Roj: **SAP L 435/2025** - **ECLI:ES:APL:2025:435**

Id Cendoj: **25120370022025100403**
Órgano: **Audiencia Provincial**
Sede: **Lleida**
Sección: **2**
Fecha: **16/06/2025**
Nº de Recurso: **1195/2022**
Nº de Resolución: **464/2025**
Procedimiento: **Recurso de apelación**
Ponente: **ANA CRISTINA SAINZ PEREDA**
Tipo de Resolución: **Sentencia**

Resoluciones del caso: **SJPI, Lleida, núm. 5, 21-07-2022 (proc. 1506/2021), SAP L 435/2025**

Sección nº 02 de la Audiencia Provincial de Lleida. Civil

Calle Canyeret, 1 - Lleida - C.P.: 25007

TEL.: 973705820

FAX: 973700281

EMAIL:aps2.lleida@xij.gencat.cat

N.I.G.: 2512042120218297872

Recurso de apelación 1195/2022 -B

Materia: Procedimiento Ordinario

Órgano de origen:Juzgado de Primera Instancia nº 5 de Lleida

Procedimiento de origen:Procedimiento ordinario 1506/2021

Entidad bancaria BANCO SANTANDER:

Para ingresos en caja. Concepto: 2206000012119522

Pagos por transferencia bancaria: IBAN ES55 0049 3569 9200 0500 1274.

Beneficiario: Sección nº 02 de la Audiencia Provincial de Lleida. Civil

Concepto: 2206000012119522

Parte recurrente/Solicitante: Banco de Santander Sa

Procurador/a: Xavier Pijuan Sanchez

Abogado/a: MARTIN MARTINEZ GARRO

Parte recurrida: Pedro Jesús

Procurador/a: Ares Jene Zaldumbide

Abogado/a: Mercedes Regany Terradellas

SENTENCIA Nº 464/2025

Presidente:

Ilmo. Sr. Albert Guilanyà i Foix

Magistrado/as:

Ilmo. Sr. Albert Montell Garcia

Ilma. Sra. Ana Cristina Sainz Pereda

Lleida, 16 de junio de 2025

Ponente: Ana Cristina Sainz Pereda

ANTECEDENTES DE HECHO

PRIMERO. En fecha 27 de septiembre de 2022 se han recibido los autos de Procedimiento ordinario 1506/2021 remitidos por el Juzgado de Primera Instancia nº 5 de Lleida a fin de resolver el recurso de apelación interpuesto por el Procurador Xavier Pijuan Sanchez, en nombre y representación de Banco de Santander Sa contra Sentencia n.º 236/2022 de fecha 21/06/2022, y en el que consta como parte apelada la Procuradora Ares Jene Zaldumbide, en nombre y representación de Pedro Jesús .

SEGUNDO. El contenido del fallo de la Sentencia contra la que se ha interpuesto el recurso es el siguiente:

"**[...]ESTIMO íntegramente**la demanda interpuesta por el Procurador S.ª Jené en nombre y representación de D. Pedro Jesús frente a Banco Santander, SA y CONDENO a **Banco Santander, SA**a indemnizar a **D. Pedro Jesús** en la cantidad de **6.570,11 €,**devengando esta cantidad el correspondiente interés legal conforme a lo previsto en los arts. 1108 y 1109 CC.

Todo ello con expresa condena a Banco Santander al pago de las **costas**causadas en esta instancia a la actora. [...]"

TERCERO. El recurso se admitió y se tramitó conforme a la normativa procesal para este tipo de recursos.

Se señaló fecha para la celebración de la deliberación, votación y fallo que ha tenido lugar el 16/06/2025.

CUARTO. En la tramitación de este procedimiento se han observado las normas procesales esenciales aplicables al caso.

Se designó ponente a la Magistrada Ana Cristina Sainz Pereda .

FUNDAMENTOS DE DERECHO

PRIMERO. -La parte demandada interpone recurso de apelación contra la sentencia de primera instancia que estima íntegramente la demanda en la que el demandante, Sr. Pedro Jesús , reclama por los cargos fraudulentos efectuados en las cuentas corrientes que tiene contratadas con el banco demandado, derivados de compras con tarjeta en comercio electrónico y de transferencias no autorizadas.

La entidad apelante centra su recurso en los pagos con tarjeta por importe de 2.070,23 euros, y no en las transferencias bancarias, por importe de 4.500 euros, indicando que consignará voluntariamente dicha suma en el Juzgado.

Alega error en la valoración de la prueba, considerando que esta parte ha cumplido todas sus obligaciones legales y contractuales, concurriendo en cambio negligencia grave del demandante.

La recurrente residencia el error en la valoración de la prueba, en primer lugar, en el hecho de que la cesión de las credenciales de seguridad por parte del actor constituye un hecho probado; y, en segundo lugar, en la omisión valorativa en que incurre la sentencia de instancia al no dar ningún tipo de relevancia a ese hecho (cesión por parte del actor de los datos necesarios para completar el proceso de autenticación), habiendo afirmado esta parte demandada que no puede acreditar que el actor facilitó todos los datos (porque los actos con terceros escapan de su control) pero si puede demostrar el correcto funcionamiento de sus procedimientos, de donde se infiere indubitadamente que la parte actora incumplió necesariamente los deberes de custodia de sus claves personales.

