Roj: SAP S 1277/2023 - **ECLI:**ES:APS:2023:1277
Órgano: Audiencia Provincial
Sede: Santander
Sección: 2
Nº de Recurso: 206/2022
Nº de Resolución: 497/2023
Fecha de Resolución: 10/10/2023
Procedimiento: Recurso de apelación. Juicio ordinario
Ponente: LAURA CUEVAS RAMOS
Tipo de Resolución: Sentencia

Encabezamiento

S E N T E N C I A nº 000497/2023

Ilmo. Sr. Presidente.

D. José Arsuaga Cortázar.

Ilmos. Srs. Magistrados.

D. Justo Manuel García Barros.

Dª. Laura Cuevas Ramos.

==========

En la Ciudad de Santander, a diez de octubre de dos mil veintitrés.

Esta *Sección Segunda de la Ilma. Audiencia Provincial de Cantabria ha visto en grado de apelación los presentes Autos de juicio ordinario, número 513 de 2021 , Rollo de Sala número 206 de 2022, procedentes del Juzgado de Primera Instancia* núm. 5 de Santander seguidos a instancia de Bernardo contra Banco Bilbao Vizcaya Argentaria.

En esta segunda instancia ha sido parte apelante, Bernardo representado por la Procuradora Sr. Martínez Rodríguez y defendido por el Letrado Sr. Nieto Cuartango; y apelada Banco Bilbao Vizcaya Argentaria, representada por el Procurador Sra. Ruiz Sierra y defendido por la Letrada Sra. Sarabia Ortiz.

Es ponente de esta resolución la Ilma. Sra. Magistrada Dña. Laura Cuevas Ramos.

ANTECEDENTES DE HECHO

PRIMERO: Por el Ilmo. Sr. Magistrado-Juez del Juzgado de Primera Instancia núm. 5 , y en los autos ya referenciados, se dictó en fecha Sentencia cuya parte dispositiva es del tenor literal siguiente: ***"FALLO: Que*** **DESESTIMANDO LA DEMANDA** ***interpuesta por el Procurador Sr. MARTÍNEZ RODRIGUEZ en nombre y representación de Bernardo, frente a BANCO BILBAO VIZCAYA ARGENTARIA S.A. (BBVA), representado por la procuradora Sra. RUIZ SIERRA***

debo absolver a este de la pretensión ejercitada imponiendo a aquel el pago de las costas causadas.

SEGUNDO: Contra dicha Sentencia la representación de la parte actora interpuso recurso de apelación, que se tuvo por interpuesto en tiempo y forma, y dado traslado del mismo a la contraparte, que se opuso al recurso, se elevaron las actuaciones a esta Ilma. Audiencia Provincial, en que se ha deliberado y fallado el recurso en el día señalado.

TERCERO: En la tramitación del recurso se han observado las prescripciones legales salvo el plazo de resolución en razón al número de recursos pendientes y su orden.

FUNDAMENTOS DE DERECHO

Se admiten los de la Sentencia de instancia, en tanto no sean contradictorios con los que a continuación se establecen; y

PRIMERO. Resumen de antecedentes y planteamiento del recurso.

1. D. Bernardo presentó demanda de juicio ordinario contra BBVA, al amparo del Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, exigiéndole responsabilidad por una trasferencia, por importe de 9.987 €, realizada desde su cuenta corriente a la cuenta de un tercero, tras introducir, como acto reflejo el código que se le solicitaba en la pantalla, mientras consultaba su cuenta a través de la App de la entidad y aparecía un mensaje de actualización del módulo de seguridad en el que se le avisaba de la futura necesidad de insertar un código de autorización, sin que el banco procediese a cancelar o bloquear la transferencia a pesar de haberlo solicitado instantes después de realizarla y percatarse que había sido objeto de una estafa.

2. La demandada contesta a la demanda oponiéndose e instando su desestimación con el argumento que ninguna intervención tuvo la entidad porque ninguna actualización lleva a cabo ese día en su aplicación, desconociéndose si el demandado entró en la app de BBVA o en otra que al suplantaba, no siéndole imputable responsabilidad en el engaño que pudiera haber sufrido el demandante, quien incurrió en negligencia al facilitar sus claves a terceros e introdujo el código que se le facilitara sin leer siquiera el mensaje que le solicitaba dicho código para realizar la transferencia.

3. La *sentencia del juzgado de primera instancia nº 5 de Santander de 11 de enero de 2022* desestima la demanda con absolución a la entidad bancaria.

