LA RESPONSABILIDAD CIVIL DE LOS BANCOS EN LOS DELITOS DE ESTAFA POR "PHISHING"

THE CIVIL LIABILITY OF BANKS IN THE CRIMES OF FRAUD BY "PHISHING"

Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, pp. 1788-1809

María José
CALVO SAN
JOSÉ

ARTÍCULO RECIBIDO: 14 de octubre de 2022
ARTÍCULO APROBADO: 5 de diciembre de 2022

RESUMEN: Internet ha supuesto un gran avance en el mundo de las nuevas tecnologías, convirtiéndose, a su vez, en un nuevo instrumento para la comisión de delitos, valiéndose de los diferentes medios electrónicos e informáticos existentes. En la comisión de esos delitos informáticos, los ciberdelincuentes utilizan diversas técnicas para estafar a sus víctimas, como el "phishing", el "smishing" y el "vishing", entre otras muchas, con el objetivo de robar su dinero o acceder a información que almacenan en sus dispositivos; y con el problema añadido de que la víctima va a encontrar notables dificultades para perseguir al delincuente. Cuando esto sucede, es importante saber cuáles son los instrumentos de defensa a disposición de los particulares en caso de ser víctimas, y cuál es la responsabilidad que asumen las entidades bancarias frente a este nuevo tipo de delito informático. Cuestiones que serán objeto de análisis en este trabajo.

PALABRAS CLAVE: Delitos informáticos; phishing; responsabilidad civil.

ABSTRACT: *The Internet has been a great advance in the world of new technologies, becoming, in turn, a new instrument for the commission of crimes using the different existing electronic and computer means. In the commission of these computer crimes, cybercriminals use various techniques to defraud their victims, such as "phishing", "smishing" and "vishing", among many others, with the aim of stealing our money or accessing valuable information that we store on devices; and with the added problem that the victim will encounter notable difficulties in pursuing the offender. When this happens, it is important to know what are the defense instruments available to individuals in case of being victims and what is the responsibility assumed by banks in the face of this new type of computer crime. Issues that will be the subject of analysis in this work.*

KEY WORDS: *Computer crime; phishing; civil liability..*

SUMARIO.- I. INTRODUCCIÓN. - II. EL "PHISHING" COMO DELITO DE ESTAFA INFORMÁTICA. - III. INSTRUMENTOS DE DEFENSA A DISPOSICIÓN DE LOS PARTICULARES. - IV. RESPONSABILIDAD CIVIL DE LAS ENTIDADES BANCARIAS POR "PHISHING".

I. INTRODUCCIÓN.

La creciente digitalización de los servicios bancarios ha provocado un aumento significativo de los delitos de estafa bancaria, ejecutados mediante la utilización de las nuevas tecnologías (TIC). A estos efectos, Internet ha supuesto un increíble avance, convirtiéndose en un nuevo instrumento para la comisión de delitos.

Los ciberdelincuentes valiéndose de alguna manipulación informática o artificio semejante, como el "phishing" (correos electrónicos con enlaces o documentos que, una vez abiertos, infectan el dispositivo electrónico), el "vishing" (llamadas telefónicas que suplantan la identidad de la entidad financiera) o el "smishing" (en la línea de los anteriores, pero en este caso los ciberdelincuentes utilizan SMS o números de teléfono de las entidades financieras), se hacen pasar por las entidades financieras, o incluso por organismos públicos o empresas de reconocida trayectoria, suplantando su identidad y pidiendo a las potenciales víctimas que faciliten determinados datos personales y bancarios, bajo diferentes pretextos, como evitar el supuesto bloqueo de la cuenta o de una tarjeta, o prevenir un inexistente pago fraudulento, y con el verdadero fin de lucrarse, realizando operaciones de pago a cargo de la víctima. De esta forma, acceden a las cuentas bancarias del usuario a fin de sustraerle su activo patrimonial. Además, se suelen producir situaciones en las que el estafador solicita, en nombre del usuario, un crédito instantáneo que le permite sustraer más capital del que dispone el usuario estafado[1].

En muchas ocasiones, junto a dichos ciberataques, los delincuentes duplican la tarjeta SIM del móvil, de forma que, además de suplantar la identidad, consiguen también recibir los mensajes de seguridad de las entidades bancarias.

El problema que se plantea en este tipo de delitos es que la víctima va a encontrar notables dificultades para perseguir al delincuente y en muchos casos la identidad de éste nunca llega a averiguarse, razón por la cual la alternativa más viable y garantista es reclamar a la entidad bancaria la devolución de todas las

1 Barbero Bajo, J.: "Phishing y otros delitos informáticos: el uso ilícito de Internet", *Revista Lex nova*, 2008, núm. 53, pp. 6-10.

• María José Calvo San José
Profesora de Derecho Civil, Universidad de Salamanca
calvo@usal.es

cantidades apropiadas por el delincuente, al tratarse de entidades perfectamente identificables y solventes. Circunstancia que nos lleva a analizar la responsabilidad que asumen las entidades bancarias frente a este tipo de delitos informáticos.

II. EL "PHISHING" COMO DELITO DE ESTAFA INFORMÁTICA.

Desde el punto de vista penal, con fundamento en el artículo 248.2 del Código Penal (en adelante C.P.), estamos ante un delito de estafa cibernética con manipulación informática[2], sancionado con la pena de prisión de seis meses a 3 años. Y, si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses.

Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción (art. 249.1 C.P.).

El "delito informático", como tal, no ha sido introducido por la LO 1/2015, de 30 de marzo[3], como acabamos de apuntar, se trata más bien de un delito de estafa que se comete empleando los diferentes medios electrónicos e informáticos existentes. Esta Ley Orgánica, se elaboró respondiendo a la normativa europea reguladora de la delincuencia informática, llevando a cabo la transposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos, cuando no se trata de una comunicación personal.

Así, como recoge el Preámbulo de la citada Ley Orgánica, de acuerdo con la Directiva europea, con ella se introduce una separación clara entre los supuestos de revelación de datos que afectan a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad, pero que no se refieren a la intimidad personal; se tipifica la facilitación o producción de programas informáticos

diseñados para la comisión de delitos de este tipo; y se prevé la responsabilidad de las personas jurídicas.

2 Así lo manifiesta la STS 25 octubre 2012 (VLEX-414692206) al considera que, con carácter general, hechos de esta naturaleza, "en lo que tienen de operación concertada, con una estratégica distribución de roles para lograr un acto de despojo patrimonial mediante un engaño, valiéndose de terceros para poder extraer esos fondos sin suscitar sospechas en la entidad bancaria y, una vez obtenidos aquéllos, colocarlos en un país que asegure la impunidad del desapoderamiento, presentan las características que son propias del delito de estafa informática al que se refiere el art. 248.2 del CP. EDL 1995/16398".

3 Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

De esta forma, nuestro Código Penal adoptó un nuevo contenido, introduciendo novedades en su articulado, con la incorporación de modificaciones y otras redacciones, al tiempo que incluye muestras de delitos informáticos, al hacer referencia al medio utilizado para la comisión de los mismos[4], por ejemplo:

- El acceso no autorizado a sistemas informáticos, artículo 197 bis.

