Roj: **SAP B 8971/2025** - **ECLI:ES:APB:2025:8971**

Id Cendoj: **08019370172025100472**
Órgano: **Audiencia Provincial**
Sede: **Barcelona**
Sección: **17**
Fecha: **24/07/2025**
Nº de Recurso: **1213/2024**
Nº de Resolución: **477/2025**
Procedimiento: **Recurso de apelación**
Ponente: **ANA MARIA NINOT MARTINEZ**
Tipo de Resolución: **Sentencia**

Sección nº 17 de la Audiencia Provincial de Barcelona. Civil

Paseo Lluís Companys, 14-16, 1a planta - Barcelona - C.P.: 08018

TEL.: 934866210

FAX: 934866302

EMAIL:aps17.barcelona@xij.gencat.cat

Entidad bancaria BANCO SANTANDER:

Para ingresos en caja. Concepto: 0967000012121324

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

Beneficiario: Sección nº 17 de la Audiencia Provincial de Barcelona. Civil

Concepto: 0967000012121324

N.I.G.: 0801942120240170342

Recurso de apelación 1213/2024 -C

Materia: Juicio verbal

Órgano de origen:Juzgado de Primera Instancia nº 13 de Barcelona

Procedimiento de origen:Juicio verbal (250.2) (VRB) 730/2024

Parte recurrente/Solicitante: Amadeo

Procurador/a: Maria Luisa Lopez Calza

Abogado/a: Andres Serrano Clemente Parte recurrida: DEUTSCHE BANK SAE

Procurador/a: Javier Suarez-Quiñones Fernadez

Abogado/a: FRANCISCO SORIANO RUBIO

SENTENCIA Nº 477/2025

Magistrada: Ana Maria Ninot Martinez

Barcelona, 24 de julio de 2025

ANTECEDENTES DE HECHO

PRIMERO.-En fecha 17 de septiembre de 2024 se han recibido los autos de Juicio verbal (250.2) (VRB) 730/2024 remitidos por el Juzgado de Primera Instancia nº 13 de Barcelona a fin de resolver el recurso de apelación interpuesto por la Procuradora Maria Luisa Lopez Calza, en nombre y representación de Amadeo ,

contra la Sentencia de fecha 08/07/2024 y en el que consta como parte apelada el Procurador Javier Suarez-Quiñones Fernadez, en nombre y representación de DEUTSCHE BANK SAE.

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

"Que debo desestimar y desestimo íntegramente la demanda ejercitada por la representación procesal de DON Amadeo , contra DEUTSCHE BANK, absolviendo al demandado de las pretensiones contra él formuladas. No se hace especial condena en costas, debiendo pagar cada parte las causadas a su instancia y las comunes por mitad."

TERCERO.-El recurso se admitió y se tramitó conforme a la normativa procesal para este tipo de recursos. Se señaló fecha para la resolución del recurso el día 23/07/2025.

Se designó ponente a la Iltre Magistrada Dª Ana Maria Ninot Martinez.

FUNDAMENTOS DE DERECHO

PRIMERO.-El presente procedimiento se inició por demanda de juicio ordinario (luego transformado a verbal) presentada por Amadeo contra la entidad DEUTSCHE BANK SAE en ejercicio de la acción de responsabilidad y reclamación de daños y perjuicios.

Aduce el actor, titular de una cuenta en Deutsche Bank, que el día 1 de marzo de 2024 recibió una llamada telefónica de una persona que se identificó como empleado del citado banco para comunicarle que habían recibido un aviso de movimiento sospechoso desde un teléfono que no era el habitual del demandante y localizado en Valladolid. El actor manifestó no haber realizado ninguna operación, indicándole el empleado haber paralizado las operaciones y aconsejándole anular las tarjetas, lo que así hizo el demandante confirmando el mensaje que le llegó a la aplicación. Después de esta llamada, el actor contactó con el banco donde le confirman que había sido una estafa, habiéndole sustraído la cantidad total de 12.450,35 € (dos pagos inmediatos por transferencia (1.578 €), dos pagos con tarjeta de crédito (1.514,24 € y nueve pagos con tarjeta de débito (9.366,11 €), más el aumento por valoración de divisa). El demandante sostiene que Deutsche Bank es responsable por el incumplimiento de sus obligaciones contractuales como operador de banca a distancia y por falta de diligencia y cuidado en el mantenimiento del sistema. El actor reclama la cantidad sustraída de 12.450,35 €, más 2.000 € en concepto de daño moral.

