RESPONSABILIDAD DE LAS ENTIDADES FINANCIERAS ANTE EL HACKEO DE CUENTAS BANCARIAS. EN PARTICULAR, CASOS DE "PHISING"

FINANCIAL INSTITUTIONS LIABILITY IN CASE OF BANK ACCOUNTS HACKING. IN PARTICULAR, "PHISING" CASES

Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, pp. 1590-1617

Araya Alicia
ESTANCONA
PÉREZ

ARTÍCULO RECIBIDO: 6 de octubre de 20222
ARTÍCULO APROBADO: 5 de diciembre de 2022

RESUMEN: El control de las operaciones de pago no autorizadas ha sido objeto de especial atención en el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en transposición de la Directiva (UE) 2015/2366 del Parlamento y del Consejo, de 25 de noviembre, sobre Servicios de Pago en el Mercado Interior y derogando la Ley 16/2009, de 13 de noviembre, de servicios de pago), con el firme propósito de generar un entorno más seguro y fiable en el aprovechamiento de las innovaciones derivadas de los cambios tecnológicos en los servicios de pago. A lo largo de estos últimos años, han proliferado diversos medios fraudulentos para conseguir una transferencia de activo patrimonial, con ánimo de lucro y en perjuicio de terceros, a través de manipulación informática o artificio semejante (art. 248.2.a. CP): creación de órdenes de pago o de transferencias no autorizadas, duplicidad de tarjetas de pago, suplantación de identidad de la propia entidad financiera u organismos públicos, etc., como muestra el último informe del Banco de España -Memoria de Reclamaciones de 2020-. Sin perjuicio de que todos estos métodos pueden ser calificados como fraudulentos, la principal dificultad que habremos de solventar para determinar el sujeto responsable es la clasificación de la operación de pago como autorizada por el titular de la cuenta o si, por el contrario, nos encontramos ante una operación de pago no autorizada o ejecutada incorrectamente. Incluso encontrándonos ante el primer tipo de operaciones – presuntamente autorizadas por el titular-, la entidad financiera será responsable del perjuicio patrimonial sufrido por el titular de la cuenta que ha sido víctima de fraude o hackeo (art. 44 Real Decreto-ley 19/2018), como viene siendo estimado por la jurisprudencia menor más reciente. A lo largo del presente trabajo se llevará a cabo un análisis doctrinal y jurisprudencial con el que se pretende arrojar algo de luz y sistemática a una manera tan controvertida y que tanta indignación ha causado a clientes –consumidores y microempresas- víctimas de fraudes en los servicios de pago contratados con las entidades financieras.

PALABRAS CLAVE: *Phishing*; servicios de pago; hackeo; operaciones no autorizadas; entidades bancarias.

ABSTRACT: *The control of unauthorized payment transactions has received special attention in Royal Decree-Law 19/2018, of November 23, on payment services and other urgent financial measures (in transposition of Directive (EU) 2015/2366 of Parliament and the Council, of November 25, on Payment Services in the Internal Market and repealing Law 16/2009, of November 13, on payment services), with the purpose of generating a safer and reliable in taking advantage of the innovations derived from technological changes in payment services. Throughout recent years, various fraudulent activities have proliferated to achieve a transfer of patrimonial assets, for profit and to the detriment of third parties, through computer manipulation or similar artifice (art. 248.2.a. CP): creation payment orders or unauthorized transfers, duplication of payment cards, impersonation of the financial institution itself or public bodies, etc., as shown in the latest report from the Bank of Spain -2020 Complaints Report-. Without prejudice to the fact that all these methods can be classified as fraudulent, the main difficulty that we will have to solve to determine the person responsible is the classification of the payment operation as authorized by the account holder or if, on the contrary, we are before an unauthorized or incorrectly executed payment operation. Even when we are faced with the first type of operations - presumably authorized by the account holder -, the financial entity will be responsible for the patrimonial damage suffered by the account holder who has been a victim of fraud or hacking (art. 44 Royal Decree-Law 19/2018), as has been estimated by the most recent minor jurisprudence. In the present work, a doctrinal and jurisprudential analysis will be carried out with which it is intended to shed some light and systematically on such a controversial way and that has caused so much indignation to clients -consumers and micro-enterprises- victims of fraud in services payment contracted with financial institutions.*

KEY WORDS: *Cphishing; payment services; hacking; unauthorized operations; banks.*

I. INTRODUCCIÓN.

La manifiesta preocupación de los legisladores europeo y nacionales por establecer mecanismos de control de las operaciones de pago no autorizadas ha sido objeto de especial atención en el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en transposición de la Directiva (UE) 2015/2366 del Parlamento y del Consejo, de 25 de noviembre, sobre Servicios de Pago en el Mercado Interior y derogando la Ley 16/2009, de 13 de noviembre, de servicios de pago). Este Real Decreto-ley fue aprobado con el firme propósito de generar un entorno más seguro y fiable en el aprovechamiento de las innovaciones derivadas de los cambios tecnológicos en los servicios de pago ya que, lamentablemente, a lo largo de estos últimos años, han proliferado diversos medios fraudulentos para conseguir una transferencia de activo patrimonial, con ánimo de lucro y en perjuicio de terceros, a través de manipulación informática o artificio semejante. Tales operaciones, como muestra el último informe del Banco de España -Memoria de Reclamaciones de 2020, consisten en creación de órdenes de pago o de transferencias no autorizadas, duplicidad de tarjetas de pago, suplantación de identidad de la propia entidad financiera u organismos públicos, etc.

A pesar de que todos estos métodos pueden ser calificados como fraudulentos, la principal dificultad que habremos de solventar para determinar el sujeto responsable es la clasificación de la operación de pago como autorizada por el titular de la cuenta o si, por el contrario, nos encontramos ante una operación de pago no autorizada o ejecutada incorrectamente. Incluso encontrándonos ante el primer tipo de operaciones – presuntamente autorizadas por el titular-, la entidad financiera será responsable del perjuicio patrimonial sufrido por el titular de la cuenta que ha sido víctima de fraude o hackeo (art. 44 Real Decreto-ley 19/2018), como viene estimando la jurisprudencia menor más reciente, comúnmente realizado a través de técnicas de *phishing* y sus derivadas –"actuación

• Araya Alicia Estancona Pérez
Prof.ª Contratado Dr. (acredit. a TU) Derecho Civil
Universidad de Cantabria
araya.estancona@unican.es

fraudulenta que toma como punto de partida el envío masivo de mensajes de correo electrónico desde diversos sitios en la web, que tiene como destinatarios a usuarios de la banca informática –banca on-line- a quienes se les redirecciona a una página web que es una réplica casi perfecta de la original y en la que se les requiere, normalmente con el aviso amenazante de perder el depósito y la disponibilidad de las tarjetas de crédito, a que entreguen sus claves personales de acceso con el fin de verificar su operatividad" (STS 834/2012, de 25 de octubre [Rec. 2422/2011] – TOL2.712.104)-.

II. CONTRATO DE SERVICIOS DE PAGO.

1. Sujetos intervinientes: clientes de servicios de pago especialmente protegidos.

Resulta preciso, en estas primeras líneas, concretar los posibles sujetos intervinientes en la relación derivadas del contrato de servicios de pago celebrado entre las entidades bancarias y sus clientes o usuarios. En primer término, debemos precisar que las entidades bancarias se sirven de los denominados proveedores de servicios de pagos para poder ofrecer servicios u operaciones de pago a sus clientes. Los *proveedores del servicio de pago o entidades de pago* son persona jurídicas a las que el Banco de España ha otorgado una autorización administrativa para prestar y ejecutar uno o varios de los servicios de pago como ingreso de efectivo en una cuenta de pago, retirada de efectivo de una cuenta de pago, ejecución de operaciones de pago a través de una cuenta de pago mediante transferencias, adeudos domiciliados u operaciones de pago con tarjeta o dispositivo similar (Operaciones de pago a débito), ejecución de operaciones de pago cuando los fondos están cubiertos por una línea de crédito, mediante transferencias, adeudos domiciliados u operaciones de pago con tarjeta o dispositivo similar (Operaciones de pago a crédito), emisión de instrumentos de pago o adquisición de operaciones de pago, envío de dinero, iniciación de pagos, información sobre cuentas, etc[1]. Los proveedores de servicios de pago más utilizados en España son MasterCard, Visa y American Express, de los que se sirven las entidades bancarias para ofrecer estos servicios a sus clientes.