Razona el juez de instancia sus conclusiones y decisión en que la prueba practicada acredita la existencia de imprudencia por parte del actor, quien, tras recibir en su teléfono móvil un mensaje solicitándole que para realizar la transferencia de 9.987 € introdujese el Código que se le facilitaba, sin leer el mensaje con la mínima atención, introdujo el código sin el cual no podía haberse realizado la transferencia, constituyendo tales códigos un elemento de seguridad adicional a la hora de realizar una transferencia, siendo el propio cliente, que está en posesión del dispositivo - teléfono móvil - quien tiene que autorizar la operación. Concluye la sentencia que, por mucho que el presunto estafador pudiera averiguar las claves de banca on-line del demandante, o pudiera acceder a su perfil, nunca podría hacer una transferencia sin la colaboración activa de aquel, siendo el destinatario de la cuenta de

destino quien tiene que autorizar a la devolución de los fondos. El mismo modo, considera que la celeridad con que el actor comunicó al banco lo ocurrido es irrelevante en esta caso

4. El actor interpone recurso de apelación alegando error en la valoración de prueba e incorrecta aplicación de la Ley de protección de pagos y la jurisprudencia existente que concreta en que: (i) la existencia del engaño es suficiente para excluir la negligencia por parte del cliente; (ii) el recurrente comunicó el fraude de inmediato a la entidad que no actuó con la diligencia debida y no hizo nada y, a partir de la comunicación la responsabilidad recae sobre el proveedor de servicios de pago, siendo incoherente pensar entender que ha de ser el estafador quien ha de reintegrar los fondos; (iii) falta de seguridad del BBVA que, a diferencia de otras entidades bancarias no implementa un sistema de anulación de las transferencias realizadas "online" y (iv) el reconocimiento en la sentencia de que el demandante ha sido objeto de un engaño por tercero y lo ha comunicado inmediatamente, determina que puedan existir dudas de hecho o de derecho, que justifica la no imposición de las costas.

5. La actora formula expresa oposición al recurso de la comunidad, interesando su íntegra desestimación con imposición de costas a la apelante.

SEGUNDO. - Phishing. Modalidad de fraude informático.

Se centra el presente procedimiento en un supuesto de fraude informático conocido como " phishing ", denominación que proviene del inglés "fishing" (pesca) y que es resultado de la contracción de la frase "password harvesting fishing" (cosecha y pesca de contraseñas).

De acuerdo con la definición dada por la Agencia Española de Protección de Datos, en resolución de fecha 24 de mayo d 2006 "el objetivo de los ataques de " phishing " es la obtención de forma engañosa y fraudulenta de los códigos de usuarios y contraseñas de clientes de Banca Electrónica, al objeto de realizar transferencias no autorizadas... Su operatoria comienza con la adquisición en internet de un "paquete de herramientas", que incluyen programas informáticos e información necesaria para realizar los ataques. Esta información incluye "listas de equipos comprometidos" que pueden ser utilizados bien para mandar correos electrónicos, bien para alojar páginas web falsificadas. Incluyen además "bases de datos de direcciones de correo electrónico". Una vez en posesión del paquete, se remiten los correos electrónicos con carácter indiscriminado (buscando contactar con clientes de la entidad financiera) informando de la necesidad de conectarse a una página web que parece pertenecer a la citada entidad y portar los códigos de acceso y contraseñas de clientes. Dicha página web se suele alojar en un equipo conectado a Internet cuya seguridad se haya [visto] comprometida", sin conocimiento de su usuario, y que se encuentra normalmente en un país distinto al de los destinatarios del ataque. De esta forma se constituye "un fichero de datos personales con códigos de usuarios y contraseñas de clientes" recabados de forma engañosa y fraudulenta, que se ubica normalmente en el mismo "equipo remoto comprometido" en el que se aloja la página web falsificada. Con los datos obtenidos se realizan trasferencias a cuentas de colaboradores situados en España los cuales a su vez retiran el dinero en efectivo y tras descontar una comisión realizan transferencias monetarias internacionales mediante entidades especializadas."

Habitualmente se hace efectiva a través del envío de correos electrónicos o SMS engañosos, en los que se imita el lenguaje, formato e imagen de las entidades bancarias o financieras suplantando su identidad y, solicitando los datos personales de las víctimas alegando diferentes motivos. Los métodos empleados para este tipo fraude

son diversos (clonación de tarjetas, skimming o carcasa superpuesta, el pharming o introducirse en un servidor a través de hackers, capturando claves, contraseñas, etc.) y no necesariamente llega a descubrirse en todos los supuestos el concreto método empleado; si bien es evidente, en cualquier caso, que se trata de una operación no autorizada por el titular de la cuenta corriente, el cual ve sustraído sus datos y claves de una manera fraudulenta, a través de medios técnicos.

TERCERO. - Hechos y circunstancias relevantes para la decisión del Tribunal.

1. En fecha 27 de agosto de 2020, mientras D. Bernardo consultaba sus datos bancarios a través de la aplicación de banca electrónica de la entidad BBVA, apareció un mensaje en la pantalla que le avisaba de que se estaba actualizando el módulo de seguridad, requiriéndole para que permaneciera atento ya que podían solicitarse ciertas informaciones.