- Los delitos informáticos relativos a la propiedad intelectual e industrial a través de la nueva redacción del artículo 270.

- La producción, venta, distribución, exhibición, e incluso su posesión, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o personas con discapacidad (art. 189).

- La inducción a la prostitución de menores por cualquier medio (art. 187).

- Las amenazas (arts. 169 y siguientes), así como las calumnias e injurias (arts. 205 y siguientes) efectuadas y difundidas a través de cualquier medio de comunicación.

- Los fraudes informáticos para cuya consecución se manipulen datos o programas (art. 248).

- El sabotaje informático, es decir, la alteración o destrucción de datos, documentos, software que se encuentran almacenados en sistemas o redes informáticas (art. 264).

- La posesión de software informático destinado a cometer delitos de falsedad, por ejemplo, falsificar contratos, el DNI, etc.

- Delito de descubrimiento y revelación de secretos a través del acceso y difusión sin consentimiento de sus respectivos titulares de datos registrados en ficheros o soportes informáticos (arts. 197 a 201).

Por otro lado, es importante tener en cuenta, a estos efectos, que el Gobierno ha aprobado en noviembre de 2021 el Anteproyecto de Ley por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para la transposición de directivas en materia de lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, así como el establecimiento de penas aplicable al abuso de mercado. El objeto de estas modificaciones es cumplir con los compromisos normativos adquiridos con la Unión Europea (UE), adaptar la

4 Berdugo Gómez de la Torre/Arroyo Zapatero y otros: *Curso de Derecho penal. Parte General*, Ediciones Experiencia, Barcelona, 2016; Muñoz Conde, F./García Arán, M.: *Derecho penal. Parte General*, Tirant lo Blanch, Valencia, 2010.

regulación a las nuevas formas de delincuencia y contribuir a la armonización de los ordenamientos jurídicos de los diferentes Estados de la UE.

El nuevo anteproyecto transpone al ordenamiento jurídico español tres directivas comunitarias. La primera es la Directiva (UE) 2019/713 sobre lucha contra el fraude y falsificación de medios de pago distintos del efectivo. Esta Directiva tiene como objetivo luchar contra la ciberdelincuencia, especialmente la que se refiere al fraude digital, y sancionar el uso fraudulento de nuevos medios de pago, en concreto, aquellos que tienen carácter digital, cuyo uso se ha ido generalizando con el desarrollo de las nuevas tecnologías. Entre los nuevos medios de pago se incluyen el uso de las aplicaciones de pago a través del teléfono móvil o el uso de las monedas virtuales. Estos nuevos medios de pago ofrecen nuevas oportunidades para el fraude, lo que obliga a actualizar la regulación de algunos delitos, concretamente los que están relacionados con la estafa y las falsificaciones[5].

La transposición de la Directiva (UE) 2019/713 conlleva reformar, fundamentalmente, los artículos 248 y 399 bis del Código Penal para garantizar la seguridad de esta economía digital y el correcto uso de los medios de pago más actuales[6].

En lo relativo a los delitos informáticos[7], cabe destacar la modificación introducida en el artículo 264 C.P. que contempla el delito de daños informáticos,

5 La Directiva viene a ser un complemento y refuerzo, en la esfera digital, de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, que fue objeto de transposición a nuestro ordenamiento mediante Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica el Código Penal, al abordar un aspecto diferente de la ciberdelincuencia. En este caso, específicamente en los artículos 197 bis y ter, se trató de la tipificación de las interferencias en los sistemas de información (no de las transmisiones personales, que ya estaban tipificadas), así como la facilitación o la producción de programas informáticos o equipos específicamente diseñados o adaptados para la comisión de estos delitos, además de los supuestos de daños informáticos en los artículos 264 a 264 ter. Vid. La Exposición de Motivos, en su apartado III, del Anteproyecto de Ley Orgánica por la que se modifican la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para la transposición de directivas en materia de lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y abuso de mercado, y la Ley Orgánica 7/2014, de 12 de noviembre, sobre intercambio de información de antecedentes penales y consideración de resoluciones judiciales penales en la Unión Europea.

6 Junto a la Directiva (UE) 2019/713 sobre lucha contra el fraude y falsificación de medios de pago distintos del efectivo, de la que acabamos de hablar por afectar directamente a la materia que estamos tratando, el nuevo Anteproyecto transpone al ordenamiento jurídico español la Directiva 2014/57 (UE) sobre transparencia financiera, que tiene como objeto luchar contra la corrupción económica, especialmente contra las prácticas contrarias a la competencia. En este caso, para cumplir plenamente con lo establecido en la Directiva, es necesario realizar, principalmente, una reforma del art. 285 del Código Penal, con el objeto de equiparar las penas previstas de todos aquellos que hacen uso de la información privilegiada, con independencia de que ostenten un determinado cargo o ejerzan una determinada profesión. Finalmente, la tercera transposición es la de la Directiva (UE) 2019/884 respecto al intercambio de información de antecedentes penales de nacionales de terceros países.

7 El Convenio sobre la Ciberdelincuencia, celebrado en Budapest el 23 de noviembre de 2001, recoge en su artículo 1, conceptos básicos en el ámbito del delito informático. "A los efectos del presente Convenio:
a) Por «sistema informático» se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;
b) por «datos informáticos» se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

así como la incorporación a la norma penal del artículo 264 quater, con el fin de regular específicamente la pena en ese delito si el responsable es una persona jurídica[8].

En la comisión de esos delitos informáticos, los ciberdelincuentes se valen de diversas técnicas de estafa como el "phishing", "smishing" y "vishing", entre otras muchas, con el objetivo de robar el dinero de sus víctimas o acceder a la información que almacenan en sus dispositivos.

Así, tal y como señala la Sentencia de la Audiencia Nacional, 25 marzo 2020[9], "el "phishing bancario" es una modalidad de estafa que consiste en el envío de un enlace (aparentemente genuino, pero, en realidad, malicioso), normalmente de una entidad bancaria, al correo electrónico o al teléfono móvil, de manera que, cuando el receptor pincha sobre el mismo, cree estar en la página oficial por lo que, al poner las claves personales de acceso, las mismas son extraídas y utilizadas con posterioridad para realizar transferencias no consentidas. En realidad, se trata de un e-mail diseñado por el defraudador para engañar al cliente bancario y obtener, mediante esa solicitud de información, los datos necesarios para ingresar en su cuenta bancaria y transferir fondos"[10].

Con lo cual, el defraudador, denominado "phisher", suplanta la identidad del Banco para conseguir, mediante engaño, información confidencial del cliente bancario. Esta información puede consistir en las claves de acceso a las cuentas bancarias online, datos de la tarjeta de crédito, claves de firma bancaria, etc. que utiliza para sustraerle, antijurídicamente, su activo patrimonial[11].

---

c) por «proveedor de servicios» se entenderá:
i) Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y
ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;
d) por «datos sobre el tráfico» se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente".

8 Gutiérrez Mayo, E.: *Delitos informáticos. Análisis detallado de las conductas delictivas más comunes en el entorno informático*, (coord. por E. Gutiérrez Mayo), Colex, A Coruña, 2021, pp. 23-43.