Junto a los proveedores de servicios de pagos, encontramos los denominados *proveedores de servicios de iniciación de pagos* (reconocidos en la Directiva PDS1), como personas jurídicas que permiten iniciar un pago a petición del usuario, respecto a una cuenta de pago abierta en una entidad financiera ofreciendo alternativa al pago con tarjeta ya que el pago se hace a través de una plataforma intermediaria y donde el cliente tiene almacenados sus datos. Como ejemplos de las 49 entidades de pago registradas en el Banco de España encontramos

1 **https://www.bde.es/bde/es/secciones/servicios/Instituciones_fi/autorizacion-de-/entidades_de_pago-fe0bc360a9ce961.html (Consultado en fecha 22-08-2022).**

las más frecuentes: American Express Europa, SA., Global Payment Systems., Prosegur Servicios de Pago., Solred SA., UniversalPay., etc. Además, encontramos *proveedores de servicio de información de cuenta* (reconocidos en la Directiva PSD2) como personas jurídicas que proporcionan al usuario información agregada sobre sus cuentas de pago mantenidas en una misma o en distintas entidades financieras, que otorgan a los clientes una visión global de las cuentas asociadas incluyendo la relación de gastos e ingresos, incluso de los cargos a realizar a la cuenta. A modo de ejemplo encontramos 3 entidades que operan bajo autorización del Banco de España: GS Gestion Fintech Apps; Split Payments S.L., Tesaralia, S.L.

Del lado de los clientes o usuarios de los servicios de pago, podemos encontrar clientes que reúnen las características de consumidores, microempresas, personas jurídicas o entes sin personalidad (vid. ej., comunidades de propietarios). En particular, tanto la Directiva (UE) 2015/2366 del Parlamento y del Consejo, de 25 de noviembre, sobre Servicios de Pago en el Mercado Interior –Directiva PSD2- como el RD-Ley 19/2018 que la transpone parcialmente, protegen de una manera particular a los clientes consumidores y microempresas. Junto a los consumidores –definidos por el RD-Ley 19/2018 como "una persona física que, en los contratos de servicios de pago objeto de este real decreto-ley, actúa con fines ajenos a su actividad económica, comercial o profesional"-, las microempresas –definidas por el RD-Ley 19/2018 como "una empresa, considerando como tal tanto a las personas físicas que realizan una actividad profesional o empresarial como a las personas jurídicas, que, en la fecha de celebración del contrato de servicios de pago ocupa a menos de diez personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los dos millones de euros"- son protegidas por el mismo texto legal en relación a las condiciones de transparencia de las condiciones y requisitos de información aplicables a los servicios de pago, resolución y modificación del contrato marco y los derechos y obligaciones de los servicios de pago[2].

2. Tipología de operaciones de pago fraudulentas:

En el presente estudio nos centraremos en el análisis de los supuestos en los que las transferencias bancarias o las órdenes de pago de los clientes bancarios han sido realizadas de manera fraudulenta, comúnmente por un engaño derivado de la suplantación de identidad de la entidad bancaria.

2 Como indica el Preámbulo del RD-Ley 19/2018, de este régimen general de protección del consumidor aplicable a las microempresas, se excepciona *a las microempresas de la aplicación del derecho a ordenar la devolución de los adeudos domiciliados como consecuencia de una operación de pago autorizada iniciada por un beneficiario o a través del mismo, durante un plazo de ocho semanas contadas a partir de la fecha de adeudo de los fondos en su cuenta. El motivo es que la atribución de tal derecho a las microempresas distorsionaría el sistema de gestión de los adeudos domiciliados, ocasionando a las microempresas perjuicios derivados del riesgo de crédito que tendrían que asumir los proveedores de servicios de pago en dicho periodo.*

La transferencia bancaria es entendida como "un servicio que forma parte del contrato de servicio de caja entre un proveedor de servicios de pago (el banco) y sus clientes y sirve de medio de pago mediante el débito en la cuenta del ordenante y abono en la del beneficiario, tratándose, en suma, de un procedimiento financiero de movimiento de la moneda. Se trata de un medio de pago consistente en una orden dada al banco (banco emisor) por parte de un cliente (ordenante) a fin de que, con cargo a su cuenta, abone un determinado importe en otra cuenta del mismo o distinto banco (banco destinatario) abierta a nombre de un tercero (beneficiario) o del propio ordenante" (SAP Alicante, núm. 632/2018, de 12 de marzo de 2018 [Rec. 622/2017] TOL6.636.914). Por su parte, la derogada Ley 16/2009, de 13 de noviembre, de servicios de pago, definía las órdenes de pago como "toda instrucción cursada por un ordenante o beneficiario a su proveedor de servicios de pago por la que se solicite la ejecución de una operación de pago" (art. 2.16 LSP).

Ambas operaciones se enmarcan en el seno de la relación contractual entre el cliente y la entidad bancaria en la que tiene depositado su activo patrimonial y constituyen una forma de ejecución de las obligaciones contractuales asumidas. La ejecución por parte de la entidad de la orden emitida forma parte del contrato de servicios de caja celebrado que, tratándose de órdenes de pago por vía electrónica, supone que el cliente debe haber firmado un contrato de adhesión a los servicios de banca electrónica (SAP Alicante, núm. 632/2018, de 12 de marzo de 2018 [Rec. 622/2017] TOL6.636.914).

A) Operaciones realizadas por suplantación de identidad del banco. En particular, phishing.

Se trata de operaciones en las que el titular de la cuenta, presuntamente, otorga su autorización para realizar la transferencia bancaria o el pago del que se trate. Sin embargo, en estos supuestos se ha producido una suplantación de identidad del titular a través de la obtención de determinados datos personales y bancarios que facilitan el acceso a la cuenta bancaria on-line, tarjetas de crédito o cualquier otro medio de pago a distancia.

En la STS 834/2012, de 25 de octubre [Rec. 2422/2011] – TOL2.712.104, el "phishing" era definido como "actuación fraudulenta que toma como punto de partida el envío masivo de mensajes de correo electrónico desde diversos sitios en la web, que tiene destinatarios a usuarios de la banca informática –banca on-line- a quienes se les redirecciona a una página web que es una réplica casi perfecta del original y en la que se les requiere, normalmente con el aviso amenazante de perder el depósito y la disponibilidad de las tarjetas de crédito, a que entreguen sus claves personales de acceso con el fin de verificar su operatividad. De forma gráfica se dice que el autor "pesca los datos protegidos" (phishing), que permiten

el libre acceso a las cuentas de particulares y, a partir de ahí, el desapoderamiento". (FD Segundo)

Como variantes de la técnica de "phishing", encontramos algunas otras que encuentran su diferencia en el medio por el que se procede al envío del gancho que permitirá acceder a las claves del titular de la cuenta -SMS (*smishing*), llamadas telefónicas (*vishing*), páginas web falsas (*web spoofing*), etc.-

Por otra parte, el Departamento de Mercado y Reclamaciones del Banco de España –DCMR- ha detectado un mecanismo más elaborado que combina la obtención datos de la víctima y, a continuación, solicitan a la operadora de telefonía móvil el duplicado de la tarjeta SIM (*swapping)* para recibir, vía SMS las claves que desde los sistemas de banca online se envía para garantizar la autenticación del titular de la cuenta[3].

B) Operaciones no autorizadas por sus titulares o ejecutadas incorrectamente.

Además de las operaciones fraudulentas descritas en líneas precedentes y que parten de la suplantación de identidad del titular de la cuenta mediante medios informáticos que permiten obtener sus datos personales y bancarios, podemos encontrar otros supuestos de operaciones no autorizadas por los titulares de las cuentas o ejecutadas incorrectamente por la entidad bancaria y que los tribunales han tenido la oportunidad de conocer.

Estas transferencias o pagos son realizados por personas no autorizadas o sin poder de disposición de las cuentas corrientes. Comúnmente, el mayor número de controversias se presentan en cuentas cuya titularidad pertenece a personas jurídicas, comunidad de propietarios o, en su caso, co-titularidades. En estos casos, el problema deriva de la necesaria verificación que debe realizar en la entidad bancaria sobre la autorización del sujeto que pretende realizar la transferencia o pago[4].

En definitiva, lo relevante en estos estos supuestos –ya sea por suplantación de identidad, operaciones realizadas por quien carece de autorización para ello o por operaciones realizadas incorrectamente- es que, conforme a lo dispuesto en el art

3 Memoria de reclamaciones del Banco de España de 2019. https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaServicioReclamaciones/19/Documentocompleto.pdf (Consultado en fecha 12/09/2022)

4 En concreto, en el caso de los depósitos conjunto pueden distinguirse el depósito condicionado del depósito plural con mandato. En el primer caso, para efectuar los actos de restitución del dinero depositado es exigida la firma de todos los depositantes suponiendo en mínimo control de los actos de disposición. Por su parte, en el depósito plural con mandato, los depositantes que tengan la condición de mandatarios podrán practicas actos de disposición de manera separada, debiendo rendir cuentas de su actividad ante el resto. Madrazo Leal, J.: "Aproximación al depósito bancario conjunto" en *Homenaje a Luis Rojo Ajuria: escritos jurídicos*. Universidad de Cantabria, Santander, 2003, pp. 384-385.

