



Roj: **SAP M 249/2023 - ECLI:ES:APM:2023:249**

Id Cendoj: **28079370102023100011**

Órgano: **Audiencia Provincial**

Sede: **Madrid**

Sección: **10**

Fecha: **13/01/2023**

Nº de Recurso: **918/2022**

Nº de Resolución: **24/2023**

Procedimiento: **Recurso de apelación**

Ponente: **AMALIA DE SANTISIMA TRINIDAD SANZ FRANCO**

Tipo de Resolución: **Sentencia**

Audiencia Provincial Civil de Madrid

Sección Décima

c/ Santiago de Compostela, 100 , Planta 2 - 28035

Tfno.: 914933917,914933918

37007740

N.I.G.: 28.007.00.2-2021/0005945

Recurso de Apelación 918/2022

O. Judicial Origen: Juzgado Mixto nº 05 de Alcorcón

Autos de Procedimiento Ordinario 378/2021

APELANTE: BANCO SANTANDER

PROCURADOR D./Dña. MARIA JESUS GARCIA LETRADO

APELADO: D./Dña. Inocencia

PROCURADOR D./Dña. JUAN JOSE CEBRIAN BADENES

SENTENCIA N° 24/2023

ILMOS/AS SRES./SRAS. MAGISTRADOS/AS:

D./Dña. JOSÉ MANUEL ARIAS RODRÍGUEZ

D./Dña. MARIA BEGOÑA PEREZ SANZ

D./Dña. AMALIA DE LA SANTISIMA TRINIDAD SANZ FRANCO

En Madrid, a trece de enero de dos mil veintitrés.

La Sección Décima de la Ilma. Audiencia Provincial de esta Capital, constituida por los Sres. que al margen se expresan, ha visto en trámite de apelación los presentes autos civiles Procedimiento Ordinario 378/2021 seguidos en el Juzgado de 1ª Instancia e Instrucción nº 05 de Alcorcón a instancia de BANCO SANTANDER apelante - demandado, representado por el/la Procurador D./Dña. MARIA JESUS GARCIA LETRADO y defendido por Letrado, contra D./Dña. Inocencia apelado - demandante, representado por el/la Procurador D./Dña. JUAN JOSE CEBRIAN BADENES y defendido por Letrado; todo ello en virtud del recurso de apelación interpuesto contra Sentencia dictada por el mencionado Juzgado, de fecha 13/05/2022.

Se aceptan y se dan por reproducidos en lo esencial, los antecedentes de hecho de la Sentencia impugnada en cuanto se relacionan con la misma.

VISTO, Siendo Magistrada Ponente Dña. **AMALIA DE LA SANTISIMA TRINIDAD SANZ FRANCO**



ANTECEDENTES DE HECHO

PRIMERO.- Por Juzgado de 1ª Instancia e Instrucción nº 05 de Alcorcón se dictó Sentencia de fecha 13/05/2022, cuyo fallo es el tenor siguiente:

Que debo estimar y **ESTIMO** la demanda formulada por **DOÑA Inocencia**, representada por el Procurador Don Juan José Cebrián Bádenes, frente al **BANCO SANTANDER S.A.**, representado por la Procuradora Doña María Jesús García Letrado; en su consecuencia, debo condenar y **CONDENO** a la parte demandada a que abone a la demandante la suma de **17.350,00 euros**, que devengará el interés legal previsto en el Fundamento Cuarto de la presente resolución.

Se imponen las costas a la parte demandada.

SEGUNDO.- Contra la anterior resolución se interpuso recurso de apelación por la parte demandada, que fue admitido, y, en su virtud, previos los oportunos emplazamientos, se remitieron las actuaciones a esta Sección, sustanciándose el recurso por sus trámites legales.

TERCERO.- Por providencia de esta Sección, de fecha 13/12/2022, se acordó que no era necesaria la celebración de vista pública, quedando en turno de señalamiento para la correspondiente deliberación, votación y fallo, turno que se ha cumplido el día 10/01/2023.

CUARTO.- En la tramitación del presente procedimiento han sido observadas en ambas instancias las prescripciones legales.