9 SAN, 25 marzo 2020 (RAJ 2020, 1466).

10 Así mismo, la SAP de Madrid 24 enero 2018 (RAJ 2018, 513), expresa que el "phishing" por e-mail fraudulento, "se basa en el envío de correos electrónicos que, aparentando provenir de fuentes fiables, obtienen o intentan obtener datos confidenciales del usuario como sus claves bancarias, las que posteriormente se utilizan para la realización de la estafa, es decir: para acceder a su cuenta corriente y efectuar trasferencias de dinero dirigidas a un beneficiario, autor directo o colaborador necesario del fraude". Y, la SAP de Valladolid 21 junio 2010 (RAJ 2010, 263), explica su objetivo aclarando "que, mediante una manipulación informática, se efectúe una transferencia no consentida de activos en perjuicio de un tercero". Teniendo como particularidad que "en este caso, el acto de disposición patrimonial no se realiza por la víctima del engaño, sino por el propio autor, a través del sistema, por lo que la transferencia debe ser no consentida".

11 Como manifiesta la SAP de Madrid 2 junio 2020 (RAJ 2020, 4742), "La conducta de todos los acusados que resultaron condenados en la sentencia del Juzgado de lo Penal se enmarca en una técnica delictiva defraudatoria, consecuencia del desarrollo de las tecnologías y del manejo de la banca y del comercio electrónico, conocida con el nombre "phishing" y que consiste: o bien en el envío masivo a los usuarios

Cuando esto sucede, es importante saber quién debe asumir el riesgo de pérdida del dinero; cuáles son los instrumentos de defensa de que disponen los particulares en caso de ser víctimas, y cuál es la responsabilidad que asumen las entidades bancarias frente a este nuevo tipo de delito informático.

III. INSTRUMENTOS DE DEFENSA A DISPOSICIÓN DE LOS PARTICULARES.

Ante situaciones como la descrita, lo recomendable es acudir a la Policía Nacional para interponer la pertinente denuncia, así como ponernos en contacto con nuestra entidad bancaria para informar de lo ocurrido: que se han realizado pagos y/o transferencias desde nuestra cuenta sin autorización, pues el banco, como depositario de nuestro dinero tiene la obligación de contar con todas las medidas de seguridad para que esto no ocurra y, por tanto, reintegrarnos el dinero sustraído, siempre y cuando no haya existido culpa o negligencia por nuestra parte, extremo que deberá acreditar el Banco.

Para recuperar el dinero perdido por "phishing" se puede: a) iniciar un procedimiento penal mediante denuncia o querella contra el supuesto delincuente, b) o iniciar una reclamación civil contra la entidad financiera por incumplir sus obligaciones de vigilancia debida ("culpa in vigilando"), conforme a lo establecido en la normativa de servicios de pago.

En los supuestos en que la víctima no haya incurrido en negligencia grave en su obligación de preservar secretas sus credenciales, conforme establece el artículo 41 del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en adelante, RDL 19/2018)[12], cabrá acción

de mensajes de correo electrónico, SMS (smishing) o llamadas telefónicas (vishing) en los que los autores, haciéndose pasar por empresas o fuentes fiables, especialmente por entidades bancarias, y alegando supuestas razones de seguridad, solicitan de tales usuarios las contraseñas o datos confidenciales necesarios para operar telemáticamente en las webs bancarias, o les solicitan que pinchen en algún enlace que les redirecciona a una página idéntica a la oficial de dichas entidades donde los usuarios introducen tales datos; o bien les introducen virus informáticos capaces de apoderarse de tales claves (pharming). En definitiva, por todas estas vías los autores de la defraudación o estafa informática consiguen conocer las contraseñas y claves secretas de acceso de los usuarios a sus cuentas corrientes, y, por lo tanto, acceder ellos mismos a las cuentas, suplantando la identidad de su titular, y ordenar transferencias de sus activos que luego tienen que ser redirigidos para evitar su seguimiento y localización". De lo que se desprende que, es posible distinguir tres fases en el delito de estafa por "phishing": una primera, de descubrimiento de las claves y contraseñas; una segunda, de acceso a las cuentas y la realización de transferencias de activos; y una tercera, que consiste en el apoderamiento efectivo de los activos y en el desarrollo de un sistema que impida su localización mediante plataformas que dificultan el rastreo del dinero.

12 Este Real Decreto-ley 19/2018, de 23 de noviembre, derogó la Ley 16/2009, e incorporó parcialmente a nuestro ordenamiento jurídico el marco europeo creado por la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/ CE, en sustitución de la del 2007, junto al Reglamento (UE) 2015/751 del Parlamento Europeo y del Consejo, de 29 de abril de 2015. Esta nueva norma, actualmente en vigor, asumió como principales objetivos facilitar y mejorar la seguridad en el uso de sistemas de pago a través de internet, reforzar el nivel de protección al usuario contra fraudes y abusos potenciales, respecto del previsto en la Ley 16/2009, de 13 de noviembre, así como promover la innovación en los servicios de pago a través del móvil y de internet. En la misma línea de proteger al consumidor del servicio, exige

contra la entidad de servicios de pagos dada su responsabilidad cuasi-objetiva que establece el citado Real Decreto-ley. Esto significa que la responsabilidad se imputa de forma directa al banco con independencia de si la entidad ha incurrido en culpa o dolo, quedando exonerado únicamente en los casos de fuerza mayor o culpa exclusiva del perjudicado.

Concretamente, el artículo 45 del Real Decreto-ley 19/2018 establece lo siguiente:

"(…) en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada".

Sin embargo, esa "inmediatez" que proclama la normativa en la devolución de las cantidades defraudadas, en la práctica, brilla por su ausencia, pues en la mayor parte de los casos los clientes han de esperar meses para poder recuperar lo defraudado, e incluso en muchos casos ven como su reclamación es rechazada totalmente al considerarse al titular de la tarjeta como único responsable, por incumplimiento de sus obligaciones de conservación y custodia del medio de pago y del número secreto.

Hablamos de asuntos que tendrán que dirimirse en la vía judicial, donde habrán de valorarse las circunstancias del caso en concreto. Y ello por cuanto tras esa negativa de la entidad bancaria, la vía del Banco de España difícilmente será de utilidad, pues cuando, de una u otra forma, el reclamante reconoce que permitió que un tercero accediese a sus claves, aunque inicialmente lo hiciera en la creencia de que ese tercero representaba al banco, el Banco de España no emitirá pronunciamiento alguno, remitiéndose a los Tribunales de Justicia.

En el supuesto de que la víctima hubiera actuado de forma negligente en la obligación que pesa sobre ella de preservar sus claves privadas, la entidad de servicios de pago queda exonerada de responsabilidad al quebrarse la relación

ahora sistemas de autenticación reforzada, y reproduce un sistema similar de responsabilidad a cargo del proveedor del servicio, que solo cede, en caso de actuación fraudulenta o del incumplimiento, deliberado o por negligencia grave; que lo será solo en caso de actuación fraudulenta, cuando el proveedor no ha establecido el sistema de autenticación reforzada.

de causalidad por culpa de la víctima (artículo 46.1.II del RDL 19/2018). Por tanto, en este último caso, únicamente podrá accionarse contra el delincuente en la vía penal.

