Revista Electrónica de Estudios Penales y de la Seguridad
ISSN: 2531-1565

NUEVAS TECNOLOGÍAS, ESTAFA INFORMÁTICA E IGNORANCIA DELIBERADA*

NEW TECHNOLOGIES, COMPUTER SCAM AND WILLFUL BLINDNESS

Francisco Almenar Pineda
Doctor en Derecho / Profesor
Chongqing College of International Business and Economics (China)

Fecha de recepción: 4 de noviembre de 2022.

Fecha de aceptación: 26 de enero de 2023.

RESUMEN

Este trabajo constituye una aproximación a la estafa informática, en el uso de las nuevas tecnologías con fines delictivos. De forma específica, a su modalidad más frecuente, consistente en el denominado delito de phising y la ignorancia deliberada propia de su cooperador, desde el punto de vista del ordenamiento penal español. Su análisis se realiza una vez se ha producido la necesaria previsión de estos comportamientos en el Código Penal de 1995, que ha sido modificado en materia de fraudes informáticos en los años 2003 y 2010. En concreto, en el apartado 2 de su artículo 248.

ABSTRACT

This work constitutes an approximation to the computer fraud, in the use of new technologies for criminal purposes. Specifically, to its most frequent modality, consisting of the so-called crime of phishing and the willful blindness of its cooperator, from the point of view of the Spanish criminal law. Its analysis is done once a much-needed provision for these behaviors has been produced in the Criminal Code of 1995, which has been modified in terms of computer fraud in the years 2003 and 2010. In particular, in section 2 of its article 248.

* Este trabajo desarrolla la comunicación que, con el mismo título, fue seleccionada y expuesta ante el público en el Congreso internacional de Derecho penal y Comportamiento humano: desafíos desde la Neurociencia y la Inteligencia artificial, celebrado en Toledo durante los días 21 a 23 de septiembre de 2022, que se organizó en el marco del proyecto de investigación Derecho Penal y Comportamiento Humano (RTI2018-097838-B-I00).

PALABRAS CLAVE

Tecnologías, delincuencia informática, estafa informática, cibercrimen, *phising*.

KEYWORDS

Technologies, computer crime, computer scam, cybercrime, phising.

ÍNDICE

SUMMARY

1. INTRODUCCIÓN

El presente artículo trae causa de la Comunicación que bajo el título "Nuevas tecnologías, estafa informática e ignorancia deliberada" tuve la oportunidad de presentar en el Congreso Internacional sobre "Derecho penal y comportamiento humano: Desafíos desde la neurociencia y la inteligencia artificial", celebrado en la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Castilla-La Mancha en los días 21, 22 y 23 de septiembre de 2022.

De forma más específica, este trabajo se encuentra motivado por el progresivo incremento de las estafas informáticas en España, y el reiterado argumento de la falta de culpabilidad por parte del sujeto que coopera en su ejecución[1]. En concreto, la pretendida ignorancia de la ilicitud de estas operaciones por parte de las denominadas mulas, es decir, usuarios de Internet que se verían beneficiados económicamente por este tipo de actividades a cambio de una pequeña comisión[2], tratando de relevar su responsabilidad hacia un tercero ubicado en el extranjero.

Como punto de partida, a efectos de destacar la trascendencia del problema, conviene tener presente que los fraudes a través de las nuevas tecnologías ocupan, de forma destacada, el primer lugar de los ciberdelitos que fueron registrados en el año 2020 por el Observatorio Español de Delitos Informáticos, multiplicando prácticamente por veinte el número de las amenazas y coacciones que se cometen por Internet y que, a su vez, se encuentran en la segunda posición de esa estadística. Además, esa modalidad de comportamientos defraudatorios supera en 40.000 casos los mismos tipos de ilícitos del año 2019.

Dicho en otras palabras, de los 287.963 delitos constatados por esa entidad en el año 2020, 257.907 supuestos estaban relacionados con esos ilícitos contra el patrimonio, siendo una cifra registrada que se ha incrementado considerablemente respecto al año anterior[3].

Esos datos meramente estimativos de las citadas defraudaciones se corresponden fundamentalmente con una mayor sencillez para realizarlas, unida a la rapidez de ejecución, y el empleo de software[4] o aplicaciones como *Bizum*[5], que permiten realizar transferencias bancarias inmediatas para impedir la reacción de la víctima, evitando que pueda cancelar la operación desde su cuenta bancaria una vez se cerciora de la sustracción ilícita.

---

1 La falta de culpabilidad del acusado por estas acciones es uno de los argumentos de defensa más reiterados ante los órganos jurisdiccionales penales. Así, según se expondrá más adelante, entre otros, en los casos juzgados por la STS, Sección 1ª, nº 533/2007, de 12 de junio (RJ\2007\3537), Pte. Excmo. Sr. Joaquín Giménez García; la STS, Sección 1ª, nº 743/2015, de 20 de noviembre (RJ\2015\5317), Pte. Excmo. Sr. D. Juan Saavedra Ruiz; o por la SAP de Madrid, Sección 23ª, nº 92/2018, de 24 de enero (ARP\2018\278), Pte. Ilma. Sra. Dª María de los Ángeles Montalvá Sempere.

2 ALMENAR PINEDA, F., *Ciberdelincuencia*, ed. Jurua, Oporto, 2018, p. 48.

3 Estadísticas sobre ciberdelitos disponibles en https://oedi.es/estadisticas/, consultado el 13 de junio de 2022.

4 El software se define por la RAE como el conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

5 Más información sobre la aplicación *Bizum* en https://bizum.es/como-funciona/, consultado el 13 de junio de 2022.

La doctrina también ha destacado otros factores que contribuyen al incesante auge de estas conductas. Así, BARRIO ANDRÉS[6] vincula la facilidad delictiva con las pruebas dentro del proceso, que no son contundentes y pueden verse manipuladas sin dificultad, concurriendo especial lentitud en la investigación de los hechos, favoreciendo su obstaculización o la destrucción de pruebas, y al hecho de que puede concurrir cierto anonimato o enmascaramiento del autor, que normalmente emplea personalidades ficticias, dificultando así su identificación. Por ello, muchas de estas conductas no se descubren o son descubiertas tarde, produciéndose lo que el citado autor denomina "macro-victimización".

Por su parte, DÍAZ MARTÍNEZ[7] cita, como circunstancias decisivas en el ascenso de estos delitos, la ausencia de inmediación entre autor y víctima; la despersonalización de la conducta cuando se actúa en el ciberespacio, produciéndose una especie de anestesia en la relación causa-efecto; la tecnología convertida en un instrumento que facilita la ocultación de los rastros del delito; cierta ausencia de normas, tanto en la conciencia del sujeto que lleva a cabo estas conductas, que cree que actúa en un sitio ajeno al Derecho, como en la realidad por no existir un ordenamiento consolidado y eficaz que regule Internet; o la extraterritorialidad de las acciones, con los consiguientes problemas para su persecución.

La Fiscalía General del Estado ya se refería, en su Memoria del año 2016[8], a la dificultad para computar los casos de delincuencia informática "*dada la escasa frecuencia con la que los afectados/perjudicados comunican el ataque del que han sido víctimas a las fuerzas policiales y/o a los órganos de la Administración de Justicia*". Y explicaba esta circunstancia por varios motivos: (i) "*la falta de conciencia del carácter delictivo de la conducta*"; (ii) "*cierto factor de desconfianza en las capacidades de actuación frente a estas acciones*"; y (iii) "*razones de carácter reputacional cuando el conocimiento público del hecho pueda afectar al prestigio de empresas y/o instituciones públicas o privadas*". Si bien señalaba un progreso lento en el cambio de actitud, al tomarse "*una mayor conciencia de la ilicitud de estas conductas y de la necesidad de ofrecer respuestas efectivas a partir de los mecanismos del Estado de Derecho*", evolución que se evidencia en el progresivo incremento de las estafas informáticas registradas por el citado Observatorio.

En cualquier caso, el supuesto concreto de *phising*, como categoría más reiterada dentro del amplio abanico de las citadas defraudaciones, imposibles de abarcar en este trabajo, y la pretendida inculpabilidad por parte del cooperador, en base a su ignorancia, ha motivado las siguientes líneas, al haber comprobado la escasez de estudios doctrinales sobre el tratamiento jurídico que debe recibir este tipo de argumentaciones a pesar de la extensa jurisprudencia sobre la materia.

---

[6] BARRIO ANDRÉS, M., "El régimen jurídico de los delitos cometidos en Internet en el derecho español tras la reforma penal de 2010", en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012, p. 35.

[7] DÍAZ MARTÍNEZ, M., "El factor criminógeno de las TIC", en PÉREZ GIL, J. (Coord.) y VVAA, *El proceso penal en la sociedad de la información*, ed. La Ley, Madrid, 2012, p. 534-538.

[8] MADRIGAL MARTÍNEZ-PEREDA, C., *Memoria elevada al Gobierno de S.M. Presentada al inicio del año judicial por la Fiscalía General del Estado*, Centro de Estudios Jurídicos, Madrid, 2016, disponible en https://www.fiscal.es/memorias/memoria2016/FISCALIA_SITE/recursos/pdf/MEMFIS16.pdf, consultado en fecha 13 de junio de 2022.

En consecuencia, me propuse redactar el presente artículo para, en la medida de lo posible, simplificar el estudio desde el punto de vista jurídico de un comportamiento que emplea las nuevas tecnologías como herramienta, especialmente tras su necesaria regulación por primera vez en el artículo 248 del Código Penal de 1995, modificado por la Ley Orgánica 15/2003, de 25 de noviembre (en adelante, "***LO 15/2003***") y la Ley Orgánica 5/2010, de 22 de junio (en adelante, "***LO 5/2010***").

Todo ello, sin perder de vista que las conductas de *phising* constituyen la modalidad de estafa informática más habitual, razón por la cual, con las peculiaridades propias del medio empleado, comparte los elementos de esa clase de defraudaciones, creando todo un entramado de conductas en torno a los citados preceptos de difícil interpretación.

Para llevar a cabo el análisis, este artículo se ha dividido en un punto inicial dedicado a los antecedentes y evolución de las estafas informáticas, incluyendo algunos conceptos y su tratamiento en el ordenamiento penal español, lo que sirve para determinar la importancia del tema, para a continuación hacer una breve referencia al bien jurídico protegido en estos delitos en el siguiente punto, siguiendo con su naturaleza jurídica, los elementos que lo integran, y la relevancia de la citada ignorancia manifestada por el delincuente, finalizando con las conclusiones.

2. BREVE REFERENCIA A LA EVOLUCIÓN HISTÓRICA DE LAS ESTAFAS INFORMÁTICAS.

2.1. Introducción.

En los últimos años el legislador ha tomado conciencia de la revolución tecnológica acelarada que estamos experimentando, especialmente en el ámbito de las comunicaciones, en lo que parecen tan sólo los primeros pasos de una gran transformación social, ligada a la realidad de que la información es susceptible de alcanzar cualquier lugar con cualquier herramienta conectada a Internet.

Ese progreso informático y la digitalización de los datos han llegado a tal punto que incluso se ha defendido la existencia de una cibersociedad[9], que algunos autores consideran distinta al mundo analógico tradicional[10].

Ahora bien, las ventajas que suponen la universalidad y transnacionalidad de los nuevos medios de comunicación e información, p.ej. en la rápida investigación y respuesta por equipos médicos multinacionales en la última pandemia que hemos vivido, también incluyen riesgos para los derechos y libertades de las personas, que pueden verse lesionados por nuevos artificios carentes actualmente de una normativa suficientemente eficaz.

El avance de estas tecnologías ha venido acompañado de su empleo como instrumento para delinquir y atentar sobre los bienes jurídicos que ya eran objeto de tutela en nuestro

[9] LÓPEZ ZAMORA, P., *El Ciberespacio y su Ordenación*, ed. Difusión Jurídica y Temas de Actualidad, Madrid, 2006, p. 95.

[10] MORÓN LERMA, E., *Internet y Derecho Penal: <<Hacking>> y otras conductas ilícitas en la red,* ed. Aranzadi, segunda edición, Navarra, 2002, p. 21.

ordenamiento.

En este contexto, las estafas informáticas constituyen un ejemplo de la necesidad de adaptar el Derecho a las transformaciones sociales. El impulso normativo se plantea cuando un aspecto determinado de la convivencia puede lesionar o poner en peligro los derechos de las personas. En ese momento el legislador debe actuar para salvaguardar esos bienes valiéndose de los medios previstos en el ordenamiento jurídico.

A todo ello se une el fenómeno de huida hacia el Derecho penal de los últimos años, especialmente en los casos de mayor trascendencia mediática, alejándose el legislador de la idea del Derecho penal como *ultima ratio*[11] para convertirlo en herramienta de respuesta en los casos de alarma social. A pesar de esta instrumentalización, el carácter global de las TIC cuestiona que el sistema penal tenga capacidad suficiente para una eficaz regulación[12] de estas nuevas relaciones sociales.

2.2. Concepto y rasgos de la delincuencia informática.

El continuo desarrollo de los nuevos medios de comunicación e información, y las conductas delictivas relacionadas con ellos, ha supuesto que parte de la doctrina prefiera negar el concepto concreto de delito informático, para preferir los términos de delitos informáticos en general, delincuencia informática o criminalidad informática.

Así pues, con una referencia genérica, como señala HERNÁNDEZ DÍAZ, se elude el problema de la utilización del término delito informático, que puede llevar a una errónea identificación con su realidad positiva, por cuanto su mención es inexistente en la ley penal[13], mismo problema que surgiría con el empleo de la categoría Derecho penal informático. Por tanto, siguiendo el concepto de algunos autores como MENÉNDEZ MATO y GAYO SANTA CECILIA, se puede entender como delitos informáticos en general "*aquellas conductas que a través de medios tecnológicos o informáticos conculcan lo establecido en el ordenamiento jurídico*"[14].

No obstante, la citada definición se ciñe a los medios, no incluyendo los supuestos en los que el sistema informático es el objeto de ataque, como en el caso del *hacking*[15]. Por ello, parece más acertada la alusión a delincuencia informática o criminalidad informática como los

---

[11] DE URBANO CASTRILLO, E., "Los delitos informáticos tras la reforma del CP de 2010", en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012, p. 21.

[12] SÁNCHEZ MAGRO, A., "El ciberdelito y sus implicaciones procesales", en GARCÍA MEXÍA, P. (Dir.), y VVAA. *Principios de Derecho de Internet*, ed. Tirant Lo Blanch, Valencia, 2005, epígrafe 6.

[13] En este sentido, HERNÁNDEZ DÍAZ, L., "Aproximación a un Concepto de Derecho Penal Informático", en DE LA CUESTA ARZAMENDI, J. L. (Dir.) y VVAA, *Derecho Penal Informático*, ed. Civitas, Pamplona, 2010, p. 42.

[14] MENÉNDEZ MATO, J. C. y GAYO SANTA CECILIA, M. E., *Derecho e informática: ética y legislación*, ed. Bosch Editor, Barcelona, 2014, p. 319.

