resultaría afectado y no previéndose una modalidad imprudente del delito por el que ha resultado acusado solamente cabe un pronunciamiento absolutorio". Un caso similar, es el que se sobresee con el Auto de la AP Madrid núm. 332/2012 de 9 abril de 2012, en el que el día anterior a la denuncia que da lugar a la iniciación del procedimiento, la acusada se personó en la oficina de denuncias de la Comisaría de Cartagena exponiendo lo que estaba ocurriendo. El tribunal arguye en este caso, refiriéndose a la conducta de los muleros que "Es cierto que estas personas se convierten en cooperadores necesarios de las referidas estafas, pero para que la imputación por ese delito de estafa pueda dirigirse contra las mismas debe de concurrir el elemento subjetivo del delito de estafa y de lo anteriormente expuesto este Tribunal entiende que efectivamente tal como estiman el Ministerio Fiscal y la Instructora, a la vista de la conducta de la imputada, denunciando los hechos nada más realizar una operación y ante la sospecha, al recibir el segundo ingreso, de que pudiera tratarse de algo ilícito, devolviendo esta última cantidad, parece que no existen indicios suficientes, ni siquiera por aplicación de la doctrina de la ignorancia deliberada, de la concurrencia de dolo en la imputada necesario para que la misma pueda ser considerada autora como cooperadora necesaria de un delito de estafa".

[87] SAP de Burgos núm. 40/2007, de 14 de diciembre de 2007.

[88] SAP de Asturias núm. 127/2012, de 9 de julio de 2012.

[89] En el mismo sentido, la SAP de Barcelona núm. 727/2008, de 13 de octubre de 2008, afirma que el hecho de que los colaboradores no conocieran la parte fundamental de la red, no les exime en tanto en cuanto prestaron una colaboración eficiente y causalmente relevante.

[90] La SAP de Zamora núm. 11/2008, de 22 de diciembre de 2008, aunque no califica la conducta como *phishing,* condena por estafa informática al acusado que colabora con una trama de *phishing,* acudiendo a la entidad bancaria, donde debía recibir una transferencia, procedente de la cuenta, cuyo titular es la víctima, transferencia ordenada por terceras personas, desconocidos, que accediendo al sistema informático de la entidad bancaria, habían entrado en la cuenta de la víctima. El acusado recibida la transferencia, extrajo en

La STS núm. 533/2007, de 12 de junio de 2007, entraba en todas las cuestiones problemáticas que, como señalé anteriormente, plantea la actuación de los cibermuleros del *phishing*. Comenzando por el tipo penal aplicable, el TS realiza una mejor argumentación que la AP de Madrid que afirmaba que concurrían en los autores los elementos constitutivos de la estafa común, entre ellos el engaño y el acto de disposición patrimonial del engañado[94]. Frente a ello, el TS acude al tipo de la estafa

metálico una cantidad y efectuó a su vez otra transferencia, desconociéndose el destino dado a la misma.

[91] SAP de Lugo núm. 165/2008, de 26 de septiembre de 2008. Esta sentencia, sin embargo, condena al acusado como autor del delito de estafa y no como cooperador necesario, si bien es cierto que tal afirmación puede dar lugar a confusión debido a la imprecisión del CP al señalar en el artículo 28 que también serán considerados autores, los cooperadores necesarios.

[92] Como la SAP de Madrid núm. 43/2009, de 22 de enero de 2009. No obstante, en la reciente SAP de Madrid núm. 164/2012, de 4 de mayo de 2012, se condena al acusado en calidad de autor por una tentativa de estafa informática. El imputado a través del uso de la banca electrónica en Internet, aperturó una cuenta corriente en la que se recibieron dos transferencias realizadas mediante la utilización espuria de las claves obtenidas ilícitamente, dinero del que el acusado no pudo disponer al constatarse la irregularidad narrada por la entidad bancaria. El acusado alegó que no fue en ningún momento consciente de que con la retirada de las transferencias ingresadas en su cuenta estuviera cometiendo un delito de estafa al desconocer que el dinero le había sido ingresado con el desconocimiento de sus respectivos titulares. Consideraba por esto el recurrente que no procedía la imposición de pena alguna, dado que él mismo fue engañado en lo que pensaba era una oferta de trabajo por la que cobraría una comisión por control de envío de abono de pedidos de una empresa con la que además había firmado previamente un contrato de trabajo**.** La AP de Madrid, rebate el argumento del imputado, destacando que el propio acusado declaró en el juicio que en aquel momento se dedicaba a realizar traducciones y que es economista, por lo que no podía deducirse otra consecuencia distinta de la alcanzada por la juzgadora en cuanto a que tenía pleno conocimiento, o debió tenerlo, sobre la ilicitud de su actividad que consistió en recibir dinero en una cuenta de la que sólo él era titular que respondía a unos pedidos previos procedentes de empresas alemanas -de los que ninguna acreditación existe- que debía ser a su vez transferido nada más y nada menos que a Rusia sin tramitar previamente tales pedidos, recibiendo por tal gestión una comisión de aproximadamente el 5%, sin que ninguna explicación existiera para que el pago de esos supuestos clientes no pudiera hacerse directamente a una cuenta de la que la empresa fuera titular. Estimó la AP de Madrid, que en este escenario podía concluir que el acusado estaba al corriente, al menos de forma limitada, de la operación que en lo que a él se refería se concretaba en abrir una cuenta, recibir las transferencias por personas desconocidas y cobrar una cantidad por este "servicio", entregando el resto a otras personas desconocidas y en un país diferente. Concluyó la AP que en esta situación construir un juicio de inferencia que permitiera llegar a la conclusión de que el recurrente participó del operativo, es una conclusión que resulta racional y lógica pues fluía por sí sola de los indicios expuestos y no era, en contra de lo que sostenía el recurrente, contraria a las máximas de la experiencia. Y ello pese a que no conociera al resto de la red de implicados, pues se trata de una delincuencia económica de tipo informático en la que el recurrente ocupa efectivamente un nivel inferior y sólo tiene el conocimiento necesario para prestar su colaboración; pero la ignorancia del resto del operativo no borra ni disminuye su culpabilidad porque fue consciente de la antijuridicidad de su conducta, prestando su conformidad con un evidente ánimo de enriquecimiento, ya supiera o no quisiera saber -ignorancia deliberada-, o le fuera indiferente el origen del dinero que en cantidad relevante recibió, pues lo importante es que prestó su colaboración eficiente y causalmente relevante en una actividad antijurídica, y la explicación ofrecida en su defensa es de una inocencia que se desmorona por sí sola. Finalmente, declara el tribunal que cualquier persona de nivel cultural medio, y más un economista, conoce y sabe o debe saber de la ilicitud de una colaboración del tipo de la realizada por el acusado, máxime cuando no se trataba de una colaboración gratuita sino que llevaba aneja un claro enriquecimiento personal. Por todo ello considera la AP que no hay ninguna posibilidad de derivar a ningún supuesto de error la acción realizada.

[93] STS núm. 556/2009, de 16 marzo de 2009.

[94] La sentencia comienza sus fundamentos de derecho señalando que los hechos declarados probados son constitutivos de un delito continuado de estafa previsto y penado en los artículos 248.2, 250.6º y 74, todos ellos del CP, y señalando que "de todos es conocido que el delito de estafa necesita para su comisión la concurrencia de los requisitos que la jurisprudencia entre otras en sentencias 8-2-2002 (RJ 2002, 4527) y

informática, el cual exige que estemos "ante una estafa cometida a través de una transferencia no consentida por el perjudicado mediante manipulación informática, en tales casos no es preciso la concurrencia de engaño alguno por el estafador", bastando "la asechanza a patrimonios ajenos realizados mediante manipulaciones informáticas (que) actúa con automatismo en perjuicio de tercero, precisamente porque existe la manipulación informática y por ello no se exige el engaño personal". Así, aunque de nuevo algo parcamente, el TS adopta una interpretación amplia de manipulación informática que permite integrar en ella los actos del *phishing*. Es significativo, sin embargo, que el TS ni dice en ningún momento cuál es la manipulación informática que se realiza ni quién la lleva a cabo, quizás porque reconozca implícitamente que ninguno de los imputados realizó tales conductas típicas.