La entidad demandada DEUTSCHE BANK SAE se opuso alegando su falta de legitimación pasiva, el cumplimento por parte del banco de las medidas de seguridad para evitar este tipo de situaciones, la negligencia del actor y la falta de acreditación de los daños morales.

La sentencia del Juzgado de Primera Instancia nº 13 de Barcelona desestima la demanda, sin imposición de costas. La sentencia, después de señalar que en este tipo de defraudaciones hay que examinar si el cliente de la entidad actuó con la diligencia debida, sin negligencia grave, valorando la conducta del cliente en orden a la facilitación de sus claves de acceso a la banca on line y a su línea telefónica, considera *"acreditado que fue la propia parte actora quien actuó sin la debida diligencia al recibir varios SMS en su teléfono móvil solicitándole unas claves para activar su tarjeta en otro dispositivo y no sospechó en ningún momento ni lo puso en conocimiento de la entidad demandada, solo una vez que se produjo el supuesto cargo fraudulento e introdujo las claves para autorizar el registro de su tarjeta en la aplicación Apple Pay por un tercero ajeno. El hecho de que el enrolamiento de la tarjeta en la aplicación de Apple Pay se pudiera efectuar correctamente y sin ninguna incidencia demuestra una evidente conducta negligente por parte del demandante en su obligación de protección de credenciales (así como datos personales y bancarios) que permitió a un tercero acceder a absolutamente todos y cada uno de los datos necesarios para llevar a cabo el enrolamiento y, asimismo, poder llevar a cabo las operaciones de compra objeto de reclamación".*Y concluye que *"las operaciones fueron autenticadas, registradas con exactitud y contabilizadas y no se vio afectada por fallo técnico o deficiencia alguna del servicio prestado por el proveedor de servicios de pago",*descartando *"un requisito esencial determinante de responsabilidad, cual es la mala praxis bancaria en el actuar de DEUTSCHE BANK".*

Frente a dicha resolución se alza el demandante Amadeo que recurre en apelación denunciando error en la valoración de la prueba. La demandada no se opuso al recurso.

SEGUNDO.-En su recurso de apelación el demandante alega que la sentencia contiene errores de apreciación y omisiones, señalando como tales que la sentencia no examina la responsabilidad de la entidad por el incumplimiento de sus obligaciones en materia de protección de datos, que el actor no recibió ningún mensaje de texto o SMS sino solo un aviso de confirmación en la propia aplicación del banco, que no es cierto que en la demanda no se ofrezca una hipótesis de lo ocurrido afirmando el demandante que nunca facilitó a nadie sus claves ni datos personales, que la sentencia copia párrafos del escrito de contestación a la demanda sin

mencionar la prueba justificativa y, finalmente, reitera que la persona que lo llamó por teléfono disponía de todos sus datos, lo que evidencia una brecha de seguridad en el banco, y que el actor no cometió ningún acto negligente porque todo lo ocurrido fue dentro del aplicativo del banco.

La cuestión planteada debe ser resuelta a la luz de la **STS 571/2025** de 9 de abril (ROJ: **STS** 1671/2025 - ECLI:ES:TS:2025:1671) que por su carácter novedoso y exhaustividad reproducimos:

"La controversia radica en determinar quién debe responder por las operaciones de pago no autorizadas, en tanto que realizadas por un tercero que, utilizando las credenciales del usuario que ha obtenido por cualquier medio, suplanta su identidad y accede electrónicamente a su cuenta sin su consentimiento. O, dicho de otra manera, qué debe entenderse por «operaciones de pago no autorizadas», si, en general, las que han sido realizadas por un tercero sin el consentimiento del usuario titular de la cuenta, o, exclusivamente, las efectuadas sin seguir el procedimiento legal y contractualmente fijado.

(...) La respuesta a la cuestión discutida exige recodar concretar la normativa aplicable. La Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015 , sobre servicios de pago en el mercado interior, que derogó la Directiva 2007/64/CE, explica en su Considerando 7 el objetivo de la reforma:

«En los últimos años, han aumentado los riesgos de seguridad de los pagos electrónicos, debido a la mayor complejidad técnica de estos, el incesante incremento del volumen de pagos electrónicos en todo el mundo y los nuevos tipos de servicios de pago. Disponer de servicios de pago fiables y seguros es condición esencial para el buen funcionamiento del mercado de servicios de pago, por lo que los usuarios de esos servicios deben gozar de la debida protección frente a tales riesgos. Los servicios de pago son esenciales para el mantenimiento de actividades económicas y sociales de vital importancia.»