2. A las 16,10 horas de la misma fecha recibió en su teléfono móvil el siguiente SMS "para realizar la transferencia de 9.987 € y cuenta destino NUM000 utiliza el código NUM001 ". El demandante introdujo el código requerido, comunicándosele a continuación que la transferencia se había hecho efectiva. La cuenta en cuestión pertenece a la misma entidad - así resulta del código de entidad de la misma - se hizo efectiva, siendo su titular D. Eugenio, que ha resultado ser el beneficiario.

3. Según el detalle de consumo desde su teléfono móvil D. Bernardo se puso en contacto con la entidad BBVA varias veces esa misma tarde y, con posterioridad ha solicitado información sobre su reclamación. Finalmente, en fecha 16 de noviembre de 2020, el servicio de Atención del Cliente contestó a su reclamación, manifestándole que, según la Memoria del Departamento de Conducta del Banco de España del año 2019 y el criterio del Servicio de reclamaciones del Banco de España, cuando una orden de pago se ejecute conforme al identificador único, dicha orden se considerará correctamente ejecutada en relación con al beneficiario indicado en dicho identificador, no siendo responsable el proveedor de servicios de pago de la no ejecución o ejecución defectuosa de la operación cuando el identificador único que le hubiera facilitado el usurario fuera incorrecto, y cuando se trate de errores imputables al cliente ordenante, el criterio de dicho servicio de reclamaciones es que, una vez asentada la transferencia en la cuenta destinataria, incluso aunque quede demostrado que el abono es erróneo, se considera que al entidad receptora no está facultada para su retrocesión en virtud de simples instrucciones del ordenante de la transferencia ya que, en virtud del principio de irrevocabilidad de estas operaciones de pago, las cantidades abonadas en la cuenta del beneficiario no pueden ser retrotraídas si no media el oportuno consentimiento de este o la preceptiva orden o mandato legal. Con base en dichos criterios, el banco rechaza la reclamación e informa de que ha solicitado a la entidad receptora que solicitase el consentimiento de su cliente para la anulación de la operación, no habiendo sido posible obtener su autorización hasta la fecha.

TERCERO. - Marco normativo y jurisprudencial.

Las obligaciones exigibles a las entidades bancarias como proveedoras de pago, en relación con los instrumentos de y sistemas de pago que ponen a disposición de sus clientas en cuanto a la garantía del buen funcionamiento de los mismos preservándolos frente al fraude, se recoge, en el ámbito de la legislación nacional, en el Real Decreto Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en adelante, LSP),aprobado para transponer, entre otras, la *directiva UE 2015/2366* en materia de servicios de - la denominada

"PSD2" -, complementada por el Reglamento Delegado (UE) 2018/396 de la Comisión de 27 de noviembre de 2017, con el objetivo de mejorar la protección de los usuarios de los servicios de pago, obligando a las entidades a usar la autentificación reforzada incrementando la protección de los clientes frente a sus pagos.

La norma contiene la siguiente regulación:

Artículo 41. Obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas. El usuario de servicios de pago habilitado para utilizar un instrumento de pago: a) utilizará 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 y, en particular, en cuanto reciba un instrumento de pago, tomará todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas.

Artículo 42. Obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago. 1. El proveedor de servicios de pago emisor de un instrumento de pago: a) Se cerciorará de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento, sin perjuicio de las obligaciones que incumben al usuario de servicios de pago con arreglo al artículo 41. b) Se abstendrá de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso de que deba sustituirse un instrumento de pago ya entregado al usuario de servicios de pago. Esta sustitución podrá venir motivada por la incorporación al instrumento de pago de nuevas funcionalidades, no expresamente solicitadas por el usuario, siempre que en el contrato marco se hubiera previsto tal posibilidad y la sustitución se realice con carácter gratuito para el cliente. c) Garantizará que en todo momento estén disponibles medios adecuados y gratuitos que permitan al usuario de servicios de pago efectuar una notificación en virtud del artículo 41.b), o solicitar un desbloqueo con arreglo a lo dispuesto en el artículo 40.4. A este respecto, el proveedor de servicios de pago facilitará, también gratuitamente, al usuario de dichos servicios, cuando éste se lo requiera, medios tales que le permitan demostrar que ha efectuado dicha comunicación, durante los 18 meses siguientes a la misma. d) Ofrecerá al usuario de servicios de pago la posibilidad de efectuar una notificación en virtud del artículo 41.b), gratuitamente y cobrar, si acaso, únicamente los costes de sustitución directamente imputables al instrumento de pago. e) Impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación en virtud del artículo 41.b). 2. El proveedor de servicios de pago soportará los riesgos derivados del envío de un instrumento de pago al usuario de servicios de pago o del envío de cualesquiera elementos de seguridad personalizados del mismo.