En cuanto a la concreción de la forma de intervención, si bien el TS no realiza ninguna argumentación expresa y se limita a afirmar que los recurrentes prestaron su colaboración eficiente y causalmente relevante en una actividad antijurídica con pleno conocimiento y cobrando por ello, y a situar el hecho dentro del ámbito de la estafa informática[95], lo hace de forma implícita al dar validez a la resolución de la Audiencia Provincial de Madrid, que sí lleva a cabo, para la cuestión de la intervención delictiva, una breve argumentación. Señala que del delito son responsables en concepto de cooperadores necesarios todos los acusados, pues "con la apertura de las cuentas corrientes y la disposición de sus fondos y entrega a los terceros han contribuido necesariamente a la producción del resultado, siendo esta intervención una «conditio sine qua non» para que la estafa llegara a consumarse"[96]. Es en todo caso, esta cuestión de la precisión de la concreta forma de intervención, como autor

19-4-2002 (RJ 2002, 6699) enumera", y cita como requisitos un engaño precedente o concurrente, que el engaño sea bastante, un error esencial en el sujeto pasivo generado por el engaño y que a la vez le lleve a realizar el siguiente requisito, un acto de disposición patrimonial "producto de una actuación directa del propio afectado", ánimo de lucro, y un nexo causal o relación de causalidad entre el daño provocado y el perjuicio experimentado. No parece darse cuenta el tribunal de que está citando los elementos de la estafa común, que no son los mismos que los de la estafa informática que él mismo ha dicho que existe, pero que no explica. De hecho, continúa señalando que los acusados recibieron en sus cuentas corrientes, abiertas al efecto en la entidad Citibank, numerosas transferencias de dinero que no fueron autorizadas por los titulares de aquellas otras de las que provenía el dinero, habiéndose efectuado tras obtenerse por personas desconocidas e ilícitamente los números de cuentas corrientes y sus códigos PIN, procediendo tras ello a vaciarlas de dinero. Es decir, que ni está probado el engaño del sujeto activo sobre el sujeto pasivo, ni existe error por parte de aquél, ni hay un acto de disposición patrimonial llevado a cabo por engañado o perjudicado. No hay nada de eso porque el tipo penal aplicable no lo exige en realidad.

[95] Quizás sea uno de los aspectos críticos de la resolución, su parquedad en algunas argumentaciones. En este caso es evidente: en un momento en que la teoría de la imputación objetiva parece totalmente consolidada en el TS, a este parece bastarle, en cambio, la afirmación de la existencia de una causalidad relevante realizada con conocimiento, para afirmar la existencia de participación punible.

[96] De hecho, y habiendo la entidad bancaria detectado que se habían producido 102 transferencias fraudulentas, en 19 de ellas no se dispuso de los fondos al haber comunicado los titulares de esas cuentas, la extrañeza que les producían los ingresos por provenir de ordenantes desconocidos y fueron devueltos. No ocurrió así con aquellos otros que tuvieron destino en las cuentas corrientes de los acusados, al actuar estos de común acuerdo con el autor material de la estafa.

o como cooperador necesario, poco fundamentada generalmente por los tribunales españoles en general y también para este delito[97].

El que la calificación preferida de los tribunales españoles para las conductas realizadas por los muleros del *phishing* sea la de cooperadores necesarios en una estafa concuerda completamente con el sentido criminológico del papel de estos intervinientes en tal ciberdelito: son agentes que, sin realizar ninguna conducta cibernética, son necesarios para que los cibercriminales obtengan el beneficio patrimonial derivado de todas las conductas precedentes. Esto no quiere decir, sin embargo, que sea tal la calificación jurídica más adecuada ni, en el caso de que lo sea para algunos casos, que sea generalizable a cualquiera de los supuestos hechos que, conforme a su significado social, incluiríamos en el concepto de "actividades de muleros del *phishing*". Para que eso sea así será imprescindible que se pueda afirmar que se cumplen las condiciones exigidas para que un sujeto pueda ser hecho responsable por la cooperación necesaria en el delito de estafa, y a dicho análisis nos vamos a dedicar a continuación. Dado, por otra parte, que la problemática tal y como la han interpretado los tribunales estriba, en este caso, no tanto en el sentido de participación de la conducta como en el conocimiento o desconocimiento con la que la misma se lleva a cabo, sistematizaré el análisis a partir de la consideración de los requisitos necesarios para poder atribuir responsabilidad dolosa al partícipe en el delito.

3.2. *Toma de postura: diversidad de conocimientos imputados, diversidad de soluciones jurídicas*

Que la jurisprudencia de las Audiencias Provinciales no sea homogénea y difiera para la calificación de las conductas de los muleros del *phishing* entre la autoría en el blanqueo de capitales y la participación en la estafa informática no tiene porqué

[97] Por citar un ejemplo significativo de la confusión argumentativa respecto a si el sujeto interviene como autor o como partícipe, la SAP de Lugo núm. 165/2008, de 26 de septiembre de 2008, condena al acusado como autor responsable de un delito de estafa, "ya que consta en los hechos probados que, actuando de común acuerdo con personas no identificadas, a las cuales facilitó a tal fin los datos de su cuenta bancaria, y actuando con ánimo de enriquecimiento injusto, recibió en su cuenta una determinada cantidad de dinero, procedente de la cuenta bancaria de la que era titular la víctima, transferencia esta realizada sin consentimiento de su titular mediante la utilización de las claves de usuario de banca on-line del mismo que habían sido previamente obtenidas de forma fraudulenta". Añade el tribunal que "el acusado, siguiendo lo acordado con el resto de personas intervinientes en dicha operación fraudulenta y a sabiendas de la procedencia ilícita del dinero ingresado en su cuenta corriente, procedió a retirar de la misma una cantidad determinada, remitiendo el resto fuera del territorio nacional a través de una empresa de envío rápido de dinero y haciendo suyo el resto del citado importe". Y si bien todo esto parece ir en la dirección de una coautoría basada sobre la ya superada teoría del acuerdo previo, más adelante se dice que los cibermuleros ocupan "tal como ocurría con el acusado, un nivel inferior, de colaboración y para facilitar la retirada de dinero de la cuenta del perjudicado y la llegada del mismo al destino que previamente les fue indicado, prestando tales intermediarios, una cuenta bancaria a su nombre en la que se ingresa, en principio el dinero objeto de la estafa informática, para después retirarlo el intermediario (una vez deducida su pactada comisión) y enviarlo al destino que le fue indicado".

significar que haya una mera discrepancia técnica en la calificación de unos hechos por parte de los tribunales. También es posible que lo que haya son hechos (probados) distintos y, conforme a ellos, calificaciones jurídicas diversas. Y esto es lo que, esencialmente, sucede en este caso, que unos tribunales están dando por probados unos determinados hechos y los tribunales que realizan otra calificación han dado por probado otros, con la particularidad de que la parte de los hechos probados que difiere de unos a otros casos es el conocimiento que del actuar tiene el interviniente. Al fin y al cabo, el conocimiento que tenía el imputado en una determinada causa de su actuar forma parte de los hechos probados que, al ser comparados con la norma jurídica de que se trate, van a ser valorados en la fundamentación jurídica como delito o no. Es justo reconocer que también hay sentencias (las menos) que realizan una incorrecta inferencia de la calificación jurídica a partir de los hechos (y su conocimiento) que se consideran probados. Pero lo importante es comprender, y a ello me voy a dedicar a continuación, que según lo que se pruebe que conoce o desconoce el mulero, la calificación jurídica de su comportamiento podrá ser una o podrá ser otra.