Y en los Considerandos 70, 71 y 72 se aborda el problema de las operaciones de pago no autorizadas o ejecutadas incorrectamente, precisando las respectivas obligaciones y responsabilidad del usuario y del proveedor de los servicios de pago y ofreciendo pautas para valorar la diligencia exigible:

«(70) Para reducir los riesgos y las consecuencias de operaciones de pago no autorizadas o que hayan sido ejecutadas incorrectamente, el usuario de servicios de pago debe informar al proveedor de servicios de pago, lo antes posible, sobre toda reclamación en relación con operaciones de pago supuestamente no autorizadas o ejecutadas incorrectamente, siempre y cuando el proveedor de servicios de pago haya respetado sus obligaciones de información con arreglo a la presente Directiva. Si el usuario de servicios de pago respeta el plazo de notificación, debe poder hacer valer esas reclamaciones dentro de los plazos de prescripción nacionales. [...]

(71) En caso de una operación de pago no autorizada, el proveedor de servicios de pago deberá devolver inmediatamente el importe de dicha operación al ordenante. No obstante, cuando haya una sospecha fundada de que una operación no autorizada es el resultado de una conducta fraudulenta del usuario de servicios de pago y la sospecha se funde en motivos objetivos comunicados a la autoridad nacional pertinente, el proveedor de servicios de pago tendrá la posibilidad de efectuar, en un plazo razonable, una investigación antes de devolver el importe al ordenante. A fin de evitar perjuicios al ordenante, la fecha de valor del abono de la devolución no debe ser posterior a la fecha de adeudo del importe. A fin de ofrecer incentivos para que el usuario de servicios de pago comunique sin demora a su proveedor de servicios de pago toda pérdida o robo de un instrumento de pago y reducir así el riesgo de operaciones de pago no autorizadas, el usuario solo debe ser responsable por un importe muy limitado, salvo en caso de fraude o grave negligencia por su parte. A este respecto, parece adecuado fijar un importe de 50 EUR con vistas a garantizar una protección elevada y homogénea del usuario dentro de la Unión. No se le debe imputar responsabilidad al ordenante, cuando este se encuentre en una posición que no le permite tener conocimiento del extravío, el robo o la sustracción del instrumento de pago. Asimismo, una vez que el usuario de servicios de pago haya comunicado al proveedor de servicios de pago que su instrumento de pago puede haber sido objeto de uso fraudulento, no deben exigírsele responsabilidades por las ulteriores pérdidas que pueda ocasionar el uso no autorizado del instrumento. [...]

(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. Se deben considerar nulas las cláusulas contractuales y las condiciones de prestación y utilización de instrumentos de pago mediante las cuales aumente la carga de la prueba sobre el consumidor o se reduzca la carga de la prueba sobre el emisor. Además, en situaciones específicas y, más concretamente, cuando el instrumento de pago no esté presente en el punto de venta, como

en el caso de los pagos en línea, resulta oportuno que el proveedor de servicios aporte pruebas de la presunta negligencia, puesto que los medios a disposición del ordenante son limitados en esos casos.»

Con relación a las medidas de seguridad que deben adoptarse, los Considerandos 91 y 96 indican:

«(91) Los proveedores de servicios de pago son responsables de las medidas de seguridad. Dichas medidas deben ser proporcionales a los riesgos de seguridad existentes. Los proveedores de servicios de pago deben establecer un marco que permita paliar los riesgos y mantener procedimientos eficaces de gestión de incidentes.

(96) [...] Es necesario que las credenciales de seguridad personalizadas se utilicen adecuadamente, para limitar los riesgos de captación de datos mediante suplantación de identidad (phising) y otras actividades fraudulentas. A tal fin, el usuario debe poder confiar en la adopción de medidas que protejan la confidencialidad y la integridad de sus credenciales personalizadas de seguridad. Entre estas medidas figuran, en particular, los sistemas de cifrado basados en dispositivos personales del ordenante (lectores de tarjetas o teléfonos móviles, por ejemplo) o facilitados al ordenante por su proveedor de servicios de pago gestor de cuentas por otros cauces (por SMS o mensaje de correo electrónico por ejemplo). Las medidas, incluidos los sistemas habituales de cifrado, que pueden dar lugar a códigos de autenticación como las contraseñas de un solo uso, pueden aumentar la seguridad de las operaciones de pago; la utilización de este tipo de códigos de autenticación por los usuarios de servicios de pago debe considerarse compatible con sus obligaciones respecto de los instrumentos de pago y las credenciales de seguridad personalizadas...»