Artículo 43. Notificación y rectificación de operaciones de pago no autorizadas o ejecutadas incorrectamente. 1. El usuario de servicios de pago obtendrá la rectificación por parte del proveedor de servicios de pago de una operación de pago no autorizada o ejecutada incorrectamente únicamente 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, incluso las cubiertas por el artículo 60, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo. Los plazos para la notificación establecidos en el párrafo primero no se aplicarán cuando el proveedor de servicios de pago no le haya proporcionado ni puesto a su disposición la información sobre la operación de pago con arreglo a lo establecido en el título II.

Artículo 44. Prueba de la autenticación y ejecución de las operaciones de pago. 1. 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. Si el usuario de servicios de pago inicia la operación de pago a través de un proveedor de servicios de iniciación de pagos, corresponderá a éste demostrar que, dentro de su ámbito de competencia, la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable. 2. A los efectos de lo establecido en el apartado anterior, el registro por el proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 41. 3. 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. 4. El proveedor de servicios de pago conservará la documentación y los registros que le permitan acreditar el cumplimiento de las obligaciones establecidas en este Título y sus disposiciones de desarrollo y las facilitará al usuario en el caso de que así le sea solicitado, durante, al menos, seis años. No obstante, el proveedor de servicios de pago conservará la documentación relativa al nacimiento, modificación y extinción de la relación jurídica que le une con cada usuario de servicios de pago al menos durante el periodo en que, a tenor de las normas sobre prescripción puedan resultarles conveniente para promover el ejercicio de sus derechos contractuales o sea posible que les llegue a ser exigido el cumplimiento de sus obligaciones contractuales. Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, así como en otras disposiciones nacionales o de la Unión Europea aplicables.

Artículo 45. Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas. 1. Sin perjuicio del artículo 43 de este real decreto-ley, 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. La fecha de valor del abono en la cuenta de pago del ordenante no será posterior a la fecha de adeudo del importe devuelto. 2. Cuando la operación de pago se inicie a través de un proveedor de servicios de iniciación de pagos, el proveedor de servicios de pago gestor de cuenta devolverá inmediatamente y, en cualquier caso, a más tardar al final del día hábil siguiente, el importe de la operación de pago no autorizada y, en su caso, 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. Si el responsable de la operación de pago no autorizada es el proveedor de servicios de iniciación de pagos, deberá resarcir de inmediato al proveedor de servicios de pago gestor de cuenta, a petición de este, por las pérdidas sufridas o las sumas abonadas para efectuar la

devolución al ordenante, incluido el importe de la operación de pago no autorizada. De conformidad con el artículo 44.1, corresponderá al proveedor de servicios de iniciación de pagos demostrar que, dentro de su ámbito de competencia, la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable. 3. Podrán determinarse otras indemnizaciones económicas de conformidad con la normativa aplicable al contrato celebrado entre el ordenante y el proveedor de servicios de pago o el contrato celebrado entre el ordenante y el proveedor de servicios de iniciación de pagos, en su caso.

Artículo 46. Responsabilidad del ordenante en caso de operaciones de pago no autorizadas. 1. No obstante lo dispuesto en el artículo 45, el ordenante podrá quedar obligado a soportar, hasta un máximo de 50 euros, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero, salvo que: a) al ordenante no le resultara posible detectar la pérdida, la sustracción o la apropiación indebida de un instrumento de pago antes de un pago, salvo cuando el propio ordenante haya actuado fraudulentamente, o b) la pérdida se debiera a la acción o inacción de empleados o de cualquier agente, sucursal o entidad de un proveedor de servicios de pago al que se hayan externalizado actividades. El ordenante soportará todas las pérdidas derivadas de operaciones de pago no autorizadas si el ordenante ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41. En esos casos, no será de aplicación el importe máximo contemplado en el párrafo primero. En todo caso, el ordenante quedará exento de toda responsabilidad en caso de sustracción, extravío o apropiación indebida de un instrumento de pago cuando las operaciones se hayan efectuado de forma no presencial utilizando únicamente los datos de pago impresos en el propio instrumento, siempre que no se haya producido fraude o negligencia grave por su parte en el cumplimiento de sus obligaciones de custodia del instrumento de pago y las credenciales de seguridad y haya notificado dicha circunstancia sin demora. 2. Si el proveedor de servicios de pago del ordenante no exige autenticación reforzada de cliente, el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta. En el supuesto de que el beneficiario o el proveedor de servicios de pago del beneficiario no acepten la autenticación reforzada del cliente, deberán reembolsar el importe del perjuicio financiero causado al proveedor de servicios de pago del ordenante. 3. Salvo en caso de actuación fraudulenta, el ordenante no soportará consecuencia económica alguna por la utilización, con posterioridad a la notificación a que se refiere el artículo 41.b), de un instrumento de pago extraviado o sustraído. 4. Si el proveedor de servicios de pago no tiene disponibles medios adecuados para que pueda notificarse en todo momento el extravío o la sustracción de un instrumento de pago, según lo dispuesto en el artículo 42.1.c), el ordenante no será responsable de las consecuencias económicas que se deriven de la utilización de dicho instrumento de pago, salvo en caso de que haya actuado de manera fraudulenta".