[15] Si atendemos a la previsión del artículo 197 bis 1 del Código Penal, se puede entender como *hacking* "*el acceso no autorizado a todo o parte de un sistema informático, física o remotamente, con independencia de los medios y finalidad del sujeto, vulnerando las medidas de seguridad establecidas para impedirlo, o bien, tras un previo acceso lícito, la permanencia en todo o parte de un sistema contra la voluntad de quien tenga el legítimo derecho a excluirlo*". En este sentido, ALMENAR PINEDA, F., *El delito de hacking*, ed. Aranzadi, Pamplona, 2018, p. 60.

"*comportamientos en los que un sistema informático sea el medio para lesionar un bien jurídico, cualquiera, y todos aquéllos en que dicho sistema sea él mismo el propio objeto sobre el que recae la acción delictiva*", siguiendo así el concepto mayoritario que resume HERNÁNDEZ DÍAZ[16], y que también parece aplicable al de delitos informáticos en general, dando así cabida dentro de la categoría también a los equipos, redes o sistemas informáticos como objeto del ataque.

De esta forma, las defraudaciones informáticas tendrían cabida en ese grupo por concurrir sus características comunes:

1. Existe una zona de riesgo que resulta de la generalización de las nuevas tecnologías y que es común a numerosos bienes jurídicos protegidos. Con el acceso ilícito a los datos ajenos para realizar una transferencia no consentida de cualquier activo patrimonial, se produce un peligro para los intereses más importantes, incluyendo bienes de nueva aparición con el desarrollo de la informática, como la integridad o la confidencialidad del sistema que los contiene.
2. Concurre cierta sencillez para llevar a cabo estos comportamientos, donde el acceso remoto a la información y la colaboración de intermediarios puede dejar poco rastro de la intrusión, con las consecuentes dificultades para su persecución y castigo, a lo que se añade cierto anonimato del autor.
3. Ese intrusismo y la suplantación también permiten que las conductas puedan llevarse a cabo sin límites fronterizos, facilitando su impunidad.
4. La ausencia de inmediación autor-víctima, la tecnología al servicio de facilitar la impunidad de la conducta, la inexistencia de un ordenamiento supranacional suficientemente consolidado y eficaz, han determinado el mencionado incremento de estas conductas.
5. La transferencia no consentida del activo patrimonial requiere de cierta vulnerabilidad de los equipos y sistemas informáticos y la especialización en los sujetos que las llevan a cabo.

Con estas características, son múltiples los comportamientos que podemos imaginar encuadrables en esa categoría de delincuencia, hasta el punto de que hoy día prácticamente cualquier delito es susceptible de cometerse o verse favorecido a través de las nuevas tecnologías de la información y la comunicación.

El tratamiento legislativo de la materia ha tenido una evolución que a grandes rasgos se expone a continuación.

2.3. Evolución normativa supranacional.

Las circunstancias descritas han motivado la lógica alarma social. En consecuencia, puesto que los Estados europeos no han sido ajenos a los peligros que acompañan a las nuevas

[16] HERNÁNDEZ DÍAZ, L., "Aproximación a un Concepto de Derecho Penal Informático", en DE LA CUESTA ARZAMENDI, J. L. (Dir.) y VVAA, *Derecho Penal Informático*, ed. Civitas, Pamplona, 2010, p. 43; y ÁLVAREZ VIZCAYA, M., "Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red", en *Internet y Derecho penal. Cuadernos de Derecho Judicial*, nº 10, Madrid, 2001, p. 257.

tecnologías para los derechos de las personas, ha existido una tendencia a armonizar la legislación tanto en el ámbito del Consejo de Europa como en el de la Unión Europea. En resumen y como más relevantes:

i. Los orígenes se encuentran en los años 80 en los grupos de estudio de la Organización para la Cooperación y Desarrollo Económico (OCDE) y el Consejo de Europa para intentar dar respuesta legal al acceso no autorizado a sistemas informáticos. En el primero de ellos surgieron las directrices para la protección de la privacidad y los flujos transfronterizos de los datos personales, tanto públicos como privados, en la medida en que ponen en riesgo los derechos de las personas, siendo nombrado un comité de expertos en 1983, que elaboraron una propuesta de mínimos comunes en las legislaciones de los países miembros, incluyendo los fraudes informáticos, publicada en el año 1986[17]. Por su parte, en el Consejo de Europa se suscribe el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal el 28 de enero de 1981, y en el año 1989 se aprueba la Recomendación donde se incluye un listado de conductas que se deberían considerar delictivos en las legislaciones nacionales, entre ellas las citadas defraudaciones por ordenador[18].

ii. El Convenio Europeo sobre la Ciberdelincuencia, de fecha 23 de noviembre de 2001, en cuyo Preámbulo se expone "*la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional*", supone un hito fundamental para la regulación de los delitos informáticos en nuestro ordenamiento jurídico interno, incluyendo los fraudes informáticos en su artículo 8[19].

iii. El Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007, faculta al Parlamento Europeo y el Consejo para establecer directivas como instrumento de normas mínimas en materia de delincuencia informática[20].

---

[17] En concreto, la propuesta del comité de la OCDE mencionaba la necesaria inclusión de los fraudes informáticos en las legislaciones de los Estados miembros en los siguientes términos: " *a) the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit an illegal transfer of funds or of another thing of value; b) the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit a forgery;*". OCDE, *Computer-related criminality: Analysis of Legal Politics in the OECD Area*, París, 1986, p. 69-70, reimpreso en UNITED NATIONS, "United Nations Manual on the Prevention and Control of Computer-Related Crime", *International Review of Criminal Policy*, Nos. 43 and 44, Viena, 1994, disponible en https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF, consultado el 14 de junio de 2022.

[18] Recommendation R(89)9 of the Committee of Ministers to Members States on Computer-related Crime and Final Report of the European Commitee on Crime Problems, p. 37-39, disponible en http://www.oas.org/juridico/english/89-9&final%20report.pdf, consultado el 14 de junio de 2022.

[19] Según el artículo 8 del Convenio Europeo sobre la Ciberdelincuencia, "*Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:*
a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;
b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona", publicado en BOE Núm. 226, de 17 de septiembre de 2010, páginas 78847 a 78896, disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221, consultado el 14 de junio de 2022.

[20] Conforme al artículo 69 B de la Directiva, "*El Parlamento Europeo y el Consejo podrán establecer, mediante directivas adoptadas con arreglo al procedimiento legislativo ordinario, normas mínimas relativas a la definición de las infracciones penales y de las sanciones en ámbitos delictivos que sean de especial gravedad y*

No obstante la normativa orientada a regular esta materia a nivel internacional, los instrumentos comunitarios no han resultado suficientemente eficaces en la lucha contra las estafas informáticas, atendida la lentitud y la falta de medios comunitarios para legislar en la materia penal. Esto ha motivado que la respuesta del legislador sea siempre tardía frente a unas conductas que son cada vez más sofisticadas y que se incrementan cada año al ritmo que marca el crecimiento de las nuevas tecnologías.

En este marco aparece y se desarrolla la figura del *phising*, con unas estadísticas que superan el cuarto de millón de casos en España en el año 2020[21], supone el mayor peligro de ciberseguridad identificado por las organizaciones[22], números que son mayores si atendemos a la circunstancia de que estos ataques en su inmensa mayoría no son denunciados[23].

3. CONCEPTO DEL DELITO DE ESTAFA INFORMÁTICA Y DEL *PHISING* COMO SU MODALIDAD MÁS FRECUENTE.

3.1. Concepto del delito de estafa informática.

A pesar de la ausencia de tipificación de estas conductas con anterioridad al CP de 1995, la evolución de las tecnologías y la generalización del uso de Internet en los años 90 ha supuesto la aparición de nuevos comportamientos, que han perfilado un concepto de estafa informática, al resultar cada vez más habitual valerse del ciberespacio para la realización de acciones con ánimo de lucro en perjuicio de tercero, como la ciberextorsión, o la citada modalidad de fraude por ordenador[24].

En este último caso, se puede distinguir, como hace ALONSO GARCÍA, entre estafas cometidas a través del medio digital y estafas informáticas[25], en función de que, respectivamente, exista engaño bastante sobre tercero o este elemento sea sustituido por una manipulación informática. Así, sería un ejemplo del primero el *auction fraud*, que comprende tanto supuestos en los que un comprador remite un cheque falso al vendedor de un producto por Internet, por un valor superior al precio, solicitando al vendedor deducir el precio para proceder a depositar el pago y después devolver la diferencia, como los casos de

---

tengan una dimensión transfronteriza derivada del carácter o de las repercusiones de dichas infracciones o de una necesidad particular de combatirlas según criterios comunes.

Estos ámbitos delictivos son los siguientes: el terrorismo, la trata de seres humanos y la explotación sexual de mujeres y niños, el tráfico ilícito de drogas, el tráfico ilícito de armas, el blanqueo de capitales, la corrupción, la falsificación de medios de pago, la delincuencia informática y la delincuencia organizada", disponible en https://www.boe.es/buscar/doc.php?id=DOUE-Z-2007-70005, consultado el 14 de junio de 2022.

21 *Vid*. Nota 3.

22 En concreto, en una encuesta elaborada entre más de 1300 profesionales se detectó que el 56% identificaba al *phising* como el mayor peligro en su seguridad informática en el año 2018. Así, CYBERARK, "Cyberark global advanced threat landscape report 2018", en *Ciberark Report*, Boston, 2018, p. 5. disponible en https://www.cyberark.com/resources/white-papers/cyberark-global-advanced-threat-landscape-report-2018-the-cyber-security-inertia-putting-organizations-at-risk, consultado el 14 de junio de 2022.

23 *Vid*. Nota 8.

24 ALMENAR PINEDA, F., *Ciberdelincuencia ... , cit*., Nota 2, p. 46.

25 ALONSO GARCÍA, J., *Derecho penal y redes sociales*, ed. Thomson Reuters Aranzadi, primera edición, Navarra, 2015, p. 401.

subastas y compraventas donde finalmente no se envía el producto[26] o se remite uno de distintas características a las ofertadas.

Mientras que en las denominadas estafas informáticas, según la copiosa jurisprudencia, se incluyen "*aquellos casos que mediante una manipulación informática o artificio semejante se efectúa una transferencia no consentida de activos en perjuicio de un tercero admitiendo diversas modalidades, bien mediante la creación de órdenes de pago o de transferencias, bien a través de manipulaciones de entrada o salida de datos, en virtud de los que la máquina actúa en su función mecánica propia".* Así pues, *"Subsiste la defraudación y el engaño, propio de la relación personal,* (que) *es sustituido como medio comisivo defraudatorio por la manipulación informática o artificio semejante en el que lo relevante es que la máquina, informática o mecánica, actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquéllos que permite su programación, o por la introducción de datos falsos*"[27].

En consecuencia, siguiendo este criterio, sus variantes son múltiples, por cuanto mediante una manipulación informática se consigue la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. Por tanto, en puridad no existe engaño ni error, reduciéndose la conducta a la manipulación informática o artificio semejante, con ánimo de lucro y disposición patrimonial[28].

En esta línea, en el artículo 248.2 del CP, en su redacción originaria, y especialmente tras las reformas de la LO 15/2003 y de la LO 5/2010, se puede llegar a la conclusión de que

---

[26] Para más información sobre el *auction fraud*, entre otros, THE FBI FEDERAL BUERAU OF INVESTIGATION, "Online auction fraud – don't let it happen to you", en *Stories*, junio 2009, disponible en https://archives.fbi.gov/archives/news/stories/2009/june/auctionfraud_063009, consultado el 1 de diciembre de 2017.

[27] El concepto de estafa informática se reitera, entre otros en el ATS, Sala Segunda, nº 1012/2017, de 15 de junio de 2017 (JUR 2017\197875), Pte. Excmo. Sr. D. Andrés Palomo del Arco, donde se inadmitía el recurso de casación y confirmaba la sentencia condenatoria por un delito de estafa informática porque, según exponía en su Razonamiento Jurídico Único: "*la acusada realizó peticiones de recarga de móviles, sin que éstas fueran solicitadas por cliente alguno. Además, también declara probado cómo las eliminaba del listado de ventas para ocultarlas a la mercantil perjudicada*".

En el mismo sentido, entre otros, el FD 2º de la STS, Sala Segunda, nº 860/2008, de 17 de diciembre de 2008 (RJ 2009\131), Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre, donde se recordaba que "*El tipo penal del art. 248.2. "tiene la función de cubrir un ámbito al que no alcanzaba la definición de la estafa introducida en la reforma de 1983. La nueva figura tiene la finalidad de proteger el patrimonio contra acciones que no responden al esquema típico del art. 248.1 CP. pues no se dirigen contra un sujeto que pueda ser inducido a error. En efecto, los aparatos electrónicos no tienen errores como los exigidos por el tipo tradicional de la estafa, es decir, en el sentido de una representación falsa de la realidad. El aparato se comporta según el programa que lo gobierna y, en principio, "sin error*...."; castigando en el caso concreto a quien había realizado transferencias *online* sin autorización, accediendo al servicio mediante remisión a la entidad bancaria de un fax firmado por un administrador de la empresa defraudada autorizando una transferencia a favor de un tercero real y válida, pero enviando el fax primero a un número inexistente para que la operación quedase frustrada y, después, realizar la transferencia *online* a la propia cuenta de la acusada, aparentando ser la cuenta del tercero que debía ser el beneficiario, concluyendo que se trataba de un supuesto de *"artificio semejante a la manipulación informática" que consigue la transferencia inconsentida de fondos*".

[28] SUÁREZ-MIRA RODRÍGUEZ, C., JUDEL PRIETO, Á., y PIÑOL RODRÍGUEZ, J.R., "Las estafas", en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012, p. 226.

toda estafa informática es la transferencia de un activo patrimonial mediante la alteración o modificación de instrumentos informáticos[29].

3.2. Concepto de *phising*

Con las citadas premisas, de forma genérica se ha empleado el término *scam* como equivalente a estafa *online*, donde el delincuente explota la confianza de una persona para averiguar sus datos personales con el fin de lograr un beneficio patrimonial[30]. Y dentro de la generalidad de esos supuestos, imposibles de abarcar en este trabajo, se encuentra el más frecuente, denominado *phising*.

El término es un anglicismo que proviene de la palabra inglesa *fishing* (pescar), ya que en ambos casos se trata de lanzar un cebo y esperar que la víctima pique[31], y se define como "*el intento de obtener información confidencial (contraseñas y datos de tarjetas de crédito, por ejemplo) de manera fraudulenta, usurpando la personalidad de un interlocutor fiable en una comunicación electrónica*"[32], y que a su vez presenta numerosas variantes. Entre ellas, el *pharming*, consistente en la manipulación de direcciones DNS que utiliza el usuario para dirigirlos a una página distinta a la auténtica, pero con la misma apariencia, para conseguir datos confidenciales, todo ello modificando un pequeño archivo denominados *hosts*[33]; o el establecimiento de archivos espías (*spyware*) en el ordenador de la propia víctima para el envío de información a otro sistema informático.

