Roj: **SAP L 379/2025** - **ECLI:ES:APL:2025:379**

Id Cendoj: **25120370022025100347**
Órgano: **Audiencia Provincial**
Sede: **Lleida**
Sección: **2**
Fecha: **16/05/2025**
Nº de Recurso: **1064/2022**
Nº de Resolución: **395/2025**
Procedimiento: **Recurso de apelación**
Ponente: **ANA CRISTINA SAINZ PEREDA**
Tipo de Resolución: **Sentencia**

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.: 2500942120218090274

Recurso de apelación 1064/2022 -B

Materia: Procedimiento Ordinario

Órgano de origen:Sección Civil. Juzgado de 1ª Instáncia e Instrucción nº 1 de Vielha e Mijarán (UPSD)

Procedimiento de origen:Procedimiento ordinario 136/2021

Entidad bancaria BANCO SANTANDER:

Para ingresos en caja. Concepto: 2206000012106422

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

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

Concepto: 2206000012106422

Parte recurrente/Solicitante: Caixabank Sa

Procurador/a: Ares Jene Zaldumbide

Abogado/a: Ignacio Benejam Peretó

Parte recurrida: Virgilio

Procurador/a: Mª Jose Fernandez-Vallmayor Carrasco

Abogado/a: Angel Buerba Mur

SENTENCIA Nº 395/2025

Presidente:

Ilmo. Sr. Albert Guilanyà i Foix

Magistrado/as:

Ilmo. **Sr. Albert Montell Garcia**

Ilma. Sra. Ana Cristina Sainz Pereda

Lleida, 16 de mayo de 2025

Ponente: Ana Cristina Sainz Pereda

ANTECEDENTES DE HECHO

PRIMERO. En fecha 5 de septiembre de 2022 se han recibido los autos de Procedimiento ordinario 136/2021 remitidos por la Sección Civil del Juzgado de 1ª Instancia e Instrucción nº 1 de Vielha e Mijarán (UPSD) a fin de resolver el recurso de apelación interpuesto por la Procuradora Ares Jene Zaldumbide, en nombre y representación de Caixabank Sa, y la impugnación formulada por la Procuradora Mª Jose Fernandez-Vallmayor Carrasco, en nombre y representación de Virgilio . contra Sentencia n.º 30/2022 de fecha 15/03/2022 . Ambas partes se han opuesto a la impugnación y al recurso planteados de contrario.

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

"[...] ESTIMO LA DEMANDA presentada por la Procuradora de los Tribunales Doña María José FERNANDEZ-VALLMAYOR CARRASCO, en nombre y representación de Virgilio y asistida por el Letrado D. Ángel BUERBA MUR, contra CAIXABANK SA representada por la Procuradora de los Tribunales Doña Ares JENE ZALDUMBIDE y asistido en calidad de Letrado por D. Ignacio BENEJAM PERETÓ y en consecuencia declaro que la actuación de la demandada en la gestión del fraude sufrido por la actora ha supuesto un incumplimiento de las obligaciones contractuales asumidas en los contratos de 1 de enero de 2014 y de las obligaciones extracontractuales en virtud de las normas vigentes en nuestro ordenamiento jurídico; y que dicha actuación de la demandada ha ocasionado daños y perjuicios a la actora por el total de 49.500,00€, de los que deberá pagar 34.500,00€ resultado de la compensación de la cantidad de 15.000,00€ por la liquidación total del préstamo número NUM000 y con más los intereses legales y se le condena a estar y pasar por las anteriores declaraciones y a que pague a la actora la cantidad de TREINTA Y CUATRO MIL QUINIENTOS (34.500,00€) más los intereses legales. Y todo ello con expresa imposición de costas a la parte demandada.[...]"

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 16/05/2025.

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 sentencia de primera instancia estima íntegramente la demanda en la que el Sr. Virgilio ejercita acción de responsabilidad y de reclamación de cantidad contra la entidad bancaria CAIXABANK SA por la ejecución de operaciones bancarias no autorizadas, en concreto, dos transferencias internacionales por importe de 38.500 y 11.000 euros y un préstamo de 15.000 euros. Su pretensión se estima en aplicación de lo dispuesto en la Ley de Servicios de Pago (LSP) y demás normativa sobre la materia, concluyendo que no fue el actora quien autorizó esas operaciones de forma expresa y voluntaria, sino que fue un tercero quien ejecutó, consiguiendo las claves personales del cliente a través de una estafa (engañó al cliente haciéndose pasar por un tercero legítimo para conseguir sus claves), sin que el banco pueda quedar exento de la obligación de devolver los fondos al no haber acreditado que el cliente actuó con negligencia grave. En consecuencia, se declara que la actuación de la entidad CAIXABANK en la gestión del fraude sufrido por el actor supone un incumplimiento de las obligaciones contractuales derivadas de la relación contractual y de las obligaciones extracontractuales en virtud de las normas vigentes sobre la materia, debiendo abonar al actor la suma de 34.500 euros, más intereses legales.