En efecto, el hecho de que el delito de blanqueo de capitales esté configurado como la tipificación expresa de formas de intervención específica en determinados delitos, hace que en ocasiones la delimitación entre la responsabilidad por esta figura delictiva y la cooperación necesaria o la complicidad por el "delito principal" vayan a depender únicamente del conocimiento que se pueda atribuir que tiene el sujeto que realiza la concreta aportación. Esto es, precisamente, lo que sucede en el caso de los muleros del *phishing:* su responsabilidad como partícipes de una estafa o como autores de un blanqueo dependerá del conocimiento que se impute que tenía el mulero en el momento de realizar una conducta que, en lo objetivo, si imaginamos que es posible tal separación entre objetivo y subjetivo, es idéntica: recibir dinero ajeno en una cuenta bancaria, sacarlo de la cuenta y transferirlo a un tercero. Lo que no lo es, y será por tanto esencial para determinar la responsabilidad del mulero, es el conocimiento que el sujeto tiene del significado de sus actos, lo cual es esencial para poder identificar el hecho imputado que luego va a ser valorado como negación de una determinada norma. A continuación concretaré qué conocimiento imputado determinará qué responsabilidad en el caso del mulero.

3.2.1. *"Conocimiento imputado" y responsabilidad del mulero como partícipe doloso en la estafa informática*

El mulero podrá ser considerado cooperador necesario de la estafa informática llevada a cabo por los autores que, por medio de cualquier tipo de manipulación informática han desviado previamente de una cuenta bancaria dinero de un titular sin su autorización y en su perjuicio a otra cuenta titularidad del mulero, siempre que pueda probarse que su conducta de recibir el dinero y de retirarlo posteriormen-

te para enviarlo a los autores es dolosa. Al fin y al cabo, el delito de estafa informática es doloso, y aun cabiendo en abstracto la responsabilidad por participación imprudente, al no existir tipo imprudente de estafa, sólo si se considera que el partícipe actúa con dolo podrá éste responder por estas figuras. En el caso de que haya tal actuar doloso la conducta puede ser considerada de participación punible: el mulero, con su actuar, se integra en el injusto de estafa que, antes de su intervención, pertenecía únicamente a los *hackers* que habían accedido a las cuentas y desviado el dinero. Al transferirles el dinero, sin embargo, el mulero se integra en tal injusto, lo hace propio también, dado que permite con su actuar la consumación del delito al no existir disponibilidad sobre el mismo hasta que no se da tal transferencia. El injusto, en todo caso, está protagonizado por otros sujetos, los autores, al no realizar él actos que, por sí mismos, conllevarían la esencia del injusto de que se trata. Su conducta es de participación en un injusto del que también responde él pero en el que, conforme al sentido social de su actuar, no puede ser considerado autor. Acierta, pues, en esto el propio TS cuando señala que el papel de los muleros se sitúa generalmente en un eslabón inferior de la cadena criminal en relación con los que preparan los correos del *phishing,* quienes logran las claves y quienes finalmente envían el dinero y lo reciben. Estos son los autores del delito de estafa informática, los que tras obtener las claves bancarias gracias a un engaño directo (ingeniería social) o a la utilización de *malware, spyware* o por medio de un acceso informático ilícito *(pharming* y *DnS based phishing),* realizan la manipulación informática (entrar en el banco haciéndose pasar por el usuario y teclear sus claves) y llevan a cabo la transferencia no consentida. Nada de esto llevan a cabo los cibermuleros que, en términos de semántica social (o de valoración social de tal comportamiento) no realizan por sí mismos (aunque sí por medio de otros) el injusto penal en el que consiste la estafa, sino a lo máximo una apropiación ilícita de activos bancarios. Al fin y al cabo, nuestro CP establece que responden de los delitos, no sólo los autores, sino también los partícipes, cooperadores necesarios, inductores y cómplices. Y sí podría afirmarse de las conductas de los cibermuleros, utilizando la terminología de la teoría de la participación como un integrarse en el injusto de otros[98], que con las mismas el sujeto se integra, se suma, a un proyecto delictivo, a un injusto que era de otro y que con sus actos, pasa a serle también propio. El acto de recibir cantidades de dinero procedentes del *phishing* y su envío por medios seguros a los autores del mismo, sólo puede valorarse socialmente como que el que lo realiza ha decidido sumarse al, o integrarse en, el proyecto delictivo llevado a cabo por el autor. En otras palabras, el mulero que recibe importantes ingresos y los transfiere por los medios que le han ordenado, realiza un comportamiento cuyo único sentido social es, a todas luces, hacer posible a otros

[98] Véase al respecto, MIRÓ LLINARES, F.: *Conocimiento e imputación en la participación delictiva. Aproximación a una teoría de la intervención como partícipe en el delito,* Atelier, Barcelona, 2009.

sujetos, determinados o indeterminados, la consumación final del delito[99]. Por eso, además, acierta el TS al definir la intervención del mulero como cooperación necesaria: la intervención del mulero es casi insustituible como forma de lograr el perjuicio patrimonial por medio de la estafa informática, puesto que si bien con la transferencia patrimonial ya se entiende producido el perjuicio, no ocurre lo mismo con el éxito del ataque para el cibercriminal que lo protagoniza y que le obliga a contar con muleros sin los cuales no obtiene las ganancias y, por tanto, no llevaría a cabo el ataque.

Afirmado esto, pues, parece claro que la clave en este caso no estriba tanto en realizar un juicio de valoración (denominado de imputación objetiva) acerca del sentido de participación de sus conductas, como en imputar el conocimiento necesario para que tales conductas puedan atribuírsele como propias y, por tanto, imputársele y valorarse su actuar en sentido doloso.

3.2.1.1. Cuestión previa I: ¿Qué queda de la voluntad del mulero?

Siendo la esencial cuestión problemática para la atribución de responsabilidad penal en los muleros del *phishing* la de la determinación de que su participación resulta dolosa, es esencial recordar qué elementos se exigen, según doctrina y jurisprudencia, para la existencia de dolo de participación, en general[1], y de complicidad o cooperación necesaria en particular. Concretamente convendría analizar qué conocimiento se exige para la responsabilidad del partícipe pero, incluso antes, si junto a él se demanda la presencia de algún tipo de voluntad. Pues bien, la doctrina afirma mayoritariamente la necesaria concurrencia de conocimiento y voluntad del partícipe[100] para la complicidad y cooperación necesaria dolosas. Es cierto, sin embargo, que en estas figuras el elemento volitivo aparece mucho más difuminado que en lo que parece exigirse para la inducción. Las referencias a que el cooperador necesario o el cómplice quiera, persiga, o desee que el autor ejecute el delito, no están presentes en la explicación del dolo de participación de gran parte de la doctrina[101], y aunque aún hay voces que exigen un querer o "voluntad del cómplice de contribuir eficazmente a la conducta del autor"[102], hay también otras,

[99] Deja entrever esta misma idea FLOR, cuando afirma que estos actos "podrían ser penalmente relevantes sólo a título de participación ", haciendo referencia expresa a "los casos de voluntaria "concesión de uso" de la cuenta corriente para facilitar al autor la transferencia de fondos o para poner en marcha operaciones bancarias y financieras", para concluir posteriormente que "Una solución político criminal distinta, además de no ser respetuosa con los principios de ofensividad y de *ultima ratio* del Derecho penal, contribuiría a "demonizar" la evolución tecnológica"; FLOR, R.: "*Phishing* y delitos relacionados…", *ob. cit.,* pp. 116 y 117.