El ejercicio de una acción u otra o, de ambas a la vez, dependerá de las circunstancias de cada caso. En este sentido, el art. 116.1 del Código Penal establece que "toda persona criminalmente responsable de un delito lo es también civilmente si del hecho se derivaren daños o perjuicios". Al mismo tiempo, en su artículo 120. 3.º admite la responsabilidad civil subsidiaria de la entidad bancaria al disponer que: "Son también responsables civilmente, en defecto de los que lo sean criminalmente: 3.º Las personas naturales o jurídicas, en los casos de delitos cometidos en los establecimientos de los que sean titulares, cuando por parte de los que los dirijan o administren, o de sus dependientes o empleados, se hayan infringido los reglamentos de policía o las disposiciones de la autoridad que estén relacionados con el hecho punible cometido, de modo que éste no se hubiera producido sin dicha infracción". La responsabilidad civil subsidiaria a que hace referencia el artículo 120.3 del C.P. parte necesariamente del reconocimiento judicial de haberse cometido un delito generador de un daño, ya sea a título de dolo o de culpa. La sentencia penal incorporará un dictado de condena indemnizatoria a cargo del acusado, primer y directo responsable civil (art. 116 C.P.).

De esta forma, como ha manifestado de manera reiterada la Sala de lo Penal del Tribunal Supremo con ocasión de aplicar el artículo 120.3 del C.P., no nos movemos aquí en el marco específico del derecho penal, sino precisamente en el del derecho civil resarcitorio de los perjuicios derivados de la infracción penal cometida. Se ejercita así una acción distinta, aunque acumulada al proceso penal por razones de utilidad y economía procesales, con la finalidad de satisfacer los legítimos derechos (civiles) de las víctimas; de modo que, las acciones civiles no pierden su naturaleza propia por el hecho de ejercitarse ante la jurisdicción penal. Y ello hasta el punto de llegar a una cuasi-objetivación basada en la teoría del riesgo, o bien del aprovechamiento de la actividad que lo genera ("cuius commoda eius incommoda"). Teoría del riesgo que, aunque no permita hablar en sentido estricto de que en esta esfera impere un criterio de absoluta responsabilidad objetiva, sí puede decirse que prima o prevalece un criterio de "ponderado objetivismo"[13]. Lo que nos está poniendo de manifiesto que, las acciones civiles no pierden su naturaleza propia por el hecho de ejercitarse ante la jurisdicción penal. Ello da entrada a la analogía como criterio de interpretación, que si bien está vedado cuando se trata de normas penales, no ocurre lo mismo en relación a las de naturaleza civil.

13 Vid.: SSTS 4 abril 2010 (RAJ 2010, 108); 29 abril 2013 (RAJ 2013, 357); 11 febrero 2014 (RAJ 2014, 64); 18 noviembre 2015 (RAJ 2015, 778); 12 febrero 2020 (RAJ 2020, 49).

Sin embargo, en este tipo de delitos o fraudes digitales, la víctima va a encontrar notables dificultades para perseguir al delincuente y en muchos casos la identidad de éste nunca llega a averiguarse, razón por la cual, dada la dificultad de identificar al autor del delito de estafa bancaria y de poder resarcir el daño, la alternativa más viable y garantista es reclamar a la entidad bancaria la devolución de todas las cantidades apropiadas por parte del delincuente. El Banco es una entidad perfectamente identificable y solvente, consiguiendo mediante la oportuna reclamación una fórmula más directa para recuperar el dinero.

En ningún caso pueden emprenderse acciones legales de forma acumulada tanto frente al delincuente como frente al Banco, es decir, no podremos reclamar el reembolso de la cantidad defraudada al estafador, y a su vez solicitar la entrega de esa misma cantidad a la entidad bancaria.

Pero sí es posible perseguir la responsabilidad penal del estafador por vía penal, y reclamar a la vez la responsabilidad civil y entrega de importes a la entidad bancaria frente a los Juzgados de Primera Instancia.

IV. RESPONSABILIDAD CIVIL SUBSIDIARIA DE LA ENTIDAD BANCARIA POR "PHISHING".

La responsabilidad civil puede definirse como la obligación de reparar los daños y/o perjuicios causados a una persona o grupo de personas. Dicho daño puede ser provocado:

A) por un incumplimiento contractual (responsabilidad contractual), como sucede en el caso que nos ocupa, la base de esta responsabilidad deriva del hecho de que las entidades bancarias, como depositarias y custodias del dinero de sus clientes, tienen que velar porque las transferencias se hagan correctamente y siempre autorizadas por los titulares (del mismo modo que hay una responsabilidad también de las entidades bancarias en los casos de pago de cheques falsos).

B) o por la ocurrencia de un hecho lesivo sin vínculo contractual previo (responsabilidad extracontractual). La obligación de repararlo abarca tanto la reparación "in natura" (colocando al perjudicado en la situación inmediatamente anterior al hecho lesivo) o por equivalente monetario, que generalmente se refiere al pago de una indemnización por daños y perjuicios[14].

Al mismo tiempo, el Código Civil en el artículo 1089, especifica que las obligaciones "nacen de la ley, de los contratos, y cuasicontratos, y de los actos y

14 Santos Briz, J.: *La responsabilidad civil. Temas actuales*. Montecorvo, Madrid, 2001; Reglero Campos, F.: "Los sistemas de responsabilidad civil", *Tratado de responsabilidad civil*, (coord. por F. REGLERO CAMPOS, Thomson Aranzadi, Cizur Menor, 2008, pp. 247-300.

omisiones ilícitos o en que intervenga cualquier género de culpa o negligencia"; en cuyo caso cabe distinguir, en esta última categoría, el acto u omisión ilícito penal y el ilícito civil que se regulan por normas distintas; este último en el art. 1902 del CC y, por el contrario, las acciones que nacen del ilícito penal se han de regir por el Código y las disposiciones especiales que regulan el derecho punitivo, de las que el CC será solo supletorio en virtud de lo dispuesto en el art. 1092 CC[15]. De lo que se deduce que "las resoluciones dictadas por los tribunales de lo penal, no producen la excepción de cosa juzgada en el orden civil". La extinción de la acción penal no lleva consigo la de la civil, a no ser que la extinción proceda de haberse declarado por sentencia firme que no existió el hecho del que la acción civil hubiere podido nacer[16].

Por otro lado, la (STS 19 junio 1984)[17] declara que, para que opere la responsabilidad contractual con exclusión de la aquiliana (extracontractual), "no basta con que haya un contrato (o una preexistente relación de otra naturaleza) entre las partes, sino que se requiere para ello que la realización del hecho dañoso acaezca dentro de la rigurosa órbita de lo pactado", por lo que, es posible "la concurrencia de ambas clases de responsabilidad en yuxtaposición, "sin otro límite que la indemnidad del patrimonio económico"[18].