Ambas partes interponen recurso de apelación. La demandada alega en primer lugar que las pruebas practicadas acreditan la concurrencia de negligencia grave del actor en su obligación de custodia diligente de las credenciales de seguridad personalizadas, conforme a lo dispuesto en los arts. 41 a) y 46 de la LSP , lo que exime a esta parte de responsabilidad, constando acreditado que no ha existido fallo o deficiencia técnica por parte de la entidad bancaria, mientas que el actor facilitó unilateralmente sus credenciales de seguridad a terceros, habiéndose efectuado todas las operaciones desde el mismo ordenador y la misma IP, contraviniendo así la más elemental y básica obligación de custodia que se deriva de los citados preceptos.

Subsidiariamente, reitera las alegaciones vertidas en su contestación a la demanda en cuanto a la pluspetición de que adolece la pretensión del demandante al reclamar la indemnización de 34.500 euros, obviando que esta parte, sin ser responsable de ello, se ha hecho cargo de un total de 11.000 euros

transferidos a la cuenta de un tercero y que provenían de un préstamo solicitado por el actor o por aquél a quién ha permitido el acceso a sus datos y terminales, por lo que la suma reclamada debe minorarse en esa cantidad, hasta los 23.500 euros.

La parte actora se opone al recurso formulado de adverso y, a su vez, impugna la sentencia de primera instancia denunciando incongruencia *infra petita*al haber estimado la demanda por la suma de 34.500 euros, sin tener en cuenta que en la audiencia previa incrementó la petición a la cantidad de 38.500 euros, añadiendo a la suma inicial los 4.000 euros que no había reclamado por haber sido objeto de compensación con el sobrante del falso préstamo, procediendo después la demandada, en fecha posterior a la interposición de la demanda, a extraer esa cantidad de la cuenta bancaria, aún en contra de su expresa oposición.

SEGUNDO. - Para centrar el debate es preciso tener en cuenta que el principal punto de discrepancia no radica en este caso en la eventual existencia de deficiencias técnicas o fallos del sistema en lo que se refiere, en concreto, al registro, contabilización y autenticación de las operaciones bancarias cuestionadas, según resulta del documento nº6 de la contestación (respuesta remitida por la Caixa al actor frente a su reclamación extrajudicial, no impugnado por la parte actora según indicó en la audiencia previa) y de las explicaciones del testigo Sr. Alejandro . Tampoco se cuestiona que el demandante interpuso denuncia al día siguiente de los hechos, personándose el primer día hábil en la sucursal bancaria para relatar lo sucedido e iniciar la correspondiente reclamación La discrepancia de la entidad bancaria recurrente se centra en el proceder del usuario, que califica de negligencia grave, alegando que el propio demandante Sr. Virgilio reconoce en su demanda que consintió el acceso a su ordenador a unos estafadores, admitiendo que permitió que terceros desconocidos accedieran libremente al ordenador y estuvieran trabajando en él durante dos días seguidos, con el pretexto de arreglárselo.

En este sentido, ambas partes admiten que estamos ante la estafa o fraude conocida como "falso empleado de Microsoft", cuyo *modus operandi*se explica en el documento nº3 de la contestación (recomendaciones de la entidad sobre seguridad a sus clientes, en previsión de potenciales ataques electrónicos, publicada en su web en el año 2021, meses después de las operaciones fraudulentas que aquí nos ocupan) y viene a coincidir, en lo esencial aunque no en su totalidad, con lo que relata el actor en su demanda, coincidente con lo que manifestó al interponer la denuncia y lo que manifestó en prueba de interrogatorio, señalando que confió en la llamada telefónica que recibió, en la que el interlocutor dijo ser técnico de la empresa Microsoft, habiendo detectado problemas en su ordenador y precisando haber pruebas para agilizarlo, de forma gratuita, mostrando él su conformidad habida cuenta que el ordenador hacía tiempo que funcionaba lento, creyendo que así podrían solucionárselo, sin que por otro lado sospechara por el hecho de que la revisión durara tanto tiempo porque en otra ocasión llevó el ordenador a reparar por un técnico y el proceso también fue muy lento.