Estas indicaciones se plasman en los arts. 64 y 69 y ss. de la Directiva 2015/2366 . Así, el art. 64, titulado «Consentimiento y retirada del consentimiento», dispone:

«1. Los Estados miembros velarán por que las operaciones de pago se consideren autorizadas únicamente cuando el ordenante haya dado su consentimiento a que se ejecute la operación de pago. [...]

2. El consentimiento para la ejecución de una operación de pago o de una serie de operaciones de pago se dará en la forma acordada entre el ordenante y el proveedor de servicios de pago. El consentimiento para la ejecución de una operación de pago podrá darse también por conducto del beneficiario o del proveedor de servicios de iniciación de pagos.

En ausencia de consentimiento, la operación de pago se considerará no autorizada.

[...] 4. El ordenante y el proveedor o proveedores de servicios de pago correspondientes convendrán en el procedimiento de notificación del consentimiento.»

Los arts. 69 y 70 de la Directiva regulan las obligaciones del usuario y del proveedor de servicios de pago en relación con los instrumentos de pago. Así, el art. 69 ordena:

«1. El usuario de servicios de pago habilitado para utilizar un instrumento de pago:

a) utilizará el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago que deberán ser objetivas, no discriminatorias y proporcionadas;

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

2. En particular, a los efectos del apartado 1, letra a), el usuario de servicios de pago, en cuanto reciba un instrumento de pago, tomará todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas del instrumento de pago.»

Y, paralelamente, el art. 70.1 establece respecto del proveedor de servicios de pago las siguientes obligaciones:

«a) se asegurará de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar el instrumento, sin perjuicio de las obligaciones que incumben al usuario de servicios de pago con arreglo al artículo 69;

[...]

c) garantizará que en todo momento estén disponibles medios adecuados que permitan al usuario de servicios de pago efectuar una notificación en virtud del artículo 69, apartado 1, letra b), o solicitar un desbloqueo del instrumento de pago en virtud del artículo 68, apartado 4; el proveedor de servicios de pago facilitará al usuario de dichos servicios, cuando este así lo solicite, medios que le permitan demostrar que ha efectuado dicha notificación durante los dieciocho meses siguientes a la misma;

d) ofrecerá al usuario de servicios de pago la posibilidad de efectuar una notificación en virtud del artículo 69, apartado 1, letra b), gratuitamente y cobrar, si acaso, únicamente los costes de sustitución directamente imputables al instrumento de pago;

e) impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación en virtud del artículo 69, apartado 1, letra b).»

El art. 71.1 de la Directiva prevé la obligación del proveedor de servicios de pago de rectificar la operación si el usuario lo comunica sin demora injustificada:

«El usuario de servicios de pago obtendrá la rectificación por parte del proveedor de servicios de pago de una operación de pago no autorizada o ejecutada incorrectamente únicamente si el usuario de servicios de pago se lo notifica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 89, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo.»

Y el art. 72 añade, en relación con la prueba de la autenticación y ejecución de las operaciones de pago, cuando el usuario niegue haberla autorizado o alegue que se ejecutó de manera incorrecta:

«1. Los Estados miembros exigirán que, cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que esta se ejecutó de manera incorrecta, corresponda al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago. [...]

2. Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ejecutada, la utilización de un instrumento de pago registrada por el proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, no bastará necesariamente para demostrar que la operación de pago ha sido autorizada por el ordenante, ni que este ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 69. El proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, aportará pruebas para demostrar que el usuario del servicio de pago ha cometido fraude o negligencia grave.»

Por último, los arts. 73 y 74 de la Directiva ordenan el régimen de responsabilidad del proveedor y del usuario en caso de operaciones de pago no autorizadas. El art. 73.1 señala:

«1. Sin perjuicio del artículo 71, los Estados miembros velarán por que, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devuelva a este el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito a la autoridad nacional pertinente. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada...»

Y el art. 74.1 contempla la posibilidad de que, en determinados casos, el ordenante pueda quedar obligado a soportar las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado o robado, hasta un máximo de 50 €.