FUNDAMENTOS JURIDICOS

PRIMERO.- Por la representación procesal de Dª Inocencia se interpone demanda contra la entidad BANCO DE SANTANDER SA, en la que se ejercita acción de reclamación de daños y perjuicios, conforme a los arts. 41 y ss. del RD Ley- 19/2018 de 23 de noviembre de servicios de pago y otras medidas urgentes en materia financiera. Se reclama la suma de 17.350 euros, más los intereses legales desde el requerimiento de pago extrajudicial hasta su completo pago, por negligencia en la gestión de las cuentas corrientes que la actora tiene suscritas en la entidad bancaria demandada y del contrato de tarjeta, con restitución de la cantidad de dinero de las que dispusieron fraudulentamente terceras personas.

En fecha 13 de mayo de 2022 se dictó sentencia por la Magistrada-Juez del Juzgado mixto nº 5 de Alcorcón, en la que se estima la demanda y se condena a la demandada al abono de la suma de la cantidad reclamada, más los intereses legales desde la interposición de la demanda y las costas procesales. En la sentencia se argumenta que, conforme a los arts. 41 y ss. del RD Ley- 19/2018 de 23 de noviembre de servicios de pago y otras medidas urgentes en materia financiera, la entidad que presta el servicio de pago solo puede exonerarse de responsabilidad, mediante la prueba de culpa grave del usuario que emite la orden de pago. Según la sentencia no queda acreditado que la demandante incurriese en una negligencia grave en el uso y custodia de sus claves y credenciales para el uso de la banca electrónica que la demandada puso a su disposición. Por el contrario, sí estima probado que la entidad bancaria ha incumplido su obligación de diligencia que le es exigible en la autenticación de las operaciones de pago.

SEGUNDO .- Por la representación procesal de la entidad BANCO DE SANTANDER SA se interpone recurso de apelación. Se alega como motivos del recurso, error en la valoración de la prueba. Cumplimiento de las obligaciones legales y contractuales por el BANCO DE SANTANDER SA. Concurrencia de negligencia en la parte actora e incorrecta aplicación de la Ley y doctrina jurisprudencial. Todo ello con base en que existió por parte de la actora un incumplimiento del deber de custodia de las claves y códigos para operar en la banca online, ya que todos los movimientos fueron autorizados mediante SMS/OTP, remitidos al teléfono móvil de la actora. Existió una autenticación de doble factor y las operaciones fueron registradas y contabilizadas correctamente.

Sobre la errónea valoración de la prueba, las partes en virtud del principio dispositivo y de rogación pueden aportar prueba pertinente siendo su valoración competencia de los Tribunales, sin que sea lícito tratar de imponerla a los juzgadores, y por lo que se refiere al recurso de apelación debe tenerse en cuenta el citado principio de que el juzgador que recibe la prueba puede valorarla de modo libre, aunque nunca de manera arbitraria, y por otro que si bien la apelación transfiere al Tribunal de la segunda instancia el conocimiento pleno de la cuestión, esta queda reducida a verificar si en la valoración conjunta del material probatorio se ha comportado el juez a quo de forma arbitraria o si, por el contrario, la apreciación conjunta del mismo es la procedente por su adecuación a los resultados obtenidos en el proceso. En este sentido, la valoración y apreciación de las pruebas es función del órgano de enjuiciamiento y no revisable en apelación cuando se haya ajustado a las normas de la sana crítica y de la experiencia común, de manera que si las conclusiones probatorias se mantienen razonables deben ser mantenidas, siendo así que en este caso actuando el Juzgador



de Instancia como órgano unipersonal la valoración de la prueba practicada en el juicio corresponde a dicho órgano jurisdiccional, y esta valoración, hecha imparcialmente y debidamente razonada debe prevalecer sobre la opinión parcial que dichos medios probatorios merezcan a las partes del proceso.