43 del Real Decreto-ley 19/2018, de 23 noviembre, el usuario de servicios de pago debe comunicar los movimientos en su cuenta tan pronto tenga conocimiento de ello o, como máximo, a los 13 meses desde la fecha en que se ha producido el adeudo. De este modo, la rectificación por el proveedor de servicios de pago debe cumplirse con los presupuestos legalmente contemplados, como veremos en líneas sucesivas.

3. Contrato de servicios de pago vs. contrato de depósito bancario.

El punto de partida por el que proceder al análisis del régimen de responsabilidad de las entidades bancarias o los proveedores de servicios de pagos debe encontrarse en la determinación de las obligaciones que son asumidas por estos en virtud del contrato celebrado con el cliente o titular de la cuenta corriente. En este sentido, es preciso concretar la tipología contractual derivada de la titularidad de una cuenta corriente en una entidad bancaria.

En primer lugar, encontramos el contrato de depósito bancario. El contrato de depósito bancario es definido como "aquel mediante el cual una parte (cliente depositante) entrega a otra (entidad bancaria depositaria) el objeto del depósito (comúnmente, dinero), obligándose a custodiarlo y restituirlo en cualquier momento en que el primero así lo requiera o bien pasado el plazo establecido"[5]. Bajo su régimen jurídico, por lo tanto, podemos afirmar que la obligación principal es de custodia del bien depositado. Sin embargo, tratándose de un contrato de depósito de dinero "bancario", la obligación principal podría ser concretada en la obligación de devolución de lo que denominamos "idem receptum", "desapareciendo esa obligación de custodia que ni siquiera podría estar referida al tantudem"[6]. De este modo, como indica Hualde Manso, "la inserción del depósito de dinero en la empresa bancaria operaría de esta forma una transformación interna de especial envergadura en el régimen jurídico del contrato atendiendo a la cualidad de una de las partes en el contrato (el depositario)"[7].

Con independencia de la variada tipología de contratos de depósito bancarios[8], se ha llegado a afirmar que la particularidad del contrato de depósito de dinero

5 Tomillo Urbina, J.L.: "El depósito bancario" en *Contratación bancaria,* Tomo I, Dir. F.J. Orduña Moreno y J.L. Tomillo Urbina, Tirant Lo Blanch, Valencia, 2001, p. 237.

6 Se trata de un contrato atípico por estar las normas del Código Civil y Código de Comercio pensadas para ello, pero socialmente aceptados y sobradamente conocidos por el cual *el depositante entrega el dinero a la entidad de crédito depositaria, que adquiere la propiedad del mismo, obligándose a devolver otro tanto una vez llegado el plazo.* Díaz Ruíz, E., y Ruíz Bachs, S.: "El depósito bancario estructurado" en Revista de derecho bancario y bursátil, Núm. 89, 2003, p. 22.

7 Hualde Manso, M.T.: "Causa, función y perversión del depósito bancario a la vista", *Revista de derecho bancario y bursátil,* Núm. 136, 2014.

8 Al margen de la habitual clasificación entre contratos de depósito a la vista y contratos de depósito a plazo, a interés variable, en divisas, etc., podemos encontrar los depósitos estructurados como contratos de carácter bancario, de carácter completo, resultado de la integración de un depósito a plazo fijo y un instrumento financiero derivado, y atípico, que regirán fundamentalmente con las cláusulas contractuales

bancario caracterizado por la desaparición de una obligación de custodia existiendo exclusivamente una obligación de restitución, permite negar su categoría[9]. Esta obligación de restitución viene reforzada por la normativa sectorial bancaria "para reequilibrar la desaparición de la obligación de custodia y del otorgamiento al banco de la plena (cuasi plena) disponibilidad"[10]. En este sentido, la obligación de custodia no sería considerada objeto de prestación típica, "sino un simple criterio de responsabilidad para el caso que quede incumplida la obligación de restitución"[11].

Desde el punto de vista del depositante bancario, podría afirmarse que su interés en la puesta en custodia de la entidad bancaria "no busca obtener una ganancia ni aumentar su capital, sino sólo seguridad, que no sólo es la que se deriva de la custodia asumida por el Banco" –concretada en la prevención de operaciones de pago no autorizadas por el titular o, de producirse, en asegurar que la entidad procederá a su devolución- "sino de que la suma no sea empleada en operaciones arriesgadas"[12].

A pesar de las posturas doctrinales discordantes, creemos que puede afirmarse que, derivado del contrato de depósito de efectivo, la entidad financiera depositaria debe cumplir con la obligación de custodia como "fin fundamental de depósito y explica la función económica ya que el deber de restituir es un deber cuyo cumplimiento extingue la situación"[13]. Pero ¿en qué consiste la custodia del dinero? Se pregunta García-Pita si de verdad el Banco "custodia" la suma depositada, cuando invierte y gasta los fondos depositados superando, con mucho, la necesidad de mantener el "tantundem". Podríamos decir que esa obligación de custodia se materializa en el tráfico económico actual en la asunción del riesgo de pérdida, total o parcial, de la suma depositada pues no siendo un depósito de monedas o billetes especificados, "es obvio que la posibilidad de desarrollar las conductas orientadas a su custodia o conservación ni resultan ni legal ni físicamente imposibles… luego no queda extinguida la obligación del depositario" (art. 1184 Cc, "sensu contrario")[14].

pactadas. Díaz Ruíz, E., y Ruíz Bachs, S.: "El depósito bancario estructurado", *Revista de derecho bancario y bursátil,* Núm. 89, 2003, pp. 31-32.

9 Vicent Chuliá, F.: *Compendio crítico de Derecho Mercantil*, Barcelona, 1990, pp. 433-434.

10 Hualde Manso, M.T.: "Causa, función y perversión del depósito bancario a la vista", *Revista de derecho bancario y bursátil,* Núm. 136, 2014.

11 Emparanza Sobejano, A y Martínez Giner, L.A.: "El depósito bancario. Las libretas de ahorro" en *Contratos bancarios,* Tomo X, Aranzadi, Cizur Menor, 2014. p. 105 y ss.

12 Hualde Manso, M.T.: "Causa, función y perversión del depósito bancario a la vista", *Revista de derecho bancario y bursátil,* Núm. 136, 2014.

13 Hualde Manso, M.T.: "El depósito bancario a la vista", en *Operaciones bancarias de activo y pasivo en el contexto de crisis económica: hacia la unificación de la contratación privada*, Aranzadi, Cizur Menor, 2015, pp. 328-329.

14 García-Pita y Lastres, J.L.: "Bases para una revisión del régimen de los depósitos bancarios de efectivo", *Revista de Derecho Bancario y Bursátil,* Núm. 143, 2016.

Diferente es el *contrato de cuenta corriente bancaria*. Se trata de un contrato que, a pesar de su origen como contrato accesorio al de depósito, en la actualidad tiene virtualidad propia constituyendo un contrato autónomo cuya principal característica es permitir al cliente hacer uso del "servicio de caja" –el cliente puede disponer del dinero y realizar ingresos, todo ello por diversos mecanismos, permitiendo conocer en todo momento el saldo resultante de la cuenta[15]. De este modo, podemos afirmar que el banco, a través del contrato de cuenta corriente bancaria, se convierte en el gestor de pagos e ingresos del cliente, permitiendo que la condición de titular de la cuenta determine la propiedad de los fondos depositados. Por ello, en el contrato de cuenta corriente bancaria concurren características propias de los contratos de mandato o comisión[16]. Así, la entidad bancaria deberá asumir las instrucciones de su cliente y actuar en interés de éste, debiendo imputarle su responsabilidad como comisionista[17]. Como claramente se indica en la SAP de Zaragoza, núm. 215/2013, "el contrato de cuenta corriente cada vez va recabando mayor autonomía respecto al contrato de depósito, que le sirve de base. De modo que la cuenta corriente sólo actúa como soporte contable, expresando una disponibilidad de fondos contra el banco que los retiene y que encuentra su causa tanto en operaciones de activo como de pasivo". [De esta relación se derivan] "deberes de rendición de cuentas, de información y el deber de actuar conforme a las instrucciones recibidas" (FD Segundo).

Como afirmábamos, al contrato de cuenta corriente bancaria le acompaña el contrato de "servicios de pago". Se antoja complicado imaginar en el tráfico económico actual que los clientes bancarios puedan tener interés en depositar su dinero en la entidad financiera sin contratar, a su vez, los servicios de pago que los proveedores puedan proporcionarle y que facilitarán las transacciones económicas a través de transferencias bancarias, domiciliación de pago periódicos, pagos con tarjetas de crédito o débito, compras vía banca on-line, etc., teniendo la disponibilidad permanente de su dinero al tratarse de *depósitos a la vista*[18]. Así, cobran especial relevancia los denominados *servicios de caja* –o servicios de banca

15 Pablo-Romero Gil-Delgado, M.C.: "El contrato de cuenta corriente bancaria", en *Operaciones bancarias de activo y pasivo en el contexto de crisis económica: hacia la unificación de la contratación privada,* Aranzadi, Cizur Menor, 2015, p. 348.