Pues bien, partiendo de lo anterior y por lo que se refiere al marco normativo aplicable en estos casos de operaciones fraudulentas, 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 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) y, en la más reciente, de 17 de febrero de 2025 (nº 167/2025), recogiendo los criterios de las anteriores. Igualmente, 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. 5 ª, 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 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 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".

Todos estos criterios se corresponden con los seguidos en la reciente STS 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 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 (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."

CUARTO. - La normativa y los criterios jurisprudenciales que han quedado expuestos resultan de plena aplicación al caso y conforme a ellos no cabe acoger las alegaciones de la recurrente, debiendo mantener en esta alzada el criterio valorativo del juzgador de instancia cuando concluye que no ha quedado acreditada la negligencia grave del usuario.

Como ya dijimos inicialmente el demandante fue víctima de una estafa (estafa de ingeniería social, conocida como *vishing,*que según el documento nº3 de la contestación, ofrece a los criminales la posibilidad de ser muy convincentes ya que les permite mediante un argumento determinado ir adaptando su discurso en función de la respuesta de la víctima, para así poder dar mayor credibilidad a la llamada), sin que su proceder pueda calificarse como negligencia grave por el mero hecho de que haber confiado en que estaba tratando con un empleado de la empresa Microsoft, habiendo negado el actor en todo momento que facilitara el acceso a su teléfono móvil, ni que proporcionara ninguna clave ni acceso a la aplicación bancaria. La declaración testifical del empleado de la entidad bancaria no permite obtener conclusión distinta puesto que tras indicar la operativa (ordinaria) a través de las que se hicieron las operaciones y el correcto funcionamiento del sistema de autenticación, manifestó que no es necesario en todo caso que el cliente autorice finalmente la operación a través de su teléfono móvil, porque si concede permiso para la conexión remota en el móvil otra persona puede hacer la operación en control remoto, sin necesidad de tener físicamente el teléfono móvil, señalando también que los delincuentes tenían el control del dispositivo porque se lo facilitó el demandante y que "no sabemos cuál era el programa pero las operaciones se firmaron con ese dispositivo y según este tipo de estafa los clientes dan acceso y los terceros instalan programas de conexión y otros programas para funcionar con este dispositivo, pudiendo eliminar mensajes y demás", añadiendo que "las operaciones o bien las firma el cliente o bien da acceso a terceros para que accedan a estas aplicaciones" y, finalmente, a preguntas del juzgador de instancia sobre la seguridad del sistema, manifestó que las aplicaciones de firma y de banca on line son seguras, siempre que no se faciliten las claves a terceros, pero los clientes sin saberlo facilitan datos a terceros, entre ellos el acceso a sus dispositivos".

De acuerdo con lo anterior no cabe apreciar la negligencia grave que la recurrente reprocha al actor, Hay descartar en todo caso el análisis retrospectivo de lo sucedido, cuando ya se conoce que las operaciones

bancarias se realizaron fraudulentamente, debiendo situarnos en el momento inicial, cuando el usuario toma determinadas decisiones en la confianza de que se está moviendo en un entorno seguro, que le proporciona en este caso el (falso) servicio técnico de ayuda de la Microsoft, de modo que su voluntad estaba viciada por el engaño y lo único que cabría reprochar sería un exceso de confianza, pero sin alcanzar la significativa importancia que se exige para poder calificarlo como grave, resultando en este sentido muy significativo el razonamiento seguido en la ya citada STS de 9-4-2025 (nº 571/2025) cuando indica: *"Asimismo, el hecho de que la filtración o el conocimiento de las claves por el tercero no sea imputable a la entidad bancaria tampoco la libera de obligación de responder ni traslada al usuario la obligación de soportar las pérdidas, ya que el proveedor de servicios de pago, además de demostrar que el servicio se prestó correctamente -lo que no sucedió-, debía acreditar la concurrencia de fraude o incumplimiento deliberado o gravemente negligente por parte del usuario, y, en relación con este extremo, las sentencias de instancia y de apelación coinciden en que no se ha probado fraude ni incumplimiento doloso o por negligencia grave de las obligaciones que correspondían al demandante, y, en concreto, las de tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas y de notificar al proveedor de servicios de pago la utilización no autorizada del instrumento de pago, tan pronto tuvo conocimiento de ello, lo que así hizo, participando las tentativas de acceso a su cuenta con una antelación de tres semanas.*

Obsérvese que, contra lo que mantiene por la recurrente, el que un tercero hubiera podido acceder a las claves de acceso a la banca digital del demandante no supone per se que haya incurrido en negligencia alguna, pudiendo existir múltiples explicaciones, muchas de las cuales resultan difícilmente atribuibles a título de negligencia, y menos aún, de negligencia grave".