Si bien, la responsabilidad contractual y la extracontractual tienen su punto de arranque en la existencia o no de una relación negocial, con puntos de coincidencia comunes como son la producción de un daño o lesión[19], imputabilidad del mismo a un sujeto, y deber de indemnizar o resarcir; tienen sus diferencias en que mientras que la contractual nace como consecuencia del incumplimiento o infracción de los términos de un negocio, la extracontractual tiene su origen en un ilícito civil productor del daño, al margen o además de todo incumplimiento o infracción, todo lo cual determina que en ambas clases de culpa su finalidad sea reparadora, sin perjuicio de las específicas que puedan derivar del incumplimiento del contrato[20].

15 Pasquau Liaño, M.: "Art. 1902", *Comentarios al Código Civil*, (dir. R. Bergovitz Cano), Tirant lo Blanch, Valencia, 2013.

16 STS 25 noviembre 1974 (RAJ 1974, 261).

17 STS 19 junio 1984 (RAJ 1984, 3250).

18 STS 2 enero 1990 (RAJ 1990, 30). En igual sentido la STS 10 junio 1991 (RAJ 1991, 4434).

19 La delimitación de los daños contractuales, con claros precedentes en el derecho romano, es un criterio que se ha sostenido hasta los instrumentos europeos de unificación más modernos, entre los que cabe mencionar los Principios Europeos de Derecho de Contratos, art. 9:503; el Marco Común de Referencia para el Derecho Privado Europeo, DCFR, III. 3:703; en los Principios Latinoamericanos de Derecho de Contratos, PLDC, art. 107. En el Common Law, también se indemnizan, como daños, por regla general, las pérdidas económicas derivadas del incumplimiento, con fundamento en la denominada confianza esencial. Vid. Martín Casals, M.: "Reflexiones sobre la elaboración de unos "Principios europeos de responsabilidad civil", Ponencia presentada en el 2º Congreso de la Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguro, Granada, disponible en www.asociacionabogadosrcs.org/ponencias/pon2-7.pdf (fc: 01.09.2014).

20 Martín Casals, M.: "Art. 1902", *Comentarios al Código Civil* (dir. A. Domínguez Luelmo), *Lex Nova,* Valladolid, 2010, pp. 2046- 2055.

En este contexto, es importante señalar que, las acciones de reintegración del dinero sustraído ilícitamente contra las entidades financieras de servicios de pago, requieren la concurrencia simultanea de tres requisitos:

a) que la operación de pago no haya sido autorizada por la víctima. La existencia de una operación no autorizada se producirá siempre en los casos de "phishing", ya que, el usuario de los servicios de pago no es la persona que emite el consentimiento. En estos casos, el usuario cede las claves privadas inconscientemente al delincuente ante una apariencia errónea de profesionalidad de los medios telemáticos utilizados para que éstos, en contra de su voluntad, utilicen los instrumentos de pago.

b) la existencia de un daño, el cual se traduce en el montante total sustraído por los delincuentes del delito de "phishing".

c) que exista relación de causalidad entre la conducta (acción u omisión) y el daño producido. El legislador ha establecido una imputación de responsabilidad cuasi-objetiva a los proveedores de servicios de pago haciéndolos responsables siempre y cuando no quiebre la relación de causalidad por existencia de diligencia cualificada en las obligaciones del proveedor de servicios de pago o culpa de la víctima por negligencia grave o fraude. La diligencia cualificada en las operaciones no autorizadas consiste en la obligación de proporcionar al usuario mecanismos de seguridad acordes para garantizar la seguridad y privacidad de las credenciales privadas (artículo 42.1.a) del RDL 19/2018)[21].

La única posibilidad que existe para que quiebre la relación de causalidad por culpa de la víctima se contempla en el artículo 46 del Real Decreto-ley. Dicho artículo descarga la responsabilidad del proveedor de servicios de pagos cuando la víctima haya actuado con fraude o negligencia grave en sus obligaciones de conservar sus claves privadas derivadas de la obligación establecida en el artículo 41.b) del citado cuerpo legal.

Por tanto, salvo que se den las circunstancias anteriores, existen motivos suficientes para concluir la responsabilidad civil que en este caso incumbe a la

21 Así queda expresado en la STS 12 febrero 2020 (RAJ 2020, 49), en ella el Alto Tribunal recoge los motivos por los cuales la entidad financiera es responsable civil subsidiaria. Considera que, "la actividad propuesta por la entidad bancaria a sus clientes mediante la operativa online presenta algunos riesgos derivados de la posibilidad de suplantación de la identidad de quien contrata con la entidad para la realización de operaciones sin la autorización del auténtico contratante". Al mismo tiempo, reconoce que "excluyendo actuaciones dolosas o gravemente negligentes por parte de los clientes, la entidad bancaria es responsable de ofrecer y poner en práctica un sistema seguro, de manera que las consecuencias negativas de los fallos en el mismo no deberán ser trasladados al cliente. Todo ello con independencia de la determinación de quien sea el auténtico perjudicado en estos casos, en atención a la correcta interpretación de los preceptos que regulan esta clase de depósitos». Doctrina plenamente aplicable al supuesto que ahora nos ocupa. Los deberes de seguridad que los bancos deben observar para llegar a consolidar un espacio seguro de actuación, han tenido su reflejo legal armonizando nuestro ordenamiento interno con la normativa europea sobre la materia.

entidad bancaria, a partir del deber objetivo de cuidado que la normativa específica impone a las mismas, como proveedoras de servicios de pago, descartando causas de exclusión de su responsabilidad[22].

La ventaja que tiene la víctima es que, es el proveedor de servicios de pago quien deberá demostrar que el titular de las cuentas y tarjetas de servicios de pagos ha actuado con negligencia o fraude (art. 44.1 y 3 del RDL 19/2018). Por tanto, existe una presunción "iuris tantum" de que la víctima ha cumplido con sus obligaciones legales de mantenimiento de las credenciales, salvo que el proveedor de los servicios de pago demuestre lo contrario.

De esta forma, cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago. Y, será el Banco quien tenga que probar que el usuario del servicio de pago cometió fraude o negligencia grave.

Por otro lado señalar que, si bien es cierto que los servicios que ofrecen las entidades bancarias se presumen seguros y confiables, sin embargo, actos de esta naturaleza está poniendo de manifiesto la ineficacia de los servicios informáticos de estas entidades a la hora de evitar actos fraudulentos, en el sentido de permitir o de rechazar movimientos dinerarios a requerimiento de clientes (reales o aparentes), lo que invita a reflexionar sobre el deber de diligencia que pesa sobre las mismas[23].

Ese deber de diligencia "conecta tanto con la confianza del cliente en la adecuada defensa de sus intereses y derechos, como en el hecho de que la ejecución de las operaciones suele quedar encomendada a la entidad en la mayor parte de las ocasiones. De ahí que, cualquier anomalía que determine un perjuicio para el consumidor motivado por un mal funcionamiento del sistema determinará una responsabilidad propia de la entidad emisora, sin que deba admitirse la limitación o exoneración de esa responsabilidad por la vía de las condiciones generales aplicables"[24].