La jurisprudencia ha venido refiriendo este delito a los comportamientos por los cuales a una persona le hacen disposiciones no consentidas contra su cuenta corriente y otra, denominada mula o mulero, participa como intermediario para transferir a los delincuentes el dinero, a sabiendas del fraude con el que está colaborando[34]. Se distinguen así dos fases: (i) una primera etapa de captación de información, que es la que da nombre al mismo; y (ii) la

---

29 En este sentido, BAJO FERNÁNDEZ, M., actualizado por GUÉREZ TRICARICO, P., "Estafa", en MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento Penal*, ed. Francis Lefebvre, Madrid, 2017, p. 1214.

30 Definición contenida en INTERPOL, "Social engineering fraud", en *INTERPOL Connecting Police for a safer world*, disponible en https://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud, consultado el 1 de diciembre de 2017.

31 Sobre esta materia, resulta destacable el trabajo de GAVRAILOVA, G., "¿Qué es el phising?", en *Mailjet by sinch*, 10 de diciembre de 2019, disponible en https://www.mailjet.com/es/blog/entregabilidad/que-es-phishing/#tipos , consultado el 18 de junio de 2022.

32 Concepto contenido en la Nota 2 de la Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones - Hacia una política general de lucha contra la ciberdelincuencia, COM (2007) 267, *cit*., nota 29.

33 Definición de FERNÁNDEZ TERUELO, J. G., *Derecho Penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, ed. Lex Nova, Valladolid, primera edición, 2011, p. 38.

34 Como indica MIRÓ LLINARES, el reclutamiento del mulero se suele hacer por medio de falsas ofertas de trabajo, consistentes en recibir un dinero, quedarse un porcentaje, y enviar el resto a un tercero, siendo denominados estos muleros como las otras víctimas del phising, dados que son los que se ven implicados en los procesos delictivos por este tipo de defraudaciones. MIRÓ LLINARES, F., "La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phising", *Revista Electrónica de Ciencia Penal y Criminología*, 15-12 (2013), Universidad de Granada, Granada, 2013, pp. 31 y 32.

segunda, de utilización ilícita de esos datos, disponiendo traspasos desde la cuenta del perjudicado[35].

Se trata de obtener dinero mediante el fraudulento acceso a las claves bancarias de confiados usuarios de Internet y, a partir de ahí, buscar una fórmula que permita colocar esos remanentes dinerarios en un país seguro, a nombre de personas de difícil identificación por los agentes de policía del Estado en cuyo territorio se efectúa el acceso inconsentido a las cuentas de la víctima y las transferencias a terceros países[36].

Por tanto, el *phising* se configura como una modalidad de estafa informática, que sería el género, admitiendo diferentes mecánicas, dirigidas a obtener datos de cuentas bancarias para acceder a estas y disponer de sus fondos, mediante transferencias o entregas en efectivo. Así, señala VELASCO NÚÑEZ el supuesto en que el sujeto envía correos electrónicos desde una dirección incierta, con suplantación, haciéndose pasar por entidad bancaria, reclamando los datos de acceso a cuentas bancarias de forma engañosa a sus titulares, indicando que los necesitan para actualizarlos, para finalmente acceder con esa información y transferir o sacar y disponer del dinero que tienen los sujetos estafados[37].

4. EL TRATAMIENTO DE ESTOS DELITOS EN EL ORDENAMIENTO PENAL ESPAÑOL

4.1. La situación antes del año 1995

Antes de su tipificación por primera vez en el Código Penal de 1995, los comportamientos que aquí se tratan no tenían una consecuencia penal concreta, no siendo posible reconducirlos al tradicional delito de estafa. Así, el Tribunal Supremo ya se había referido en su Sentencia de 19 de abril de 1991 (RJ 1991\2813) a la imposibilidad de calificar estas conductas como delito de estafa, por cuanto "*a las máquinas no se las puede engañar, a los ordenadores tampoco, por lo que los casos en los que el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se produce ni el engaño ni el error necesarios para el delito de estafa. Sin engaño, elemento cardinal de la estafa, no puede entenderse producida ésta*".

En ese caso juzgado, el obstáculo se encontraba en que, al no ser posible la aplicación del tipo de estafa, puesto que se trataba de una alteración contable realizada utilizando un ordenador por el apoderado de un Banco, que se apropiaba de los fondos, sí que se podía calificar como apropiación indebida por la condición de responsable jurídico de los fondos. Sin embargo, como indica QUINTERO OLIVARES, si no concurría esa condición de apoderado tampoco era posible la citada calificación jurídica sin forzar la legalidad, razón por la cual era

[35] Entre otras, SAP de Valencia, Sección 5ª, nº 491/2016, de 5 de septiembre (JUR\2018\61725), Pte. Ilma. Sra. Dª Beatriz Goded Herrero, con cita de otras.

[36] STS, Sección 1ª, nº 834/2012, de 25 de octubre (RJ 2013\1442), Pte. Excmo. Sr. Manuel Marchena Gómez.

[37] VELASCO NÚÑEZ, E., "Tipos delictivos", en VELASCO NÚÑEZ, E., y SANCHIS CRESPO, C., *Delincuencia informática*, ed. Tirant lo blanch, Valencia 2019, p. 31.

necesaria una tipificación expresa de las estafas informáticas[38].

4.2. La versión inicial del Código Penal de 1995

Con los citados antecedentes, el legislador de 1995 opta por innovar en la regulación de la figura de la estafa, incluyendo el criterio que se venía defendiendo en la dogmática alemana, es decir, que, puesto que las máquinas no podían ser engañadas, debían ampliarse expresamente esos tipos de defraudaciones para dar cobertura a las acciones sobre programas informáticos vinculados a las transferencias patrimoniales[39].

En concreto, en el texto original del actual Código Penal se decide mantener en el primer apartado del artículo 248 que "*Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno*", de forma similar al anterior artículo 528 del texto derogado[40]. Pero además, como novedad, en el segundo párrafo se amplía el concepto para incluir que "*También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero*".

Por tanto, desde el punto de vista legislativo se daba respuesta al problema del enriquecimiento no autorizado por el perjudicado y provocado por el uso de las nuevas tecnologías, y las estafas informáticas se incluyen por primera vez en el Código Penal español.

4.3. La reforma de 2003

La regulación de la materia que nos ocupa fue ampliada de nuevo en el año 2003. Así, la LO 15/2003, extendía el delito de estafa con un apartado tercero, en el que se ordenaba que "*La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo*".

Dicho en otras palabras, se equipara al fabricante, introductor, poseedor o facilitador de software destinado de forma específica a la comisión de estafas, con la estafa misma.

De esta forma, como indica VELASCO NÚÑEZ, el legislador altera lo que son inicialmente meros actos exteriores de preparación de la ejecución, que incluso podrían dar lugar a formas imperfectas de ejecución, y pena con la ejecución consumada del delito. Esto supone que la posesión de los programas específicos sin alternativa legal equivale a la

[38] QUINTERO OLIVARES (Dir.) y VVAA, *Comentarios a la parte especial del Derecho penal*, ed. Aranzadi, Navarra, 2016, p. 652.

[39] PASTOR MUÑOZ, N., *La determinación del engaño típico en el delito de estafa*, ed. Marcial Pons, Madrid, 2004, p. 50 y ss.

[40] Así, según el texto del artículo 528 del Código Penal de 1973, tras la reforma de la Ley Orgánica 8/1983, de 25 de junio, de Reforma Urgente y Parcial del Código Penal, "*Cometen estafas los que con ánimo de lucro utilizan engaño bastante para producir error en otro, induciéndole a realizar un acto de disposición en perjuicio de sí mismo o de tercero*".

consumación ante la imposibilidad de otro uso. Si bien para este autor esta es la única forma de castigar a los sujetos que crean, poseen o facilitan ese material fundamental para que exista la infracción, y que no pueden ser sorprendidos de otra forma en el procedimiento estratégico del delito, por cuanto normalmente lo facilitan por Internet[41].

En cualquier caso, esta postura legislativa puede entenderse como un adelantamiento de las barreras de protección, técnica que permite la tutela de los intereses individuales que pueden verse amenazados por las nuevas formas de criminalidad y las nuevas tecnologías[42]. Por ejemplo, en el caso de que ese programa de ordenador fabricado, introducido, poseído o facilitado permitiese acceder al sistema informático ajeno para permitir la transferencia patrimonial, también se vería comprometida la seguridad del dispositivo en el que se produce la entrada o incluso la intimidad de su titular[43].

4.4. La reforma de 2010

A pesar de la introducción de las estafas informáticas en el texto de 1995 y de su ampliación en el año 2003, finalmente en fecha 23 de junio de 2010 se publicaba la Ley Orgánica 5/2010, de 22 de junio, que modificaba el Código Penal afectando a las estafas informáticas.

Aunque la reforma iba dirigida, según el apartado XV de su Preámbulo, a "*incorporar la cada vez más extendida modalidad consistente en defraudar utilizando las tarjetas ajenas o los datos obrantes en ellas, realizando con ello operaciones de cualquier clase en perjuicio de su titular o de un tercero*", "*entre las estafas descritas en el artículo 248 del Código Penal, cuyo catálogo en su momento ya se había acrecentado con los fraudes informáticos*", también supuso la reestructuración del precepto, para mantener intacto el primer párrafo, pero incorporar en su apartado 2 los tres supuestos equiparados a la estafa: "*a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero*".

Esta última modalidad zanja el debate sobre la posible calificación de estas acciones como robo con fuerza en las cosas por uso de llaves falsas, y supone la incorporación de estafas por Internet utilizando tarjetas de crédito, débito, cheques de viaje o datos legítimos que consten en ellos sin consentimiento de su titular. Es decir, robo de datos para su uso en el ciberespacio, que no deben confundirse con la falsificación de tarjetas del artículo 399 bis CP, por cuanto estas falsedades implican construcción física sobre soporte real para uso no virtual, mientras que la tipificación del uso de los datos reales en Internet forma parte de

41 VELASCO NÚÑEZ, E., "Tipos delictivos" ... , *cit*., nota 37, p. 29.

42 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal*, *parte general*, ed. Tirant Lo Blanch, Valencia, 2016, p. 255.

43 ALMENAR PINEDA, F., *El delito de hacking* ... , *cit*., nota 15, p. 139.

nuevos supuestos de estafa informática[44].

Así pues, siguiendo a MENÉNDEZ MATO y GAYO SANTA CECILIA, cualquier sujeto con conocimientos informáticos puede en la actualidad, prácticamente desde cualquier lugar, realizar modificaciones que le supongan un beneficio económico no autorizado en perjuicio de tercero, simplemente necesitando de un terminal y un instrumento de transmisión de datos. De ahí que la actual regulación incluya los fraudes o estafas informáticas, castigando tanto las estafas a través de manipulaciones informáticas como la fabricación de programas para estos fines[45].

Por tanto, tras la citada modificación, el legislador ha optado por ampliar las defraudaciones tecnológicas, pero mantiene la cobertura inicial del *phising*, que se encuentra tipificado en el citado artículo 248.2.a del CP.

5. EL BIEN JURÍDICO PROTEGIDO Y EL OBJETO MATERIAL

5.1. Introducción

Las estafas informáticas se caracterizan por la existencia de alguna manipulación de los sistemas de información, es decir, acceso, modificación o eliminación no autorizada de datos, o intromisión indebida en sistema informático, pudiendo afectar a la confidencialidad, a la integridad o a su disponibilidad, o artificio semejante, y que suponen como resultado la transferencia de fondos en perjuicio de tercero, atentando contra el patrimonio en cualquier caso.

Cuando se plantea el bien jurídico afectado por estas acciones, la primera cuestión es determinar si la aparición de los sistemas informáticos supone una nueva herramienta de alcance global que implica el nacimiento de nuevos bienes jurídicos que sean merecedores de protección penal o no.

Por lo general, podemos distinguir dos grupos de delitos relativos a las nuevas tecnologías: el primero viene referido a aquellos cuya finalidad es la protección de esas herramientas, consideradas como objeto material; y la segunda categoría la constituirían aquellos delitos relacionados con la utilización de esas tecnologías con fines delictivos. En el caso de *phising*, estafa informática más frecuente, entiendo que no podemos quedarnos sólo con una de esas categorías, puesto que en ocasiones afecta al sistema de información mediante el acceso ilícito, su borrado, alteración, bloqueo integral o parcial y, además, se utiliza el sistema informático con una finalidad criminal, como es la obtención de un lucro propio o ajeno.

5.2. *Phising* como delito contra el patrimonio

Desde un primer momento, el *phising* se caracteriza por el intento de obtener la información confidencial de un tercero mediante la usurpación de la personalidad de otro

[44] En este sentido, VELASCO NÚÑEZ, E., "Tipos delictivos" ... , *cit*., nota 37, p. 30.
[45] MENÉNDEZ MATO, J. C. y GAYO SANTA CECILIA, M. E., *Derecho e informática..., cit.*, nota 14, p. 327.

sujeto confiable, y el delito de estafa informática se regula por primera vez en el Código Penal de 1995.

Por tanto, con estas nuevas defraudaciones surge la cuestión de si el legislador estaba protegiendo un nuevo bien jurídico o más bien, al ubicar el precepto entre los delitos contra el patrimonio, era este el bien jurídico tutelado.

Se trata de dilucidar si el patrimonio, entendido en el contexto actual de las nuevas tecnologías y las relaciones de las personas con los sistemas informáticos, constituye el bien jurídico protegido con el delito de *phising*, defraudación informática más habitual, y, más concretamente, si supone un ataque contra los bienes o derechos de contenido económico del titular del sistema informático.

Ese es el bien tutelado si atendemos al criterio sistemático y la expresa referencia del tipo a ese interés que se ve perjudicado con la comisión del delito, con la introducción de las estafas informáticas en el artículo 248.2 CP. No obstante, el artículo 3 de la Decisión Marco del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo (2001/413/JAI), se refiere a los delitos informáticos y a la obligación de que "*Cada Estado miembro adoptará las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada: realización o provocación de una transferencia de dinero o de valor monetario que cause una pérdida no autorizada de propiedad a otra persona, con el ánimo de procurar un beneficio económico no autorizado a la persona que comete el delito o a terceros, mediante:*

- la introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, o

- la interferencia indebida en el funcionamiento de un programa o sistema informáticos".

Mientras que el Preámbulo de la LO 1/2015, de 30 de marzo, por la que se modifica el Código Penal (en adelante, "LO 1/2015"), establece que: "*no es lo mismo el acceso al listado personal de contactos, que recabar datos relativos a la versión de software empleado o a la situación de los puertos de entrada a un sistema. Por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos*".

De esta forma, también se está protegiendo la integridad de los sistemas informáticos, que puede verse comprometida en determinados supuestos de *phising*, en los que, como se ha expuesto, el *modus operandi* puede consistir en la alteración o borrado de datos, o en el mero acceso ilícito, intrusismo informático o violación de la esfera de exclusividad del titular del sistema para la obtención de esa información.