Añade que en la demanda y en las respuestas del actor en prueba de interrogatorio existen omisiones deliberadas, no ofreciendo explicaciones, ni siquiera indiciarias, sobre la forma en que el estafador pudo hacerse con las claves personales, resultando que si el demandante hubiera desplegado una diligencia media en su deber de custodia de las claves no se habría producido el suceso. Añade que no se ha valorado debidamente la prueba documental, porque los certificados REDYS y sus anexos acreditan que se trata de un sistema seguro, ofreciendo un servicio de verificación de que las operaciones han sido registradas,

autenticadas y contabilizadas correctamente, sin haberse visto afectadas por ninguna incidencia, habiendo cumplido esta parte con el contenido del art. 44 LSP.

También aduce que no se ha aplicado correctamente la normativa y la doctrina jurisprudencial sobre este tipo de supuestos, indicando la sentencia que esta parte no ha acreditado suficientemente la existencia de medios de especial protección cuando, en realidad, la prueba aportada no ha sido suficientemente valorada, constando acreditado que el sistema funcionó perfectamente, no siendo oponible a esta parte que bien la actora o bien el estafador operase con conocimientos de las credenciales de seguridad. Seguidamente cita y extracta diversas resoluciones judiciales de las que, según dice, resulta que no cabe imputar responsabilidad a la entidad bancaria cuando el cliente incumple los deberes de custodia en casos de recepción de comunicaciones electrónicas, siendo en este caso la parte actora la que negligentemente facilito los datos a un tercero.

SEGUNDO.-Las alegaciones de la recurrente no pueden ser admitidas, advirtiendo ya desde un inicio que parte de premisas equivocadas pues no sólo da por probado la cesión de las credenciales por parte del usuario (que en modo alguno se estima acreditada en la resolución recurrida) sino que considera, en primer lugar, que la cesión de las credenciales de seguridad por parte del usuario bancario integra en todo caso un supuesto de negligencia grave en los términos que se derivan del art. 46 de la Ley de Servicios de Pago (LSP) y, en segundo lugar, que el hecho de que sus procedimientos de verificación hayan funcionado correctamente le exime de responsabilidad, siendo el usuario el que incumplió los deberes de custodia de sus claves personales.

Este planteamiento resulta claramente insuficiente para rebatir la extensa, fundada y correcta exposición de los hechos y de la normativa aplicable que se contiene en la resolución recurrida, en la que se explican ampliamente los criterios a seguir a efectos de poder valorar y apreciar si hubo o no negligencia grave del usuario de los servicios de pago, en consonancia con la doctrina jurisprudencial sobre la materia, que es también la que hemos seguido en esta esta Sala en supuestos muy similares al que nos ocupa.

Además, falla el silogismo que pretende hacer valer la recurrente, porque el hecho de que sus procedimientos hayan funcionado correctamente (lo que tampoco aprecia la resolución recurrida) no significa sin más que haya negligencia grave por parte del usuario, obviando en este punto la apelante los razonamientos seguidos en la resolución recurrida a efectos de determinar en qué circunstancias puede llegar a considerarse que existe negligencia grave.

A renglón seguido dice que estamos ante un supuesto de fraude consumado y que hay negligencia grave porque no se habría consumado si el ciber delincuente no hubiera dispuesto de la información tan sensible, de modo que, si no hubo fallo, necesariamente debió mediar la cesión de credenciales, prescindiendo nuevamente de las razones ofrecidas en la resolución recurrida para rebatir ese planteamiento.

Expuesto lo anterior, para centrar el debate es preciso acudir al marco normativo aplicable en estos casos de operaciones fraudulentas, por lo que hay que tener en cuenta que el 23 de diciembre de 2015 entró en vigor la Directiva 2015/2366, sobre Servicios de Pago en el Mercado Interior (DSP2). La Segunda Directiva de Servicios de Pago tiene por finalidad fomentar la innovación, la competencia y la eficacia del mercado y, más concretamente, "modernizar los servicios de pago en Europa en beneficio tanto de los consumidores como de las empresas", según la Comisión. Así pues, la Directiva tiene por objeto garantizar un acceso justo y abierto a los mercados de pago y reforzar la protección del consumidor.

Más concretamente, apoya la apertura de los sistemas de información de los bancos a nuevos actores, la banca abierta, y, por otra parte, fortalece la seguridad de los pagos en línea para combatir el fraude y el delito cibernético (robo de identidad). La PSD2 se aplica a los servicios de pago en línea, ya sea que se trate de pagos con tarjeta o no - en la Zona Única de Pagos en Euros (por sus siglas en inglés, SEPA)- desde un banco, una fintech o un comerciante electrónico, y requiere ahora la implementación de un sistema de autenticación fuerte.

En los Considerandos (7), (33), (69), (91) y (95) de la Directiva ya se advierte claramente que, ante el incremento de los riesgos de seguridad debido a la mayor complejidad técnica de los pagos y fraudes, es esencial disponer de servicios de pago fiables y seguros, de forma que los usuarios gocen de la debida protección frente a los riesgos inherentes a estos nuevos medios de pago. De hecho, la DSP2 introduce como novedad la obligación de que todas las operaciones de acceso a la banca digital y de pago se realicen por medio de una autenticación reforzada de cliente (Art. 97 DSP2).