22 STS 12 febrero 2020 (RAJ 2020, 49), Ponente: Excma. Sra. D.ª Ana María Ferrer García: https://www.poderjudicial.es/search/TS/openDocument/66911d985804 1ff4/20200217

23 Sánchez-Calero Guilarte, J.: "Tarjeta de crédito y tutela del consumidor", *Nuevas formas contractuales y el incremento del endeudamiento familiar, Revista de Derecho Bancario y Bursátil,* 2005, núm. 98, pp. 83-120; Gómez Mendoza, M.: "Cancelación de una tarjeta de crédito sin justa causa", *Revista de Derecho Bancario y Bursátil,* núm. 57, 1995, p. 16.

24 Nieto Carol, U.: "Contratación bancaria y condiciones generales", en AA.VV.: *Contratos bancarios y parabancarios*, Lex Nova, Valladolid, 1998, p. 204 y ss.; Montés Rodríguez, M.P.: "Las condiciones generales de los contratos bancarios y la protección de los consumidores y usuarios", *Estudios sobre jurisprudencia*

Cuando una entidad bancaria presta un servicio de banca online tiene la obligación de dotarse de las medidas suficientes que garanticen al usuario la seguridad de las operaciones. Por este motivo, si hay una omisión, insuficiencia o funcionamiento defectuoso de estas medidas, tienen que ser las propias entidades bancarias las que asuman las consecuencias derivadas del fallo del sistema de seguridad. Teniendo en cuenta que, los sistemas de verificación de autenticidad de las operaciones se diseñan y se establecen por parte de las entidades bancarias, si un banco no ha sido capaz de limitar el acceso de los delincuentes a su sistema no puede pretender trasladar la responsabilidad a la propia víctima[25].

Por tanto, la jurisprudencia confirma que es la entidad bancaria quien tiene la obligación de facilitar un sistema de banca telemática segura, y no son sus clientes-usuarios los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva.

Si bien es cierto que, en la práctica, cuando el usuario denuncia que ha sido víctima del "phishing", la estrategia habitual que utilizan los Bancos consiste en imputar negligencia a la propia víctima, por haberse dejado engañar y haber facilitado a los hackers los códigos de seguridad que han permitido las transferencias no consentidas, tratando así de disuadir a las víctimas de exigir la responsabilidad de la entidad bancaria y hacerlos creer que el único camino que tienen para recuperar su dinero es la incierta vía de un proceso penal, con el fin de que los delincuentes devuelvan el dinero; sin embargo, como hemos apuntado anteriormente, esto no es así, ya que, es posible por la vía civil reclamar el importe de las cantidades sustraídas, por el sistema del "phishing", a las entidades bancarias.

bancaria, (coord. por R. Marimón Durá, F. González Castilla), (dir. R. Ballarín Hernández y V. Cuñat Edo), Aranzadi, Pamplona, 2000, pp. 73-138.

25 Nuestros tribunales entienden que las entidades bancarias tienen la obligación de garantizar la seguridad de sus clientes y, por tanto, responden por los defectos de sus propios sistemas de autenticación. Por ejemplo, la AP de Valencia en su Sentencia 26 noviembre 2014 (RAJ 2014, 25), señala que: "Estimadas como no autorizadas las operaciones bancarias descritas, habrá de estarse a lo que establece el siguiente artículo 31 de la LSP (hoy artículo 45 de la Ley 19/2018) (…) por lo que, en tal perspectiva, y teniendo en cuenta las irregularidades apreciadas, es pertinente apreciar que la entidad bancaria no desplegó toda la diligencia exigible al buen comerciante en el sector del tráfico de que se trata". Y confirma la AP de Alicante en su Sentencia 12 marzo 2018, aclarando que: 1.º) El proveedor de los servicios de pago (la Entidad Bancaria) "debe implementar las medidas necesarias para asegurar la autenticación e identidad del ordenante a la hora de prestar su consentimiento. Por ello y para su ejecución, el banco debe comprobar en todo caso la autenticidad de la orden"; 2.º) "La falsedad de la transferencia (es decir, que el ordenante no sea el titular de la cuenta) es un riesgo a cargo del banco porque, en principio, el deudor sólo se libera pagando al verdadero acreedor por lo que, si el banco cumple una orden falsa, habrá de reintegrar en la cuenta correspondiente las cantidades cargadas". 3.º) "La responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse ésta autorizada al haberse realizado de acuerdo con los sistemas de autenticación del banco. Los sistemas de autenticación se establecen por los proveedores de servicios de pago y si un banco no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante víctima de esta práctica fraudulenta sea el único responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo". 4.º) "Las medidas de seguridad no solamente están destinadas a proteger la seguridad de las órdenes de pago emitidas por los clientes, sino que su eficacia exonera a las entidades de crédito de su responsabilidad frente a las órdenes de pago no emitidas por sus clientes de tal forma que el incumplimiento de este específico deber de vigilancia da lugar a una responsabilidad por "culpa invigilando" o responsabilidad objetiva por el mal funcionamiento de los servicios de banca electrónica".

Por tanto, si un banco cumple una orden de transferencia falsa (ordenada por el delincuente informático), tiene que reintegrar el importe de esta transferencia al cliente-víctima[26].

La excepción la encontraríamos en aquellos supuestos de negligencia real del usuario, muy difícil de demostrar por parte del banco. En un procedimiento civil, la carga de la prueba, es decir, quien tiene que demostrar que el cliente no ha sido diligente es el propio Banco que ha creado el riesgo y ha permitido la vulnerabilidad de su sistema de seguridad. Si el banco no es capaz de demostrar esta hipotética falta de responsabilidad del usuario será condenado a devolver las cantidades estafadas[27].

De todo lo expuesto, cabe colegir que, la jurisprudencia es unánime a la hora de considerar que el Banco debe restituir las cantidades antijurídicamente sustraídas por un tercero, en tanto que, como depositaria de los fondos tiene la obligación legal de conservar y devolver el dinero depositado[28]. Por tanto, las entidades bancarias serán responsables frente a sus clientes cuando hubiesen sido víctimas por "phishing", consiguiendo así, mediante la oportuna reclamación, una fórmula más directa para recuperar el dinero.

Únicamente se les podrá exonerar de dicha obligación cuando pudieran acreditar que el cliente ha actuado fraudulentamente o con negligencia grave a la hora de proteger sus datos personales y confidenciales, no pudiéndose considerar como negligencia o culpa haber caído en el fraude de un correo o página web aparentemente verídicos.

No obstante, según lo dispuesto en el artículo 43 del RDL 19/2018, de forma previa a la reclamación, la víctima del engaño deberá poner en conocimiento del Banco que se ha realizado una operación de pago no autorizada o ejecutada

26 Tanto la normativa europea (Directiva 2015/2366 de servicios de pago) como la estatal (Real-Decreto Ley 19/2018, de 23 de noviembre, de servicios de pago) hacen responsables a las entidades bancarias en caso de "phishing".