Así pues, aunque en cualquier caso, los delitos que nos ocupan son un ataque contra el patrimonio ajeno, entendido como bien jurídico tradicionalmente protegido en los códigos españoles, pero no podemos omitir las normas comunitarias que también se han referido desde el Preámbulo del Convenio Europeo sobre Cibercriminalidad[46] a la tutela de la

[46] En su Preámbulo se dice: "*el presente Convenio es necesario para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así*

confidencialidad, integridad y disponibilidad de los sistemas informáticos, que integran la seguridad de ese sistema. Esos nuevos intereses considerados dignos de amparo y vinculados a las nuevas tecnologías[47], también se han reiterado en el Informe de la Comisión de estudios e informes del CGPJ emitido en fecha 18 de febrero de 2009, al Anteproyecto de LO por la que se modifica el CP y la DM 2005/222/JAI, Considerando 2, Considerando 3 y Considerando 14.

Por tanto, el tratamiento del delito de *phising* entre las estafas informáticas o defraudaciones, no excluye la protección de otros bienes jurídicos. De hecho, con la introducción del *hacking* en el Código Penal por la LO 5/2010[48], la protección de la seguridad de los sistemas informáticos implica el adelantamiento de las barreras de tutela que supone la tipificación del mero acceso al sistema informático, protegiendo directamente tanto la confidencialidad, integridad y disponibilidad del sistema como, indirectamente, cualquier otro bien jurídico que con el acceso y la puesta en peligro de la seguridad del sistema pudiera verse afectado, tanto el patrimonio, como la intimidad, la propiedad, el secreto de empresa u otro bien jurídico protegido, cuya efectiva lesión o puesta en peligro dará lugar al correspondiente concurso.

Por ello, aunque el *phising* se integra en la figura del delito de estafa, en la medida que supone la transferencia no consentida del activo patrimonial en perjuicio de tercero, la conducta va más allá, por cuanto existe una manipulación informática, que puede afectar a la seguridad del sistema informático ajeno o incluso causar un daño sobre el mismo, con el fin de "pescar" los datos ajenos, concurriendo en esos supuestos con el citado delito de *hacking* o con un delito de daños. Podemos hablar por ello en estos casos de una estafa informática más sofisticada o compleja.

No obstante, en estos casos, siguiendo a RODRÍGUEZ RÁMOS[49], podemos concluir que la especificidad de la conducta que nos ocupa resultará de preferente aplicación cuando concurra con estos otros tipos penales, con mayor motivo si son de penalidad inferior.

5.3. El objeto material afectado por *phising*

Como sucede en la estafa tradicional, el objeto material del delito de *phising* es el activo patrimonial.

Sin embargo, según se expondrá en el apartado 7, dedicado al análisis del artículo 248.2.a del CP, en la modalidad ejecutada a través de las nuevas tecnologías debe existir la

---

como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, como los descritos en el presente Convenio".

47 En este sentido, entre otros, HURTADO ADRIÁN, A., "Accesos informáticos ilícitos", en JUANES PECES, A. (Dir.) y VVAA, *Reforma del Código penal. Perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio. Situación jurídico-penal del empresario*, ed. El Derecho, Madrid, 2010, p. 127.

48 El *hacking* puede entenderse como el equivalente al intrusismo informático o violación de una esfera de exclusividad del titular del sistema, siendo intrascendente el contenido del sistema, y bastando el mero acceso no autorizado al sistema de información o parte del mismo vulnerando las medidas de seguridad establecidas para impedirlo, con independencia de que se acceda o no a los datos. En este sentido, ALMENAR PINEDA, F., *El delito de hacking ... , cit*., nota 15, p. 203.

49 Así, entre otros, RODRÍGUEZ RAMOS, L. (Dir.) y VVAA, *Código Penal. Concordado y comentado con jurisprudencia y leyes penales especiales y complementarias*, ed. La Ley, quinta edición, Madrid, 2015, p. 1291.

manipulación informática o artificio semejante, que es la forma comisiva mediante la que torticeramente se hace que la máquina actúe; y también tiene que concurrir un acto de disposición económica en perjuicio de tercero que se concreta en una transferencia no consentida[50].

El término "activo patrimonial" se identifica mayoritariamente[51] con el objeto con valor económico en sentido amplio, incluyendo desde un apunte contable, datos o valores patrimoniales hasta una cosa física con valor económico; mientras que la manipulación puede definirse como alteración o manipulación tanto de programas como de datos informáticos o el propio sistema, al no quedar excluido. Por último, artificio semejante implica operaciones similares a la manipulación informática, por su interpretación sistemática.

Por último, desde el año 2003, en el artículo 248 del CP se amplía el delito de *phising* también para el fabricante, introductor, poseedor o facilitador del software destinado de forma específica a la obtención del citado activo patrimonial.

6. NATURALEZA JURÍDICA DEL *PHISING.*

En el delito de *phising*, el engaño propio de la estafa tradicional, que implica relación personal, es sustituido como medio comisivo defraudatorio por la manipulación informática o artificio semejante, según se ha expuesto en el apartado anterior.

Por tanto, a diferencia de la modalidad genérica, al no precisar aquel delito del engaño personal, no se trata de un delito de encuentro, es decir, en esta modalidad de estafa informática no necesariamente debe concurrir la colaboración viciada de la víctima[52].

Por otra parte, constituye un delito de medios indeterminados ("*valiéndose de alguna manipulación informática o artificio semejante*") y, siguiendo la distinción que en esta categoría realiza LAURENZO COPELLO, entre delito de resultado y de lesión o un delito de resultado y de peligro[53], el *phising* se configura como un delito de resultado y de lesión, por cuanto es preciso conseguir una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro para la consumación.

Lo expuesto se entiende sin tomar en consideración los supuestos de facilitar o poseer programas informáticos específicos para cometer estos delitos, del citado artículo 248, el apartado 2.b CP, por cuanto se da la circunstancia de que, en estos casos, se castiga la acción porque es posible que con esa conducta se lesione el patrimonio ajeno. Empleando los términos de ORTS BERENGUER y GONZÁLEZ CUSSAC, parece que el legislador ha optado por adelantar la línea de protección con este tipo, aumentado con esta técnica la tutela de los

[50] En este sentido, STS 2175/2001, de 20 de noviembre (RJ 2002\805), Pte. Excmo. Sr. Andrés Martínez Arrieta.

[51] Por todos, BAJO FERNÁNDEZ, M., actualizado por GUÉREZ TRICARICO, P., "Estafa" ...., *cit*., nota 29, p. 1214.

[52] QUERALT JIMÉNEZ, J. J., *Derecho penal español. Parte especial*, ed. Tirant lo Blanch, primera edición, Valencia, 2015, p. 498.

[53] LAURENZO COPELLO, P., *El resultado en Derecho Penal*, ed. Tirant Lo Blanch Alternativa, Valencia, 1992, p. 117.

intereses individuales amenazados por nuevas formas de criminalidad y las nuevas tecnologías[54]. Así, como dice QUINTERO OLIVARES, los delitos de peligro son de importancia creciente político-criminalmente, acudiendo el legislador cada vez más a ellos como consecuencia de los avances de la técnica, con los consiguientes riesgos, y la necesidad de proteger bienes jurídicos de especial importancia que requieren una protección anticipada castigando conductas peligrosas para ellos, sin que esto signifique que el intérprete deba despreciar el cumplimiento de los principios esenciales del Derecho penal[55]. En el mismo sentido MÉNDEZ RODRÍGUEZ destaca el adelantamiento de las barreras de protección penal como una de las características de los delitos de peligro[56]. Y, en palabras de MUÑOZ CONDE y GARCÍA ARÁN, el delito de peligro es el que no exige para su consumación la lesión del bien jurídico sino sólo la amenaza para este, siendo de peligro concreto cuando el resultado típico consiste en la puesta en peligro del bien jurídico y peligro abstracto cuando se describe una conducta que según la experiencia suele ser peligrosa para un bien jurídico aunque en el caso concreto no lo sea[57].

Por tanto, con estos presupuestos, en el caso de las conductas del artículo 248.2.b del CP nos encontraríamos ante un delito de peligro abstracto, al no exigir el efectivo menoscabo de un patrimonio ajeno determinado.

7. LA REGULACIÓN DEL ARTÍCULO 248.2.A CP

El tipo del artículo 248.2.a del CP incluye elementos que se caracterizan por su vaguedad, a diferencia de otros Códigos penales de nuestro entorno, como el alemán, donde se tipifica la estafa informática de forma descriptiva para castigar a cualquier persona que, con la intención de obtener una ventaja financiera ilícita para sí o para un tercero, dañe los bienes de otra persona al dañar el resultado de una operación de procesamiento de datos al diseñar incorrectamente el programa, al usar datos incorrectos o incompletos, mediante el uso no autorizado de datos o de otra manera influenciado por la influencia no autorizada en el proceso [58].

---

54 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal...*, *cit*., nota 42, p. 255.

55 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general del Derecho penal,* ed. Aranzadi, Navarra, 5ª edición, 2015, p. 349.

56 MÉNDEZ RODRÍGUEZ, C., "Delitos de peligro y bienes jurídicos colectivos", en *Nuevo Foro Penal*, nº 44, junio, 1989, pp. 167, 169, 171.

57 MUÑOZ CONDE, F. y GARCÍA ARÁN, M., *Derecho Penal. Parte General*, ed. Tirant lo Blanch, 9ª edición, Valencia, 2015, p. 325.

58 § 263a: "*Computerbetrug. (1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. (2) § 263 Abs. 2 bis 6 gilt entsprechend. (3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er 1. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt oder 2. Passwörter oder sonstige Sicherungscodes, die zur Begehung einer solchen Tat geeignet sind, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.*

En concreto, en el Código Penal español, el medio es la manipulación informática o artificio semejante, entendidos como instrumentos informáticos, recayendo la acción sobre la transferencia de un activo patrimonial.

No obstante, la amplitud de los conceptos, un sector doctrinal ha defendido que el continuo cambio de las nuevas tecnologías exige no reducir las acciones posibles a un listado que pudiera ser adecuado en un determinado momento pero atrasado al poco tiempo, resultando peligroso para la eficacia de las normas[59].

En la modalidad de *phising*, mediante manipulación informática o artificio semejante se trata de obtener información confidencial mediante comunicación electrónica para realizar una transferencia no autorizada de un activo patrimonial en perjuicio de su titular.

7.1. Sujeto activo y pasivo

El ilícito que nos ocupa, previsto en el artículo 248.2.a del CP se caracteriza por ser un delito común. Sin embargo, como señala MIRÓ LLINARES, lo más usual es que quien realice la manipulación informática sea una persona con conocimientos técnicos necesarios para llevar a cabo una conducta que en principio se presenta como tecnológicamente compleja[60]. Pues bien, es evidente que el sujeto activo en estos casos tan sofisticados como *phising* necesita unos conocimientos informáticos avanzados.

Aquí resulta indiferente que el sujeto que consiga los datos personales sea el mismo que la persona que realiza desde su cuenta bancaria la transmisión de los activos obtenidos ilícitamente. De hecho, habitualmente serán dos personas distintas: (i) quien consigue la información; y (ii) el sujeto que transfiere a otra cuenta el dinero que ha recibido ilícitamente.

La concurrencia de la pluralidad de sujetos viene motivada por la estrategia de no levantar sospechas en las mercantiles encargadas de la custodia de los activos patrimoniales.

Por tanto, en la mayoría de los casos se produce una intervención plural de sujetos activos para facilitar la comisión del delito, evitar su descubrimiento y, especialmente, impedir su bloqueo. De nada sirve obtener las claves de los usuarios de banca electrónica sin que alguien se preste en España a ofrecer su cuenta para sacar el dinero del país, por lo que es lógico que los primeros en lugar de utilizar una cuenta que serviría para identificarles lo hagan a través de la intermediación de una persona, que también será sujeto activo del delito[61].

El titular de la información confidencial obtenida mediante la manipulación informática o artificio semejante, y en perjuicio del cual se realizará la transferencia no autorizada del activo patrimonial, será el sujeto pasivo del delito de *phising*.

(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend".

59 QUINTERO OLIVARES, G., *Comentarios a la parte especial ... , cit*., nota 38, p. 653.

60 MIRÓ LLINARES, F., "Los Delitos Informáticos", en ORTIZ DE URBINA GIMENO, Í. (Coord.) y VVAA, *Memento experto. Reforma penal 2010. Ley Orgánica 5/2010*, ed. Francis Lefebvre, Madrid, 2010, p. 147.

61 En este sentido, SAP de Madrid, Sección 30ª, nº 669/2013, de 19 de diciembre (ARP\2014\161), Pte. Ilma. Sra. Dª María Inmaculada Iglesias Sánchez.

7.2. La conducta típica

El ciberataque del *phising* presenta numerosas variantes: desde el engaño al titular del sistema simulando una página web confiable, para que introduzca sus datos y así posteriormente acceder el sujeto activo a la página real, introduciendo esa información con la finalidad de autorizar una transferencia de activos no consentida por su titular; hasta el empleo de programas específicos que permiten acceder a sistemas informáticos ajenos para robar esas claves o contraseñas y, con ellas, realizar las operaciones en perjuicio del sujeto pasivo.

Precisamente la estafa informática admite múltiples modalidades, siempre que se refieran a la manipulación informática o artificio semejante y a la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro, elementos que concurren en el *phising*:

i. En cuanto a la transmisión no autorizada de cualquier activo patrimonial mediante manipulación informática o medio semejante, las conductas que nos ocupan se caracterizan por la pesca de datos personales a través de las nuevas tecnologías, para posteriormente ser utilizados en la transferencia no autorizada y en perjuicio del titular de esa información.

Así, aunque en la estafa informática subsiste la defraudación, el engaño, que implica relación personal, es sustituido como medio comisivo defraudatorio por la manipulación informática o artificio semejante en el que lo relevante es que la máquina, informática o mecánica, actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquellos que permite su programación, o por la introducción de datos falsos[62].

Cuando la conducta que desapodera a otro de forma no consentida de su patrimonio se realiza mediante manipulaciones del sistema informático, bien del equipo, bien del programa, se incurre en la tipicidad del citado artículo 248.2 del Código penal. También cuando se emplea un artificio semejante.

Este último término es el que puede plantear mayores problemas en la práctica. Para la jurisprudencia, una de las acepciones del término artificio hace que este signifique artimaña, doblez, enredo o truco. Y debe ser idóneo para producir el daño patrimonial, siendo equivalente que se modifique el programa informático indebidamente o que se utilice sin la debida autorización[63].

En el caso del *phising*, la transferencia de activos patrimoniales, no consentida por el perjudicado, se realiza mediante manipulación informática[64], como una modalidad de estafa informática, que sería el género, admitiendo diferentes mecánicas, pero todas ellas dirigidas a obtener códigos de acceso, claves o contraseñas[65] de cuentas bancarias para acceder a estas

---

62 STS nº 860/2008, de 17 de diciembre (RJ 2009\131), Pte. Excmo. Sr. Juan Ramón Berdugo y Gómez de la Torre.

63 STS nº 1476/2004, de 21 de diciembre (RJ 2004\8252), Pte. Excmo. Sr. Enrique Bacigalupo Zapater.

64 STS nº 533/2007, de 12 de junio (RJ\2007\3537), Pte. Excmo. Sr. Joaquín Giménez García.

65 La diferencia entre contraseña, es decir, "*información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso*", según la RAE; y el código de acceso o "*cifra para formular y comprender mensajes secretos*" (artículo 5.2.c del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica

y disponer de sus fondos, mediante transferencias o entregas en efectivo.

ii. La falta de autorización prevista desde el primer momento en el Código Penal de 1995 y mantenida en la redacción actual de su artículo 248.2.a, carece de definición en su texto, pero resulta válido el concepto del artículo 1.d) de la DM 2005/222/JAI, donde se declara: "*A los efectos de la presente Decisión marco se entenderá por: (…) d) «sin autorización», el acceso o la intromisión no autorizados por el propietario o titular de otro tipo de derecho sobre el sistema o parte del mismo o no permitidos por la legislación nacional*".