En el supuesto objeto de recurso la Sala, una vez examinada la documental aportada y visualizada la grabación del juicio, comparte la valoración de la prueba que se hace en la sentencia apelada, que no es arbitraria ni ilógica y que debe prevalecer frente a la subjetiva, parcial e interesada de la recurrente. Quedan acreditados los siguientes hechos: El día 29 de octubre de 2020 la actora accedió a la banca electrónica del Banco de Santander para realizar una transferencia y, pese a que lo intentó de forma reiterada, no se le remitió la clave de seguridad al móvil para poder hacerla. El día 30 de octubre de 2020 se personó en su sucursal bancaria, expuso a una empleada lo sucedido y se comprobó por ésta que el número de teléfono que les figuraba era el mismo y que no advertía ninguna irregularidad. Por la tarde, la demandante se dio cuenta que el saldo de la cuenta era inferior al que tenía por la mañana, por lo que de forma inmediata se puso en contacto telefónico con la entidad bancaria, informándole que había sido víctima de un fraude, cancelando sus tarjetas de crédito y la banca electrónica. El sábado 31 de octubre de 2020, llama al departamento de fraude del banco y le informan de que aún hay más movimientos irregulares pendientes de cargar en su cuenta y que debía denunciar ante la policía lo sucedido. Envío un correo electrónico a cada una de las oficinas bancarias en las que tiene abierta cuenta advirtiéndole de lo sucedido para que no cargasen ninguna cantidad. También presentó denuncia en comisaría. Se le cargaron de forma fraudulenta en su cuenta corriente nº NUM000, entre el día 30 de octubre y el 02 de noviembre de 2020, la suma total de 17.350,00 euros.

La acción ejercitada es la prevista en el Real Decreto Ley 19/2.018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en adelante, LSP), que establece: "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".

TERCERO. - A tenor de lo establecido en dichos preceptos, la entidad que presta el servicio de pago solo puede exonerarse de responsabilidad, mediante la prueba de culpa grave del usuario que emite la orden de pago. En el supuesto objeto de recurso, estamos ante un fraude llamado "phishing", por el que se suplanta la identidad de la entidad bancaria para obtener información sobre las claves o credenciales de las cuentas bancarias o tarjetas de crédito/débito. Se envía un correo electrónico con la apariencia de ser remitido por la entidad bancaria, que contiene un enlace a una página que aparenta ser sitio oficial de ésta, pero que en realidad pertenece a un dominio bajo control del phisher.

Se reconoce en el propio recurso que la demandante fue víctima de una estafa, que la llevó a creer que estaba operando en la WEB del Banco de Santander, pero necesariamente era una WEB distinta y, como consecuencia del engaño, en ella facilitó todas sus claves personales de acceso a la banca online o introdujo los códigos SMS/OPT remitidos para cada operación o se instaló desde dicha WEB algún troyano en el dispositivo móvil de la demandante. Se aduce en el recurso que, los certificados de REDSYS y SMS/OTP, acreditan que las compras se autorizaron mediante un OTP previo y los SMS se remitieron al teléfono del que la actora era titular por lo que, o la actora introdujo los códigos recibidos o el dispositivo móvil sufrió una infección/hackeo a través de un malware.

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 2015\151311), 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 2015\151311), 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).

La SAP Alicante 632/2018 - ECLI:ES:APA:2018:632 Id Cendoj: 03014370082018100070 Sección: 8 Fecha: 12/03/2018 N° de Recurso: 622/2017 N° de Resolución: 107/2018 , es especialmente apropiada para servir de referencia en la presente resolución por su claridad y extensión, aclarando el tema de la carga de la prueba referenciada anteriormente, señalando:



..... " Y 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 contraponen 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". (...) Así resulta además del particular régimen jurídico de responsabilidad en la prestación de servicios de pago que, con la llamada del 217.6 LEC, penetra en la configuración de la específica modalidad de responsabilidad que asume este prestador y con ello, la variación del régimen legal del sistema de gravamen probatorio, regulación legal de los servicios de pago que constituye una legislación ad hoc a no ignorar por el hecho de que se haya positivizado en la ley posterior a los hechos que nos ocupa -la Ley 16/2009, de 13 de noviembre, de servicios de pago (en vigor desde el día 4 de diciembre de ese mismo año) porque dicha norma transpone (fuera del plazo dado en la misma) la Directiva 2007/64/CE, del Parlamento Europeo y del Consejo Europeo de 13 de noviembre de 2007 vigente al tiempo de los hechos (hoy derogada por la Directiva 2015/2366, de 25 de noviembre), donde se establece -art 59 - el siguiente contenido normativo que ha sido traspuesto al art. 30 de la Ley 16/2009 , de servicios de pago: " Los Estados miembros exigirán que, cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que esta se ejecutó de manera incorrecta, corresponda a su 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 o cualquier otra deficiencia..".