27 La cuestión que en ocasiones se ha planteado al respecto es si el Banco podría exonerarse de toda responsabilidad en estos casos, estableciendo en los contratos de servicios bancarios online alguna cláusula de exoneración de responsabilidad por uso fraudulento de las claves y contraseñas del cliente. Respuesta que ha de ser forzosamente negativa si tenemos en cuenta que las cláusulas de exoneración de responsabilidad fueron consideradas abusivas por la Sala de lo Civil del Tribunal Supremo en la sentencia 16 diciembre 2009, con el argumento principal de que son las entidades de crédito las que deben ser diligentes para detectar los usos indebidos de las claves de los clientes de conformidad a la experiencia y medios técnicos disponibles. Como con claridad expresaba la sentencia del Juzgado de Primera Instancia número 2 de Castellón de fecha 25 junio 2008 (FJ 6), con apoyo en la sentencia de la Audiencia Provincial de Madrid, Sección 13, 11 febrero 2005, argumentando que "no es dado imponer al consumidor la renuncia indiscriminada al derecho que le pueda asistir para reclamar frente a la entidad que le proporciona los medios técnicos necesarios para una mejor o más cómoda prestación de sus servicios, en aquellos supuestos en los que, no mereciendo la consideración de caso fortuito o fuerza mayor, así como los efectivamente imputables a la entidad bancaria, le ocasionen daños y/o perjuicios".

28 Entre otras, vid.: Sentencia del Juzgado de Primera Instancia e Instrucción nº 2 de Redondela (Pontevedra) 25 enero 2022; SAP de Pontevedra 21 diciembre 2021 (RAJ 2021, 539); SAP de Madrid, 28 febrero 2022 (RAJ 2022, 74); STS 12 febrero 2020 (RAJ 2020, 49) y, STS 30 marzo 2022 (RAJ 2022, 4883).

incorrectamente. Se entenderá que dicha comunicación se realizó de manera diligente siempre y cuando se efectuase en el plazo de trece meses desde la fecha del acto delictivo[29].

A estos efectos, el RDL 19/2018, establece una responsabilidad de la entidad bancaria "cuasi objetiva" cuando la víctima no haya dado autorización real a la transferencia del dinero. Como ya hemos señalado, la existencia de una operación no autorizada se producirá siempre en los casos de "phishing", pues el usuario de los servicios de pago no es la persona que emite el consentimiento. El usuario cede las claves privadas inconscientemente al delincuente ante una apariencia errónea de profesionalidad de los medios telemáticos utilizados para que éstos, en contra de su voluntad, utilicen los instrumentos de pago.

Esto significa que, la responsabilidad se imputa de forma directa al banco con independencia de si la entidad ha incurrido en culpa o dolo, quedando exonerado únicamente en los casos de fuerza mayor o culpa exclusiva del perjudicado. Es posible, por tanto, reclamar al Banco la devolución de todos los importes sustraídos por el estafador, más los intereses devengados.

Lo que nos está poniendo de manifiesto que la entidad bancaria depositaria de los fondos afectados tiene la obligación legal de devolver a la víctima la cantidad total que se le ha sustraído mediante las operaciones no autorizadas, salvo que expresamente acrediten que el usuario del servicio de pago cometió fraude o negligencia grave (art. art. 44.3 Ley Servicios de Pago).

Con fundamento en el precepto citado, se pronuncia el Juzgado de Primera Instancia e Instrucción nº 2 de Redondela (Pontevedra), en su Sentencia 25 enero 2022, en la cual se condena a la entidad BBVA a reintegrar al perjudicado la cantidad

29 Es importante recordar que, el 5 de abril de 2022, el Consejo de Ministros ha aprobado el anteproyecto de Ley de creación de la Autoridad Independiente de Defensa del Cliente Financiero (ADCF), que complementa el sistema de resolución de conflictos entre clientes y entidades financieras, actualmente articulado en tres niveles: los servicios de atención al cliente; los servicios de reclamaciones de los organismos supervisores; y los órganos judiciales. Este anteproyecto busca reforzar e impulsar el sistema de resolución extrajudicial de reclamaciones entre las entidades y los clientes de productos bancarios, valores y seguros, además de impulsar la educación e inclusión financiera, especialmente de colectivos vulnerables y personas mayores que deseen presentar reclamaciones. Uno de los requisitos que el anteproyecto contempla para la admisión y tramitación de las reclamaciones ante la Autoridad es la acreditación de la presentación previa ante el servicio de atención al cliente de la entidad financiera contra la que se pretenda reclamar. En consecuencia, cuando la reclamación ante el servicio de atención al cliente hubiese sido inadmitida, desestimada total o parcialmente, éste podrá presentar dicha reclamación ante la Autoridad. También podrá interponer el requerimiento cuando hubiese transcurrido el plazo de un mes desde la fecha de su presentación sin que haya sido resuelta. Cuando esta reclamación verse sobre servicios de pago, el plazo para interponer reclamación ante la Autoridad será de quince días hábiles. La carga de la prueba del cumplimiento de las obligaciones establecidas en las normas de conducta y en las buenas prácticas recaerá sobre la entidad financiera quien deberá aportar a la Autoridad la documentación precontractual y contractual relacionada con el servicio financiero objeto de reclamación. Estas reclamaciones podrán presentarse contra todas las entidades financieras que estén sujetas a la supervisión del Banco de España, de la Comisión Nacional del Mercado de Valores (CNMV) o la Dirección General de Seguros y Fondos de Pensiones (DGSFP) y entidades análogas, incluyendo las procedentes tanto de otro Estado Miembro de la Unión Europea como de un tercer país, que operen en España ejerciendo la libertad de establecimiento.

defraudada mediante la técnica de suplantación de identidad. El elemento fáctico determinante para la condena en este caso a BBVA fue la imposibilidad de ésta de demostrar que la operación fraudulenta se hubiera realizado desde la dirección IP habitual del cliente pues, tal y como se afirma en la Sentencia, "la entidad bancaria debe tener un gran nivel de diligencia y cuidado cuando la transacción se produce desde una IP (representación numérica del punto de Internet donde está conectado un dispositivo) que no es la que corresponde al cliente habitualmente, ya que, esta circunstancia es una clara señal para que salten las alarmas de la entidad bancaria antes de aceptar el movimiento bancario".

El Juzgador se basa para dictar su resolución en la dicción literal del art. 44 de la Ley de Servicios de Pago que impone una inversión legal de la carga de la prueba, debiendo ser la entidad bancaria quien demuestre "que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago". Asimismo, el perjudicado aportó a la causa los pantallazos de los mensajes fraudulentos recibidos, quedando acreditado que la página que le solicitaba las claves bancarias era exactamente igual a la página oficial de esta entidad bancaria, desmintiendo con ello cualquier atisbo de negligencia por el particular[30].