Por tanto, el consentimiento deberá proceder del propietario o titular del sistema donde se consiguen sus datos personales, o bien, si es distinto el titular del sistema y el del activo patrimonial, la autorización de este último[66]. Y, todo ello, sin perjuicio de los casos en que se pueda acceder a un sistema por autorización judicial[67].

En el caso del *phising* el consentimiento directamente no existe. La obtención de la información se produce aprovechando un fallo en la seguridad del sistema, suplantando páginas web o por cualquier otro artificio semejante que implique el uso de un dispositivo informático.

iii. Además, tras la reforma del Código Penal en el año 2003, se castiga igualmente fabricar, introducir, poseer o facilitar programas informáticos específicamente destinados a la comisión de esas estafas. Por lo que se puede producir la situación de que un sujeto sea sorprendido con un programa informático específicamente destinado a cometer el delito de *phising* sin haber llegado a realizar la captación de información ni la transferencia de activos, siendo igualmente castigado con la misma pena que en el primer supuesto.

7.3. La relevancia penal de las conductas de facilitar el *phising* mediante programas específicos

Tras la LO 15/2003, también será posible castigar al que facilite la conducta de *phising* con las mismas penas previstas para el autor del delito de estafa informática. Así, el tipo del artículo 248.2.a del CP contempla al que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro, y con la citada reforma se ha introducido, en el mismo artículo 248, apartado 2.b, que también son reos de estafa "*Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo*".

15/1999, de 13 de diciembre, de protección de datos de carácter personal), se suele establecer comúnmente en que la contraseña se asocia a códigos alfanuméricos (o PIT - Personal Identification Text), mientras que el código de acceso se suele vincular a la utilización de algún código numérico (llamado PIN - Personal Identification Number), mientras que el término clave se entiende como "*Código de signos convenidos para la transmisión de mensajes secretos o privados*" en la definición de la RAE.

66 Por ejemplo, caso de que se obtengan los datos del sistema informático de un Banco en perjuicio de sus clientes. En estos supuestos, conviene recordar la posible responsabilidad civil subsidiaria de la entidad bancaria. Así, entre otras, STS, Sección 1ª, nº 743/2015, de 20 de noviembre (RJ\2015\5317), Pte. Excmo. Sr. D. Juan Saavedra Ruiz.

67 Así, los supuestos de los artículos 588 *bis* y siguientes de la LECrim, introducidos por la LO 13/2015.

Por tanto, se puede producir la situación de que un sujeto sea sorprendido con un programa informático específicamente destinado a cometer el delito de *phising* sin haber llegado a realizar la captación de información ni la transferencia de activos, o que facilite ese software a terceros para que sean ellos quienes obtengan la información personal y realicen la transmisión ilícita, siendo igualmente castigado con la misma pena que estos últimos.

En consecuencia, la inclusión de estas acciones relativas a facilitar el *phising* supone una criticable tipificación expresa de actos de cooperación elevados a categoría de autoría, y en la práctica va a suponer la equiparación entre autoría y participación en supuestos que, en principio, deberían encuadrarse en este último grupo, dentro de los delitos de estafa informática en general y del *phising* en particular.

7.4. La conducta de facilitar una cuenta bancaria para el *phising*

La puesta a disposición de una cuenta bancaria para recibir dinero y enviarlo a un tercero, sin consentimiento del titular de esas cantidades, constituye el supuesto más común de *phising* cuando en su comisión interviene más de un sujeto[68], por cuanto en la mayoría de los casos, al autor principal no le será suficiente con disponer de la información precisa sobre las claves personales para ejecutar el acto de desapoderamiento. Necesitará una cuenta corriente que no levante sospechas y que, mediante la extracción de las cantidades transferidas pueda llegar a obtener el beneficio económico perseguido. Precisamente por ello, la contribución de quien se presta interesadamente a convertirse en depositario momentáneo de los fondos sustraídos, también integra este delito[69].

El problema que concurre en esas situaciones es la pretendida inocencia angelical del facilitador de la cuenta bancaria, respecto de quien es difícil probar que haya realizado una manipulación informática o artificio semejante para captar los datos personales del sujeto pasivo, por cuanto su conducta consiste en recibir cantidades en su cuenta para transferirlas a otra. En principio, se trataría de una operación legal.

Esta acción obliga a interpretar los matices que concurren en esa transmisión aparentemente lícita para definirla como maquinación fraudulenta o, al menos, artificio semejante.

En esta línea, la jurisprudencia viene reiterando los indicios de criminalidad de ese tipo

---

[68] Entre otras, STS, Sección 1ª, nº 743/2015, de 20 de noviembre (RJ\2015\5317), Pte. Excmo. Sr. D. Juan Saavedra Ruiz, donde se expone el caso de *phising* donde "*el recurrente contactó con personas desconocidas por internet y, a través de su correo electrónico, le ofrecieron trabajar para una empresa ficticia como "agente bancario" para ganar un 8% o un 10% del valor de las transferencias de dinero que recibiera en su cuenta corriente, para luego depositarlas en otro lugar. El acusado aceptó colaborar en estas operaciones, con conocimiento de la ilícita procedencia del dinero que debía sacar de su cuenta y enviar a través de empresas de transporte de dinero a otra persona con residencia en Kiev. Tal es así que el día 19-9- 2012 recibió en su cuenta corriente la cantidad de 2.167,29 euros procedente de otra cuenta de Ávila, cuyo titular es Joaquín , que no consintió la transferencia, que se llevó a cabo por personas desconocidas por internet, a través del procedimiento denominado "phishing", obteniendo las claves de seguridad del Sr. Joaquín . Una vez recibida dicha transferencia, el acusado la sacó de su cuenta dejando el saldo a cero*".

[69] En este sentido, con cita de numerosa jurisprudencia, la SAP de Madrid, Sección 23ª, nº 92/108, de 24 de enero (ARP\2018\278), Pte. Ilma. Sra. Dª María de lo s Ángeles Montalvá Sempere.

de operaciones, refiriéndose[70]:

(i) a la prestación de una colaboración eficiente y relevante, cobrando por ello;

(ii) al hecho de abrir una cuenta corriente concreta para recibir un importe e inmediatamente transmitirlo a otro destino, que indica que el acusado conocía el origen ilícito del dinero, ya que es una operación inusual en el tráfico mercantil, recibir en una cuenta una suma de dinero importante sin conocer su procedencia;

(iii) por qué se realiza esa prestación onerosa por parte del facilitador de la cuenta, es decir, jurídicamente se trataría de una relación laboral, pero la relación laboral es totalmente ilógica. Si se atiende al contrato de trabajo, no consta la identidad del empleador, ni la sede laboral, ni medios técnicos sobre ella y sobre todo hay una indefinición total de la función laboral;

(iv) que no se cuestionen las transacciones por el sujeto que las realiza;

(v) a que no es preciso el engaño personal, por cuanto estamos ante una estafa informática, actuando con automatismo en perjuicio de tercero[71].

Por tanto, con la concurrencia de los citados indicios en la facilitación de una cuenta bancaria, incluso aun prescindiendo de una intervención calificable de coautoría, porque se entendiera que el sujeto intermediario no tenía el dominio del plan total[72], constaría una participación que habría de ser comprendida en el artículo 28 b) del CP, al tratarse de una cooperación necesaria. La recepción del dinero procedente de una cuenta extraña y su transmisión a otra persona, también extraña, implica una colaboración que cuanto menos es necesaria, por tratarse de un bien de escasa obtenibilidad y determinante del que la operación fructifique[73].

---

[70] Entre otras, la STS, Sección 1ª, nº 533/2007, de 12 de junio (RJ\2007\3537), Pte. Excmo. Sr. Joaquín Giménez García; o la citada STS, Sección 1ª, nº 743/2015, de 20 de noviembre (RJ\2015\5317), Pte. Excmo. Sr. D. Juan Saavedra Ruiz.

[71] En este sentido, STS nº 2175/2001, de 20 de noviembre (RJ 2002\805), Pte. Excmo. Sr. Andrés Martínez Arrieta.

[72] Así, desde el punto de vista de la teoría del dominio del hecho, WELZEL explicaba que el autor final es señor y dueño de su decisión y su ejecución, y con esto, dueño y señor de "su"hecho, al cual le da forma conscientemente en su existencia y forma. Instigador y cooperador tienen también un cierto dominjio sobre el "hecho", pero solo sobre su contribución. El hecho en sí está solo bajo el dominio final del autor. El instigador incita al hecho ajeno y el cooperador lo apoya, pero el dominio final sobre la decisión y su ejecución real lo tiene solo el autor. WELZEL, H., *Estudios de Derecho penal*, ed. B de F, reimpresión, traducido por EDUARDO ABOSO, G., y LOW, T., Buenos Aires, 2007, p. 83.

Desde la misma perspectiva, ROXIN defendía que hay dominio del hecho y, por tanto, el sujeto es autor: (i) si realiza la acción típica personalmente (dominio de la acción); (ii) si hace ejecutar el hecho mediante otro cuya voluntad, según parámetros jurídicos, no es libre, o no conoce el sentido objetivo de la acción de su comportamiento o lo abarca en menor medida que el sujeto de detrás o que es sustituible a voluntad en el marco de una maquinaria de poder organizada (dominio de la voluntad); y (iii) si presta en la fase ejecutiva una aportación al hecho funcionalmente significativa (dominio del hecho funcional). En ROXIN, C., *Autoría y dominio del hecho en Derecho penal*, ed. Marcial Pons, Barcelona, traducido por CUELLO CONTRERAS, J., y SERRANO GONZÁLEZ DE MURILLO, J.L., 2000, p. 337.

[73] STS, Sección 1ª, nº 556/2009, de 16 de marzo (RJ 2009\4823), Pte. Excmo. Sr. D. Siro Francisco García Pérez.

Según la teoría de los bienes escasos, expuesta en esa Sentencia y defendida por GIMBERNAT, toda actividad claramente criminal que, por serlo, el ciudadano corriente no está dispuesto a llevar a cabo es escasa y constitutiva de cooperación necesaria. En GIMBERNAT ORDEIG, E., "A vueltas con la imputación objetiva, la

Todos los elementos del artículo 248.2.a del CP existen en estos casos, con la manipulación de datos de la cuenta corriente expoliada y la introducción en la misma, la transferencia efectuada a otra cuenta distinta a fin de disponer de la cantidad mediante la actuación del sujeto que pone a disposición su entidad bancaria previo descuento por él de una comisión en su propio beneficio y en perjuicio todo ello del titular de la cuenta manipulada, evidenciando su connivencia con los autores directos de la manipulación y la relevante intervención de aquel para la realización del apoderamiento de los fondos[74].

7.5. Aspecto subjetivo

Estas conductas suponen un ataque planificado, programado y ejecutado para una finalidad concreta, siendo dolosas. Sin embargo, a diferencia de la estafa tradicional, el ilícito penal no se comete ya en el marco de una relación interpersonal, sino que el sujeto activo se sitúa ante una máquina, mecánica o informática, frente a la que se efectúa una manipulación, ardid, truco o engaño (bien en sus elementos físicos, bien en su programación) o artificio semejante[75].

El elemento intencional era expresamente mencionado en la DM 2005/222/JAI, artículo 2.1, para el "*acceso intencionado sin autorización al conjunto o una parte de un sistema de información*". Esa circunstancia se refiere a la consciencia y voluntad de acceder sin autorización al sistema de información o, más concretamente, a los datos personales que contiene, pues precisamente la primera fase del *phising* se caracteriza por su búsqueda para, una vez obtenidos, realizar en la segunda etapa la posterior transferencia no autorizada del activo patrimonial[76].

Y es ese segundo momento el que puede plantear mayores problemas en el aspecto subjetivo. Así, como indica ROSO[77], el sujeto que prefiere mantenerse en el desconocimiento para no ser implicado en la realización de un delito, pese a sospechar que puede favorecer conductas ilícitas de terceros, se mantiene voluntariamente en un estado de ignorancia, y la jurisprudencia ha atendido a la existencia de los indicios expuestos en el apartado anterior para concluir que el sujeto actúa dolosamente en la segunda fase, llegándose a afirmar que cualquier persona con un nivel cultural medio no puede desconocer que recibir en su cuenta corriente unas cantidades considerables de otra cuenta corriente titularidad de una persona a la que de nada conoce y con la que no tiene ningún tipo de trato mercantil para posteriormente remitirla a otra persona también desconocida en un país extranjero y recibir por ello una comisión, es una operación ilícita, y si deliberadamente no quiere saber en qué

participación delictiva, la omisión impropia y el Derecho penal de la culpabilidad", *Nuevo Foro Penal*, nº 82, Universidad EAFIT, Medellín, 2014, p. 73.

74 ATS, Sección 1ª, nº 1548/2011, de 27 de octubre (JUR 2011\393198), Pte. Excmo. Sr. Alberto Jorge Barreiro.

75 SAP de Madrid, Sección 23ª, nº 92/2018, de 24 de enero (ARP\2018\278), Pte. Ilma. Sra. María de los Ángeles Montalvá Sempere.

76 SAP de Valencia, Sección 5ª, nº 491/2016, de 5 de septiembre (JUR\2018\61725), Pte. Ilma. Sra. Dª Beatriz Goded Herrero.

77 ROSO CAÑADILLAS, R., "Algunas reflexiones sobre los nuevos fenómenos delictivos, la teoría de delito y la ignorancia deliberada", *Revista General de Derecho Penal*, 22 (2014), ed. iustel, Madrid, 2014, p. 18.

actividad ilícita está cooperando, está asumiendo las consecuencias de su actuar al menos con dolo eventual[78].

No obstante, alguna resolución judicial minoritaria ha concluido que el acomodo del *phising* en el tipo de la estafa informática se supedita a que el intermediario, bien haya participado en la manipulación informática de la cuenta bancaria de la víctima, o bien haya colaborado con las personas desconocidas que llevaron a cabo dicha manipulación, en una fase posterior pero con conocimiento de dicha manipulación, del carácter fraudulento de la transferencia, y, en fin, con el ánimo de defraudar o con dolo de estafar[79], sin que se exija el engaño característico de la estafa pura y simple.

Este aspecto subjetivo nos lleva al planteamiento, en el siguiente punto, de la ignorancia respecto a ese conocimiento, como argumento que habitualmente expone el sujeto que interviene voluntariamente en la segunda fase del delito, poniendo a disposición del tercero su cuenta bancaria para que transfiera a ella los fondos empleando las claves o contraseñas pescadas, para remitirlos a este último sujeto previo cobro de una comisión.