En cuanto a la más reciente jurisprudencia en la materia, señala la ***SAP de Madrid, Sec. 10ª, de 13 de enero de 2023***

"Sobre la jurisprudencia aplicable, la sentencia de la Audiencia Provincial de Madrid, sección 11ª, de fecha 28 de febrero de 2022 , hace un compendio de la misma y se menciona la sentencia de la Audiencia Provincial de Madrid (Sección 9ª) núm. 178/2015 de 4 mayo de 2015 (JUR 201551311), que se pronuncia en el sentido siguiente: ..." Salvo actuación fraudulenta, incumplimiento deliberado o

negligencia grave del ordenante (Art. 32), la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago " no se vio afectada por un fallo técnico o cualquier otra deficiencia" (art 30).

La responsabilidad contemplada en esta Ley es cuasi-objetiva, es decir, se trata de una responsabilidad de la entidad que presta servicios de pago que sólo permite exonerarse mediante la prueba de la culpa grave del ordenante.

Esta interpretación efectuada de la Ley 16/2009, de 13 de noviembre, de servicios de pago, es absolutamente acorde no sólo con la literalidad de la norma, sino con el espíritu y finalidad de la misma (ex. art. 3 CC), en función de lo previsto, por tanto, en los artículos 30 y 32 de la mentada Ley 16/2009, de 13 de noviembre , de servicios de pago.

En base a todos estos criterios la sentencia de la Audiencia Provincial de Madrid Sección 9ª 178/2015 de 4 mayo de 2015 (JUR 201551311), condena a la entidad al reembolso de las cantidades, señalando que la Ley de los Servicios de Pago establece un sistema de responsabilidad cuasi objetiva para la entidad financiera, previendo que en caso de disposiciones fraudulentas el proveedor de servicios de pago deberá devolver de inmediato el importe de la operación no autorizada, (art. 31), quedando exento de esta obligación solo en el caso de que la operación no autorizada sea fruto de la actuación fraudulenta del cliente o del incumplimiento, deliberado o por negligencia grave, de una o varias de sus obligaciones (art. 32). Además, la Ley prevé una inversión de la carga de la prueba en tanto es el proveedor de los servicios, quien debe probar que la operación fue debidamente autenticada, cuando el usuario de los servicios lo niegue (art. 30)" .

El carácter de cuasiobjetiva de la responsabilidad de la entidad bancaria, que sólo puede exonerarse si acredita la concurrencia de actividad fraudulenta o culpa grave del cliente, ha sido indicado también, entre otras, por las *sentencias de las AAPP de Badajoz, de 7 de febrero de 2023* , *la Rioja, de 17 de febrero de 2023* y *Alicante, de 12 de marzo de 2018* .

Especial mención merece la última *sentencia citada, de la* ***Audiencia Provincial de Alicante (632/2018, de 12 de marzo*** , como referencia por su claridad y extensión sobre la cuestión de la carga de la prueba, señalando:

"..... es que no es cierto que la carga de la prueba sobre la implementación de medidas de seguridad adecuadas, suficientes, eficientes y actuales al nivel de riesgo modalidades de ataques informáticos en la red bancaria de banca online lo sea a cargo del usuario del sistema, pues el marco de responsabilidad establecido para el caso de operaciones de pagos hechos por proveedores de servicios no autorizadas o ejecutadas incorrectamente, es el de la cuasi-objetividad tal cual se desprende de la regulación específica sobre la materia -a la que seguidamente aludiremos-, sin perjuicio del régimen general de la carga de la prueba. Tres son las razones que abogan la contrariedad del argumento del recurrente, a saber, el contenido del precepto que se dice infringido - art 217 LEC - y, por llamada del mismo, la legislación de consumo y la legislación específica de servicios de pago. Por lo que hace al contenido del art. 217 LEC, hemos de recordar que párrafo séptimo establece que " para la aplicación de lo dispuesto en los apartados anteriores de este artículo el Tribunal deberá tener presente la disponibilidad y facilidad probatoria que corresponde a cada una de las partes del litigio". Para valorar el alcance de esta norma al caso hemos de entender que la regla general aplicable a la prestación de servicios que no