3.- El *Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017 , por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros, avanza un paso más en esta línea y, además de desarrollar el contenido y las exigencias en materia de autenticación reforzada, impone en su art. 2 a los proveedores de servicios de pago el deber 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:*

«1. Los proveedores de servicios de pago dispondrán de mecanismos de supervisión de las operaciones que les permitan detectar operaciones de pago no autorizadas o fraudulentas a efectos de la aplicación de las medidas de seguridad a que se hace referencia en el artículo 1, letras a) y b).

Dichos mecanismos se basarán 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.

2. Los proveedores de servicios de pago garantizarán que los mecanismos de supervisión de las operaciones tengan en cuenta, como mínimo, todos los factores basados en el riesgo siguientes: a) listas de elementos de autenticación comprometidos o sustraídos; b) el importe de cada operación de pago; c) supuestos de fraude conocidos en la prestación de servicios de pago; d) señales de infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación; e) 1. en caso de que el dispositivo o el programa informático de acceso sea facilitado por el proveedor de servicios de pago, un registro de la utilización del dispositivo o el programa informático de acceso facilitado al usuario de los servicios de pago y de su uso anormal.»

4.- La mencionada *Directiva 2015/2366 ha sido traspuesta al ordenamiento jurídico interno por el Real Decreto Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, cuyos arts. 36 y 41 a 46 reproducen casi miméticamente los preceptos que se acaban de transcribir. Así, el art. 36.1 proclama:*

«1. Las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución. A falta de tal consentimiento la operación de pago se considerará no autorizada. El consentimiento para la ejecución de una operación de pago podrá darse también por conducto del beneficiario o del proveedor de servicios de iniciación de pagos.

El ordenante y su proveedor de servicios de pago acordarán la forma en que se dará el consentimiento, así como el procedimiento de notificación del mismo.»

El art. 41 recoge las obligaciones del usuario en relación con los instrumentos de pago y las credenciales de seguridad personalizadas, indicando que:

«a) utilizará el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago que deberán ser objetivas, no discriminatorias y proporcionadas y, en particular, en cuanto reciba un instrumento de pago, tomará todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas;

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

Y el art. 42.1 del Real Decreto Ley reitera el contenido del art. 71.1 de la Directiva, con el matiz de insistir en el carácter gratuito de los medios que permitan al usuario efectuar la notificación a que hace referencia el art. 41.b).

Lo mismo sucede con los arts. 43 y 44, en relación con los arts. 71 y 72 de la Directiva. En particular, el art. 44 atribuye al proveedor de los servicios de pago la carga de la prueba de que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago, así como que el usuario del servicio de pago cometió fraude o negligencia grave:

«1. Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago. [...]

2. A los efectos de lo establecido en el apartado anterior, el registro por el proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 41.

3. Corresponderá al proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, probar que el usuario del servicio de pago cometió fraude o negligencia grave. [...]»

Igualmente, los arts. 45 y 46 del Real Decreto Ley recogen lo dispuesto en los arts. 73 y 74 de la Directiva acerca de la responsabilidad del proveedor de servicios de pago y del usuario en caso de operaciones de pago no autorizadas. En este sentido, el art. 45.1 establece:

«1. Sin perjuicio del artículo 43 de este real decreto-ley, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al

Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada.»

Y el art. 46, después de recoger en su apartado 1 la posibilidad de que el ordenante pueda quedar obligado a soportar, hasta un máximo de 50 €, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero, vincula la responsabilidad del ordenante a la existencia de fraude o por incumplimiento deliberado o por negligencia grave de las obligaciones que pesan sobre el mismo:

«1. No obstante lo dispuesto en el artículo 45, el ordenante podrá quedar obligado a soportar, hasta un máximo de 50 euros, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero, salvo que:

a) al ordenante no le resultara posible detectar la pérdida, la sustracción o la apropiación indebida de un instrumento de pago antes de un pago, salvo cuando el propio ordenante haya actuado fraudulentamente, o

b) la pérdida se debiera a la acción o inacción de empleados o de cualquier agente, sucursal o entidad de un proveedor de servicios de pago al que se hayan externalizado actividades.

El ordenante soportará todas las pérdidas derivadas de operaciones de pago no autorizadas si el ordenante ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41. En esos casos, no será de aplicación el importe máximo contemplado en el párrafo primero.

En todo caso, el ordenante quedará exento de toda responsabilidad en caso de sustracción, extravío o apropiación indebida de un instrumento de pago cuando las operaciones se hayan efectuado de forma no presencial utilizando únicamente los datos de pago impresos en el propio instrumento, siempre que no se haya producido fraude o negligencia grave por su parte en el cumplimiento de sus obligaciones de custodia del instrumento de pago y las credenciales de seguridad y haya notificado dicha circunstancia sin demora.