8. LA IGNORANCIA DELIBERADA

8.1. Concepto de ignorancia deliberada

A diferencia del error, que tradicionalmente se entiende como un conocimiento deformado de la realidad o de su significación social o jurídica, la ignorancia implica la ausencia de conocimiento perceptivo o valorativo sobre algo[80].

Por ello, la ignorancia, que difícilmente puede concurrir en la primera etapa del *phising* al definirse como la pesca intencionada de datos, es la excusa más extendida por parte del sujeto que interviene en su segunda fase, al argumentar que no conoce al titular de la cuenta desde donde se le transmite los activos, ni tampoco al sujeto al cual remite parte de esos fondos[81].

Para dar respuesta a la pretendida ignorancia de estos sujetos, la jurisprudencia ha reiterado que en el delito de *phising* no se exige un dolo directo, bastando el eventual o siendo incluso suficiente situarse en la posición de ignorancia deliberada. Y define el citado desconocimiento como aquel en que incurre quien pudiendo y debiendo conocer, la naturaleza del acto o colaboración que se le pide, se mantiene en situación de no querer saber, pero no obstante presta su colaboración[82].

Como defiende RAGUÉS, la ignorancia deliberada, *willful blindness* o ceguera

---

78 SAP de Las Palmas, Sección 2ª, nº 22/2013, de 11 de febrero (JUR\2013\164745), Pte. Ilma. Sra. Pilar Parejo Pablos.

79 En este sentido, SAP de León, Sección 3ª, nº 410/2014, de 17 de julio (ARP 2014\809), Pte. Ilmo. Sr. D. Luis Adolfo Mallo Mallo; o la SAP de León, Sección 3ª, nº 580/2014, de 3 de noviembre (JUR 2015\65404), Pte. Ilmo. Sr. D. Carlos Javier Álvarez Fernández.

80 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general del Derecho penal ..., cit*., nota 55, p. 172.

81 *Vid*. Nota 1.

82 STS nº 33/2005, de 19 de enero (RJ 2005\944), Pte. Excmo. Sr. D. Joaquín Giménez García.

intencionada[83], describe situaciones en las que un sujeto podía haber obtenido determinada información pero, por razones muy diversas, ha preferido no adquirirla y mantenerse en un estado de incertidumbre[84].

Según se expone en el siguiente apartado, desde la suficiencia del dolo eventual basta situarse en la citada posición de ignorancia deliberada para convertir al sujeto en acreedor de las consecuencias penales que se deriven de su antijurídico actuar[85].

8.2. Consecuencias de la ignorancia deliberada en el *phising*

Efectivamente, con la premisa de la ignorancia deliberada equiparada al dolo[86], la consecuencia no es otra que convertir al sujeto en acreedor de las consecuencias penales que se deriven de su antijurídico actuar, por cuanto la doctrina jurisprudencial acerca del dolo eventual, y la teoría del asentimiento, determinan que incumbe a quien lleva a cabo una acción el despejar las dudas que puedan surgir acerca de la verdadera naturaleza y contornos de su misma estructura[87].

Así, como viene reiterando la Sala Segunda, el citado desconocimiento no exime de su responsabilidad a quien pudiendo y debiendo conocer el sentido de su acción se niega a conocerlo, y trata de obtener ventaja de tal situación[88].

Dicho en otras palabras, quien no quiere saber aquello que puede y debe saberse, y sin embargo busca un beneficio de la situación, está asumiendo y aceptando todas las posibilidades del origen del negocio en el que participa, y por tanto debe responder de sus consecuencias[89].

Y es 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 el *phising*, no constando además indicio alguno que pudiera ser sugestivo de un desconocimiento de la ilicitud de la colaboración que se le pedía, máxime cuando no se trata de una colaboración gratuita, sino que lleva aneja un claro enriquecimiento personal. No hay por tanto ninguna posibilidad de derivar a ningún supuesto de error la acción del sujeto[90].

---

83 RAGUÉS I VALLÈS, R., "La teoría de la ignorancia deliberada", *Amachaq*, nº 2, ed. Amachaq escuela jurídica, Lima (Perú), 2021, p. 32.

84 RAGUÉS I VALLÈS, R., "Sobre la doctrina de la ignorancia deliberada en Derecho penal", *Revista Discusiones*, nº 13, 2, 2013, Universidad Nacional del Sur, Bahía Blanca (Argentina), 2013, p. 11.

85 STS nº 338/2007, Sección 1ª, de 25 de abril (RJ 2007\3327), Pte. Excmo. Sr. Miguel Colmenero Menéndez de Luarca.

86 RAGUÉS advierte que la inclusión de semenjantes casos en el concepto de dolo impedirá seguir definiendo esta figura a partir del conocimiento, y se pronuncia sobre la necesidad de replantear un sistema de imputación subjetiva basado exclusivamente entre dolo e imprudencia, por los problemas que plantea obtener una definición generalmente válida de dolo y la sobrecarga conceptual de esta figura. En RAGUÉS I VALLÈS, R., "Sobre la doctrina de la ignorancia deliberada en Derecho penal", *cit.* Nota 84, p. 33.

87 STS nº 953/2008, de 26 de diciembre (RJ 2008\8019), Pte. Excmo. Sr. Julián Sánchez Melgar.

88 STS nº 785/2003, de 29 de mayo (RJ 2003\6321), Pte. Excmo. Sr. D. Joaquín Giménez García.

89 STS nº 16/2006, de 13 de marzo (RJ 2006\2238), Pte. Excmo. Sr. D. Joaquín Giménez García.

90 STS nº 533/2007, de 12 de junio (RJ 2007\3537), Pte. Excmo. Sr. D. Joaquín Giménez García.

Cualquier persona con un nivel intelectivo medio es sabedora, sin necesidad de especial sabiduría técnica y/o especial formación académica, de que para realizar una transferencia no es preciso valerse de la cuenta corriente de un tercero, lo que junto el cobro de la suma percibida como remuneración muestra indudablemente que la conducta voluntariamente llevada a cabo en modo alguno puede valorarse por quien realiza como lícita, sino al contrario[91].

Lo expuesto, no significa que estas personas deban conocer toda la operación, por cuanto en la mayoría de los casos se está ante un supuesto de delincuencia económica de tipo informático de naturaleza internacional, en el que las personas que se prestan a poner a disposición de personas desconocidas sus cuentas bancarias ocupan un nivel inferior y sólo tienen un conocimiento necesario para prestar su colaboración, sin que la ignorancia del resto del operativo borre o disminuya su culpabilidad en el delito de estafa cometido[92].

De esta forma, aun cuando el sujeto no hubiera conocido que los fondos se le transferían a su cuenta sin consentimiento del titular de los mismos mediante una manipulación informática realizada por un tercero, habría de apreciarse la concurrencia de unos presupuestos para apreciar que actuó desde una posición de ignorancia deliberada que haría que el hecho delictivo le fuera imputable a título de dolo. En concreto:

1.- La conducta antijurídica:

Si el sujeto ha proporcionado una cuenta bancaria para que se le transfiriesen fondos de personas con la que no tenía relación alguna ni conocía, conviniendo hacer suyos una parte de los mismos y, por otra parte, remitirlos a una persona de identidad distinta a la titular de los fondos y distinta también a la supuesta empresa que le había encomendado la gestión.

Esta persona no podía ignorar que, al no conocer ni tener relación alguna con las personas cuyos fondos bancarios serían ingresados en la cuenta que ella proporcionaba, a tal efecto estaba incrementando el riesgo de que pudieran las transferencias ser realizadas sin el consentimiento de los titulares de los fondos, ni podía ignorar que sin contar con el consentimiento de la persona que supuestamente le transfería el dinero los actos de disposición por él realizados eran antijurídicos, ni tampoco podía obviar que su intervención en el operativo le irrogaba un pingüe beneficio superior a cualquier comisión de las que son habituales en el tráfico.

2.- La permanencia voluntaria en la ignorancia:

Si el sujeto omite toda acción encaminada a informarse de cuál fuera la realidad de las operaciones en que aceptaba participar, a pesar de que fácilmente podía hacerlo simplemente comprobando, a través de alguna de las instituciones públicas o privadas o incluso de internet, la ficción de la empresa o el sujeto con el que iba a colaborar, o contactando con la persona que supuestamente le transfería dinero para inquirir sobre su consentimiento para participar en el negocio. Más aun cuando su nivel cultural implica ya que necesariamente y por sus estudios tuviera que representarse la más que segura evidencia del más que probable carácter

91 ATS nº 1548/2011, de 27 de octubre (JUR 2011\393198), Pte. Excmo. Sr. D. Alberto Jorge Barreiro.
92 STS nº 533/2007, de 12 de junio (RJ 2007\3537), Pte. Excmo. Sr. D. Joaquín Giménez García.

delictivo de su actuación. De ahí que sea indudable que podía haber conocido perfectamente la ilicitud de su intermediación y que si voluntariamente permaneció en la pretendida situación de ignorancia fue porque ello le era indiferente para su propósito de obtención de un dinero rápido, fácil y relevante.

3.- La motivación antijurídica de la permanencia en la ignorancia que se concreta en el propósito de hacer suya la comisión, pese a conocer la ilicitud de su conducta, lo que integra evidentemente un claro y patente ánimo de lucro.

En consecuencia, con estos elementos, la argumentación de la ignorancia por parte de los acusados resulta mayoritariamente rechazada por los tribunales[93]. Se concluye así que el sujeto conocía la falta de justificación de los ingresos que recibió en sus cuentas y de la retribución por su participación, y por ello y aun cuando inicialmente no conociera fehacientemente que los fondos se le transferían a su cuenta lo eran sin consentimiento del titular de los mismos mediante una manipulación informática realizada por un tercero, actuó desde una posición de ignorancia deliberada por la que el hecho delictivo le es imputable a título de dolo[94].

Todo ello, por cuanto 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 el extranjero, es consciente del alto riesgo de que el origen del dinero trasladado sea ilícito. Pudiéndose afirmar que la única razón para "no querer saber nada" es, obviamente, la convicción de que se trata de una actividad ilícita[95].

9. FORMAS DE APARICIÓN

Se plantean en este subepígrafe las cuestiones relativas a la autoría y participación y el *iter criminis* del delito de *phising* como modalidad más habitual de estafa informática:

i. Sin presentar especiales problemas la autoría inmediata porque un sujeto adquiera la información personal y la utilice para realizar una transferencia de activos no consentida, siguiendo el criterio jurisprudencial[96], para que exista coautoría será preciso que la pesca de datos personales y posterior transferencia de activos, aprovechando esas claves o contraseñas, se produzca de forma concertada entre varios sujetos, interviniendo cada uno de ellos en su ejecución como autores, todos ellos con un dominio del hecho. Así, el sujeto que ha obtenido las claves o contraseñas del sujeto pasivo, normalmente está en el extranjero y para evitar un envío directo a su cuenta bancaria que motive la reacción inmediata del Banco o su posible bloqueo, colabora con un sujeto nacional, que recibe el activo en su cuenta para

93 Salvo excepciones, como las citadas sentencias de la Ilma. Audiencia Provincial de León. *Vid*. Nota 79.

94 En este sentido, con cita de numerosa jurisprudencia, la SAP de Cantabria, SEcción 1ª, nº 226/2016, de 25 de abril (JUR\2017\60691), Pte. Ilma. Sra. Paz Mercedes Aldecoa Álvarez-Santullano.

95 SAP de Valencia, Sección 3ª, nº 579/2012, de 31 de julio (JUR\2012\370119), Pte. Ilma. Sra. Dª Sandra Silvana Schuller Ramos.

96 Entre otras, la STS nº 1315/2005, de 10 de noviembre de 2005 (RJ 2006\3099), Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre.

su remisión inmediata al extranjero[97] y al que comúnmente se le asigna el nombre de "mula"[98].

La concurrencia de la pluralidad de sujetos con reparto de funciones en el *phising* viene motivada por la estrategia de no levantar sospechas en la entidad bancaria. Así, el sujeto que ha logrado esa información no autorizada del sujeto pasivo normalmente está en otro país y, para evitar un envío directo a su cuenta bancaria que motive la reacción inmediata del Banco o su posible bloqueo, colabora con un sujeto nacional, que recibe el activo en su cuenta para su remisión inmediata al extranjero[99].

En consecuencia, en la mayoría de los casos se produce coautoría o, al menos, cooperación necesaria, para facilitar la comisión del delito, evitar su descubrimiento y, especialmente, impedir su bloqueo. Resulta inútil obtener las claves de los usuarios de banca electrónica sin que alguien se preste en España a ofrecer su cuenta y ayudar a sacar el dinero del país, por lo que es lógico que los primeros en lugar de utilizar una cuenta que serviría para identificarles lo hagan a través de la intermediación de una persona[100].

Por lo que respecta a la participación, se integraría por los demás casos previstos en el artículo 28.2, apartados a y b, y en el artículo 29 CP, es decir, por la inducción, la participación necesaria y la no necesaria[101].

La inducción del delito de *phising*, se produciría en el supuesto del sujeto que influye en otro para que lleve a cabo la obtención de información y/o transferencia de activos, siempre y cuando el sujeto que lo ejecuta no estuviese ya decidido a cometer el delito antes[102], y siendo necesaria la efectiva ejecución, puesto que en caso contrario estaríamos en el

---

97 En este sentido, entre otras, SAP de Tarragona, Sección 2ª, nº 197/2018, de 20 de abril (ARP\2018\962), Pte. Ilmo. Sr. D. Ángel Martínez Saez.

98 El término mula se emplea normalmente en referencia tanto al sujeto al que se transfieren las cantidades para su posterior remisión a otra persona, como a la cuenta donde se reciben para su reenvío. Así, en este último sentido y en referencia a la segunda fase del *phising*, posterior a la obtención de la información personal, SAP de Guipúzcoa, Sección 3ª, nº 97/2015, de 13 de octubre (ARP\2015\1482), Pte. Ilma. Sra. Dª Juana María Unanue Arratíbel: "*una cuenta "mula" a la que se transfieren las cantidades fraudulentamente obtenidas y posterior retirada de las mismas o envió a terceras personas de los importes obtenidos*".

99 En este sentido, entre otras, SAP de Tarragona, Sección 2ª, nº 197/2018, de 20 de abril (ARP\2018\962), Pte. Ilmo. Sr. D. Ángel Martínez Saez.

100 En este sentido, SAP de Madrid, Sección 30ª, nº 669/2013, de 19 de diciembre (ARP\2014\161), Pte. Ilma. Sra. Dª María Inmaculada Iglesias Sánchez.

101 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general del Derecho penal*, *cit*., nota 55, p. 657.

102 Así, la STS, Sala Segunda, de 14 de septiembre de 1989 (RJ 1989\6644), Pte. Excmo. Sr. D. Francisco Soto Nieto, establecía en su FJ 5º que "*El inducido no ha de haber resuelto antelativamente la ejecución del hecho delictual sino que ello ha de ser consecuencia de la excitación influenciante del inductor, sin que ello signifique que previamente aquél haya de ser indiferente al hecho, o que no pueda apreciarse algún otro factor confluyente y adherido, siempre de estimación secundaria, en la determinación delictiva del agente. La inducción implica que la persona influida o instigada, además de adoptar la resolución ejecutiva del hecho antijurídico, entre en la fase realizadora del mismo, cualquiera que sea el grado alcanzado en ella. Doctrina, la expuesta que tiene su reflejo en Sentencias de esta Sala de 12 de abril de 1986 y 8 de febrero de 1988".*

supuesto de la proposición previsto en el artículo 17.2 CP[103], que se castigaría con la pena inferior en uno o dos grados a la establecida para la estafa, conforme al artículo 269 del CP.