La DSP2 también obliga a los proveedores de servicios de pago a realizar controles adecuados para gestionar sus riesgos operativos y de seguridad (Art. 96 DSP2). Y en desarrollo de estas obligaciones, el Reglamento Delegado 2018/389, de 27 de noviembre de 2017, que complementa la DSP2 en lo relativo a las normas técnicas para la autenticación reforzada de cliente, establece la obligación de realizar un análisis de riesgo en tiempo real basado en el análisis de operaciones y en los elementos que caracterizan al usuario en un contexto de uso normal de las credenciales de seguridad.

Ese análisis de riesgo debe tener en cuenta los siguientes factores: (i) importe de las operaciones, (ii) supuestos de fraudes conocidos, (iii) gastos o pautas de comportamiento anormales en el ordenante, (iv) información inusual sobre el dispositivo o programa informático de acceso del ordenante, (v) infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación, (vi) supuestos conocidos de fraude en la prestación de servicios de pago, (vii) una ubicación anormal del ordenante, y (viii) una ubicación de alto riesgo del beneficiario.

En cuanto a la normativa interna, el Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, incorporó parcialmente a nuestro derecho los instrumentos europeos que se aprobaron a partir de 2015, para dar respuesta a la necesidad de generar un entorno más seguro y fiable para el desarrollo de unos servicios de pago sometidos a constantes innovaciones, tanto lícitas como ilícitas. En este sentido, la Exposición de Motivos de este RDL indica que *" El aprovechamiento de las innovaciones producidas en los últimos años y la necesidad de generar un entorno más seguro y fiable para su desarrollo se encuentran en la base de la aprobación de la nueva Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior. Este nuevo marco europeo, que este real decreto-ley incorpora parcialmente a nuestro ordenamiento jurídico, tiene como principales objetivos facilitar y mejorar la seguridad en el uso de sistemas de pago a través de internet, reforzar el nivel de protección al usuario contra fraudes y abusos potenciales, respecto del previsto en la Ley 16/2009, de 13 de noviembre, así como promover la innovación en los servicios de pago a través del móvil y de internet"*.

En esta norma se regulan las obligaciones esenciales tanto del usuario de servicios de pago como de las entidades que los prestan. Y asi, el usuario está obligado (art. 41 a]) a utilizar el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del mismo, y, en particular, a tomar "todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas".

Por su parte, el proveedor de esos servicios está obligado (art. 42.1 a]) a cerciorarse que 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 [...]".

En los casos de operaciones no autorizadas o ejecutadas incorrectamente, el usuario está obligado (art. 43.1) a comunicar su existencia "sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones [...]", y debe soportar (art. 46.1.3º) "todas las pérdidas derivadas de operaciones de pago no autorizadas si [...] 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".

Fuera de esos tres supuestos -ausencia de comunicación en tiempo de las operaciones, actuación fraudulenta del usuario y negligencia grave- la proveedora del servicio está obligada a realizar la rectificación del cargo (art. 43.1) y devolución del importe (art. 45.1). Por un lado, ante la negación por el usuario de haber autorizado la operación o la afirmación de que la misma fue realizada de manera incorrecta, corresponde a la proveedora del servicio (art. 44.1º) "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 otro lado, la proveedora del servicio también tiene la carga de acreditar (art. 44.3º) "que el usuario del servicio de pago cometió fraude o negligencia grave". Y, por último, el registro de la utilización del instrumento por el proveedor no basta por sí solo y 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 [...]" (art. 44.2º).

Además, la responsabilidad de la entidad proveedora del servicio de pago se acentúa aún más cuando el proveedor no exige "autenticación reforzada" del cliente, supuesto en que éste último únicamente responde de haber actuado de forma fraudulenta (art. 46.2º). La autenticación reforzada se define en el art. 2.5 como "la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), que son independientes -es decir, que la vulneración de uno no compromete la fiabilidad de los demás-, y concebida de manera que se proteja la confidencialidad de los datos de identificación". Como ya se ha dicho inicialmente, en el presente caso, no se discute que las operaciones controvertidas se ejecutaron con el sistema de autenticación reforzada.

Estos preceptos vienen a configurar un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago, con inversión de la carga de la prueba, de manera que se presume *ex lege*la falta de autorización si el titular la niega, salvo que se prueba por parte de la entidad que el cliente ha actuado de forma fraudulenta o con negligencia grave a la hora de aplicar los medios de protección de seguridad personalizados o caso de no haber comunicado a la entidad el pago no autorizado en cuanto tenga conocimiento del mismo,

posición que claramente vienen recogiendo los Tribunales al establecer a cargo del emisor de la tarjeta la prueba del fraude o de la culpa grave.

Como viene estableciendo constante jurisprudencia (SSAP Oviedo de 11 de abril de 2024, 21 de marzo de 2024 y 13 de diciembre de 2023), dicho régimen está *"sin duda inspirado en la idea de que los beneficios que comporta (tanto para el tráfico económico, como para la actividad del proveedor de los servicios) el avance tecnológico en los instrumentos de pago, debe estar justamente compensado con la protección reforzada de quien los emplea y se ve expuesto a actuaciones fraudulentas [...]"*

TERCERO. -Sobre la existencia de dicha responsabilidad cuasi objetiva nos hemos pronunciado en esta Sala en Sentencias de 29 de junio de 2023 (nº 463/2023), de 19 de abril y 30 de julio de 2024 (nº303 y 575/2024, respectivamente, siendo parte en ésta última la misma entidad bancaria aquí demandada) y, en la más reciente, de 17 de febrero de 2025 (nº 167/2025), recogiendo los criterios de las anteriores. Igualmente, citábamos en dichas resoluciones la SAP Rioja, sec. 1ª de 17 de febrero de 2023; SAP Almería, sec. 1ª, de 31 de enero de 2023; SAP Madrid, sec. 10ª, de 13 de enero de 2023, SAP Oviedo, sec. 4ª, de 11 de abril de 2024 y sec. 5ª, de 22 de junio de 2023, entre muchas otras, siendo igualmente muy ilustrativa la reciente **STS** nº **571/2025**, de 9 de abril, a la que más adelante nos referiremos.