16 Pablo-Romero Gil-Delgado, M.C.: "El contrato de cuenta corriente bancaria", en *Operaciones bancarias de activo y pasivo en el contexto de crisis económica: hacia la unificación de la contratación privada*, Aranzadi, Cizur Menor, 2015, pp. 349-350.

17 Sánchez-Calero Guilarte, J.: "La cuenta corriente y la transferencia bancaria (observaciones a sus aspectos más discutidos)", *Revista de Derecho Bancario y Bursátil,* Núm. 86, 2002, pp. 110-112.

18 En sentido contrario, el mal llamado depósito a plazo cumple con funciones más propias del préstamo o mutuo, advirtiéndose notas propias de éste: *operación de crédito o financiación se cambian bienes presentes por bienes futuros, el prestamista pierde totalmente la propiedad del dinero y su disponibilidad y es el plazo y el pacto de intereses los que ostentan el protagonismo.* Hualde Manso, M.T.: "Causa, función y perversión del depósito bancario a la vista", *Revista de derecho bancario y bursátil,* Núm. 136, 2014.

on-line-, sin perder de vista que es "importante retener y resaltar que el fin o motivo esencial del depósito de dinero es la seguridad"[19].

A continuación, desarrollaremos el régimen de responsabilidad del proveedor de servicios de pago, a partir del análisis de las obligaciones asumidas y exigibles.

III. RESPONSABILIDAD DEL PROVEEDOR DE SERVICIOS DE PAGO.

Al margen de los deberes de información precontractual exigibles en virtud de la *Orden EHA 2899/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios*, como deber de transparencia de las entidades bancarias (art. 16 Directiva 2014/49/UE relativa a los sistemas de garantía de los depósitos) con obligación de proporcionar a los depositantes la información que identifica el sistema de garantía de depósitos al que pertenece la entidad y sus sucursales, en este análisis nos limitaremos a concretar las obligaciones contractuales y legales exigibles vigente el concreto.

En este sentido, hemos de centrar nuestra atención en la identificación de las obligaciones derivadas del proveedor de servicios de pago que determinará el régimen de responsabilidad imputable. Si atendiéramos al contrato base en el que queda incluido el contrato de servicios de pago, el contrato de cuenta corriente, habría de remitirnos a la normativa de servicios de pagos, por tratarse de un contrato atípico. Esta atipicidad característica del contrato de cuenta corriente, ha llevado a la doctrina a abogar por aplicar, analógicamente, la regulación del contrato de comisión de los arts. 254 a 259 Ccom. De este modo, el cumplimiento de las instrucciones dadas por el comitente eximiría de toda responsabilidad al comisionista en el desempeño de sus funciones.

Sin embargo, el vigente Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago, impone obligaciones particulares a las entidades bancarias relativas a la seguridad de transacciones realizadas que permitirán exigir responsabilidad al proveedor de servicios ante su incumplimiento[20].

En definitiva, podemos afirmar que, ya sea porque tratándose de un contrato de depósito, el depositario asume el deber de guarda o custodia del dinero depositado, o porque derivado del contrato de cuenta corriente, la entidad

19 Hualde Manso, M.T.: "Causa, función y perversión del depósito bancario a la vista", *Revista de derecho bancario y bursátil,* Núm. 136, 2014.

20 No obstante, la casuística recogida en las Memorias del Servicio de Reclamaciones del Banco de España demuestra que los supuestos de incumplimiento de sus deberes de gestión y seguridad por parte de las entidades bancarias permiten imputarles la responsabilidad, por ejemplo, por no asegurar la identificación del cliente ordenante de un determinado pago. Pablo-Romero Gil-Delgado, M.C.: "El contrato de cuenta corriente bancaria", en *Operaciones bancarias de activo y pasivo en el contexto de crisis económica: hacia la unificación de la contratación privada*, Aranzadi, Cizur Menor, 2015, p. 379.

proveedora de los servicios de pago debe cumplir con la obligación de seguridad de los cargos a cuenta o las operaciones de compra realizadas a través de las tarjetas de crédito, débito o por el servicio de banca on-line, Bizum … asegurando que las instrucciones son dadas por el propio titular de la cuenta y no están siendo realizadas por ningún medio fraudulento, la entidad bancaria o el proveedor del servicio de pago será responsable del uso fraudulento de medios de pago o acceso fraudulento a las cuentas de sus clientes que suponga un daño patrimonial.

En este sentido, es preciso matizar que el régimen específico de responsabilidad civil contenido en el Real Decreto-ley 19/2018, establece un sistema de imputación del proveedor de servicios de pago (o, en su caso, de proveedor de iniciación de servicios de pago), sin que la entidad bancaria con la que se ha celebrado el contrato de cuenta corriente sea reconocida como responsable de los daños patrimoniales sufridos. Sin embargo, la totalidad de las sentencias analizadas y recogidas en este texto demuestran que, los consumidores y usuarios de los servicios de pago, interponen sus demandas frente a la entidad bancaria en la que tienen depositado su activo patrimonial. Puede estimarse que concurre el régimen de responsabilidad solidaria del art. 132 del TRLGDCU de todas las personas responsables –en este caso, entidades bancarias y proveedores de servicios de pago- ante el perjudicado –consumidores o clientes bancarios-. De este modo, los consumidores o clientes ejercitarán acción directa frente a las entidades bancarias que habrán de responder por los perjuicios causados sobre su activo patrimonial y sin perjuicio la acción de repetición que, en su caso, tendría frente a los proveedores de servicios de pago.

Para determinar la extensión del régimen de responsabilidad, en primer lugar, habremos de atender al clausulado contractual del contrato de cuenta corriente y, consecuentemente, del servicio de pagos contratado. En este sentido, cobra especial relevancia la STS núm. 792/2009, de 16 diciembre [Rec. 2114/2005], que en aplicación de la derogada Ley 16/2009, de 13 de noviembre, de servicios de pago, analiza la posible abusividad de tres cláusulas controvertidas:

- 1ª) Cláusula que exonera de responsabilidad a la entidad, en todo caso, por el uso de la tarjeta de crédito o débito antes de la notificación de su sustracción o extravío; 2ª) Cláusula que exonera de responsabilidad a la entidad, en todo caso, del uso del número de identificación personal (PIN) de las tarjetas de crédito y débito, limitando aquélla a los supuestos de fuerza mayor o coacción; y 3ª) Cláusula que establece la exención de responsabilidad de la entidad por fallos en sus aparatos en la realización de operaciones con las tarjetas.

El Alto Tribunal, además de determinar que el clausulado podrá requerir del titular de la tarjeta que habrá de comunicar a la entidad bancaria el extravío, sustracción o similar *sin demora indebida* desde que sea conocida la desaparición,

declara la abusividad de las cláusulas previamente citadas en los siguientes extremos (FD Noveno):

- en primer lugar, declara desproporcionada "una cláusula que se limite a la exoneración de responsabilidad, en todo caso, por el uso de la tarjeta antes de la notificación de la sustracción o extravío [porque] son advertibles situaciones en que, si la entidad actúa con la diligencia puede apercibirse de utilizaciones indebidas de tarjetas, aun sin la comunicación, o un eventual conocimiento de la sustracción o extravío".

- en segundo lugar, "la carga de la prueba de una fuerza mayor o coacción que dio lugar a que el titular del instrumento de pago, único que conoce y puede modificar el PIN, corresponde al que la sufrió […]". Sin embargo, "no resulta proporcionado en la perspectiva del equilibrio contractual, tratar de reducir, explícita o implícitamente, la responsabilidad bancaria a los casos de revelación del número secreto del PIN por fuerza mayor o coacción [ya que] no cabe desconocer la posibilidad de captaciones subrepticias, con independencia de otras manipulaciones varias a causa de las deficiencias del sistema de tarjetas, que no permiten sentar una cláusula que exonere de responsabilidad". De este modo, "es notorio que, en ciertas circunstancias, las entidades bancarias pueden advertir utilizaciones indebidas empleando la diligencia que les es exigible en armonía con su experiencia y medios técnicos".

- en definitiva, "no se trata de derivar la responsabilidad a la entidad bancaria, sino de estimar abusiva una cláusula que le exonere de responsabilidad en todo caso".

En el marco del estudio que presentamos, cobra relevancia el deber de seguridad exigible a los proveedores de servicios de pago en relación a la prevención de transacciones fraudulentas, no autorizadas por los titulares de las cuentas o tarjetas, evitando que se acceda a las mismas sin autorización "con medidas paliativas y mecanismos de control adecuados para gestionar los riesgos operativos y de seguridad relacionados con los servicios de pago que prestan". De este modo, "los proveedores de servicios de pago establecerán y mantendrán procedimientos eficaces de gestión de incidentes, en particular para la detección y la clasificación de los incidentes operativos y de seguridad de carácter grave" (art. 66.1 Real Decreto-ley).