En los casos de pluralidad de sujetos activos, cuando uno de ellos ha logrado esa información no autorizada del sujeto pasivo, está en el extranjero y colabora con un sujeto nacional para el envío de dinero, cabe la posibilidad de que este último no pueda ser coautor, porque pueda entenderse en algún caso que no tiene el dominio total. Pero la jurisprudencia viene reiterando que sin duda será cooperador necesario, por la recepción del dinero de una cuenta extraña para su transmisión a otra persona extraña, y por tratarse de un bien de escasa obtenibilidad y determinante de la operación *ex ante*[104].

Por otra parte, la distinción práctica entre la autoría y la cooperación necesaria en el delito de *phising* se difuminará en la medida en que, de conformidad con el artículo 248.2.a del CP serán autores tanto el que "*con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro"* como, según el artículo 248.2.b del CP, "*los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo*", lo que supone en estos casos elevar a la categoría de autoría las conductas de cooperación.

En consecuencia, resultan difícilmente imaginables supuestos de complicidad en estos delitos, atendida, por una parte, la amplitud con la que la jurisprudencia interpreta la coautoría y la cooperación necesaria, y la consideración como autor del artículo 248.2.b del CP del mero facilitador de programas informáticos específicos para estas conductas.

ii. En cuanto al *iter criminis*, en primer lugar, en el supuesto del *phising*, como modalidad de estafa, está expresamente tipificada la conspiración, proposición y provocación para cometer el delito en el citado artículo 269 del CP.

En segundo lugar, según se ha expuesto en el anterior punto 6, el *phising* se configura como un delito de resultado y de lesión[105], al exigir el menoscabo del patrimonio ajeno. De esta forma, sería posible la tentativa acabada si se ha conseguido la transferencia pero no se ha causado perjuicio, p.ej. la entidad bancaria de la que es cliente la víctima advierte el movimiento del activo a una cuenta en el extranjero y retiene el movimiento hasta confirmarlo con el titular, que anula la orden.

Pero es difícilmente imaginable la tentativa inacabada, que en la estafa común se produciría con el engaño sin error y ya es complicada *per se*[106] , por cuanto en el *phising* se da la circunstancia de que se debe emplear manipulación informática o artificio semejante. Podría darse el caso que no se llega a utilizar ese medio, pero el sujeto tuviera ya un programa informático específicamente destinado a la comisión de la estafa, con lo cual habría

---

103 En este sentido ha concluido, entre otras, la STS nº 1994/2002, de 29 de noviembre de 2002 (RJ 2002\10874), Pte. Excmo. Sr. D. José Ramón Soriano Soriano, FJ 2º.

104 STS, Sección 1ª, nº 556/2009, de 16 de marzo (RJ 2009\4823), Pte. Excmo. Sr. D. Siro Francisco García Pérez.

105 LAURENZO COPELLO, P., *El resultado en Derecho Penal ...* , *cit*., nota 53, p. 117.

106 QUINTERO OLIVARES, G., *Comentarios a la parte especial ...* , *cit*., nota 38, p. 652.

consumado la modalidad del artículo 248.2.b del CP. Si ni siquiera tuviera el programa, y sin el empleo de la manipulación informática, la conducta sería atípica.

Distintos son los supuestos en los que no se realiza la transferencia porque el sujeto activo decida interrumpir voluntariamente la acción iniciada, dando lugar al desistimiento, o bien porque realice una ejecución completa sin éxito voluntario, produciendo el arrepentimiento activo.

La distinción resulta trascendente a los efectos de exención de responsabilidad penal por este delito, sin perjuicio de la que pudiese concurrir por los actos ya ejecutados, de conformidad con el artículo 16 CP, apartados 2 y 3. El problema se encuentra en delimitar cuándo existirá voluntariedad para interrumpir la transferencia o para que no llegue a producirse ese resultado a pesar de haber ejecutado todos los actos.

Para establecer esa delimitación, aquí se sigue una vez más el criterio que ha venido fijando la jurisprudencia respecto a otros delitos, y que atiende a que "*el desistimiento, ha de ser, propio, voluntario, personal y definitivo, pudiéndose destacar que cuando, el citado desistimiento, se produce porque han surgido obstáculos insuperables que impiden de modo absoluto la continuación delictiva, dicho desistimiento, se reputa involuntario e ineficaz*"[107]. De tal manera que si el sujeto que inicia el ciberataque, de forma voluntaria, personal y definitiva, y sin ningún obstáculo insuperable que le impidiese ejecutar la transferencia, decide no culminar todos los actos de ejecución, estaremos ante el desistimiento, tal y como sucedería en el ejemplo del sujeto que, introducidos los datos personales de la víctima para realizar la transferencia, decide no confirmarla, evitando que el titular de la cuenta resulte perjudicado. En caso contrario, siguiendo el criterio anterior de la tentativa acabada, si ha surgido un obstáculo insuperable para alcanzar ese resultado, impidiendo la ejecución de todos los actos, como sucedería si ha sido el Banco el que ha impedido la confirmación e inesperadamente el sujeto no puede transferir los activos, no existirá un desistimiento, sino una tentativa acabada. El sujeto no recibirá los fondos porque no puede adquirirlos.

Pero si se han ejecutado todos los actos para la transmisión, y el resultado no se produce por la decisión del sujeto que realiza ese acceso, tendrá lugar el arrepentimiento activo, lo que ocurriría en el ejemplo del que se conecta remotamente a otro sistema para transferir ilícitamente y, ejecutada la orden que permite recibir los fondos, antes de producirse decide apagar su ordenador y, por tanto, no acceder. Por el contrario, si no ha sido el sujeto quien ha llevado la actuación para evitar que el resultado se produzca, se producirá de nuevo la tentativa acabada, lo que tendría lugar si el titular de la cuenta a la que se pretende acceder se cerciora de que se están tratando de transferir sus fondos y lo impide reforzando las medidas de seguridad, hasta tal punto de resultar un escollo insalvable para el sujeto que pretendía acceder.

Por último, en cuanto a la tentativa inidónea y al delito imposible[108], la conducta deberá ser idónea para poner en peligro el patrimonio ajeno. Esto implica que, en los

[107] En este sentido, STS, Sala de lo Criminal, de 7 de junio de 1985 (RJ 1985\2973), Pte. Excmo. Sr. D. Luis Vivas Marzal.

[108] Sobre la tentativa inidónea y el delito imposible, el parrafo 2.° del articulo 52 del CP aprobado por Decreto 692/1963, de 26 de marzo, cuando hablaba de imposibilidad de ejecución y de imposibilidad de producción del delito, distinguía entre imposibilidad por inidoneidad de los medios e imposibilidad por

supuestos en que los medios utilizados no sean idóneos para producir la transferencia de activos, por ejemplo si se pretendiera enviarlos mediante señales de humo, estaremos ante la tentativa inidónea del delito. Mientras que si lo que sucede es que falta el objeto, como en el caso hipotético de que se pretendiera enviarlos desde una cuenta inexistente, tendría lugar un delito imposible[109].

---

inexistencia del objeto. En este sentido, RODRÍGUEZ MOURULLO, G., "Delito imposible y tentativa de delito en el Código penal español", *Anuario de derecho penal y ciencias penales*, Tomo 24, Fasc/Mes 2, Ministerio de Justicia, Madrid, 1971, pg. 373.

Por otra parte, la doctrina mayoritaria ha abandonado la distinción entre tentativa absolutamente inidónea, entendida como la que no solo era incapaz de producir la consumación en el caso concreto, sino también en cualquier otra circunstancia; y la tentativa relativamente inidónea, es decir, la tentativa que en otras circunstancias no habría sido inidónea. Por todos, MIR PUIG, S., "Sobre la punibilidad de la tentativa inidónea en el Código Penal", en *Revista Electrónica de Ciencia Penal y Criminología*, RECOC 03-06 (2001), Universidad de Granada, Granada, 2001.

No obstante, algún sector doctrinal mantiene la distinción entre inidoneidad relativa, es decir, aquellos en que los medios utilizados, objetivamente valorados *ex ante* y desde una perspectiva general, son abstracta y racionalmente aptos para ocasionar el resultado típico; tentativa irreal (o absolutamente inidónea), cuando en el propio momento de realizar la acción esta se revela a un hombre medio como incapaz de producir el resultado, como un intento de matar mediante conjuros (esta variante de la tentativa real se ha denominado tentativa mágica o supersticiosa), entendiendo que la tentativa idónea y la relativamente inidónea, por inidoneidad en los medios o en el objeto son punibles, mientras que no lo es en ningún caso la tentativa irreal. En este sentido, MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento Penal*, ed. Francis Lefebvre, Madrid, 2022.

En esta línea también se ha pronunciado alguna sentencia. Así, con cita de otras, la STS 183/2013, de 12 de marzo (RJ 2013\2039), Pte. Excmo. Sr. D. Cándido Conde-Pumpido Tourón, FJ 10º: "*el art. 16 del Código Penal 1995 ha redefinido la tentativa, añadiendo la expresión "objetivamente" ("practicando todos o parte de los actos que objetivamente deberían producir el resultado"). Objetivamente quiere decir, en la interpretación consolidada de esta Sala, que el plan o actuación del autor, "objetivamente" considerados, son racionalmente aptos para ocasionar el resultado.*

Ello deja fuera de la reacción punitiva los supuestos de tentativas irreales o imaginarias (cuando la acción es, en todo caso y por esencia, incapaz de producir el fin ilusoriamente buscado por su autor); los denominados "delitos putativos" (cuando el sujeto realiza una acción no tipificada penalmente, creyendo que sí lo está), error inverso de prohibición que en ningún caso podría ser sancionado penalmente por imperativo del principio de tipicidad; los supuestos de delitos absolutamente imposibles por inexistencia de objeto, que carecen de adecuación típica; y, en general, los casos de inidoneidad absoluta (STS 899/2012, de 2 de noviembre , y las sentencias que en ella se citan).

Ahora bien deben encuadrarse en los supuestos punibles de tentativa, conforme a su actual definición típica, los casos en que los medios utilizados, "objetivamente" valorados "ex ante" y desde una perspectiva general, son abstracta y racionalmente aptos para ocasionar el resultado típico (de lesión o de peligro). Se trata de supuestos en los que la intervención penal se justifica plenamente porque el autor ha decidido vulnerar el bien jurídico tutelado, a través de una acción incardinada en la órbita del tipo y utilizando medios generalmente idóneos, aun cuando no lo sean en el caso concreto (STS 899/2012, de 2 de noviembre,y las sentencias que en ella se citan)".

[109] Con referencia al CP vigente, la STS 822/2008, de 4 de diciembre (RJ 2009\433), Pte. Excmo. Sr. D. Diego Antonio Ramos Gancedo, FJ 5, diferencia entre tentativa inidónea para los casos de inidoneidad de medios, y delito imposible por falta de objeto: "*como modalidad de la tentativa puede considerarse la denominada por los penalistas franceses y los de habla hispana delito imposible, en tanto los alemanes utilizan la expresión de tentativa inidónea, aunque también suele, entre nuestros penalistas, reservar este término a los supuestos de inidoneidad de los medios y el de delito imposible, propiamente dicho, a la falta de objeto (en este sentido, STS de 16 de febrero de 1.989 (RJ 1989, 1581), que apreció delito imposible de aborto, en mujer que se creyó embarazada). En definitiva, "en la práctica del Derecho penal, no puede terminantemente distinguirse entre tentativa inidónea por falta de medios adecuados de ejecución, de un lado, y delito imposible por inexistencia de objeto o de sujeto pasivo sobre los que recae la acción delictiva (S 30-1-92(RJ 1992, 608)) de otro" (STS 1718/93, de 5 de julio (RJ 1993, 5876);* en STS *116/94, de 26 de enero (RJ 1994, 110), indistintamente emplea ambos términos, abarcando las dos posibilidades)*".

10. CONCLUSIONES

La estafa informática se ubica entre los supuestos conocidos como ciberdelincuencia. El delito de *phishing* es su modalidad más frecuente, sofisticada y compleja, y los rasgos que lo caracterizan son la aparición de una zona de riesgo con las nuevas tecnologías, común para muchos bienes jurídicos protegidos, la sencillez para su comisión, sin límites transfronterizos, despersonalización en la conducta, la vulnerabilidad de los equipos informáticos y la especialización en los sujetos que las realizan.

La naturaleza transnacional, así como los riesgos que estos nuevos mecanismos generan para los bienes jurídicos tradicionales y los que han surgido como consecuencia de estas nuevas formas de lesión, ha supuesto que en el ámbito internacional se hayan intentado establecer las bases para su regulación, a través de diversos instrumentos de carácter vinculante en mayor o menor medida para los Estados miembros. Estas respuestas normativas han ido evolucionando desde una primera fase en torno a la privacidad y transmisiones de datos personales en el ámbito europeo en los años 80, comprendiendo en los años sucesivos las conductas de delincuencia económica, hasta el punto de que surgen paralelamente nuevos bienes dignos de protección, como es la seguridad de los sistemas informáticos, adquiriendo una progresiva mayor importancia a medida que se desarrollan las nuevas tecnologías, surgiendo así la necesidad de regular las conductas de estafas informáticas.

El trabajo del legislador español regulando estas conductas, con la primera redacción del CP y la posterior ampliación a los facilitadores de estas acciones mediante programas informáticos específicos, tan solo ha mitigado en parte el esfuerzo hermenéutico que realizaban los órganos jurisdiccionales para tratar de incluirlos como estafas tradicionales.

La alternativa podría haber sido una regulación ordenada, tipificando estas conductas en una norma, título o capítulo autónomo[110], estableciendo definiciones sobre los conceptos básicos y regulando a continuación el tipo básico y sus modalidades. Y en este caso, estos ciberataques tendrían una respuesta a partir de su consideración como una forma de defraudación informática, en la que no es necesario el engaño personal al actuar frente a una máquina. Todo ello sin duda ayudaría al intérprete en un campo tan complejo y en continuo cambio como el que nos ocupa y podría evitar la amalgama de acciones, participaciones y referencias que actualmente regula el Código Penal español.

Se toma en consideración el patrimonio como bien jurídico directamente protegido en el delito de *phising* regulado en el artículo 248.2.a 1 del CP, pero estas conductas también pueden comprometer, en su *modus operandi*, la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, atendiendo a los compromisos internacionales por los cuales se introdujo la protección de estos últimos intereses en el artículo 197.3 del CP por la LO 5/2010 y, después, el 197 *bis* 1 del CP por la LO 1/2015, tratándose por tanto de una estafa informática más amplia que las defraudaciones tradicionales.