La negligencia grave del usuario como causa de exoneración de la entidad bancaria es tratada por la Directiva (UE) 2015/2366 en un sentido restrictivo. Según su considerando 72 "[a] la hora de evaluar la posible negligencia o la negligencia grave del usuario de servicios de pago, deben tomarse en consideración todas las circunstancias. Las pruebas de una presunta negligencia, y el grado de esta, deben evaluarse con arreglo a la normativa nacional. No obstante, si el concepto de negligencia supone un incumplimiento del deber de diligencia, la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros".

Respecto a la actuación del cliente de la entidad financiera y usuario del servicio de pagos, puesta en relación con la conducta del defraudador, decíamos en nuestra sentencia nº 303/2024, de 19 de abril, y reiteramos en las posteriores, lo siguiente:

*"Es sabido que los ciberdelincuentes usan estrategias con las que engañan al usuario. En ocasiones le hacen creer, por ejemplo, que su banco le pide actualización de datos. El cliente atiende porque la solicitud le llega por medio de su correo electrónico o a través de una web casi idéntica a la de la entidad bancaria. Responde al pedido y entrega sus datos. Así comienza el **phishing** [...] estos mensajes engañosos suelen parecer proceder de fuentes fiables y utilizan tácticas de ingeniería social para crear una sensación de urgencia, curiosidad o miedo con el fin de manipular al destinatario para que realice una acción no deseada.*

*La jurisprudencia reciente es unánime a la hora de sentenciar que el banco debe reembolsar las cantidades sustraídas a su cliente, y ello porque, el Tribunal entiende que el banco está obligado a custodiar la información confidencial de los usuarios. Por lo tanto, generalmente son los bancos los que tienen la obligación de devolver el dinero a la víctima del **phishing**. La excepción a este criterio es, como hemos adelantado, que el cliente haya cometido una negligencia grave. Es importante considerar el carácter de "grave" de la negligencia del usuario. Aunque se reconozca que el cliente cometió un descuido, este descuido tiene que ser grave para que se le adjudique la responsabilidad.*

Y aquí es donde entra el análisis de la carga de la prueba y de la consideración de cuando es y cuando no tributaria la negligencia de ser considerada o calificada de grave. Pues bien, para empezar, hay que recordar que la condición de grave de la negligencia es cuestión que ha de ser atribuida por el Tribunal. Y así la Audiencia Provincial de Madrid ha definido la negligencia grave del cliente como una conducta que se produce por iniciativa del usuario y no por consecuencia del engaño realizado por un delincuente profesional. Según esta definición, la persona que ha sido engañada para robarle su identidad no estaría cometiendo negligencia grave. Casos de negligencias graves son, por ejemplo: la persona extravía los datos personales y de su cuenta bancaria con las contraseñas anotadas en el mismo papel, en una libreta o similar; la web o correo electrónico de los estafadores es muy diferente de la real del banco, y a simple vista es fácil deducir que no es la legítima.

*Incidiendo más en esa característica de grave, la Sala Penal del Tribunal Supremo tiene declarado que el "**phishing**" es una estafa informática en la que se integran todos los elementos del tipo penal del Art. 248.2 CP : el ánimo de lucro, la manipulación informática, el acto de disposición y el engaño bastante (**STS** (Penal), sec. 1ª, nº 379/2019, de 23 de julio de 2019). Con respecto al "engaño bastante", la Sala Penal del Tribunal Supremo afirma que "no debe desplazarse indebidamente sobre los perjudicados la responsabilidad de comportamientos en los que la intención de engañar es manifiesta, y el autor ha conseguido su objetivo, lucrándose en perjuicio*

*de su víctima" porque " el engaño no tiene que quedar neutralizado por una diligente actividad de la víctima" (**STS** (Penal), sec. 1ª, nº 51/2020, de 17 de febrero de 2020).*

Por su parte, de los Arts. 1101 y 1104 del Código Civil se infiere que la negligencia grave se equipara a la culpa lata, que "consiste en no proceder ni siquiera con la más elemental diligencia" o en "la más grave falta de diligencia, no hacer lo que todos hacen, no prever lo que todos prevén". Se alude a la culpa con previsión o dolo eventual, cuando el incumplimiento no es directamente querido, pero se han previsto los hechos. Se incurren en este tipo de negligencia cuando se omite las precauciones más elementales, dejando de prever lo que el resto de las personas habría previsto.

Asimismo, el Considerando 72 de la DSP2 dice que "A la hora de evaluar la posible negligencia o la negligencia grave del usuario de servicios de pago, deben tomarse en consideración todas las circunstancias. (...) si el concepto de negligencia supone un incumplimiento del deber de diligencia, la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros".