Uno de los mecanismos exigidos legalmente para prevenir los accesos fraudulentos es la denominada autenticación reforzada de clientes, cuando el ordenante: "a) acceda a su cuenta de pago en línea; b) inicie una operación de pago electrónico; y c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos" (art. 68 Real Decreto-ley).

En definitiva, el art. 45 Real Decreto-ley, determina la responsabilidad del proveedor de servicios de pago en operaciones de pago no autorizadas. En virtud del precepto, la constatación de la realización de operaciones de pago no autorizadas para el titular de la cuenta obliga al proveedor a la devolución inmediata de la operación no autorizada o, a más tardar, al final de día siguiente de observar o notificar la operación. A esta obligación de reembolso inmediato le acompaña una excepción: "salvo que el proveedor tenga motivos razonables para sospechar de la existencia de fraude y este hecho sea comunicado al Banco de España". Al margen de esta excepcionalidad, el proveedor estará obligado a restituir la cuenta al estado anterior al que se efectuó la operación no autorizada[21].

1. Tipo de responsabilidad imputable.

Una vez concretada la tipología de cláusulas contractuales declaradas abusivas por el TS y que impedirían a los proveedores de servicios de pagos su auto-exoneración de responsabilidad por la efectiva ejecución de pagos no autorizados, hemos de determinar el régimen jurídico de responsabilidad imputable.

En una primera aproximación, diríamos que el demandante ejercitará acción de responsabilidad contractual frente al proveedor de servicios de pago por existir una relación jurídico-contractual previa celebrada con el titular de la cuenta corriente –como indicábamos en líneas precedentes, ya sea ésta contrato de depósito bancario o contrato de cuenta corriente bancaria-. De este modo, el régimen de responsabilidad imputable sería el de los arts. 1101 Cc y ss., por incumplimiento de las obligaciones que en cumplimiento del contrato celebrado debía asumir. En definitiva, la entidad habría de cumplir con el establecimiento de las medidas de seguridad legalmente o contractualmente exigibles para garantizar el acceso y utilización seguros de la cuenta y los medios de pago a disposición del titular –por ejemplo, la falta de establecimiento de un sistema de autenticación reforzada-, debiendo analizar el dolo o culpa de la entidad en su incumplimiento.

No obstante, entre la jurisprudencia analizada encontramos ejemplos de demandas que son planteadas en ejercicio de la acción de responsabilidad contractual concurrente con la extracontractual (art. 1902 Cc). Los clientes demandantes pretenden el ejercicio de la acción de responsabilidad extracontractual por falta de diligencia debida tras la denuncia del fraude informático padecido, evitando la pérdida patrimonial definitiva. En este sentido, encontramos la SAP Alicante, núm. 632/2018, de 12 de marzo de 2018 [Rec. 622/2017]- TOL6.636.914, en la

21 En caso de que la operación haya sido autorizada por el proveedor de servicios de iniciación de pagos, en virtud del apartado segundo del citado precepto, será el proveedor de servicios de pago gestor de la cuenta quien devolver la cuenta al estado anterior. No obstante, si resulta responsable el proveedor de servicios de iniciación de pagos, éste deberá resarcir al proveedor gestor de la cuenta, previa petición, de las sumas abonadas o pérdidas sufridas.

que tras declarar que la responsabilidad de la entidad bancaria Barclays, como prestadora de servicios de banca online y en relación a los perjuicios derivados de su uso, tiene naturaleza cuasi-objetiva o de riesgo por razón legal, determina que "Barclays sí infringió sus obligaciones, tanto contractuales –de implementación del sistema de las medidas de seguridad exigibles para un uso seguro por su cliente-, como extracontractuales –al no haber actuado con diligencia tras la denuncia del fraude informático padecido en la cuenta de la cliente al acceder al sistema online terceros no autorizados para operar con aquella. [Es decir,] la no acreditación de las necesarias medidas de seguridad, la acreditación de la diligencia de la usuaria y la inacreditación de la conducta posterior a la denuncia del fraude del banco, omitiendo las medidas necesarias para evitar, en su caso, la pérdida definitiva del dinero, constituyen los presupuestos que permiten apreciar la realidad de una causalidad adecuada entre la conducta omisiva de la entidad y el resultado dañoso".

Parece, en todo caso, que conforme a las previsiones legales establecidas en el Real Decreto-Ley 19/2018, el proveedor de servicios de pago asume la obligación de rectificación de las operaciones de pago no autorizadas "si el usuario de servicios de pago se lo comunica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo". Esta obligación de rectificación trae causa de la relación contractual previamente celebrada entre el titular de la cuenta y el proveedor de servicios de pago por lo que el ejercicio de responsabilidad extracontractual puede decirse subyacente a la contractual y que fundamentaría la imputación del régimen de responsabilidad cuasi-objetiva o de riesgo por razón legal. Para ello, habríamos de determinar el tratamiento de la actividad desarrollada por los proveedores de servicios de pago como actividad peligrosa o de riesgo. En su momento, Alvarez Lata tuvo la oportunidad de pronunciarse acerca de este extremo, concluyendo su exclusión del elenco de actividades peligrosas, por ejemplo, "prestación por las entidades bancarias de servicios de caja a sus clientes mediante el sistema de cajeros automáticos"[22]. Sin embargo, creemos que los factores de desarrollo tecnológico actuales, (sobre todo, tratándose de operaciones realizadas a distancia a través de tarjetas o banca online) permiten afirmar que la situación de riesgo en la que se sitúa el cliente por posibles fraudes o estafas de terceros es manifiesta, produciendo pérdidas patrimoniales de relevante cuantía.

En definitiva, no interesa aquí ahondar en la dicotomía entre responsabilidad contractual *vs.* responsabilidad extracontractual, debate superado por la jurisprudencia a través del principio de unidad de culpa civil y la yuxtaposición

22 Alvarez Lata N.: "La responsabilidad civil por actividades empresariales en sectores de riesgo", en, *Tratado de responsabilidad civil, II* (coord. por. L. F. Reglero Campos), Cizur Menor, Aranzadi, 2008, p. 1329.

de responsabilidades contractual y extracontractual, como pone de manifiesto en esta materia la sentencia Juzgado de Primera Instancia Núm. 9 de Valladolid, núm. 362/2009, de 10 de marzo [Rec. 884/2007] – TOL1.465.875: "entiende la actora que la demandada actuó con negligencia, bien en el cumplimiento de sus obligaciones contractuales, bien en su forma extracontractual, al posibilitar el trasvase patrimonial de la cuenta del actor a la cuenta de terceros".

Como adelantábamos en línea precedentes, mayor importancia presenta la determinación del régimen de responsabilidad culpabilístico o por riesgo de la actividad practicada e imputable al proveedor de servicios de pago. Los riesgos operativos y de seguridad a los que se enfrentan los proveedores de servicios de pago han sido reglamentariamente reconocidos en el Capítulo V, Título III del Real Decreto-ley 19/2018, debiendo articular las *medidas paliativas y mecanismos de control adecuados para su gestión*. Por lo que, de algún modo, el propio legislador está reconociendo la existencia de una actividad de riesgo merecedora de un tratamiento particular. Entre esas particularidades, se establece un sistema de inversión de la carga de la prueba, correspondiendo al proveedor demostrar que efectivamente estableció todos los sistemas de seguridad necesarios para garantizar que terceros no puedan acceder a las cuentas –por ejemplo, sistema de autenticación reforzada de claves de acceso a cuentas on-line- o advertir de movimientos sospechosos –por ejemplo, realizar transferencias a países con los que habitualmente no comercializa o advertir de varias transferencias continuas por la misma cuantía en un corto espacio de tiempo-.

En definitiva, conforme al art. 17 Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores y, en particular, conforme al art. 44 Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, "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, en todo caso,] corresponderá al proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, probar que el usuario del servicio de pago cometió fraude o negligencia grave". En este sentido, puede afirmarse que los proveedores de servicios de pago quedan sometidos a un régimen de responsabilidad cuasi-objetiva por riesgo con inversión de la carga de la prueba (vid. SSAP Madrid 386/2017, de 21 diciembre 2017 [Rec. 498/2017], núm. 178/2015, de 4 mayo 2015 [Rec. 661/2013], Alicante, núm. 632/2018, de 12 de marzo de 2018 [Rec. 622/2017]- TOL6.636.914 y Madrid, núm. 74/2022, de 28 de febrero de 2022 [Rec. 35/2021], entre otras).