[100] Así CEREZO MIR es de los pocos que habla del elemento subjetivo de participación, identificando el mismo como el acuerdo de voluntades entre autor y partícipe que supone la concurrencia del dolo del partícipe: "el sujeto debe actuar con conciencia y voluntad de cooperar en la conducta típica y antijurídica llevada a cabo por el autor" (CEREZO MIR, J.: *Derecho penal. Parte general,* Bdef, Buenos Aires, 2008, p. 952).

[101] MIR PUIG, S.: *Derecho penal. Parte general,* Reppertor, Barcelona, 2004 (7ª edición), pp. 404 – 405.

[102] ORTS BERENGUER, E. /GONZÁLEZ CUSSAC, J.L.: *Compendio de Derecho Penal (Parte general y Par-*

no "sospechosas" de cognitivismo, como la de Jescheck, que señalan que "para el dolo del cómplice no es necesaria la aprobación personal del hecho principal", apoyando tal parecer en resoluciones judiciales de los Tribunales alemanes[103].

En cuanto a la jurisprudencia también es unánime en cuanto a lo de "decir una cosa y hacer otra", dado que si bien es general la idea expresada de que el "dolo del cómplice radica en la conciencia y voluntad de coadyuvar a la ejecución de un hecho punible"[104], también lo es la de que el dolo eventual es perfectamente posible en la participación[105]. De hecho puede decirse que, para la jurisprudencia, lo relevante de la exigencia de un elemento volitivo no es tanto que el sujeto quiera o desee que el autor cometa el delito, como que se decida a colaborar con él pese a saberlo, de modo que con la constatación del conocimiento de que con su aportación se facilitará o se hará nacer el delito de otro ya parece que habría dolo. Lo mismo sucede con la doctrina en última instancia: la gran mayoría de ella coincide, pese al disenso terminológico, en no exigir más motivación o deseo del partícipe que la de llevar a cabo la acción que efectivamente realiza con el conocimiento exigido para la responsabilidad a título doloso. Así, cuando se afirma que el partícipe debe querer facilitar el delito de otro o hacer nacer su idea criminal, lo que se está afirmando es que para que se pueda imputar la participación resulta necesario que el sujeto haga algo que sabe que supone su integración en el injusto del autor cuando haya podido no hacerlo[106]. No habrá acción de participación cuando la facilitación a otro deviene de un movimiento reflejo o, por ejemplo, de un actuar inconsciente. En el resto de los casos, siempre que haya conocimiento, habrá imputación y, por eso, puede afirmarse que siempre que hay un hecho realizado con conocimiento habrá voluntad[107]. No, como se ha dicho respecto de aquéllos que defienden esta posición, porque entienda que la voluntad (como control) no es

te especial), Tirant lo Blanch, Valencia, 2004, p. 241. También hacen referencia a que el cómplice debe actuar con un común propósito con el autor, o de voluntad de facilitar la ejecución, SUÁREZ-MIRA RODRÍGUEZ, C. (COORD.): *Manual de Derecho penal, Tomo I: Parte general,* Civitas, Cizur Menor, 2006 (4ª edición), p. 413.

[103] JESCHECK, H.H./WEIGEND, T.: *Tratado de Derecho penal. Parte general* (traducido de la 5ª edición alemana por Miguel OLMEDO CARDENETE), Comares, Granada, 2002, p. 748.

[104] Véase entre otras las SSTS de 9 de mayo de 1972 y de 12 de mayo de 1998, y la STS de 24 de abril de 2000, STS núm. 1036/2003, de 2 de septiembre de 2003 y STS núm. 1031/2003, de 8 de septiembre de 2003.

[105] Véanse en este sentido la STS núm. 1531/2007, de 27 de septiembre de 2007, STS núm. 1031/2003, de 8 de septiembre de 2003 y la STS núm. 1531/2002, de 27 de septiembre de 2002.

[106] Lo cual puede denominarse voluntad, control, capacidad de determinación o, en una fórmula también válida y utilizada por el autor en el mismo sentido, como "compromiso de actuar" (VIVES ANTÓN, T.S.: *Fundamentos del sistema penal,* Tirant lo Blanch, Valencia, 2008, p. 238). Sobre éste véase también, MARTÍNEZ-BUJÁN PÉREZ, C.: "El concepto significativo de dolo: un concepto volitivo normativo", en MUÑOZ CONDE, F. (Coord.): *Problemas actuales del Derecho penal y de la Criminología: estudios penales en memoria de la Profesora Dra. María del Mar Díaz Pita,* Tirant lo Blanch, Valencia 2008, pp. 323 y ss.

[107] Conocimiento y voluntad (en el sentido de volición) se dan imbricados, si bien pueden deslindarse. La volición sigue al conocimiento, al actuar, pero, al imputar, comenzamos por la volición, en cuanto control, que es lo que se ve, y subimos al conocimiento.

autónoma del conocimiento[108], sino porque la voluntad existe (en el sentido de "se imputa") en el hacer algo que se sabe y que se puede no hacer. Como dijo Hruschka, entre el elemento cognitivo y el volitivo existe una relación de dependencia conforme a la cual siempre que concurre el primero, concurre el segundo[109], de modo que, ahora en palabras de Vives Antón, una vez determinada la conducta de una persona "y lo que, en el momento de realizarla sabía, está dado cuanto es necesario para afirmar o negar el dolo"[110].

Lo que esto quiere decir es que las motivaciones del mulero con respecto a su conducta y en relación con los autores de la estafa son totalmente irrelevantes para la atribución de responsabilidad a él como partícipe en el delito. Lo serán sus objetivos, las razones éticas por las que actuó o la identificación (o su ausencia) con los objetivos de los autores. Es indiferente que el mulero compartiese los objetivos del autor o que desease que se produjese el delito. Basta con que actúe con el conocimiento exigido y queriendo realizar lo que hace. Evidentemente la constatación de las motivaciones internas del partícipe y su vinculación emocional con las consecuencias delictivas derivadas de su aportación pueden ser relevantes a efectos de la prueba del saber. Como ya he señalado en otro lugar, lo habitual será que aquél que hace algo que sabe que va a desembocar en que otro cometa un delito, se "alegre" o "desee" el éxito criminal del autor[111]; y que, viceversa, si se prueba que alguien quería o deseaba que otro cometiera un delito cuya realización ha sido posible gracias a algo por él mismo aportado, pueda entenderse que en el momento de hacerlo conocía las consecuencias relevantes (integración en el injusto del otro mediante un comportamiento con único significado de participación) de su actuar. Y al revés. Pero ni esto siempre va a ser así, pues normalmente la prueba del querer es tan complicada como la del conocimiento y ambos no tienen por qué ir unidos en una misma dirección, ni, cuando sea, significa que la intención del mulero sea relevante a los efectos de que exista o no.

3.2.1.2. Conocimiento (imputado) necesario para la responsabilidad del mulero como cooperador del delito de estafa

[108] ROMEO CASABONA, C. Mª.: "Sobre la estructura monista del dolo. Una visión crítica", en JORGE BARREIRO, A. /BAJO FERNÁNDEZ, M. / SUÁREZ GONZÁLEZ, C. J. (Coords.): *Homenaje al Profesor Dr. Gonzalo Rodríguez Mourullo,* Civitas, Cizur Menor, 2005, p. 932.