*La SAP de Madrid, Sec. 20ª, nº 184/2022, de fecha 20/5/2022, Rec. 945/2021 , afirma que "en la normativa europea antes referida [la negligencia grave] se equipara a la comisión de un fraude" y que "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 (...)". Este razonamiento guarda relación directa y necesaria con: (a) la doctrina de la Sala Penal de Tribunal Supremo (**STS** (Penal), sec. 1ª, nº 51/2020, de 17 de febrero de 2020), según la cual no se pude desplazar sobre el perjudicado la responsabilidad de comportamientos en los que la intención de engañar es manifiesta, porque el engaño no tiene que quedar neutralizado con una actividad de diligencia de la víctima y (b) con la finalidad de la Directiva 2015/2366, de Servicios de Pago (DSP2), cuyos considerandos declaran esencial el desarrollo de un mercado único integrado por pagos electrónicos en el que los usuarios gocen de la debida protección frente a los riesgos inherentes a estos nuevos medios de pago.*

*Así pues, la negligencia grave debe surgir como consecuencia de la iniciativa del usuario, no como consecuencia de la iniciativa de un delincuente profesional, porque el engaño típico de la estafa excluye la negligencia grave. Si el **phishing** está caracterizado por el "engaño bastante", que es algo más que un burdo engaño, en el que caen multitud de personas, la víctima nunca puede haber actuado con negligencia grave, que es la más grave falta de diligencia, hacer lo que nadie más hace o no prever lo que todos prevén, o como dice el Considerando 72 de la DSP2 " una conducta caracterizada por un grado significativo de falta de diligencia". En caso de "criminalizar" a la víctima por dejarse engañar no sólo se subvierte la finalidad de la norma, sino que, además, se puede llegar al absurdo de descriminalizar estas estafas, porque la declaración de que el cliente actúa con negligencia grave podría excluir el engaño bastante y con ello la rebaja del tipo penal. Por ello, una interpretación errónea del concepto de "negligencia grave" que lleve a penalizar a los clientes por su falta de diligencia por el hecho de haber sido víctimas de una estafa punible, puede llevar al absurdo de proteger a los delincuentes.*

En relación con la carga de la prueba, la SAP de Alicante, Sec. 8ª, nº 107/2018, de 12/3/2018 considera que la responsabilidad de la Entidad Bancaria es de "naturaleza cuasi-objetiva o de riesgo por razón legal". Esta declaración se reitera, entre otras, en la SAP de Zaragoza, Sec. 5ª, S. 01-07-2022, nº 804/2022, rec. 1130/2021 .

Pero es que, además, los proveedores de servicios de pago no sólo están obligados a rastrear las páginas web que suplantan su identidad, también están obligados a realizar un análisis de riesgo de las operaciones y a implementar medidas de seguridad acorde a los riesgos presentes. Como dice la Sentencia de 16 de septiembre de 2022 del Juzgado de 1ª Instancia nº 3 de Santander " los bancos deberían incorporar sus propios "detectores de humo" para anticipar cuando puede estar teniendo lugar una estafa e intervenir", afirmación que guarda relación con la obligación que impone el Reglamento Delegado 2018/389 de realizar un análisis de riesgos en tiempo real para detectar cuándo una orden de pago es fraudulenta.

Asimismo, la Sentencia nº 88/2023, de 7 de junio de 2023, dictada por el Juzgado de 1ª Instancia nº 7 de Cerdanyola del Vallés , se pronuncia en un sentido análogo cuando razona "11. 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 lo 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. (...)

12.-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. (...) 13.- Las medidas de seguridad no solamente están destinadas a proteger la seguridad de las órdenes de pago emitidas por los clientes sino que su eficacia exonera a las entidades de crédito de sus responsabilidades frente a las órdenes de pago no emitidas por sus clientes de tal forma que el incumplimiento de este específico deber de vigilancia da lugar a una responsabilidad por "culpa in vigilando" o responsabilidad objetiva por el mal funcionamiento de los servicios de banca electrónica".

*Finalmente y teniendo en cuenta el incremento de este tipo de fraudes, cuyas cifras de criminalidad rebasan las de otros sectores de actividades peligrosas y siendo la finalidad de la DSP2, que los usuarios gocen de la debida protección frente a los riesgos inherentes a los medios de pago digitales, la doctrina jurisprudencial establece que quien tiene las ventajas de un negocio por el que obtiene un lucro, debe soportar los inconvenientes de ese negocio como contraprestación por el lucro obtenido (**STS**, Sala 1ª, S. 3-6-2006, nº 328/2006, rec. 281/1999). En consonancia con ello el Tribunal Supremo tiene declarado que en sectores de actividades peligrosas debe regir una responsabilidad objetiva, en razón al riesgo inherente al servicio prestado, cuyo título de imputación se fundamenta en la falta de la diligencia debida, que en estos casos debe ser rigurosa, ajustada las circunstancias concurrentes.*