El régimen de responsabilidad cuasi-objetiva de la entidad bancaria pivota sobre la base de la falta de diligencia en su actuación, por no contar con los mecanismos de seguridad y control necesarios en la banca on-line sin que pueda ser imputada al cliente una falta de autoprotección salvo que … "se trate de un engaño burdo o fácilmente perceptible que hubiera podido ser evitado por cualquier sujeto pasivo con una mínima reacción defensiva" (STS 2 diciembre de 2014 (Rec. 982/2013) TOL4.586.924). Es decir, la entidad bancaria, como proveedora de servicios de pago en línea, debe asegurar la custodia de las claves de acceso y proporcionar los medios de seguridad para proteger el acceso. De producirse el hecho delictivo sin adoptar los medios necesarios para prevenirlo deberá "reestablecer en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haber efectuado la operación de pago no autorizada" (SAP de Asturias núm. 351/2012, de 18 de septiembre (Rec. 594/2011). De este modo, si el proveedor de servicios de pagos no puede demostrar que su sistema contaba con los medios necesarios para garantizar la seguridad de las transferencias en línea, será responsable por la pérdida patrimonial sufrida por el titular de la cuenta (SAP de Vizcaya de 10 noviembre de 2016)[23].

Una vez determinado el régimen de responsabilidad imputable al proveedor de servicios de pago, veamos la evolución de su aplicabilidad judicial en los casos de *phishing*.

En este sentido, en la SAP de Burgos, núm. 242/2008, de 23 de julio 2008 [Rec. 183/2008] TOL1.393.816, el tribunal declara la falta de responsabilidad de la entidad financiera por estimar que la falta de diligencia es únicamente imputable al cliente *por "no poner otra clave o no sustituir" la clave o firma electrónica que la entidad le entregó por defecto*.

Sin embargo, en la SAP Zaragoza, de 14 mayo de 2013 (Rec. 116/2013) - TOL3.864.383, se condena a Barclays a reintegrar 20.947 € a la víctima de *phishing* por no haber podido demostrar una conducta o actuación fraudulenta o por negligencia grave del titular de la cuenta. Del mismo modo, en la SAP Vizcaya, núm. 429/2016, de 10 noviembre de 2016 [Rec. 386/2016] – TOL 5. 937.477, se condena al Banco Santander S.A. a abonar a los actores la cantidad de 59.327,18 euros más los intereses legales de dicha cantidad desde el 21 de septiembre de 2006 como víctimas de *phishing*. En este caso, a falta prueba de una conducta gravemente negligencia por los demandantes, queda demostrado que: "a) el fraude se comete creando los delincuentes una página web similar a la del Banco, que se realizan a través de la línea bancaria reiteradas operaciones en la misma semana (hasta 30

23 Al contrario, no será imputada responsabilidad a la entidad bancaria proveedora de los servicios de pago que haya bloqueado las transferencias indebidas y recuperado los montantes de dinero de las transferencias, siendo devueltas al usuario y condenado el responsable del delito de estafa informática (SAP de Valencia 37/2017, de 25 enero (Rec. 1402/2016)).

movimientos) y por cantidades elevadas, lo cual no era propio de estos clientes; b) que, además de las transferencias, se emitieron órdenes de venta de valores de los que el Banco tiene suscrito un contrato de guarda y custodia y cobrando por dicha prestación que resulta obvia que ha sido burlada fácilmente sin ninguna comprobación exhaustiva; c) que por el Banco no se realizó ninguna comprobación cuando además, tras obtener la cantidad de la venta, dicha cantidad se transmitía a cuentas de terceros y de éstas a cuentas en el extranjero por las que recibían una comisión". Igualmente, en la SAP de Alicante, núm. 107/2018, de 12 de marzo de2018 [Rec. 622/2017] –TOL6.636.914, se condena a Barclays a pagar 8.400 € por daños y perjuicios, más intereses dejados de percibir, prestadora de los servicios de banca online, como responsable por la transferencia fraudulenta. La sentencia declara que han sido infringidas las obligaciones contractuales –"implantación de sistemas de seguridad exigibles para un uso seguro de sus clientes"- y extracontractuales –"al no actuar con la diligencia debida tras denunciar el fraude informático por acceso de terceros no autorizados para operar"-. Es decir, "la no acreditación de las necesarias medidas de seguridad, la acreditación de la diligencia de la usuaria y la falta de acreditación de la conducta posterior a la denuncia del fraude por el banco", fundamentan la condena como responsable de la proveedora de servicios de banca online. Por su parte, la SAP de Valencia, núm. 228/2019, de 8 de abril de 2019 [Rec. 7/2019] TOL7.335.108, estima la pretensión y condena a La Caixa a la devolución a Megazoo S.L. de 4.498,25 euros, por producirse 9 transferencias desde la cuenta de la sociedad por valor de 38.500 euros. Tras comunicarlo a la oficina, la entidad financiera consiguió recuperar y devolver 34.001, 25 euros. Respecto al restante, la AP estima concurrente la "responsabilidad contractual del banco al ejecutar una orden de pago sin comprobar su legitimidad, es decir, que provenía efectivamente del titular (o autorizado) de la cuenta, al no disponer de un sistema adecuado de seguridad que previniera tal tipo de órdenes fraudulentas ni adoptar medidas concretas y específicas en el caso y a verificar cualquier orden que se diera en relación a las cuentas de la demandante".

Al margen de los casos de *phishing,* mención especial por su frecuencia merecen los supuestos en los que la responsabilidad de la entidad bancaria –como proveedor de servicios de pago- deriva de actuaciones realizadas por un ordenante no legitimado o por operaciones realizadas sin el consentimiento del titular, sin necesidad de que exista fraude alguno. En este sentido, como afirmara la STS 311/2016, de 12 de mayo [Rec. 85/2014], "conforme a la naturaleza y función del contrato de cuenta corriente bancaria, el cercioramiento o comprobación de la veracidad de la firma del ordenante constituye un presupuesto de la diligencia profesional exigible a la entidad bancaria con relación a sus obligaciones esenciales de gestión y custodia de los fondos depositados por el titular de la cuenta, cuyo incumplimiento da lugar a la indemnización de daños y perjuicios, conforme a la dispuesto en los arts. 1101 y 1106 Cc".

De este modo, la SAP de Valencia, núm. 332/2014, de 26 de noviembre [Rec. 709/2014] TOL4.575.029 determina la falta de consentimiento de la titular de la cuenta de las operaciones transferencias realizadas por su sobrino –"los poderes que la actora otorgó a su sobrino que conferían a éste amplísimas facultades de administración, disposición, comparecencia y firma, fueron dados cuatro meses después de la apertura de la cuenta corriente afectada por las transferencias, siendo estas iniciadas el mismo día de su apertura. […] La situación acreditada, en tanto supone disposición de fondos depositados en una cuenta corriente por parte de una persona que no podía hacerlo por no ser la titular ni estar autorizada por ésta, supone un incumplimiento contractual, dada la obligación esencial del Banco de conservar y devolver los fondos depositados"-. En relación a casos en los que el titular de la cuenta es una persona jurídica o comunidad de propietarios, podemos destacar la SAP de Castellón, núm. 39/2014, de 4 de febrero [Rec. 552/2013 – TOL 4.225.111, en la que se condena a Banco Español de Crédito S.A. a pagar a la comunidad de propietarios 5.733,20 euros por transferencias realizadas desde su cuenta a través de la banca on-line por quien carecía de autorización para ello, siendo únicamente autorizada la empresa Servicom Oropesa S.L. En este sentido, "no consta una disposición de código de usuario y clave de acceso fuera del ámbito de Servicom y no hay atisbo, en todo caso, de vinculación de un uso negligente de dichas contraseñas con la realización de transferencias litigiosas cuya ausencia de autorización se niega". Por su parte, la SAP de Valencia, núm. 208/2020, de 13 de mayo de 2020 [Rec. 820/2019] TOL8.174.287, imputa responsabilidad al BBVA SA por incumplimiento contractual de las obligaciones derivadas del contrato de cuenta corriente frente a la titular de la cuenta-Forn Sueca SL. Se condena al reintegro de 29.000 euros, por haber autorizado una transferencia por una persona no autorizada para ello –"en el presenta caso, la cuenta estaba abierta a nombre de un único titular, la mercantil Forn Sueca SL, por tanto, únicamente dicha mercantil podría disponer. La citada mercantil acordó que la administración de la sociedad se regiría por el sistema de administrador único, designándose a Dña. Herminia, única representante de la mercantil y con facultades para disponer".