[109] HRUSCHKA, J.: "Sobre la difícil prueba del dolo", en DEL MISMO: *Imputación y Derecho penal* (traducido por Pablo SÁNCHEZ-OSTIZ GUTIÉRREZ), Aranzadi, Cizur Menor, 2005, p. 146, añadiendo que "siempre que alguien lleva a cabo una conducta determinada bajo determinadas circunstancias conociendo las características tanto de la conducta como de las circunstancias, quiere a la vez realizar la conducta con dichas circunstancias".

[110] VIVES ANTÓN, T.S.: "Reexamen del dolo", en MUÑOZ CONDE, F. (COORD.): *Problemas actuales…, ob. cit.,* p. 371, si bien dice el autor "en la práctica totalidad de los casos –aunque quizás no siempre".

[111] En ese sentido dice FRISCH que la voluntad "si acaso puede llegar a ser relevante si en ella se pone de manifiesto a la vez que el sujeto actuante ni siquiera se ha percatado de la referencia de sentido delictiva de su acción" (FRISCH, W.: *Comportamiento típico e imputación del resultado* (traducido por Joaquín CUELLO CONTRERAS y José Luis SERRANO GONZÁLEZ DE MURILLO), Marcial Pons, Madrid, 2004).

La cuestión del conocimiento que debe tener el mulero para poder ser hecho responsable como cooperador necesario de un delito de estafa fue afrontada por la Audiencia Provincial de Madrid en la sentencia núm. 71/2006, de 6 de julio de 2006, que originó la Sentencia del TS núm. 533/2007, de 12 de junio de 2007. La citada resolución, en una parca explicación, se limitaba a afirmar dos cosas: la primera, que los imputados tuvieron puntual conocimiento del dinero que pasaba por sus cuentas corrientes y del que disponían íntegramente, bien fuese para ellos mismos, bien para entregar a un tercero; la segunda, que no es aceptable la alegación de los acusados de que pensaban actuar lícitamente, "pues es el propio sentido común el que dicta que el recibir dinero en una cuenta corriente donde se ingresan cantidades millonarias de origen desconocido, actuación por la que paga un tercero un porcentaje por el solo hecho de hacer los oportunos reintegros y entregárselos a dicha persona, tiene toda la apariencia de «negocio ilícito», como así fue". En el recurso, el TS sí realiza una auténtica argumentación acerca de la actuación con conocimiento de los muleros. El Tribunal declara como probado que los sujetos implicados estaban al corriente de "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 desconocidas"[112]. A partir de ahí, afirma el TS que los recurrentes "participaron y estaban al corriente, en lo necesario, de todo el operativo", y si bien no conocían el resto de la red de implicados, tal conocimiento es considerado por el Tribunal como no necesario, dado que se trata de sujetos que participan en un caso de delincuencia económica en el que "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

[112] Estos elementos del conocimiento son la base utilizada para la resolución posterior sobre la materia, concretamente la STS núm. 556/2009, de 16 marzo de 2009, en la que se señala que la acusada tenía "pleno conocimiento de la ilicitud de su actividad pues: a) tiene la titulación de diplomada en Ciencias Empresariales, b) trabajaba en el momento de los hechos como subdirectora de la sucursal núm. 180 de la entidad bancaria Caixa de Gerona, en Hospitalet de Llobregat (Barcelona), c) conocía que el percibo por su parte del 7% de las cantidades transmitidas superaba con creces cualquier interés o comisión bancaria por idéntica operación, d) desconocía la identidad de la titular de las cantidades recibidas en cuenta y causa de su remisión a ella y e) desconocía la identidad del destinatario en Rusia de sus transferencias y la causa de las mismas".

cantidad tan relevante recibieron"[113]. El TS afirma la existencia de dolo y, casi paralelamente, de hecho típico, al señalar consecutivamente a lo anterior que "es obvio que prestaron su colaboración eficiente y causalmente relevante en una actividad antijurídica con pleno conocimiento y cobrando por ello".

Para afirmar la existencia de dolo se apoya el TS, aunque de forma casi velada, en la tesis de la denominada "ignorancia deliberada", al afirmar que supieran, no quisieran saber, o les fuera indiferente el origen del dinero que recibían, tienen "un conocimiento necesario para prestar su colaboración, y la ignorancia del resto del operativo no borra ni disminuye su culpabilidad porque fueron conscientes de la antijuridicidad de su conducta". De hecho sentencias posteriores de audiencias provinciales han seguido esta argumentación, como la reciente SAP de A Coruña núm. 34/2013, de 22 enero de 2013, que condena a la acusada como cooperadora de un delito de estafa informática, desestimando el recurso de la apelante alegando ausencia del dolo necesario para ser condenada por el art. 248.2, pues considera el tribunal de aplicación al caso concreto la doctrina de la ignorancia deliberada para atribuir responsabilidad a la acusada[114]. Argumentos parecidos utiliza la AP de Valencia en su Sentencia núm. 579/2012 de 31 julio de 2012, para atribuir el conocimiento necesario a la acusada de estafa, que trayendo a colación la Sentencia de la AP de La Rioja, de 21 de diciembre de 2011, explica que "quien, con una capacidad cognitiva ordinaria, acepta, sin explicación plausible, y a cambio de una apreciable retribución, ofrecer su cuenta corriente como refugio de transferencias significativas de dinero para, sin solución de continuidad, trasladarlas a cuentas sitas en Rusia, es consciente del alto riesgo de que el origen del dinero trasladado sea ilícito".

Con el teórico apoyo de la doctrina de la ignorancia deliberada un gran número de sentencias de Audiencias Provinciales están atribuyendo dolo de participación en la estafa informática pese a imputar (o declarar probado) como único conocimiento el de que el sujeto participaba en "algo ilícito". Equiparan, de ese modo, el conocimiento (imputado) de estar participando en un injusto concreto (aun desconociendo los detalles del mismo), con el mero hecho de aceptar la potencial participación en una actividad ilícita. Con tal proceder dichas Audiencias se separan, a mi

[113] En el mismo sentido posteriormente, la SAP de Burgos núm. 40/2007, de 14 de diciembre de 2007, tan sólo dos días después de la del TS, señalando también respecto a los imputados que "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". En similar sentido, aunque no con idénticas palabras, la SAP de Madrid núm. 43/2009, de 22 de enero de 2009, donde se señala ante la alegación del recurrente de que ignoraba realmente el entramado, que "de ser cierto lo que expone, su posición es de "ignorancia deliberada", lo que le hace igualmente punible, teniendo en cuenta que es persona instruida, que opera regularmente en Internet".

[114] La sentencia, para atribuir dolo, se apoya en argumentos como el "alto porcentaje de un 7% que adquiriría Petra sobre el valor de cada transferencia que se efectuase en la cuenta bancaria abierta en España a tal fin, para su posterior remisión a donde le ordenasen"

parecer, del auténtico sentido en el que se está aplicando por el TS tal pseudo-doctrina, y certifican el riesgo que la supuesta flexibilización de la exigencia de conocimiento derivada de la misma puede conllevar.