*Como se explica en la **STS** (Civil Pleno), S. 15-3-2021, nº 141/2021, rec. 1235/2018 (Caso Uralita), F.D. Cuarto [sic]: "En estos supuestos de actividades peligrosas permitidas, por ser socialmente útiles, colisionan los intereses de los terceros de no resultar perjudicados, con el propio y legítimo de los titulares que las gestionan de obtener los mayores rendimientos económicos posibles derivados de su explotación, a veces sometida, aunque no siempre, a un régimen de responsabilidad objetiva bajo aseguramiento obligatorio. Esa desigualdad, en las posiciones de ambas partes, se pone fácilmente de manifiesto por la circunstancia de que mientras los terceros soportan la amenaza eventual de sufrir daños significativos, con la única ventaja de obtener a cambio, en el mejor de los casos, un beneficio meramente difuso, el titular de la actividad, por el contrario, se beneficia de las ganancias generadas de su explotación en su particular provecho. Esta asimetría conduce a la posibilidad de justificar decisiones normativas que, por razones de justicia conmutativa, impongan a quien se aproveche de ese stock de riesgos, las cargas económicas de los perjuicios causados a los terceros ajenos a la misma, con la finalidad de compensar esa especie de daños expropiatorios o de sacrificio. De esta manera, se han utilizado las fórmulas latinas ubi emolumentum, ibi onus (donde está la ganancia está la carga) o cuius commoda, eius incommoda (quien obtiene una ventaja debe padecer los inconvenientes)".*

*Dado que el artículo 16 de la LSP obliga a los proveedores de servicios de pago a dotarse de un seguro de responsabilidad civil profesional, es dable declarar la responsabilidad objetiva de los proveedores de servicios de pago en aquéllos casos en los que sus clientes sean víctimas de una estafa de **phishing**, porque los pagos digitales se trata de un sector de actividad en auge, con constante incremento del índice delictivo, caracterizado por técnicas de engaño basadas en ingeniería social y uso de programas informáticos maliciosos imposibles o difícilmente detectables por los usuarios, en el que el principal constante incremento del índice delictivo, caracterizado por técnicas de engaño basadas en ingeniería social y uso de programas informáticos maliciosos imposibles o difícilmente detectables por los usuarios, en el que el principal beneficiario del uso de este sistema de pagos son los proveedores de estos medios -cuando menos son quienes obtienen el beneficio económico-, mientras que los clientes, que se ven obligados al uso de estos medios de pago -tanto por las restricciones legales al uso de dinero metálico como por el interés de los proveedores de servicios de pago en el uso de estas tecnologías-, sólo obtienen un interés difuso por el ahorro de tiempo en desplazamientos presenciales a la sucursal".*

CUARTO.-Todos estos criterios se corresponden con los seguidos en la reciente sentencia del Tribunal Supremo nº **571/2025**, de 9 de abril, que analiza un supuesto en el que la entidad bancaria recurrente sostenía que posiblemente se había producido una suplantación de identidad o «**phishing**», pero que las operaciones se autorizaron al haber cumplido el doble factor de autenticación, sin detectarse incidencia alguna, conforme a lo dispuesto en el art. 44 del RD-ley 19/2018, por lo que una vez acreditada la doble autenticación no corresponde a la entidad bancaria determinar si las operaciones de pago cuestionadas las autentificó un cliente o un tercero que disponía de los datos, o incluso del dispositivo móvil utilizado, constando que en los contratos de banca digital y de cuenta corriente y/o depósitos se prevé expresamente que la entidad bancaria queda exenta de los perjuicios que se pudieran derivar por intromisiones ilegítimas de terceros en el sistema elegido por el cliente, fuera del control de la entidad bancaria.

En esta **STS** nº **571/2025** se recoge ampliamente toda la normativa sobre la materia, para después referirse a lo que debe entenderse por "operaciones de pago no autorizadas", y por "fallos de seguridad", argumentando en el Fundamento de Derecho Segundo. 6:

"En suma, la responsabilidad del proveedor de los servicios de pago, en los casos de operaciones no autorizadas o ejecutadas incorrectamente, tiene carácter cuasi objetivo, en el doble sentido de que, primero, notificada la existencia de una operación no autorizada o ejecutada incorrectamente, el proveedor debe responder salvo que acredite la existencia de fraude; y, segundo, cuando el usuario niegue haber autorizado la operación o alegue que ésta se ejecutó incorrectamente, corresponde al proveedor acreditar 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, sin que el simple registro de la operación baste para demostrar que fue autorizada ni que el usuario ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave.

Profundizando en este último punto, la expresión «operaciones no autorizadas» incluye aquellas que se han iniciado con las claves de usuario y contraseña del usuario -necesarias para acceder al sistema de banca digital- y confirmado mediante la inserción del SMS enviado por el propio sistema al dispositivo móvil facilitado por el usuario, siempre que éste niegue haberlas autorizado, en cuyo caso el banco deberá acreditar 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 que presta.

A este respecto, la mención «deficiencia del servicio» no significa error o fallo del sistema informático o electrónico -posibilidad que estaría prevista en el concepto de «fallo técnico»-, sino que abarca cualquier falta de diligencia o mala praxis en la prestación del servicio, en el entendimiento de que el grado de diligencia exigible al proveedor de los servicios de pago no es el propio del buen padre de familia, sino que la naturaleza de la actividad y los riesgos que entraña el servicio que se presta, sobre todo en una relación empresario/consumidor, obliga a elevar el nivel de diligencia a un plano superior, como es el del ordenado y experto comerciante.

Lógicamente, las buenas prácticas pasan por adoptar las medidas de seguridad necesarias para garantizar el correcto funcionamiento del sistema de servicios de pago, entre las cuales destacan las orientadas a detectar de forma automática la concurrencia de indicios de que puede tratarse de una operación anómala y generar una alerta o un bloqueo temporal (v.gr. reiteración de transferencias sin solución de continuidad, horario en que se producen, importe de las mismas, destinatarios, antecedentes en el uso de la cuenta...), o las dirigidas a incrementar el control y vigilancia cuando se han recibido noticias o alertas de un posible aumento del riesgo."