Una combinación entre técnicas de ingeniería social y *phishing* se encuentra en lo que la jurisprudencia ha denominado como "fraude del CEO". La SAP de Madrid, núm. 74/2022, de 28 de febrero de 2022 [Rec. 35/2021] – TOL 8.888.153 determina la responsabilidad de BBVA S.A. por ejecutar una orden de transferencia por un solicitante que no figuraba entre la lista de apoderados de la empresa para realizarlas. Se condena a la entidad financiera al pago de 303.234,44 € por el conocido como "fraude del CEO"[24]. En este sentido, "al no disponer de

24 Según explica el tribunal, la técnica del "fraude del CEO", *mezcla técnicas de ingeniería social y phishing para que conseguir que una persona con acceso a las cuentas de una empresa piense que su jefe le está encargando hacer un envío de dinero ligado a una operación. O, en todo caso, que le proporcione datos bancarios de la empresa. […] Las víctimas suelen ser estudiadas previamente para que el engaño sea creíble. Habitualmente se atacan*

un sistema adecuado de seguridad que previniera tal tipo de órdenes fraudulentas ni adoptar medidas concretas y específicas en el caso cuando toma conocimiento de una situación operativa anormal que debió, cuando menos de forma puntual y excepcional, verificar cualquiera orden que se diera en relación a las cuentas de la demandante".

2. Causas de exoneración.

Como veníamos indicando, tratándose de un régimen de responsabilidad cuasi-objetivo por riesgo de la actividad y con inversión de la carga de la prueba, hemos de valorar cuáles serán las causas de exoneración de responsabilidad alegables por parte del proveedor de servicios de pago.

En primer término, habremos de estar a las causas contractualmente pactadas y siempre que no sean declaradas nulas por abusivas, en su caso –vid. ej., cláusulas que aumenten la carga de la prueba sobre el consumidor (Directiva PSD2). En este sentido se pronunció, como veremos en el epígrafe sucesivo, la SAP Sevilla núm. 289/2021, de 30 julio 2021 [Rec. 8540/2021] – TOL8.644.596, que moderó la devolución de la cantidad transferida sin autorización a la mitad del total, por falta de cumplimiento de una de las cláusulas contractualmente pactadas con el cliente-empresario.

Superado el análisis contractual, las causas de exoneración han sido legalmente establecidas en el RD-Ley 19/2018, de 23 de noviembre, con el precedente en el art. 32 de la Ley 16/2009. El proveedor de servicios de pago responderá de las operaciones no autorizadas o ejecutadas incorrectamente con la rectificación de la misma si el usuario lo "comunica sin demora injustificada", en cuanto tenga conocimiento de las operaciones que sean objeto de reclamación y, en todo caso, en el plazo de 13 meses contados desde la fecha del adeudo (art. 43). Por lo tanto, le corresponde al proveedor de servicios de pago o, en su caso, al proveedor de servicios de iniciación de servicios de pago, *probar que el usuario cometió fraude o negligencia grave* en su actuación en cumplimiento con alguna o varias de las obligaciones asumidas conforme al art. 41[25]. En este caso, el usuario soportará todas las pérdidas por operaciones de pago no autorizadas (art. 46), quedando

pequeños negocios, donde la relación del CEO con los empleados es cercana y un correo de estas características puede tener sentido. […] se realiza normalmente por correo, pero puede ser por WhatsApp o cualquier otra vía de comunicación por la que el jefe de la empresa podría solicitar algo. Como ocurre en otros ataques, normalmente los atacantes suelen utilizar direcciones de correo con un nombre similar al real para que la víctima no se percate a primera vista. Haciendo uso de ingeniería social (una forma de engaño), los ciberdelincuentes hacen clickar a la víctima en su enlace de Google Drive o Google Docs. A partir de aquí, los atacantes pueden desde colocar un malware en el ordenador del empleado, hasta proseguir con la estafa e intentar que se realice la transferencia supuestamente dictada por el CEO.

25 Las obligaciones del usuario de servicios de pago son (art. 41):
a) utilizar el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago que deberán ser objetivas, no discriminatorias y proporcionadas
b) proteger las credenciales de seguridad

el ordenante exento de toda responsabilidad sin soportar las consecuencias económicas, salvo actuación fraudulenta:

- por sustracción, extravío o apropiación indebida de un instrumento de pago: si las operaciones se han efectuado de forma no presencial utilizando datos de pagos impresos

- si el proveedor de servicios no exige autenticación reforzada –por ej., con el envío del SMS con clave para autorizar el pago-.

En definitiva, las actuaciones fraudulentas o por negligencia grave del ordenante son causas de exoneración de toda responsabilidad del proveedor de servicios de pagos. En este sentido, lo determinante será concretar qué hemos de entender por supuestos de negligencia grave del ordenante. Tomando como referencia lo expuesto en el Considerando 72 de la Directiva (UE) 2015/2366, del Parlamento y del Consejo, de 25 de noviembre, sobre Servicios de Pago en el Mercado Interior –Directiva PSD2-, el ordenante debe incumplir su deber de diligencia de manera grave o significativa, por ejemplo, guardando las credenciales usadas para dar autorización del pago junto al propio instrumento del pago, en formato abierto y fácilmente detectable para terceros. Este ejemplo ofrecido por la Directiva parece fácilmente comprensible, pero llevando este ejemplo al supuesto objetivo de análisis en este estudio –casos de fraude vía *phishing*-, ¿hacer click en el enlace recibido a través de un SMS o correo electrónico e introducir las claves de usuario de la banca online, sería un acto gravemente negligente del usuario?

3. Concurrencia de culpas.

Por el momento, los supuestos en los que los tribunales españoles estiman la minoración de la responsabilidad de la entidad bancaria como proveedor de servicios de pago se limitan a aquellos casos en los que el usuario es una persona jurídica, a la que se le exige una diligencia reforzada o cualificada como profesionales (Considerando 73 Directiva PSD2).

Como ejemplos más relevantes entre la jurisprudencia menor, encontramos las siguientes sentencias:

- Sentencia Juzgado de Primera Instancia Núm. 9 de Valladolid, núm. 362/2009, de 10 de marzo [Rec. 884/2007] – TOL1.465.875 –. Se trata de un caso en el que se determina la concurrencia de culpas de la demandante –titular de la cuenta- y de la entidad bancaria –Banco Santander-. La demandante "proporcionó datos a

c) en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, lo notificará al proveedor de servicios de pago o a la entidad que este designe, sin demora indebida en cuanto tenga conocimiento de ello

terceros sin atender a las más elementales normas de seguridad de la banca online, puesto que la actora no es quien busca el portal del Banco Santander, sino que recibe un correo electrónico en el que le invita a entrar en una página, lo cual hace, y una vez dentro, entrega las claves de seguridad sin cerciorarse que está en la página correcta". Por su parte, la entidad financiera tampoco actuó con la diligencia debida ya que: "a) comunicó a los clientes el ataque masivo de *phishing* sufrido por la entidad vía correo ordinario, ni siquiera con acuse de recibo; b) permitió que se hicieran disposiciones de dinero por encima de lo que consta en el contrato de banco online como límite y que solo puede superarse con autorización escrita del cliente; c) tampoco actuó correctamente a la hora de rescatar las partidas transferidas, ya que la petición de reintegro y paralización de pagos fue realizada dos días después de la comunicación por parte del cliente".

Por ello, la sentencia reconoce la existencia de concurrencia de culpas y "no existiendo nada que indique que la negligencia de una u otra parte tuvo una incidencia mayor o menor en el resultado, procede atribuir a cada una de ellas el 50% de la responsabilidad".

- SAP Barcelona, núm. 31/2019, de 29 de enero [Rec. 552/2017] TOL 7.048.198 –. El tribunal estima la concurrencia de falta de diligencia tanto de la entidad financiera como de la sociedad titular de la cuenta corriente víctima de *phishing*. Se condena a la entidad al reintegro de 59.450 euros más 366, 70 euros de gastos de transferencia, así como los intereses legales, en concepto de una de las transferencias que no fueron firmadas por D. Benedicto, como administrador único de la empresa. A pesar de la negligente pasividad con la que actuó la sociedad titular de la cuenta, "también hubo falta de cuidado por parte del Banco, que debía emplear la diligencia del comerciante experto que custodia el dinero de otros. El propio banco denomina orden informal al encargo de la transferencia por correo electrónico. La orden formal es la orden escrita que firmaba el Sr. Benedicto, una vez cumplimentada por el banco. El banco no esperó al consentimiento escrito, no hizo una llamada de comprobación al cliente ni utilizó ningún otro procedimiento de confirmación".

- SAP Sevilla, núm. 289/2021, de 30 julio 2021 [Rec. 8540/2021] – TOL8.644.596. El tribunal determina la responsabilidad de Banco Santander condenada al pago de 1.238.907,26 € -50% de las cantidades transferidas- más intereses legales desde la fecha de la primera reclamación extrajudicial por *phishing*. Es probada la falta de diligencia de la entidad bancaria por no asegurarse de la autenticidad de las órdenes de pago, ya que "debió exigir órdenes con firma original autógrafa o haber llamado al Sr. Abel o a alguien con mayor poder de decisión en la empresa que la propia administrativa que cursaba la orden y que como tal , en el plano hipotético, aunque no sea este el caso, pudiera estar involucrada en un intento

de fraude a Syrsa", aunque las órdenes fueran solicitadas a través de la cuenta de correo electrónico de una empleada de la empresa que, en alguna ocasión puntual, había sido autorizada a realizar una transferencia.