Al fin y al cabo, y como ya he señalado en otro lugar, pese al caos aplicativo de esta pseudo-doctrina de la ignorancia deliberada en el TS y en Audiencias Provinciales, son clara mayoría las resoluciones del TS en las que la doctrina de la ignorancia deliberada no supone la sustitución del conocimiento como elemento del dolo sino, más bien, una forma de argumentar sobre la presencia de aquél a partir de los indicios existentes y pese a la declaración del procesado de «actuar sin saber». Así podrían citarse como claros ejemplos la STS núm. 145/2008, de 8 abril de 2008[115] referida a un caso de blanqueo de capitales, la STS de 20 de noviembre de 2006[116] y muy particularmente la citada STS núm. 533/2007, de 12 de junio, referida a un caso de *phishing*. Es decir, que el Tribunal Supremo sigue exigiendo generalmente la existencia de conocimiento para la atribución del delito doloso, si bien es cierto que en ocasiones se hace uso de la doctrina de la ignorancia deliberada para flexibilizar la argumentación sobre la prueba de tal saber». Y hace bien el TS puesto que, frente a lo señalado por un sector de la doctrina[117], no es que en la ignorancia deliberada no se exija conocimiento, sino que más bien el hecho que se imputa y que se valora como injusto se configura con un conocimiento «menor» o, más bien es un hecho (también con conocimiento) anterior, al hecho con conocimiento que antiguamente daba lugar al consenso social sobre cuando hay dolo.

De ahí el riesgo de la doctrina de la ignorancia deliberada: para lo que puede servir la misma es para debilitar la argumentación sobre los hecho probados en lo que corresponde, especialmente, a la atribución de la relación subjetiva entre el procesado y sus hechos. Sobre la única base de que un sujeto evitaba conocer algo no se puede construir la responsabilidad dolosa por lo cometido. Yo diría que ni siquiera la imprudencia. Es necesario realizar una valoración sobre el hecho ejecutado que parta, además, de imputar ordinaria (con conocimiento) o extraordinariamente (sin conocimiento) aquello que después va a ser valorado como injusto. Por eso, los tribunales deben seguir argumentando acerca de lo que, conforme a su proceso racional de imputación, sabía o no sabía el sujeto, como paso previo esencial, el de los antecedentes de hecho, a la valoración, en los fundamentos de derecho, de si un determinado proceder es merecedor o no de la responsabilidad que se atribuye por el injusto doloso.

Volviendo, pues, al tema que nos ocupa, la atribución de responsabilidad por la participación dolosa al mulero del *phishing* exige algo más que la prueba de que éste sabía que "podía estar participando en un hecho ilícito". Deberá saber aquello

[115] Ponente José Manuel Maza Martín.
[116] Ponente Giménez García.
[117] RAGUÉS I VALLÈS, R.: *La ignorancia deliberada en Derecho penal, Atelier, Barcelona, 2008.*

que se exige a cualquier partícipe para responder, a título de dolo, como tal. Pues bien, nuestros tribunales exigen para el cómplice y el cooperador necesario el denominado "doble dolo", con el que hacen referencia al supuesto doble objeto del conocimiento del partícipe. Éste debe saber qué ayuda presta y, también, las circunstancias del hecho principal que se va a ver beneficiado con su aportación. No debe extrañar que sea este último conocimiento, el de "aquello que va a hacer el autor con mi aportación", el que dé lugar al mayor número de problemas prácticos de imputación. Al fin y al cabo, ante la comisión de un determinado delito por un autor, y con la constatación de que el mismo se ha visto facilitado en su actuar por la intervención de un tercero, el argumento de defensa de que el sujeto no sabía lo que hacía parece mucho más condenado al fracaso que el de "no sabía lo que iba a hacer el autor". La prueba del "segundo elemento del dolo", pues, es central en muchas de las resoluciones relacionadas con la posible intervención de partícipes en el delito, y su ausencia el más común criterio de absolución[118] . Como ha señalado la reciente STS núm. 258/2007, de 19 de julio de 2007, el dolo del partícipe "requiere el conocimiento de la propia acción y, además, de las circunstancias esenciales del hecho principal que ejecuta el autor, en el que colabora. Dicho con otras palabras: el partícipe debe haber tenido una representación mental del contenido esencial de la dirección del ataque que emprenderá el autor. No se requiere, por el contrario, conocimiento de las particularidades del hecho principal, tales como dónde, cuándo, contra quién, etc., será ejecutado el hecho"[119].

Si, tal y como se ha dicho, el mulero sólo responderá como partícipe de la estafa informática si se integra, dolosamente, en tal injusto, es lógico entender que sólo será responsable por tal infracción penal cuando se pruebe que ha actuado con conocimiento de que su comportamiento tenía como único sentido, el formar parte de la realización de un determinado injusto. Es decir, que sólo aquellos resultados delictivos que el partícipe previera como potencialmente derivados del injusto al que supiera que se estaba integrando, darán lugar a responsabilidad a título de participación. No es necesario que el sujeto conozca el ataque del sujeto pasivo, pero sí la capacidad lesiva del mismo; tampoco es necesario que conozca la identidad del autor, pero sí que el mismo existe; por último, para que haya participación punible, no se requiere que el partícipe sepa exactamente las características completas del injusto que lleva a cabo el autor (en esto es en lo que hay ignorancia deliberada), pero sí los caracteres esenciales del injusto en el que se integra, así como que su conducta supone precisamente el conformar un hecho delictivo. Los muleros del *phishing,* conforme a la declaración de hechos probados del supuesto que enjuició el TS en la sentencia sobre los muleros del *phishing*, no sabían a quienes se estaba afectando con el injusto principal, pero sí preveían que las cantidades

[118] Véanse las resoluciones citadas en MIRÓ LLINARES, F.: *Conocimiento e imputación…, ob. cit.*
[119] Véase en este sentido la STS núm. 258/2007, de 19 de julio de 2007.

que recibían provenían de cuentas bancarias de clientes estafados; tampoco conocían el nombre concreto de los autores, pero sí sabían que enviaban las cantidades que ingresaban indebidamente a unas direcciones determinadas; por último, es cierto que no sabían exactamente cómo se había logrado el dinero de los otros clientes, pero sí sabían, al menos, lo esencial del injusto de estafa informática: que se les había quitado el dinero a través de la banca electrónica; y pese a todo, decidieron intervenir en el hecho mediante una conducta que, por las cantidades que cobraban, ellos sabían esencial para el éxito de la actividad criminal.

Más que ignorancia deliberada, pues, lo que hay en todos estos casos, es un conocimiento suficiente de un hecho que puede valorarse como la integración en el injusto de la estafa informática en la forma del *phishing.* Eso se deriva al menos, de los elementos que el TS dice que tienen que conocer, y que se corresponden con los que he señalado que deben poder imputarse como conocidos al partícipe. Hay que recordar, además, que la prueba del conocimiento no consiste en la inferencia de un estado mental, sino que el conocimiento se imputa, fruto de la aplicación de reglas lógicas que atribuyan significado a lo realizado por el sujeto en su contexto. Esto es lo que tienen que hacer los tribunales. Esto es, de hecho, lo que hace en la citada sentencia el TS cuando afirma que "en la sociedad actual el acervo de conocimientos de cualquier persona de nivel cultural medio conoce y sabe de la ilicitud de una colaboración que se le pueda pedir del tipo de la que se observa en esta causa, y al respecto, hay que recordar que los recurrentes vivían en Madrid y no consta en los autos nada que pudiera ser sugestivo de un desconocimiento de la ilicitud de la colaboración que se le pedía, máxime cuando no se trataba de una colaboración gratuita sino que llevaba aneja un claro enriquecimiento personal". El Alto Tribunal está atribuyendo al sujeto un determinado conocimiento y, por tanto, imputándole un hecho como conocido a partir de la aplicación de reglas de imputación básicas como, en este caso, la de la transmisión del conocimiento[120]. A mi parecer, además, el TS no sólo acierta en considerar el dolo como imputación del conocimiento, sino que realiza acertadamente el proceso de imputación en el caso concreto, al entender que los muleros sabían lo suficiente como para que se les imputara un hecho valorado como injusto. Cuando sea así, podremos entonces afirmar que el mulero coopera necesariamente integrándose en el injusto de la estafa informática que, con su conducta, pasa a serle también propio.