Tampoco podría quedar exonerada de responsabilidad la entidad bancaria con el argumento de que se trata de estafas informáticas que se producen con mucha frecuencia y que la entidad genera los correspondientes avisos a través de sus páginas web. En el presente caso las recomendaciones de seguridad que la demandada aporta como documento nº3 de la contestación son posteriores a la fecha en que se produjeron las operaciones fraudulentas y, en cualquier caso, no puede exigirse al usuario/cliente medio tener conocimientos informáticos y estar al corriente de las sofisticadas técnicas fraudulentas de apropiación de datos personales, sino que el planteamiento ha de ser a la inversa, porque según se deriva de la normativa y los criterios jurisprudenciales expuestos lo que se exige a las entidades proveedoras de servicios de pago es dotarse de tecnología suficiente y adecuada, implantando medidas activas, sin que puedan considerarse suficientes los avisos generales o estereotipados, o las recomendaciones en página web, que tienen carácter meramente informativo o divulgativo.

En este sentido, en relación a las medidas de seguridad la ya citada STS nº 571/2025, de 9 de abril , argumenta:

"Por otra parte, los avances de la tecnología actual hacen relativamente sencillo diseñar sistemas o aplicaciones informáticas idóneas para detectar ciertas anomalías en la prestación de los servicios de pago. Operaciones que, tratándose de empresas o sociedades con un concreto objeto social, pueden calificarse como ordinarias, deben inmediatamente levantar sospechas y dar lugar a una respuesta cuando afectan a personas físicas ajenas a tales actividades. A este respecto, sería suficiente un control automático de determinados factores, como el número y sucesión de operaciones, el intervalo en que se ejecutan, la hora del día, su importe, entidades de destino..., para generar un aviso que reforzara los requisitos de confirmación y minimizara los posibles riesgos. No puede considerarse como normal e irrelevante que una persona que jamás efectúa operaciones de madrugada, de repente, proceda a llevar a cabo hasta diecisiete operaciones seguidas y por un importe tan elevado. Del mismo modo que el sistema rechazó dos de Bizum por exceder del máximo diario, el proveedor de servicios de pago ha de adoptar las medidas de seguridad que garanticen su correcto funcionamiento y minimicen los riesgos y los efectos nocivos de su materialización".

Lo anterior es claramente extrapolable al supuesto enjuiciado, y así se pone también de manifiesto en la sentencia de primera instancia al referirse a los mecanismos de supervisión de los que deben proveerse los bancos para detectar operaciones de pago fraudulentas, según el Reglamento Delegado (UE) 2018/389 , argumentando que deben poder detectar que los elementos de autenticación (las claves personales) han sido comprometidas o sustraídas, debiendo poder detectar señales de infección por programas informáticos maliciosos en el proceso de autenticación, considerando que en estos casos un factor indicativo es el importe de la operación.

En efecto, el demandante Sr. Virgilio nunca había operado a través de este sistema (afirma en su demanda que es pensionista, y que carece totalmente de conocimientos suficientes para realizar operaciones por vía telemática) limitándose a consultar los movimientos de su cuenta, sin haber efectuado ni una sola operación de abono o de cargo por vía telemática. Así se afirma en la demanda y lo confirmó en el juicio el testigo Sr. Alejandro , analista de fraudes que presta sus servicios para la entidad demandada.

Partiendo de lo anterior, y teniendo en cuenta el tipo de operaciones que reflejan los extractos bancarios y sus importes -básicamente, cobro de la pensión del INSS, reintegros y cargos de recibos domiciliados- claramente se advierte que, con arreglo a los criterios antes indicados, las operaciones de que se trata resultaban totalmente inusuales, disponiendo previamente el actor de un saldo en su cuenta bancaria de 40.363,21 euros, efectuándose entre los días 19 y 20 de noviembre de 2020 las operaciones no autorizadas por el actor que ahora nos ocupan, consistentes en una transferencia internacional por valor de 38.500 euros a favor de Juan Ramón , hacia una cuenta de Bangkok no determinada (Bangkok Bank Public Company LI); un ingreso (por contratación de préstamo personal) de 15.000 euros y a continuación otra transferencia internacional, por importe de 11.000 euros, a favor de Isidro , hacia una cuenta de Bangkok, no determinada. Todo ello con las comisiones correspondientes por el servicio.