Por otro lado, también es probada la falta de diligencia debida del titular al que se le condena a la mitad de las cantidades transferidas por falta de diligencia debida por parte de SYRSA SA (demandante) ya que se le debe exigir la diligencia de un comerciante experto que debía haber dado aviso a tiempo e impedir que hubieran hecho tantas transferencias. Y, además, el tribunal estima que debía haber cumplido con la condición general Sexta del Contrato de adhesión firmado con la entidad bancaria, en la que se exigía la empresa demandante la revisión diaria de los movimientos de la cuenta y comunicar inmediatamente cualquier anomalía (plazo máximo de 2 días).

IV. CONCLUSIONES.

El elevado número de supuestos en los que los clientes bancarios se ven afectados por actuaciones fraudulentas que, a través de un acceso ilícito a sus cuentas corrientes, provocan pérdidas sustanciosas de su activo patrimonial, ha llevado a los legisladores europeo y nacionales a desarrollar una regulación que garantice unos mínimos niveles de seguridad a cargo de las entidades bancarias depositarias. En nuestro ordenamiento jurídico, el control de las operaciones de pago no autorizadas ha sido objeto de especial atención en el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en transposición de la Directiva (UE) 2015/2366 del Parlamento y del Consejo, de 25 de noviembre, sobre Servicios de Pago en el Mercado Interior y derogando la Ley 16/2009, de 13 de noviembre, de servicios de pago), con el firme propósito de generar un entorno más seguro y fiable en el aprovechamiento de las innovaciones derivadas de los cambios tecnológicos en los servicios de pago.

Los artificios tecnológicos utilizados por quienes actúan de manera fraudulenta para conseguir ese enriquecimiento patrimonial son utilizados para crear órdenes de pago o de transferencias no autorizadas, duplicar tarjetas de pago, suplantar de identidad de la propia entidad financiera u organismos públicos, etc. En particular, a lo largo de los últimos años han proliferado los casos de *phishing* y sus variantes –"actuación fraudulenta que toma como punto de partida el envío masivo de mensajes de correo electrónico desde diversos sitios en la web, que tiene destinatarios a usuarios de la banca informática –banca on-line- a quienes se les redirecciona a una página web que es una réplica casi perfecta del original y en la que se les requiere, normalmente con el aviso amenazante de perder el depósito y la disponibilidad de las tarjetas de crédito, a que entreguen sus claves personales

de acceso con el fin de verificar su operatividad" (STS 834/2012, de 25 de octubre [Rec. 2422/2011] – TOL2.712.104).

De este modo, la primera de las cuestiones a analizar para concretar el sujeto responsable del perjuicio patrimonial causado es determinar si nos encontramos ante una operación realizada con o sin autorización del titular de la cuenta y, en su caso, si esa autorización ha sido obtenida mediante engaño por haber sido víctima de fraude o hackeo del que responderá, conforme al art. 45 Real Decreto-ley, el proveedor de servicios de pago. Nos encontramos, por lo tanto, ante un régimen de responsabilidad cuasi-objetivo con inversión de la carga de la prueba imputable a los proveedores de servicios de pago o de las entidades bancarias (responsabilidad solidaria del art. 132 TRLGDCU). El régimen de responsabilidad cuasi-objetiva de la entidad bancaria pivota sobre la base de la falta de diligencia en su actuación, por no contar con los mecanismos de seguridad y control necesarios en la banca on-line sin que pueda ser imputada al cliente una falta de autoprotección salvo que … "se trate de un engaño burdo o fácilmente perceptible que hubiera podido ser evitado por cualquier sujeto pasivo con una mínima reacción defensiva". Es decir, desde el punto de la vista de la conducta del cliente, son dos las causas de exoneración de responsabilidad que habrán de ser probadas por la entidad: fraude o negligencia grave del titular de la cuenta bancaria.

En definitiva, únicamente las actuaciones fraudulentas o por negligencia grave del ordenante son causas de exoneración de toda responsabilidad del proveedor de servicios de pagos. En este sentido, lo determinante será concretar qué hemos de entender por supuestos de negligencia grave del ordenante. Tomando como referencia lo expuesto en el Considerando 72 de la Directiva (UE) 2015/2366, del Parlamento y del Consejo, de 25 de noviembre, sobre Servicios de Pago en el Mercado Interior –Directiva PSD2-, el ordenante debe incumplir su deber de diligencia de manera grave o significativa, por ejemplo, guardando las credenciales usadas para dar autorización del pago junto al propio instrumento del pago, en formato abierto y fácilmente detectable para terceros. Este ejemplo ofrecido por la Directiva parece fácilmente comprensible, pero llevando este ejemplo al supuesto objetivo de análisis en este estudio –casos de fraude vía *phishing*-, ¿hacer click en el enlace recibido a través de un SMS o correo electrónico e introducir las claves de usuario de la banca online, sería un acto gravemente negligente del usuario? Conforme a la jurisprudencia desarrollada hasta la actualidad, podemos afirmar que los tribunales españoles, por regla general, consideran que estas conductas engañosas no son fácilmente reconocibles por los usuarios por tratarte de técnicas sofisticadas de suplantación de identidad de las entidades bancarias. Sin embargo, auguramos que esta protección al usuario víctima de estafa a través de esta técnica puede no ser definitiva o eternamente mantenida a medida que la educación de consumidor o cliente bancario le permita ignorar cualquier mensaje

mínimamente sospechoso de ser irregular o, en su caso, acudir directamente a la entidad bancaria para comprobar su veracidad.

BIBLIOGRAFIA

AA.VV.: *Jurisprudencia sobre hipotecas y contratos bancarios y financieros.*, C.C. Castillo Martínez (dir.), Tirant Lo Blanch, Valencia, 2019.

Alonso Espinosa, F.J.: "Orden falsa de transferencia y responsabilidad del banco: comentario a la STS (Sala 1ª) de 25 de julio de 1991", *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía,* Núm. 1, 1992.

Alvarez Lata N.: "La responsabilidad civil por actividades empresariales en sectores de riesgo", en Reglero Campos, L. F. (coord.), *Tratado de responsabilidad civil, II,* Cizur Menor, Aranzadi, 2008

Díaz Ruíz, E. y Ruíz Bachs, S.: "El depósito bancario estructurado" en *Revista de derecho bancario y bursátil,* Núm. 89, 2003.

Emparanza Sobejano, A y Martínez Giner, L.A.: "El depósito bancario. Las libretas de ahorro" en *Contratos bancarios,* Tomo X, Aranzadi, Cizur Menor, 2014.

Garcia Garcia, D.E.: "El phising como delito de estafa informática. Comentario a la SAP de Valencia 37/2017, de 25 de enero (Rec. 1402/2016)", *Revista Boliviana de Derecho,* Núm. 25, 2018.

García-Pita y Lastres, J.L.: "Bases para una revisión del régimen de los depósitos bancarios de efectivo" en *Revista de Derecho Bancario y Bursátil,* Núm. 143, 2016.

Hualde Manso, M.T.:

"Causa, función y perversión del depósito bancario a la vista" en *Revista de derecho bancario y bursátil,* Núm. 136, 2014.

"El depósito bancario a la vista" en *Operaciones bancarias de activo y pasivo en el contexto de crisis económica: hacia la unificación de la contratación bancaria,* M.A., Egusquiza Balmaseda, Rafael Lara González (coord..), Aranzadi, Cizur Menor, 2015.

Madrazo Leal, J.: "Aproximación al depósito bancario conjunto" en *Homenaje a Luis Rojo Ajuria: escritos jurídicos.* Universidad de Cantabria, Santander, 2003.

Martín Santisteban, S.: *El depósito y la responsabilidad del depositario.* Aranzadi, Cizur Menor, 2002.

Pablo-Romero Gil-Delgado, M.C.: "El contrato de cuenta corriente bancaria" en *Operaciones bancarias de activo y pasivo en el contexto de crisis económica: hacia la unificación de la contratación privada,* Aranzadi, Cizur Menor, 2015.

SÁNCHEZ-CALERO GUILARTE, J.: "La cuenta corriente y la transferencia bancaria (observaciones a sus aspectos más discutidos)" en *Revista de Derecho Bancario y Bursátil,* Núm. 86, 2002.

TOMILLO URBINA, J.L.: "El depósito bancario" en *Contratación bancaria: doctrina, jurisprudencia y formularios.* J.L., Tomillo Urbina, F.J., Orduña Moreno, A.B., Campuzano Laguillo (coord..), Tirant Lo Blanch, Valencia, 2001.

VICENT CHULIÁ, F.: *Compendio crítico de Derecho Mercantil*, Bosch, Barcelona 1990.