tenga adjetivada una especial peligrosidad o requiera de un particular cuidado ha de ser la regla general del art. 217 LEC , de manera que cuando se trata de prestaciones contractuales o no contractuales, del tenor del art. 1101 y 1902 Cc en relación al art. 217.2 LEC se desprenderá que corresponde al perjudicado demandante la carga de la prueba de la culpa del causante del daño demandado. Ahora bien, no es así cuando " una disposición legal expresa" -art 217.6- imponga al demandado la carga de probar que hizo cuanto le era exigible para prevenir el daño; o cuando tal inversión de la carga de la prueba venga reclamada por los principios de " disponibilidad y facilidad probatoria " a los que se refiere el artículo 217.7 LEC , y ello sin perjuicio de que en aplicación de lo dispuesto en el artículo 386 LEC el tribunal pueda imputar la culpa al demandado del resultado dañoso acaecido cuando, por las especiales características de éste y conforme a una máxima de la experiencia, pertenezca a una categoría de resultados que típicamente se produzcan (sean realización de un riesgo creado) por impericia o negligencia, y no proporcione el demandado al tribunal una explicación causal de ese resultado dañoso que, como excepción a aquella máxima, excluya la culpa por su parte. La lógica de la norma de acceso a la fuente de la prueba y facilidad probatoria en lo que hace a la implementación de medidas de seguridad en la prestación de un servicio que se da por las entidades de crédito a sus clientes a través de una oficina virtual que se desenvuelve en redes bien de internet, bien de comunicaciones móviles, se presenta como criterio más que de razonable atención al caso en el que la propia seguridad y debida reserva de la red se contrapone al acceso por parte de un tercero distinto al titular de la misma que asume poner en la red pública un conjunto de comunicaciones para permitir operaciones bancarias que requiere de soluciones tecnológicas muy avanzadas que minimicen las amenazas contra la autenticidad, integridad y la confidencialidad de los datos que circulan a través de la red. Por otro lado, el apartado 6 del artículo 217 LEC dispone que las normas contenidas en los apartados precedentes "se aplicarán siempre que una disposición legal expresa no distribuya con criterios especiales la carga de probar los hechos relevantes". (...) En este caso, la disposición expresa existe, tanto en el ámbito de consumo, como e la regulación de los servicios de pago".

Indica la sentencia que la configuración de la específica modalidad de responsabilidad que asume le prestador y, con ellos la variación del régimen legal del sistema del gravamen probatorio y, concluye, en relación con la carga de la prueba, que la responsabilidad del proveedor de los servicios de banca online, es de riesgo y consecuentemente, es por ley que a la entidad corresponde acreditar que la operación ordenada sí fue auténtica y que no estuvo afectada por un fallo técnico o por otra deficiencia como, por ejemplo, por un ataque informático de naturaleza fraudulenta al sistema bancario que hubiera permitido el acceso a las cuentas de sus clientes y disponer ilícitamente, de las mismas ordenando operaciones en detrimento de aquellos. Y recuerda que, siendo Internet una red pública de comunicaciones, la seguridad de las operaciones bancarias precisa de soluciones tecnologías avanzadas a los efectos de garantizar tanto la autenticidad como la integridad y la confidencialidad de los datos motivo por el que las entidades prestadoras del servicio de banca online deben dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones, siendo consecuencia de dicha omisión, deficiencia o defectuoso funcionamiento que deban asumir la responsabilidad por los fallos de seguridad del sistema.

Según lo expuesto, salvo la actuación fraudulenta, incumplimiento deliberado o negligencia grave del usuario, la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago " no se vio afectada por un fallo técnico o cualquier otra deficiencia". La

interpretación efectuada por la Juzgadora ad quem de la Ley 16/2009, de 13 de noviembre, de servicios de pago, es acorde no sólo con la literalidad de la norma, sino con el espíritu y finalidad de la misma (ex. *art. 3 CC*), lo que obligó a la determinación de la responsabilidad de la entidad bancaria a pesar de sus afirmaciones sobre la implementación de un modelo seguro de banca online, lo que no implica que el sistema fuera genéricamente seguro, pero como es evidente no lo fue en el presente caso. Tampoco sirve de excusa a la entidad apelada la inclusión de avisos en web y otros medios de la entidad sobre el comportamiento seguro que en el uso de la plataforma había de tener el cliente, sino que la entidad bancaria debe dotar a la banca electrónica de las medidas de seguridad necesarias para prevenir unos tipos de fraude ya muy extendidos y que, como lo prueba el supuesto que nos ocupa, siguen produciéndose por falta de una medida adecuadas por la entidades bancarias, que ponen a disposición de sus clientes la banca online y la contratación electrónica como dotados de una seguridad que no garantizan.

Y la ***SAP de Madrid, Sec. 20ª de 20 de mayo de 2022*** **,** argumenta sobre este mecanismo de fraude informático.