Como ya se ha dicho anteriormente 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 con el sistema implementado por la entidad, puesto que se trata de operaciones totalmente ajenas a la operativa ordinaria de la cuenta bancaria, inusuales en este usuario, tanto por el tipo de operación como por su elevado importe y destino, y sin que figure el concepto al que responden, 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, 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 incidir en 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.

QUINTO. - De forma subsidiaria alega la recurrente que la reclamación planteada por el actor incurre en pluspetición, obviando que esta parte, sin ser responsable de ello, se ha hecho cargo de un total de 11.000 euros transferidos a la cuenta de un tercero y que provenían del préstamo de 15.000 euros solicitado por el actor o por aquél a quién ha permitido el acceso a sus datos y terminales, por lo que la suma reclamada debe minorarse en esa cantidad, hasta los 23.500 euros.

Este motivo de recurso ha de resolverse conjuntamente con la impugnación de sentencia planteada por el demandante, adelantando ya que procede acoger la tesis de éste, descartando a su vez la pluspetición invocada de contrario.

No puede admitirse la tesis de la entidad demandada cuando sostiene que al no haber solicitado el actor la nulidad del préstamo de 15.000 euros resulta que se ha visto favorecido por los 11.000 euros que se transfirieron a un tercero y de los que se ha hecho cargo la entidad bancaria. Las pruebas practicadas acreditan que esta operación de préstamo personal se enmarca dentro de la misma operativa fraudulenta, efectuada a través del canal de banca electrónica, y lo mismo cabe decir de la transferencia internacional efectuada a continuación. Por tanto, la consecuencia jurídica ha de ser la misma que la ya expuesta anteriormente, y así lo entendió la demandada desde el momento en que procedió a la cancelación del préstamo y a la retrocesión de todos los cargos realizados como consecuencia del mismo, según se indica en los respectivos escritos de demanda y contestación, y en los extractos bancarios, admitiendo expresamente que "el préstamo ha resultado ser fraudulento", según figura en el documento nº36, al que seguidamente nos referiremos.

También consta acreditado, por las manifestaciones de la parte demandada y por lo que figura en los documentos nº 10 de la contestación y nº 35 y 36 aportados por el actor en la audiencia previa, que en fecha posterior a la de interposición de la demanda la entidad procedió a "rectificar el apunte contable de referencia", (documento nº36), esto es, a realizar un cargo de 4.000 euros en la cuenta del actor, para

recuperar aquellos 4.000 euros que quedaron en la cuenta procedentes del préstamo de 15.000 euros, de los que los delincuentes dispusieron mediante la transferencia internacional de 11.000 euros efectuada el 20-11-2020, habiendo procedido la demandada a la cancelación del referido préstamo.

Así se puso de manifiesto por la parte actora en las alegaciones complementarias efectuadas al inicio de la audiencia previa, incrementando la cuantía de la demanda y de los daños reclamados, de 34.500 a 38.500 euros, aportando a tal efecto los documentos nº 35 y 36. Por tanto, procede acoger las alegaciones del impugnante, sin que quepa apreciar la pluspetición que aduce la demandada en su recurso, considerando en cambio que, por las razones ya expuestas en el Fundamento anterior, debe asumir la entidad bancaria su responsabilidad, quedando el Sr. Virgilio totalmente indemne, en igual situación en la que se encontraba antes de producirse los hechos y, por ende, con el mismo saldo en su cuenta bancaria, como si aquellas operaciones fraudulentas no se hubieran producido.

SEXTO. - En materia de costas es de aplicación lo dispuesto en el art. 398 de la LEC , por lo que han de imponerse a la demandada las correspondientes a su recurso, sin que proceda efectuar especial pronunciamiento sobre las derivadas de la impugnación del demandante.

Vistos los artículos citados y demás de general y pertinente aplicación

FALLAMOS

ESTIMAMOS el recurso de apelación interpuesto la representación procesal de D. Virgilio contra la sentencia dictada por el Juzgado de Primera Instancia de Vielha en los autos de Juicio Ordinario nº136/2021 , y REVOCAMOS PARCIALMENTE la citada resolución, en el único sentido que la cantidad que la entidad bancaria demandada debe abonar el actor asciende a 38.500 euros, más los intereses legales procedentes. Sin costas de este recurso.

DESESTIMAMOS el recurso de apelación interpuesto la representación procesal de CAIXABANK SA contra la referida 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.