La normativa y los criterios jurisprudenciales que han quedado expuestos resultan de plena aplicación al caso y, conforme a ellos, una vez reexaminadas las actuaciones, consideramos que no cabe acoger las alegaciones de la entidad bancaria recurrente, debiendo mantener en esta alzada el recto e imparcial criterio valorativo del juzgador de instancia cuando concluye que estamos ante una actuación delictiva realizada por un tercero no autorizado, y que no ha quedado acreditada la negligencia grave del usuario, tratándose en este caso de una responsabilidad cuasi objetiva de la entidad bancaria, argumentando que los documentos aportados por la demandada para acreditar el correcto cumplimiento de las normas y protocolos de seguridad, en lo que se refiere a los pagos con tarjeta, únicamente permite compartir la tesis de que las operaciones se realizaron con la introducción de la clave de acceso, y con verificación con firma electrónica, pero no permiten saber si la aplicación del usuario o la propia web o app del banco falló en un momento anterior al permitir el acceso previo del estafador a las claves de acceso y firma del usuario, sin que la demandada haya practicado ninguna prueba que permita saber cómo pudo el estafador descargar la aplicación y obtener las credenciales, destacando en este punto la obligación impuesta por el Reglamento Delegado 2018/389 en cuanto a los mecanismos de supervisión para detectar operaciones fraudulentas, enumerando factores de riesgo que deben tenerse en cuenta, para acabar señalando que en este caso la entidad demandada no ha aportado ningún medio de prueba que acredite el desarrollo, aplicación e implementación de dichos mecanismos en su sistema, concluyendo, en suma, que no se ha acreditado el cumplimiento del deber de diligencia exigible, lo que se predica tanto de las operaciones consistentes en pagos con tarjeta como de las transferencias fraudulentas, dos de las cuales sí fueron bloqueadas.

A lo anterior se añade que tampoco se ha practicado prueba adecuada y suficiente para acreditar la negligencia grave que se imputa al actor, constando en cambio su actuación positiva e insistente tan pronto como tuvo conocimiento de que se estaban realizando las operaciones sospechosas en su cuenta bancaria.

Frente a tan contundente y razonada argumentación, ajustada al resultado que ofrece la conjunta valoración de las pruebas practicadas, la recurrente se limita a hacer valer afirmaciones genéricas sobre el correcto cumplimiento de sus obligaciones, amparadas en la prueba documental que ya ha sido convenientemente examinada y valorada en la resolución recurrida, mezclando en su recurso unas cuestiones con otras y obviando la respuesta ofrecida por el juzgador de instancia a cada una de ellas.

Difícilmente podrían admitirse las alegaciones de la recurrente sobre su adecuado proceder cuando resulta que inicialmente, en su contestación a la demanda, defendía el correcto registro y autenticación de todas las operaciones que el actor describe en su demanda, tanto en lo que se refiere a los cargos realizados en la tarjeta como a las transferencias, haciendo valer respecto de unas y otras la inexistencia de fallo técnico o de cualquier otra deficiencia, indicando en cuanto a las transferencias que (sin perjuicio de que algunas de ellas fueron correctamente bloqueadas por el Banco) la autenticación se llevó a cabo a través de un sistema similar al de las compras con tarjeta. Sin embargo ahora, en el recurso, se acepta sin mayor explicación el criterio seguido en la resolución recurrida en lo que se refiere a las transferencias (este pronunciamiento ha devenido firme, por consentido), indicando claramente en la sentencia las razones por las que se descarta la tesis de la parte demandada en cuanto al estricto cumplimento de sus deberes y sobre la negligencia grave que imputa al demandante, tanto en lo que se refiere a las diversas compras con tarjeta (por un total de 2.070,23 euros) como a las diversas transferencias (total 4.500 euros), concluyendo que se trata de operaciones fraudulentas -mediante la técnica conocida como *phising*-,que fue la propia entidad bancaria la que alertó al actor mediante un primer SMS enviado el 6-8-2021, y un segundo mensaje recibido al día siguiente, desplazándose a la entidad para formular la reclamación el primer día laborables (lunes 9 de agosto de 2021), según se le había indicado telefónicamente por parte de la entidad, interponiendo al día siguiente, 10 de junio, la correspondiente denuncia en la que relata lo sucedido, en consonancia con lo que explica en su demanda, y con lo que manifestó el Sr. Pedro Jesús en prueba de interrogatorio, indicando que no recibió ningún SMS supuestamente del Banco pidiéndole datos personales, ni tampoco por correo electrónico o llamada telefónica, no habiendo autorizado ninguna de esas operaciones, descargado ninguna aplicación a través del link del Banco, ni facilitado en ningún momento sus datos, siendo la primera noticia el SMS remitido por el Banco el 6-6-2021 alertando sobre lo que estaba sucediendo.