" TERCERO.- La aplicación de la normativa anteriormente indicada al caso presente, nos lleva a estimar la impugnación formulada por el demandante en cuanto, no discutiéndose la forma en que se llegaron a materializar las 6 retiradas de efectivo por un importe total de 6.000 € , iniciadas por una actuación fraudulenta de tercero, no cabe apreciar en el demandante un comportamiento negligente de la gravedad y entidad para con base en el mismo hacerle responsable, ni siquiera de la primera disposición de efectivo realizada con la tarjeta usada de manera fraudulenta por un tercero. Como se indica en la Directiva 2015/2036 la negligencia que le hace responder al cliente, es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que ha sido inducido por un delincuente profesional. Tampoco puede calificarse como grave dicho comportamiento conforme a la normativa del código civil, pues siendo exigible al demandante la diligencia que exija la naturaleza de la obligación y correspondan a las circunstancias de las personas, tiempo y lugar (art. 1.104 del cc), el método fraudulento empleado - phishing - es de una complejidad y grado de perfección, difícilmente detectable por un cliente de las características del demandante, sin que la forma en que se denominaba al Banco en el SMS recibido o el error gramatical al emplear la palabro "lo" en lugar de "le", sean errores de entidad suficiente para detectar con base en ellos el fraude de que estaba siendo objeto. En esas circunstancias, era preciso ser un experto en la materia para poder detectar que la comunicación obedecía a una estafa o fraude. Es cierto que dicho comportamiento no puede considerarse diligente, pero para hacer soportar al cliente las consecuencias, aún parciales como se concluye en la sentencia apelada, es preciso apreciar en él una negligencia y que además sea grave, que en la normativa europea antes referida se equipara a la comisión de un fraude, actuación en la que no se ha acreditado incurriese el demandante, por el hecho de haber pinchado el link que se le ofrecía y facilitar los datos y clave de la tarjeta

CUARTO .- Por el contrario, la responsabilidad exigida a la entidad demandada, como proveedora del servicio, es la que se deriva de la naturaleza de tal prestación y de la posición contractual en la que se encuentran las partes, lo que le obliga a adoptar una serie de medidas de seguridad y dotarse de mecanismos de supervisión que permitieran detectar operaciones fraudulentas en la prestación de servicios de pago, tal como señala el artículo 2 del Reglamento Delegado 2018/389 , pues como se indica también en la sentencia citada de la Audiencia de

Pontevedra, incluyendo la técnica del phishing, la creación y puesta en la red de páginas que clonan las del sitio oficial de las entidades emisoras de instrumentos de pago, el deber de diligencia de la entidad demandada exigía dotarse de la tecnología antiphishing precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas, lo que, de producirse, impediría que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace del correo electrónico haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor. Dicha actuación diligente no puede considerarse acreditada por las informaciones que se facilita a los clientes a través de su página web, en cuanto la efectividad de esas obligaciones preventivas, lo que requerían era implementar en el sistema informático el mecanismo tecnológico adecuado para evitarlo; es decir mediante una con una conducta activa y no simplemente informativa o divulgativa" .

En el mismo sentido en que lo hace la Audiencia Provincial de Madrid, de incidir en la insuficiencia de avisos o advertencias genéricas a través de la web, se pronuncian las *SSAAPP La Rioja, de 17 de febrero de 2023* , que recuerda que" *es el banco quien ofrece este producto, en principio seguro, y es cierto que remite avisos y advertencias genéricas sobre su utilización; pero conociendo los distintos riesgos de los que avisa, le corresponde adoptar las medidas de seguridad o control necesarias, que en este caso no consta que se adoptaran. Y no basta con medidas genéricas de protección o avisos estereotipados de cuidado, pues tales avisos ostentarían la calificación de "formulas predispuestas", vacías de contenido. No son los clientes los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, o estar al tanto de los mismos, ni prevenir con su asesoramiento experto dichos riesgos"* ; la de Asturias, Sec. 7ª, de 30 de junio de 2023, que cita la anterior; y la de Pontevedra, Sec. 3ª de 23 de marzo de 2023, que, a propósito del estudio de la negligencia grave del usuario indica *" partiendo del admitido criterio de responsabilidad cuasi-objetiva de la entidad en la prestación del servicio de banda virtual respecto a operaciones de pago como la transferencia, reiterada jurisprudencia considera que dicha negligencia debe ser grave en atención a las circunstancias demostradas del caso, atribuyéndose en todo caso la carga probatoria de la misma al proveedor del servicio con arreglo a art. 217 LEC . En interpretación de directiva 2015/2366 , la negligencia que hace responder al cliente es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que haya podido ser inducido por un delincuente profesional. Como parámetro del actuar negligente también cabrá acudir al art. 1.104 CC , que exige la diligencia asociada a la naturaleza de la obligación y a las circunstancias personales, de tiempo y lugar. Ello destacándose la complejidad y grado de perfección que presenta en la actualidad el método de " phishing " de difícil detección por persona de formación media, así como el deber de la proveedora, del servicio de dotarse de tecnología suficiente y adecuada con exigencia de medidas implantadoras activas, sin entenderse suficientes avisos generales o en página web de mero carácter informativo o divulgativo".*

De la legislación de protección de servicios de pago (RDL 19/2018, como de la jurisprudencia que lo aplica y lo interpreta pueden extraerse como conclusiones: (i) la ley establece un sistema de responsabilidad cuasiobjetiva de la entidad o proveedor de pagos, que deriva del incumplimiento por su parte de los deber de diligencia en la garantía de operaciones de pago, implementando todos los mecanismos y controles de autenticación necesarios, incluido dotarse de tecnología "antiphising", para para proteger al cliente de la actuación fraudulenta de terceros y (ii) la entidad solo puede liberarse de tal responsabilidad si prueba que la orden de pago no se vio afectada por "un fallo técnico u otra deficiencia del servicio prestado por dicho proveedor", que el

cliente ha actuado fraudulentamente o con negligencia grave a la hora de aplicar los medios razonables de protección de que haya sido provisto o cuando no haya comunicado a la entidad el pago no autorizado en cuanto tenga conocimiento del mismo.