En similares términos se ha pronunciado la Audiencia Provincial de Pontevedra en su Sentencia 21 diciembre 2021, por la que se revoca la Sentencia dictada en primera instancia y se condena a ABANCA a reintegrar a la víctima de un delito de "phishing" las cantidades sustraídas pues, según se afirma, el banco no habría conseguido acreditar el cumplimiento de las obligaciones de diligencia exigibles tanto para la autentificación de las operaciones de pago como para disponer de la tecnología "antiphishing" precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas. Correlativamente, aprecia el tribunal que no puede atribuirse negligencia al usuario que introduce sus claves de acceso en una página idéntica a la oficial de la entidad bancaria, ni siquiera cuando el mensaje contenga pequeños indicadores de su origen fraudulento tales como faltas de ortografía o falta de concreción de la operación auténtica a la que supuestamente se refiere, pues según afirma el tribunal, con acierto: "En el phishing se usan técnicas de ingeniería social para ganarse la confianza del usuario del instrumento de pago

30 Igualmente, la AP de Madrid, en su Sentencia 28 febrero 2022 (RAJ 2022, 74), se ha pronunciado, condenando a BBVA al amparo de la Ley de Servicios de Pago a restituir a una sociedad mercantil las cantidades defraudadas por la vía del conocido como "fraude del CEO" que, según se afirma por el tribunal, consiste en un tipo de fraude que mezcla técnicas de ingeniería social y "phishing" para conseguir que un trabajador o empleado con acceso a las claves bancarias de la empresa (normalmente, de pequeñas dimensiones y con relación cercana entre los empleados) crea que su jefe o superior le ha pedido hacer una transferencia, envío de dinero o pago de algún tipo o, en su caso, que le ha pedido los datos bancarios de la empresa. Se afirma en este caso por la Audiencia Provincial que, atendida la naturaleza cuasi objetiva de la responsabilidad impuesta por la Ley de Servicios de Pago, únicamente la prueba de una "culpa grave" del ordenante podrá exonerar al banco de su obligación de restituir las cantidades defraudadas.

y aprovecharse de los sesgos cognitivos en la toma de decisiones, lo que, en el caso se habría concretado en la simulación del envío a nombre de una entidad de confianza para la usuaria (Correos y Telégrafos), y en el aprovechamiento del sesgo de confirmación por el cual se tiende a favorecer la información que confirma las opiniones que ya se tenían o que resulta consistente con los hechos ya conocidos".

Teniendo en cuenta todo lo expuesto, cabe concluir que, la normativa sobre servicios de pago configura un sistema de responsabilidad de las entidades bancarias cuasi objetiva, con inversión de la carga probatoria. Razón por la cual, se presume, "ex lege", la falta de autorización si el cliente lo niega. Es la entidad financiera la que debe probar que el cliente ha actuado de forma fraudulenta o con negligencia grave o, por otro lado, que el cliente no comunique a la entidad el pago no autorizado en cuanto tenga conocimiento del mismo.

En esta línea argumental, la Sección 10.ª de la Audiencia Provincial de Madrid se ha pronunciado sobre esta cuestión en la Sentencia 08 abril 2022[31], desestimando el recurso de apelación interpuesto por Banco Santander, S.A. contra la Sentencia dictada por el Juzgado de Primera Instancia e Instrucción nº 1 de Alcorcón de fecha 11 noviembre 2021. En esta resolución recurrida, el órgano judicial declaró que la entidad bancaria incumplió los deberes contractuales para con su cliente, con fundamento en los artículos 41, 44, 45 y 46 del RDL 19/2018 y, por ello, condenó a la entidad Banco Santander, S.A. a la devolución de la cantidad de 5.826,73 euros, más intereses desde la reclamación extrajudicial de dicha cantidad por parte del actor. Esta regulación conlleva que la responsabilidad se imputa de forma directa a la entidad, con independencia de si la misma ha incurrido en culpa o dolo, quedando exonerada solamente en los dos supuestos señalados anteriormente: cuando la entidad pruebe que el cliente ha actuado de manera fraudulenta o con negligencia grave o cuando el cliente no comunique a la entidad el pago no autorizado en cuanto se tenga conocimiento del mismo. A tenor de lo expuesto, la actuación de la entidad demandada ha vulnerado las buenas prácticas y usos financieros, y por falta de prueba, el Tribunal descarta que el demandante incurriera en culpa grave en el uso de su tarjeta bancaria provocando el fraude.

31 SAP de Madrid 8 abril 2022 (RAJ 2022, 199).

BIBLIOGRAFÍA

BARBERO BAJO, J.: "Phishing y otros delitos informáticos: el uso ilícito de Internet", *Revista Lex Nova*, 2008, núm. 53, pp. 6-10.

BERDUGO GÓMEZ DE LA TORRE/ ARROYO TORRE/ARROYO ZAPATERO Y OTROS: *Curso de Derecho penal. Parte General*, Ediciones Experiencia, Barcelona, 2016.

FERNANDEZ DE ARAOZ GOMEZ-ACERBO, A.: "Repensar la protección del inversor: bases para un nuevo régimen de la contratación inmobiliaria", *Diario La Ley*, 2015, núm. 8549.

FERNANDEZ DE ARAOZ GOMEZ-ACERBO, A.: "El "private enforcement" en la protección del inversor minorista: de la aplicación de la doctrina del error vicio en la contratación de productos financieros a una acción de daños específica", *Revista de Derecho Mercantil*, 2020, núm. 315.

GÓMEZ MENDOZA, M.: "Cancelación de una tarjeta de crédito sin justa causa", *Revista de Derecho Bancario y Bursátil,* 1995, núm. 57, p. 16.

GUTIÉRREZ MAYO, E.: *Delitos informáticos. Análisis detallado de las conductas delictivas más comunes en el entorno informático*, (coord. por E. GUTIÉRREZ MAYO), Colex, A Coruña, 2021, pp. 23-43.

MARTÍNEZ CASALS, M.: "Art. 1902", *Comentarios al Código Civil* (dir. A. DOMÍNGUEZ LUELMO), Lex Nova, Valladolid, 2010, pp. 2046- 2055.

MARTÍN CASALS, M.: - "Reflexiones sobre la elaboración de unos "Principios europeos de responsabilidad civil", Ponencia presentada en el 2º Congreso de la Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguro, Granada, disponible en www.asociacionabogadosrcs.org/ponencias/pon2-7.pdf (fc: 01.09.2014).

MONTÉS RODRIGUEZ, M.P.: "Las condiciones generales de los contratos bancarios y la protección de los consumidores y usuarios", *Estudios sobre jurisprudencia bancaria*, (coord. por R. MARIMÓN DURÁ, F. GONZÁLEZ CASTILLA); (dir. R. BALLARÍN HERNÁNDEZ Y V. CUÑAT EDO), Aranzadi, Pamplona, 2000, pp. 73-138.

MUÑOZ CONDE, F./GARCÍA ARÁN, M.: *Derecho penal. Parte General*., Tirant lo Blanch, Valencia, 2010.

NIETO CAROL, U.: "Contratación bancaria y condiciones generales", en AA.VV.: *Contratos bancarios y parabancarios*, Lex Nova, Valladolid, 1998, p. 204 y ss.

PASQUAU LIAÑO, M.: "Art. 1902", *Comentarios al Código Civil*, (dir. R. BERGOVITZ RODRÍGUEZ CANO), Tirant lo Blanch, Valencia, 2013.

REGLERO CAMPOS, F.: "Los sistemas de responsabilidad civil", *Tratado de responsabilidad civil*, (coord. F. REGLERO CAMPOS), Thomson Aranzadi, Cizur Menor, 2008, pp. 247-300.

SANTOS BRITZ, J.: *La responsabilidad civil. Temas actuales*. Montecorvo, Madrid, 2001.

SANCHEZ-CALERO GUILARTE, J.: "Tarjeta de crédito y tutela del consumidor", *Nuevas formas contractuales y el incremento del endeudamiento familiar, Revista de Derecho Bancario y Bursátil,* 2005, núm.98, pp. 83-120.