Y tal forma de proceder en cuanto a la prueba (o imputación) del conocimiento también la están llevando a cabo algunas Audiencias Provinciales como la de Barcelona en la Sentencia de 29 de septiembre de 2011, al argumentar que "es público y notorio por constituir una noticia constante en los medios informativos, la existencia de este tipo de conductas a través de la red. No resulta en modo alguno creíble que una persona, como lo es el acusado, joven, español, residiendo en un

[120] Sobre el dolo como imputación véase, HRUSCHKA, J.: "Sobre la difícil…", *ob. cit.*

país occidental desarrollado, sea cual sea la actividad profesional a la que se dedique, no llegase a representarse como probable que esta actuación que estaba llevando en el cibercafé podía ser ilícita y bien pudo cerciorase que esa cuenta desde la que se efectuaba la transferencia a su favor era del tal " Wensol", simplemente con echar un vistazo a la pantalla del ordenador."

Ahora bien, si tal conocimiento no concurre, si, conforme a los hechos probados, no resulta posible atribuir al sujeto más que el conocimiento de que colaboraba en algo ilícito pero, bien por la experiencia y características del sujeto o bien por otros condicionantes, no puede darse por probado el conocimiento de que la actividad ilícita podría consistir en lucrarse económicamente a costa de un tercero (que son los elementos esenciales mínimos del injusto en este caso), no habrá dolo de cooperación necesaria en la estafa. En otras palabras: si realmente no se puede atribuir al sujeto el conocimiento de que recibe cantidades provenientes de defraudaciones indeterminadas realizadas por Internet, no debiera, a mi parecer, hacerse responsable al mulero del *phishing*[121] como cooperador necesario de una estafa. Lo cual no significa, como se verá a continuación, que tales hechos deban quedar impunes.

3.2.2. *"Conocimiento imputado" y responsabilidad del mulero como autor de blanqueo de capitales*

Conforme a lo visto anteriormente puede aseverarse con rotundidad que el delito de blanqueo de capitales, en su redacción actual, va a ser el más adecuado para la sanción de las conductas de los muleros del *phishing*. Será este tipo penal, especialmente su modalidad dolosa, el que recibirá la mayor parte de los supuestos al no poderse probar siempre la participación dolosa del mulero en el *phishing*. Habrá todo un conjunto de casos en los que, por la reiteración en las conductas o por otros indicios, podrá atribuirse al mulero el conocimiento de participar en un fraude, cuanto menos en el sentido de saber que el dinero que se le envía no sólo le es ajeno a él sino también a quien se lo ha enviado.

Este conocimiento, por el contrario, no es necesario para la atribución de responsabilidad dolosa por el delito de blanqueo de capitales. Lo que resulta necesario, en este caso, es atribuir al sujeto el conocimiento de que el dinero que transmite proviene de una actividad ilícita. Es irrelevante el concreto delito del que puede proceder, lo es también el grado de intervención de quienes le envían a él el dinero, como lo es también la procedencia del mismo o su propia relevancia en el delito y si éste se ha consumado ya o no. Lo que sí es relevante para que haya delito doloso es que el mulero sepa que está realizando actos relacionados con dinero de proce-

[121] No es aceptable, pues, una argumentación como la de la AP Vizcaya en Sentencia núm. 355/2006, de 9 de mayo de 2006, relativa a que el tipo subjetivo del delito de estafa "supone el conocimiento del origen ilícito de las cantidades transferidas a las cuentas abiertas por el acusado, conocimiento que no necesariamente ha de comprender todos los detalles de la operación fraudulenta, sino que basta con que abarque la fundada probabilidad de que su procedencia es delictiva".

dencia ilícita. Al fin y al cabo el injusto del blanqueo es extremadamente amplio: cualquier tipo de uso de dinero proveniente de actividades delictivas. Y es muy fácil atribuir este conocimiento al mulero: bastará con poder afirmar que, por el porcentaje que cobraba por su actividad, por el oscurantismo que rodeaba a los hechos, o por el propio sinsentido que supone el que alguien no pueda sacar dinero que le pertenece si no es por medio de otro, al sacar ese dinero y enviarlo a un sujeto se está transmitiendo un dinero no lícito o, cuanto menos, se está colaborando en una actividad ilícita con actos monetarios.

Conforme a la casuística de conductas de muleros relacionadas con fraudes de phishing parece bastante sencillo de imputar el conocimiento necesario para la responsabilidad por el blanqueo de capitales en su modalidad dolosa conforme a su nueva redacción. No hay que olvidar, en todo caso, y esta es una ventaja respecto a la calificación de la conducta como cooperación necesaria en la estafa, que el blanqueo de capitales también puede ser sancionado en su forma imprudente. Esto permite graduar la responsabilidad conforme al distinto conocimiento, o desconocimiento, del mulero. En el caso de que, por las circunstancias personales del implicado o incluso por la extrema apariencia de legalidad del contrato, no pueda probarse el conocimiento de la participación en una actividad económica ilícita, la responsabilidad imprudente será la más adecuada si logra probarse que pese a desconocer su implicación le incumbía haberse percatado de ello.

Cuando, por el contrario, y en el otro extremo, no sólo se pruebe el conocimiento de transmitir dinero en relación con una actividad delictiva, sino también la probabilidad de que ttal actividad sea un fraude o infracción patrimonial sobre un tercero sea del tipo que sea, entonces el mulero deberá ser hecho responsable como partícipe de la estafa de que se trate con la misma pena que correspondería a los autores. Estos, en todo caso, difícilmente serán hechos responsables por estos delitos en el mundo transnacional que es el ciberespacio. Se imponen, por ello, no sólo soluciones jurídicas de cooperación internacional sino, también, nuevas estrategias de prevención centradas en la educación de la víctima potencial e, incluso, de la otra víctima del phishing, el mulero responsable penalmente de un delito.

BIBLIOGRAFÍA

Alonso Royano, F.: “¿Estado de Derecho o derecho del Estado? El delito informático”, en *RGD,* núm. 498, marzo, 1986.

Carbajo Gascón, F.: *Publicaciones electrónicas y Propiedad Intelectual,* Colex, Madrid, 2002.

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.

Chiu, C. /Ku, Y./Lie, T./Chen, Y.: “Internet Auction Fraud Detection Using Social Network Analysis and Classification Tree Approaches”, en *IJEC*, vol. 15, núm. 3, 2011.

Chua, C.E.H./Wareham, J.: "Fighting Internet Auction Fraud: An Assessment and Proposal Computer", en *IEEE Computer,* núm. 10, 2004.

Clough, J.: *Principles of Cybercrime,* Cambridge University Press, Cambridge, 2010.

Corcoy Bidasolo, M. /Joshi, U.: "Delitos contra el patrimonio cometidos por medios informáticos", en *RJC,* núm. 3, Barcelona, 1988.

Cruz de Pablo, J.A.: *Derecho penal y nuevas tecnologías. Aspectos sustantivos,* Difusión Jurídica y Temas de Actualidad, Madrid, 2006.

De Miguel Asensio, P. A.: *Derecho privado de Internet,* Civitas, Madrid, 2000.

Dong, X. /Clark, J.A./Jacob, J.L.: *"Defending the weakest link: phishing websites detection by analysing user behaviours",* en *Telecommun Syst,* núm. 45, 2010.

Emigh, A.: *Online Identity Theft: Phishing Technology, Clokepoints and Countermeasures. ITTC Report on Online Identity Theft Technology and Countermeasures*, 2005.

Faraldo Cabana, P.: *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico,* Tirant lo Blanch, Valencia, 2009.

Fernández Teruelo, J.G.: *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes,* Lex Nova, Valladolid, 2011.