Esta conducta afecta como objeto material a los activos patrimoniales, que son

[110] Son ejemplos de países de nuestro entorno con ley especial sobre determinados ciberdelitos Chipre, Irlanda, Portugal o Reino Unido, y de título o capítulo propio, Bélgica, Bulgaria, Croacia, Finlandia o Hungría.

transferidos empleando manipulación informática o artificio semejante, ampliando los medios a los programas de ordenador específicos para cometer esa estafa, con la reforma de la LO 15/2003 y el expreso castigo para quien los fabrica, introduce, facilita o posee. Esta novedad supone la criticable tipificación expresa de actos de cooperación elevados a categoría de autoría, y en la práctica implica la equiparación entre autoría y participación de acciones que, en principio, deberían encuadrarse en este último grupo, en las conductas de defraudación informática en general y del *phising* en particular, incluso cuando no se llega a materializar el perjuicio del patrimonio ajeno.

La peculiaridad en la naturaleza de *phising* se encuentra en que es un delito de resultado y lesión, pero a diferencia de la estafa tradicional no exige relación o engaño personal. Y, además, desde el año 2003 se admite la modalidad consumada de poseer o facilitar programas específicos para cometer estos delitos, que no exige esa efectiva lesión, bastando con un peligro abstracto para el patrimonio ajeno para entenderlos consumados. De esta forma, se ha ampliado el delito a supuestos donde quizás nunca llegue a causarse un perjuicio a los bienes de otra persona, optando el legislador por adelantar las barreras de protección de esos intereses con la tipificación de esta última modalidad, como forma de dar respuesta al riesgo en el uso de las nuevas tecnologías que se desarrollan a mayor velocidad que las reformas legislativas, alterando con ello, a su vez, las normas generales sobre autoría y participación, al situarse al mismo nivel de responsabilidad penal en la práctica de las estafas informáticas.

Por otra parte, el artículo 248.2.a del CP se caracteriza por el empleo de términos vagos, que en la práctica generan inseguridad jurídica y que podría haberse salvado con una descripción más detallada, como en el Código Penal alemán. No obstante, se ha defendido esa amplitud a efectos de poder abarcar las nuevas tecnologías futuras.

En estos supuestos, normalmente se va a producir una pluralidad de sujetos activos, incrementando la complejidad del *phising*, facilitando su consumación y dificultando su persecución, admitiendo a su vez múltiples variantes, pero concurriendo en todas ellas las características de los fraudes informáticos. Entre esos casos, prevalecen por su reiteración las acciones en las que un sujeto facilita la cuenta bancaria para recibir los fondos ilícitamente y transmitirlos a un tercero.

Tomando en consideración la estafa informática como un delito eminentemente doloso, en esa última modalidad, referida a la conducta del facilitador de la cuenta bancaria, es donde se plantea en mayor medida la ignorancia deliberada. Y es este elemento subjetivo el que puede originar más problemas prácticos, hasta tal punto que algunos tribunales han llegado a absolver a determinados sujetos porque no habían participado en la manipulación informática de la cuenta de la víctima, o bien porque no constaba acreditada la colaboración con el tercero en esa manipulación.

Por ello, para evitar esa impunidad del intermediario, que sin duda realiza una acción determinante para el éxito del *phising*, se hace preciso comprobar en cada caso la concurrencia de los indicios que, cuanto menos, acrediten una ignorancia deliberada en esa persona y, por tanto, su actuación dolosa, como la conducta antijurídica, la permanencia voluntaria en la ignorancia y la motivación antijurídica del mantenimiento en ese

desconocimiento. Concurriendo esos presupuestos, la pretendida ignorancia del intermediario podrá ser considerada irrelevante a efectos de responsabilidad penal.

Por último, en cuanto a las formas de aparición, el delito de *phising* admite autoría y participación, siendo los casos mayoritarios de coautoría o, al menos, cooperación necesaria. Más difícil parece incluir los casos de autoría mediata entre estos delitos, dada su complejidad y el concepto de ignorancia deliberada, que impide que el sujeto pueda estar exento de responsabilidad por su acción a título oneroso y determinante del éxito del delito.

Como delito de resultado, es posible la tentativa acabada, pero la falta del engaño personal en el *phising* hace complicada la apreciación de la inacabada, ya de por sí compleja en la estafa común. Igualmente cabe el desistimiento y el arrepentimiento activo.

En definitiva, la regulación actual del delito de *phising*, equiparada al delito de estafa y ampliada con la modalidad de fabricación, introducción, posesión o facilitación de programas informáticos específicos para cometerlo, dan lugar a que la interpretación de las conductas que comprende no sea sencilla y obligue a estudiar en cada caso hasta dónde ha alcanzado la manipulación informática o artificio semejante.

Una mayor sistematización de los delitos vinculados a las nuevas tecnologías, con las definiciones de sus elementos objetivos y subjetivos, abordando el problema de la ignorancia deliberada desde el punto de vista legal, sin duda habría facilitado el tratamiento de este nuevo tipo de comportamientos, que se siguen desarrollando con motivo de la revolución tecnológica acelerada que estamos experimentando.

No haberlo tipificado así, seguramente por la amplia y criticable libertad que el legislador europeo ha otorgado a los Estados miembros para regular esta materia, con la confusión que genera la actual situación y el esfuerzo que van a tener que asumir los sobrecargados órganos jurisdiccionales, hace previsible a corto plazo una nueva reforma legislativa sobre estos delitos.

11. BIBLIOGRAFÍA CONSULTADA

ALMENAR PINEDA, F., *Ciberdelincuencia*, ed. Jurua, Oporto, 2018.

ALMENAR PINEDA, F., *El delito de hacking*, ed. Aranzadi, Pamplona, 2018.

ALONSO GARCÍA, J., *Derecho penal y redes sociales*, ed. Thomson Reuters Aranzadi, primera edición, Navarra, 2015.

ÁLVAREZ VIZCAYA, M., "Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red", en *Internet y Derecho penal. Cuadernos de Derecho Judicial*, nº 10, Madrid, 2001.

BAJO FERNÁNDEZ, M., actualizado por GUÉREZ TRICARICO, P., "Estafa", en MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento Penal*, ed. Francis Lefebvre, Madrid, 2017.

BARRIO ANDRÉS, M., "El régimen jurídico de los delitos cometidos en Internet en el derecho español tras la reforma penal de 2010", en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012.

DE URBANO CASTRILLO, E., "Los delitos informáticos tras la reforma del CP de 2010", en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012.

DE LA CUESTA ARZAMENDI, J. L. (Dir.) y VVAA, *Derecho Penal Informático*, ed. Civitas, Pamplona, 2010.

DÍAZ MARTÍNEZ, M., "El factor criminógeno de las TIC", en PÉREZ GIL, J. (Coord.) y VVAA, *El proceso penal en la sociedad de la información*, ed. La Ley, Madrid, 2012.

FERNÁNDEZ TERUELO, J. G., *Derecho Penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, ed. Lex Nova, Valladolid, primera edición, 2011.

GARCÍA MEXÍA, P. (Dir.), y VVAA. *Principios de Derecho de Internet*, ed. Tirant Lo Blanch, Valencia, 2005.

GIMBERNAT ORDEIG, E., "A vueltas con la imputación objetiva, la participación delictiva, la omisión impropia y el Derecho penal de la culpabilidad", *Nuevo Foro Penal*, nº 82, Universidad EAFIT, Medellín, 2014.

HERNÁNDEZ DÍAZ, L., "Aproximación a un Concepto de Derecho Penal Informático", en DE LA CUESTA ARZAMENDI, J. L. (Dir.) y VVAA, *Derecho Penal Informático*, ed. Civitas, Pamplona, 2010.

HURTADO ADRIÁN, A., "Accesos informáticos ilícitos", en JUANES PECES, A. (Dir.) y VVAA, *Reforma del Código penal. Perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio. Situación jurídico-penal del empresario*, ed. El Derecho, Madrid, 2010.

JUANES PECES, A. (Dir.) y VVAA, *Reforma del Código penal. Perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio. Situación jurídico-penal del empresario*, ed. El Derecho, Madrid, 2010.

LAURENZO COPELLO, P., *El resultado en Derecho Penal*, ed. Tirant Lo Blanch Alternativa, Valencia, 1992.

LÓPEZ ZAMORA, P., *El Ciberespacio y su Ordenación*, ed. Difusión Jurídica y Temas de Actualidad, Madrid, 2006.

MÉNDEZ RODRÍGUEZ, C., "Delitos de peligro y bienes jurídicos colectivos", en *Nuevo Foro Penal*, nº 44, junio, 1989.

MENÉNDEZ MATO, J. C. y GAYO SANTA CECILIA, M. E., *Derecho e informática: ética y legislación*, ed. Bosch Editor, Barcelona, 2014.

MIR PUIG, S., "Sobre la punibilidad de la tentativa inidónea en el Código Penal", en *Revista Electrónica de Ciencia Penal y Criminología*, RECOC 03-06 (2001), Universidad de Granada, Granada, 2001.

MIRÓ LLINARES, F., "Los Delitos Informáticos", en ORTIZ DE URBINA GIMENO, Í. (Coord.) y VVAA, *Memento experto. Reforma penal 2010. Ley Orgánica 5/2010*, ed. Francis Lefebvre, Madrid, 2010.

MIRÓ LLINARES, F., "La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phising", *Revista Electrónica de Ciencia Penal y Criminología*, 15-12 (2013), Universidad de Granada, Granada, 2013.

MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento Penal*, ed. Francis Lefebvre, Madrid, 2017.

MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento Penal*, ed. Francis Lefebvre, Madrid, 2022.

MORÓN LERMA, E., *Internet y Derecho Penal: <<Hacking>> y otras conductas ilícitas en la red,* ed. Aranzadi, segunda edición, Navarra, 2002.

MUÑOZ CONDE, F. y GARCÍA ARÁN, M., *Derecho Penal. Parte General*, ed. Tirant lo Blanch, 9ª edición, Valencia, 2015.

ORTIZ DE URBINA GIMENO, Í. (Coord.) y VVAA, *Memento experto. Reforma penal 2010. Ley Orgánica 5/2010*, ed. Francis Lefebvre, Madrid, 2010.

ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal*, *parte general*, ed. Tirant Lo Blanch, Valencia, 2016.

PASTOR MUÑOZ, N., *La determinación del engaño típico en el delito de estafa*, ed. Marcial Pons, Madrid, 2004.

PÉREZ GIL, J. (Coord.) y VVAA, *El proceso penal en la sociedad de la información*, ed. La Ley, Madrid, 2012.

QUERALT JIMÉNEZ, J. J., *Derecho penal español. Parte especial*, ed. Tirant lo Blanch, primera edición, Valencia, 2015.

QUINTERO OLIVARES (Dir.) y VVAA, *Comentarios a la parte especial del Derecho penal*, ed. Aranzadi, Navarra, 2016.

QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general del Derecho penal,* ed. Aranzadi, Navarra, 5ª edición, 2015.

RAGUÉS I VALLÈS, R., "Sobre la doctrina de la ignorancia deliberada en Derecho penal", *Revista Discusiones*, nº 13, 2, 2013, Universidad Nacional del Sur, Bahía Blanca (Argentina), 2013

RAGUÉS I VALLÈS, R., "La teoría de la ignorancia deliberada", *Amachaq*, nº 2, ed. Amachaq escuela jurídica, Lima (Perú), 2021.

RODRÍGUEZ MOURULLO, G., "Delito imposible y tentativa de delito en el Código penal español", *Anuario de derecho penal y ciencias penales*, Tomo 24, Fasc/Mes 2, Ministerio de Justicia, Madrid, 1971.

RODRÍGUEZ RAMOS, L. (Dir.) y VVAA, *Código Penal. Concordado y comentado con jurisprudencia y leyes penales especiales y complementarias*, ed. La Ley, quinta edición, Madrid, 2015.

ROSO CAÑADILLAS, R., "Algunas reflexiones sobre los nuevos fenómenos delictivos, la teoría de delito y la ignorancia deliberada", *Revista General de Derecho Penal*, 22 (2014), ed. iustel, Madrid, 2014.

ROXIN, C., *Autoría y dominio del hecho en Derecho penal*, ed. Marcial Pons, Barcelona, traducido por CUELLO CONTRERAS, J., y SERRANO GONZÁLEZ DE MURILLO, J.L., 2000.

SÁNCHEZ MAGRO, A., "El ciberdelito y sus implicaciones procesales", en GARCÍA MEXÍA, P. (Dir.), y VVAA. *Principios de Derecho de Internet*, ed. Tirant Lo Blanch, Valencia, 2005.

SUÁREZ-MIRA RODRÍGUEZ, C., JUDEL PRIETO, Á., y PIÑOL RODRÍGUEZ, J.R., "Las estafas", en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012.

VELASCO NÚÑEZ, E., "Tipos delictivos", en VELASCO NÚÑEZ, E., y SANCHIS CRESPO, C., *Delincuencia informática*, ed. Tirant lo blanch, Valencia 2019.

VELASCO NÚÑEZ, E., y SANCHIS CRESPO, C., *Delincuencia informática*, ed. Tirant lo blanch, Valencia 2019.

WELZEL, H., *Estudios de Derecho penal*, ed. B de F, reimpresión, traducido por EDUARDO ABOSO, G., y LOW, T., Buenos Aires, 2007.

OTRAS FUENTES

BIZUM, "¿Aún no sabes qué es Bizum y cómo funciona?", en *Bizum*, Madrid, 2022, disponible en https://bizum.es/como-funciona/, consultado el 13 de junio de 2022.

CYBERARK, "Cyberark global advanced threat landscape report 2018", en *Ciberark Report*, Boston, 2018, disponible en https://www.cyberark.com/resources/white-papers/cyberark-global-advanced-threat-landscape-report-2018-the-cyber-security-inertia-putting-organizations-at-risk, consultado el 14 de junio de 2022.

GAVRAILOVA, G., "¿Qué es el phising?", en *Mailjet by sinch*, 10 de diciembre de 2019, disponible en https://www.mailjet.com/es/blog/entregabilidad/que-es-phishing/#tipos , consultado el 18 de junio de 2022.

INTERPOL, "Social engineering fraud", en *INTERPOL Connecting Police for a safer world*, 2017, disponible en https://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud, consultado el 1 de diciembre de 2017.

MADRIGAL MARTÍNEZ-PEREDA, C., *Memoria elevada al Gobierno de S.M. Presentada al inicio del año judicial por la Fiscalía General del Estado*, Centro de Estudios Jurídicos, Madrid, 2016, disponible en https://www.fiscal.es/memorias/memoria2016/FISCALIA_SITE/recursos/pdf/MEMFIS16.pdf, consultado en fecha 13 de junio de 2022.

OCDE, *Computer-related criminality: Analysis of Legal Politics in the OECD Area*, París, 1986, p. 69-70, reimpreso en UNITED NATIONS, "United Nations Manual on the Prevention and Control of Computer-Related Crime", *International Review of Criminal Policy*, Nos. 43 and 44, Viena, 1994, disponible en https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF, consultado el 14 de junio de 2022.

THE FBI FEDERAL BUERAU OF INVESTIGATION, “Online auction fraud – don’t let it happen to you”, en *Stories*, junio 2009, disponible en https://archives.fbi.gov/archives/news/stories/2009/june/auctionfraud_063009, consultado el 26 de junio de 2022.