Y concluye en relación con la carga de la prueba:

... " En conclusión, la responsabilidad del proveedor de los servicios de banca online, en este caso Barclays, 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...".

Respecto del fondo es preciso hacer constar expresamente la descripción que esta audiencia de Alicante señala por su claridad y oportunidad de aplicación al supuesto que estamos resolviendo, a saber:



... " Para una mejor respuesta al motivo, y dado que la responsabilidad que se imputa a la entidad, derivada de la ejecución de una transferencia no autorizada por la titular de la cuenta de la cliente demandante realizada a través del sistema de banca online, lo es en tanto prestadora de servicios de pago a través del modelo de banca virtual puesta a disposición de su cliente, concretaremos el régimen legal y contractual en el que se desenvuelve la banca electrónica, cuáles son las obligaciones del prestador y del usuario conforme a la legislación aplicable, el significado jurídico de las órdenes de pago y el marco de responsabilidades que del mismo resulta y la jurisprudencia más señalada al respecto. Pues bien, tales aspectos pueden concretarse en los puntos que seguidamente numeramos. 1.- La transferencia bancaria es 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. 2.- Las transferencias se regulan, trasponiendo la Directiva 2007/64/CE del Parlamento Europeo y del Consejo Europeo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2005/65/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE, en la Ley 16/2009, de 13 de noviembre, de Servicios de Pago (LSP). La Directiva 2007/64/CE ha sido derogada por la Directiva UE 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento UE nº 1093/2010 y se deroga la Directiva 2007/64/CE. 3.- La LSP define la orden 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). 4.- Desde un punto de vista contractual toda transferencia constituye una forma de ejecución de obligaciones contractuales previamente asumidas, ejecución obligada cuando se dan las condiciones pactadas. Se entiende que la orden de transferencia constituye una declaración de voluntad o mandato (en el sentido del art. 254 CCo) en virtud del cual el banco asume la realización de transferencias por cuenta del cliente como parte del contrato de servicio de caja. 5.- Dado el carácter negocial de la orden de pago, ésta puede pactarse que tenga lugar en cualquier forma, incluida la electrónica. En particular, el consentimiento a operaciones de pago por el usuario en el ámbito de la banca electrónica supone que el cliente deba haber firmado un contrato de adhesión a los servicios de banca electrónica."

Destacar esta conclusión:... "La falsedad de la transferencia (es decir, que el ordenante no sea el titular de la cuenta) es un riesgo a cargo del banco porque, en principio, el deudor sólo se libera pagando al verdadero acreedor por lo que si el banco cumple una orden falsa, habrá de reintegrar en la cuenta correspondientes las cantidades cargadas. Una excepción a esta distribución de riesgos se produce en el caso de que el titular haya creado o elevado el riesgo de falsificación de forma imputable en el caso concreto (STS 15 de julio de 1988).(....) - Los servicios que prestan las entidades de crédito a sus clientes a través de su oficina virtual se desenvuelven en redes TCP/IP (Internet) o WAP (comunicaciones móviles). 11.- Siendo Internet una red pública de comunicaciones, la seguridad de las operaciones bancarias precisa de soluciones tecnológicas avanzadas a los efectos de garantizar tanto la autenticidad como la integridad y la confidencialidad de los datos. Por estos motivos las entidades prestadoras del servicio de banca online deben dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones. Consecuencia derivada de la omisión, insuficiencia o defectuoso funcionamiento de las adoptadas es que han de ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema. (....)-La responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse ésta autorizada al haberse realizado de acuerdo con los sistemas de autenticación del banco. Los sistemas de autenticación se establecen por los proveedores de servicios de pago y si un banco no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante víctima de esta práctica fraudulenta sea el único responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo.