Fernández Teruelo, J. G.: "Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de red", en *RDPC*, núm. 19, 2007.

Flor, R.: "*Phishing* y delitos relacionados con el fraude de identidad: un World Wide Problem en el World Wide", en V.V.A.A.: *Robo de identidad y protección de datos,* Aranzadi, Pamplona, 2010.

Flores Prada, I.: *Criminalidad informática. Aspectos sustantivos y procesales,* Tirant lo Blanch, Valencia, 2012.

Frisch, W.: *Comportamiento típico e imputación del resultado* (traducido por Joaquín Cuello Contreras y José Luis Serrano González de Murillo), Marcial Pons, Madrid, 2004.

Galán Muñoz, A.: "El robo de identidad: aproximación a una nueva y difusa conducta", en V.V.A.A.: *Robo de identidad y protección de datos,* Aranzadi, Pamplona, 2010.

Galán Muñoz, A.: *El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 CP,* Tirant lo Blanch, Valencia, 2005.

Garrote Fernández-Díez, I.: *El derecho de autor en Internet,* Comares, Granada, 2004 (2ª edición).

González Gómez, A.: *El tipo básico de los delitos contra la propiedad intelectual,* Tecnos, Madrid, 1998.

González Rus, J. J.: "Delitos contra el patrimonio y contra el orden socioeconómico", en Cobo del Rosal, M. (Coord.): *Derecho penal español: parte especial,* Dykinson, Madrid, 2005.

González Rus, J. J.: "Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en *PJ,* Número especial IX, 1989.

Guinarte Cabada, G.: "Algunas notas sobre la nueva regulación de la Propiedad Intelectual e Industrial en el Código Penal español de 1995", en *ADI*, núm. 16, 1994-1995.

Gutiérrez Francés, M. L.: "Delincuencia económica e informática en el nuevo Código penal", en *CDJ,* núm. 11, 1996.

Herrera Moreno, M.: "El fraude informático en Derecho penal español", en *AP,* núm. 39,

2001.

Hong, J.: "The State of Phishing Attacks", en *Communications of the ACM,* vol. 55, núm. 1, 2012.

Hruschka, J.: "Sobre la difícil prueba del dolo", en Del Mismo: *Imputación y Derecho penal* (traducido por Pablo Sánchez-Ostiz Gutiérrez), Aranzadi, Cizur Menor, 2005.

Jaishankar, K.: "Identity related Crime in the Cyberspace: Examining Phishing and its impact", en *IJCC*, vol. 2, enero-junio, 2008.

Jakobsson, M.: *Phishing and Countermesasures: Understanding the Increasing Problem of Electronic Identity Theft,* John Willey & Sons, 2005.

Jescheck, H.H./Weigend, T.: *Tratado de Derecho penal. Parte general* (traducido de la 5ª edición alemana por Miguel Olmedo Cardenete), Comares, Granada, 2002.

Jorge Barreiro, A.: "Comentario al artículo 270", en Rodríguez Mourullo, G. (Dir.)/Jorge Barreiro, A. (Coord.): *Comentarios al Código penal,* Civitas, Cizur Menor, 1997.

Maniyara, M.: "Post del blog Security Response de Symantec, 3 de febrero de 2010". En Internet, en http://www.symantec.com/connect/blogs/phishing-using-pornographic-content-bait. Citado el 3 de abril de 2013.

Mata y Martín, R.: "El robo de identidad: ¿una figura necesaria?", en V.V.A.A.: *Robo de identidad y protección de datos,* Aranzadi, Pamplona, 2010.

Mata y Martín, R. M.: *Delincuencia informática y Derecho penal,* Madrid, Edisofer, 2001.

Mir Puig, S.: *Derecho penal. Parte general,* Reppertor, Barcelona, 2004 (7ª edición).

Miró Llinares, F.: *El cibercrimen,* Marcial Pons, Madrid/Barcelona/Buenos Aires/ São Paulo, 2012.

Miró Llinares, F.: "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", en *RECPC,* núm. 13-07, 2011.

Miró Llinares, F.: "Cibercrímenes económicos y patrimoniales", en Ortiz de Urbina Gimeno, I. (Dir.): *Memento práctico penal y económico de la empresa 2011-2012,* Francis Lefebvre, Madrid, 2011.

Miró Llinares, F.: *Conocimiento e imputación en la participación delictiva. Aproximación a una teoría de la intervención como partícipe en el delito,* Atelier, Barcelona, 2009.

Miró Llinares, F. /García Guilabert, N.: "Encuesta Nacional de victimización en el ciberespacio", en el marco del Proyecto de Investigación financiado por el Ministerio de Ciencia e Innovación, DER2011-2605, titulado "Cibercriminalidad: detección de déficits en su prevención jurídica y determinación de los riesgos de victimización para una mejor prevención situacional criminológica", presentada en la conferencia *La victimización en el ciberespacio,* impartida en el *IX Congreso Español de Criminología*, Girona, 2012.

Muñoz Conde, F. (Coord.): *Problemas actuales del Derecho penal y de la Criminología: estudios penales en memoria de la Profesora Dra. María del Mar Díaz Pita,* Tirant lo Blanch, Valencia 2008.

Myers, S.: "Introduction to Phishing" en Jakobsson, M. /Myers, S.: *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft,* John Wiley and Sons, 2006.

Ollman, G.: *The Phishing Guide: Understanding and Preventing Phishing Attacks. Infor-*

me Técnico, NGSS, 2009.

Orts Berenguer, E. /González Cussac, J.L.: *Compendio de Derecho Penal (Parte general y Parte especial),* Tirant lo Blanch, Valencia, 2004.

Ragués i Vallès, R.: *La ignorancia deliberada en Derecho penal,* Atelier, Barcelona, 2008.

Romeo Casabona, C. Mª.: "Sobre la estructura monista del dolo. Una visión crítica", en Jorge Barreiro, A. /Bajo Fernández, M. / Suárez González, C. J. (Coords.): *Homenaje al Profesor Dr. Gonzalo Rodríguez Mourullo,* Civitas, Cizur Menor, 2005.

Romeo Casabona, C. M.: *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las nuevas tecnologías de la información,* Fundesco, Madrid, 1988.

Rovira del Canto, E.: *Delincuencia informática y fraudes informáticos,* Comares, Granada, 2002.

Sieber, U.: *Computerkriminalität und Strafrecht,* Carl Heymanns, Köln/Berlin/Bonn/München, 1980 (2ª edición).

Stadler, W. A.: "Internet Fraud", en Fisher, B. S./Lab, S. P.: *Encyclopedia of Victimology and Crime Prevention,* vol. 1, Sage Publications, California/London, 2010.

Suárez-Mira Rodríguez, C. (Coord.): *Manual de Derecho penal, Tomo I: Parte general,* Civitas, Cizur Menor, 2006 (4ª edición).

Tiedemann, K.: *Poder económico y delito,* Barcelona, Ariel, 1985.

Velasco Núñez, E.: "Fraudes informáticos en Red: del *phishing* al *pharming*", en *LL,* núm. 37, año IV, abril 2007.

Vives Antón, T.S.: *Fundamentos del sistema penal,* Tirant lo Blanch, Valencia, 2008.

Vives Antón, T.S.: "Reexamen del dolo", en Muñoz Conde, F. (Coord.): *Problemas actuales del Derecho penal y de la Criminología: estudios penales en memoria de la Profesora Dra. María del Mar Díaz Pita,* Tirant lo Blanch, Valencia 2008.

Wall, D.: *Cybercrime: the transformation of crime in the information age*, Polity Press, Cambridge, 2007.

Yar, M.: *Cybercrime and society,* London, Sage, 2006.