En este sentido, en consonancia con lo que argumenta la resolución recurrida, hay que incidir en que es la entidad bancaria la que debe acreditar cumplidamente la efectiva concurrencia de la negligencia grave que imputa al usuario, y en que el Reglamento Delegado 2018/389, de 27 de noviembre de 2017, que complementa la DSP2 en lo relativo a las normas técnicas para la autenticación reforzada del cliente, establece la obligación de realizar un análisis de riesgo en tiempo real basado en el análisis de operaciones y en los elementos que caracterizan al usuario en un contexto de uso normal de las credenciales de seguridad, estableciendo en su art. 2 que los proveedores de servicios de pago deben de incorporar mecanismos de supervisión que les permitan detectar operaciones de pago no autorizadas o fraudulentas a efectos de la adopción de terminadas medidas de seguridad, debiendo basarse esos mecanismos en el análisis de las operaciones de pago, teniendo en cuenta los elementos que caractericen al usuario de servicios de pago en el contexto de un uso normal de las credenciales de seguridad personalizadas. Ese análisis de riesgo debe tener en cuenta una serie de factores, a los que nos hemos referido anteriormente y en los que insiste la misma **STS** nº **571/2025** de continua referencia, y en el presente caso es evidente que o bien fueron obviados o bien no se detectaron oportunamente con el sistema implementado por la entidad, puesto que se trata de operaciones ajenas a la operativa ordinaria de la tarjeta (transacciones internacionales, compras de productos en Malta, según documentos 6 y 7 de la demanda), inusuales en este usuario, tanto por el tipo de operación como por su importe y destino, por lo que debió hacer saltar las alertas o avisos a fin de corroborar su autenticidad y adoptar las medidas procedentes, lo que no se produjo hasta que buena parte de ellas ya se habían materializado, evidenciando así la falta o insuficiencia de los mecanismos de supervisión y de las necesarias medidas de detección del fraude en el momento en que se produjeron los hechos que nos ocupan y, en definitiva, que el servicio no se prestó correctamente, debiendo reiterar que, como bien remarca la **STS** nº **571/2025**, el cumplimiento de las obligaciones relativas a la autenticación, registro y contabilización de la operación de pago no exime de responsabilidad al proveedor de servicio, sino que deberá acreditar además que la operación no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado, sin que mero registro de la utilización del instrumento de pago baste 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

En consecuencia, el recurso no puede prosperar y debe mantenerse lo acordado en la resolución recurrida.

QUINTO. -En materia de costas es de aplicación lo dispuesto en el art. 398-1 en relación con el 394-1 de la LEC, por lo que han de imponerse al desestimar el recurso las costas de esta alzada han de imponerse a la parte apelante.

Vistos los artículos citados y demás de general y pertinente aplicación

FALLAMOS

DESESTIMAMOSel recurso de apelación interpuesto la representación procesal de **BANCO SANTANDER SA**contra la sentencia dictada por el Juzgado de Primera Instancia nº5 de Lleida en los autos de Juicio Ordinario nº1506/2021, **y CONFIRMAMOS**la citada resolución, imponiendo las costas de este recurso a la parte apelante.

Devuélvanse las actuaciones al Juzgado de procedencia, con certificación de esta sentencia, a los oportunos efectos.

Dese el destino que proceda al depósito que ha constituido la parte recurrente para recurrir en apelación, conforme a lo dispuesto en la DA 15ª de la LOPJ.

Modo de impugnación:recurso de **CASACIÓN**en los supuestos del art. 477 LEC ante el Tribunal Supremo siempre que se cumplan los requisitos legales y jurisprudencialmente establecidos.

También puede interponerse recurso de casación en relación con el Derecho Civil Catalán en los supuestos del art. 3 de la Llei 4/2012, del 5 de març, del recurs de cassació en matèria de dret civil a Catalunya.

El recurso se interpone mediante un escrito que se debe presentar en este Órgano judicial dentro del plazo de **VEINTE**días, contados desde el siguiente al de la notificación, mediante escrito razonado que deberá contener las alegaciones en que se fundamente el recurso. Además, se debe constituir, en la cuenta de Depósitos y Consignaciones de este Órgano judicial, el depósito a que se refiere la DA 15ª de la LOPJ reformada por la LO 1/2009, de 3 de noviembre.Sin estos requisitos no se admitirá la impugnación.

Lo acordamos y firmamos.

Los Magistrados :

Puede consultar el estado de su expediente en el área privada de seujudicial.gencat.cat

Los interesados quedan informados de que sus datos personales han sido incorporados al fichero de asuntos de esta Oficina Judicial, donde se conservarán con carácter de confidencial, bajo la salvaguarda y responsabilidad de la misma, dónde serán tratados con la máxima diligencia.

Quedan informados de que los datos contenidos en estos documentos son reservados o confidenciales y que el tratamiento que pueda hacerse de los mismos, queda sometido a la legalidad vigente.

Los datos personales que las partes conozcan a través del proceso deberán ser tratados por éstas de conformidad con la normativa general de protección de datos. Esta obligación incumbe a los profesionales que representan y asisten a las partes, así como a cualquier otro que intervenga en el procedimiento.

El uso ilegítimo de los mismos, podrá dar lugar a las responsabilidades establecidas legalmente.

En relación con el tratamiento de datos con fines jurisdiccionales, los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación en el proceso en que los datos fueron recabados. Estos derechos deberán ejercitarse ante el órgano judicial u oficina judicial en el que se tramita el procedimiento, y las peticiones deberán resolverse por quien tenga la competencia atribuida en la normativa orgánica y procesal.

Todo ello conforme a lo previsto en el Reglamento EU 2016/679 del Parlamento Europeo y del Consejo, en la Ley Orgánica 3/2018, de 6 de diciembre, de protección de datos personales y garantía de los derechos digitales y en el Capítulo I Bis, del Título III del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.