La Sentencia de la Audiencia Provincial de Zaragoza de fecha 14 de mayo de 2013 condenó a BARCLAYS BANK a reintegrar 20.947 € al cliente víctima de **phising**. La Sentencia señala:... " que la Ley de Servicios de Pago expresa con claridad que, salvo una tardanza injustificada del usuario del servicio de banca electrónica en comunicar la irregularidad de las operaciones, será el banco quien deberá devolverle de inmediato el importe de la operación no autorizada y, en su caso, restablecerá la cuenta de pago en que haya adeudado dicho importe al estado que habría existido de no haberse efectuado la operación de pago no autorizada. Por ello y salvo actuación fraudulenta o negligencia grave del titular de la cuenta, la responsabilidad de la operación es del banco al que corresponde además probar el correcto funcionamiento del sistema informático....".



A tenor de 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.

Como se aduce en la sentencia apelada, no podemos calificar la posible negligencia de la demandante en la conservación de sus claves como "grave" en ningún caso. Estamos ante un tipo de fraude muy específico del que es fácil ser víctima, sin que ello implique una actuación negligente del cliente, dado lo bien articulada en su ejecución que está esta modalidad de fraude. Tanto de la declaración de la demandante en la vista, como de la declaración de los testigos, ha quedado acreditado que la Sra. Inocencia intentó varias veces hacer una transferencia a través de la banca electrónica y, al no poder hacerlo porque no recibía la clave en su teléfono móvil, acudió a la mañana siguiente a su oficina bancaria, explicando lo sucedido. La empleada no detecta ninguna irregularidad. Momento en que se debió detectar el fraude y bloquear las cuentas y tarjetas. Además, se dispuso de cantidades superiores al límite máximo pactado de disposición, sin control por la entidad bancaria, lo que fue posible por la modificación de los límites referidos, elevando los 1.200 iniciales a 6.000 euros por tarjeta, lo que realiza el tercero, al conocer sus claves como consecuencia del hackeo previo.

Al entender la Sala que la entidad bancaria actuó sin tomar las medidas de diligencia y seguridad exigidas, la consecuencia del incumplimiento es la obligación de devolver de inmediato el importe de la operación, lo que al no efectuarse de inmediato supone un nuevo incumplimiento. El recurso debe ser desestimado.

CUARTO. - En aplicación de lo dispuesto en el art. 398-1 de la LEC, se imponen a la recurrente las costas procesales causadas en esta instancia.

Vistos los preceptos legales citados y demás de general aplicación.

FALLAMOS

Que, con desestimación del recurso de apelación interpuesto por la representación procesal de la entidad BANCO DE SANTANDER SA, frente a la sentencia dictada en fecha 13 de mayo de 2022 por la Ilma. Magistrada-Juez del Juzgado de 1ª Instancia nº 5 de Alcorcón en los autos a que el presente Rollo se contrae, debemos confirmar y confirmamos la resolución indicada e imponemos a la parte apelante las costas procesales causadas en esta alzada.

La desestimación del recurso determina la pérdida del depósito constituido, de conformidad con lo establecido en la Disposición Adicional 15ª de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, introducida por la Ley Orgánica 1/2009, de 3 de noviembre, complementaria de la ley de reforma de la legislación procesal para la implantación de la nueva oficina judicial.

Remítase testimonio de la presente Resolución al Juzgado de procedencia para su conocimiento y efectos.

MODO DE IMPUGNACION: Contra esta Sentencia no cabe recurso ordinario alguno, sin perjuicio de que contra la misma puedan interponerse aquellos extraordinarios de casación o infracción procesal, si concurre alguno de los supuestos previstos en los artículos 469 y 477 de la Ley de Enjuiciamiento Civil, en el plazo de veinte días y ante esta misma Sala, previa constitución, en su caso, del depósito para recurrir previsto en la Disposición Adicional Decimoquinta de la Ley Orgánica del Poder Judicial, debiendo ser consignado el mismo en la cuenta de depósitos y consignaciones de esta Sección, abierta en BANCO DE SANTANDER, con el número de cuenta 2577-0000-00-0918-22, bajo apercibimiento de no admitir a trámite el recurso formulado.

Así, por esta nuestra Sentencia, de la que se unirá certificación literal al Rollo de Sala Nº 918/2022, lo pronunciamos, mandamos y firmamos.

La difusión del texto de esta resolución a partes no interesadas en el proceso en el que ha sido dictada sólo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran y con



pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda.

Los datos personales incluidos en esta resolución no podrán ser cedidos, ni comunicados con fines contrarios a las leyes.

FONDO DOCUMENTAL CENDOJ