CUARTO. - Resolución del recurso.

En este caso las circunstancias establecidas como relevantes tras la valoración de la prueba, determinan que deba de descartarse a la responsabilidad del banco por cuanto apreciamos negligencia grave en el usuario.

D. Remigio afirma que, mientras consultaba sus ingresos y gastos en la aplicación de la entidad BBVA apareció en la pantalla un mensaje de actualización del módulo de seguridad, donde se iba a requerir su autorización, ante lo cual nada sospecho sobre la posibilidad de que se tratase de un proceso fraudulento dado que, para realizar ciertas operaciones en la APP se pide autorización, de forma que, cuando en la pantalla de la APP bancaria apareció una ventana para escribir el Código de autorización, anotó el código de forma refleja sin leer el mensaje que lo acompañaba, reviendo seguidamente un mensaje que decía "transferencia realizada" por importe de 9.987€, percatándose en ese momento de que había sido objeto de una estafa informática.

No obstante, el relato fáctico de la demanda, el pantallazo que aporta revela que el actor entró en lo que parece ser la app auténtica de la entidad y que en la ventana que le advertía que se estaba llevando a cabo la actualización del módulo de seguridad, nada se decía de que se le solicitarían autorizaciones sino "manténgase atento, durante el proceso, algunas informaciones pueden ser solicitadas", sin que una información pueda equipararse a una autorización. Después, aparecería en la pantalla el requerimiento de una autorización, pero a la vez, como es de general conocimiento por ser lo habitual cuando se realizan operaciones a través de la app, recibió en la pantalla de su teléfono móvil un SMS, al que corresponde el otro pantallazo aportado, que, literalmente, decía "para realizar la transferencia de 9.987 € y cuenta destino NUM000 utiliza el código NUM001 ", que fue el que reconoce introdujo en la app, con el cual se materializó de transferencia. Pues bien, ni el mensaje que apareció en la ventana avisaba de que se le requeriría autorización alguna, ni el recibido en su teléfono móvil puede inducir a error a quien está acostumbrado a operar de esta manera, puesto que se refería claramente a una operación de transferencia, reflejando su importe y la cuenta destinataria, siendo idéntico a otro que había recibido con anterioridad que también aparece en el pantallazo. Así, requerida la introducción de un código para realizar la operación, habría bastado que el actor lo hubiera leído, lo cual asume que no hizo, para, si realmente en ese momento no estaba realizando una transferencia, no introducir el código, con la operación no se habría efectuado.

Sucede también que en los supuestos de " phishing " no es fácil identificar la cuenta de destino ni su titular, y, en este caso, el número aparecía en el mensaje y pertenece a la misma entidad, siendo su titular D. Eugenio, tal como consta en el documento bancario que aporta. Tal circunstancia incluso llega a generar dudas sobre si el actor realizó la transferencia de modo involuntario, lo la estaba efectuando voluntariamente.

En definitiva, las circunstancias concurrentes revelan que ha sido la negligencia del actor lo que ha provocado el traspaso de dinero desde su cuenta corriente, negligencia grave que viene determinada por el hecho de no haber observado la diligencia mínima de leer el mensaje de autorización recibido, cuyo conducido y datos

no eran susceptibles de inducir a error. De nada sirve que las entidades bancarias implementen medidas de seguridad para las operaciones realizadas a través de su app o su Web, como la solicitud del código de autorización de la operación, si el usuario realiza las autorizaciones de modo automático lo cual supone ignorar la medida de seguridad.

El recurso ha de ser desestimado.

QUINTO. - Costas procesales.

Desestimado el recurso so, en aplicación de los *arts. 393.1* y *394 LEC* , las costas de esta alzada se imponen a la recurrente, manteniéndose la imposición de costas de la primera instancia, por cuanto las circunstancias concurrentes en el supuesto no dan lugar a dudas de hecho ni de derecho.

Así, en ejercicio de la potestad jurisdiccional que nos ha conferido la Constitución Española, y en nombre de Su Majestad El Rey.

FALLAMOS

1. DESESTIMAMOS el recurso de apelación interpuesto por D. Bernardo, contra la *sentencia del Juzgado de Primera Instancia nº 5 de Santander de fecha 11 de enero de 2022* , que confirmamos en todos sus términos.

2. Imponemos al recurrente las costas de esta alzada.

DILIGENCIA: Seguidamente se procede a cumplimentar la notificación de la anterior resolución. Doy fe.