2. Si el proveedor de servicios de pago del ordenante no exige autenticación reforzada de cliente, el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta. En el supuesto de que el beneficiario o el proveedor de servicios de pago del beneficiario no acepten la autenticación reforzada del cliente, deberán reembolsar el importe del perjuicio financiero causado al proveedor de servicios de pago del ordenante.

3. Salvo en caso de actuación fraudulenta, el ordenante no soportará consecuencia económica alguna por la utilización, con posterioridad a la notificación a que se refiere el artículo 41.b), de un instrumento de pago extraviado o sustraído.

4. Si el proveedor de servicios de pago no tiene disponibles medios adecuados para que pueda notificarse en todo momento el extravío o la sustracción de un instrumento de pago, según lo dispuesto en el artículo 42.1.c), el ordenante no será responsable de las consecuencias económicas que se deriven de la utilización de dicho instrumento de pago, salvo en caso de que haya actuado de manera fraudulenta.»

5.- Al margen de la normativa expuesta, la *sentencia del Tribunal de Justicia de 2 de septiembre de 2021 (C-337/20), con ocasión de examinar el alcance del art. 58 de la anterior Directiva 2007/64 , aporta siquiera sea de modo indirecto unas pautas orientativas sobre la diligencia exigible al usuario de los servicios de pago.*

En este sentido, en las conclusiones del abogado general Sr. Henrik Saugmandsgaard, presentadas el 8 de julio de 2021 y asumidas por el Tribunal de Justicia, se dice:

«38. Por lo que respecta, en primer lugar, al tenor de los artículos 58 y 60 de la Directiva 2007/64 , cabe señalar que el artículo 58 introduce una obligación general de notificación de cualquier operación no autorizada o ejecutada incorrectamente, de modo que el usuario del servicio solo obtendrá la rectificación de una operación no autorizada o ejecutada incorrectamente si notifica dicha operación a su proveedor de servicios, notificación que deberá efectuarse a más tardar en los trece meses de la fecha del adeudo correspondiente.

39. El artículo 60 de dicha Directiva se refiere específicamente a la responsabilidad del proveedor de servicios de pago en caso de operaciones no autorizadas. Su apartado 1 establece que, sin perjuicio del artículo 58, los Estados miembros velarán por que el proveedor de servicios devuelva de inmediato al ordenante el importe de la operación no autorizada.

40. La expresión «sin perjuicio del artículo 58» que figura en el artículo 60 de la Directiva 2007/64 significa que lo dispuesto en este artículo no se establece en detrimento del artículo 58 de dicha Directiva. De ello se desprende, en mi opinión, que la responsabilidad del proveedor en caso de operaciones no autorizadas está supeditada a

que el usuario del servicio respete el procedimiento de notificación previsto en el artículo 58 de dicha Directiva, cuyo plazo no puede exceder de los trece meses siguientes a la fecha del adeudo.

41. El considerando 31 de la Directiva 2007/64 pone de manifiesto que se trata efectivamente de una condición al establecer que si el usuario del servicio de pago respeta el plazo de la notificación, debe tener la posibilidad de presentar su reclamación relativa al carácter no autorizado del pago.

[...]

51. A continuación, tanto en el caso de operaciones no autorizadas como de operaciones ejecutadas de manera incorrecta, el artículo 59 de la Directiva 2007/64 , relativo a la carga de la prueba, establece que corresponde al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada.

52. Debo subrayar que este artículo 59 efectúa una inversión de la carga de la prueba, haciendo que esta no recaiga sobre quien alega la existencia de una operación no autorizada, a saber, el usuario del servicio de pago, sino sobre el proveedor de servicios de pago. De ello se desprende que, durante un período de trece meses, este último está sujeto a una obligación de devolución casi automática e inmediata de la operación que el usuario no ha autorizado.

53. De este modo, el legislador de la Unión ha establecido un régimen de responsabilidad basado en tres elementos esenciales y vinculados entre sí, a saber: una obligación de notificación que recae sobre el usuario del servicio de pago, establecida en el artículo 58 de la Directiva 2007/64 ; la atribución de la carga de la prueba al proveedor de esos servicios, que figura en el artículo 59 de dicha Directiva, y, por último, en caso de falta de prueba, la responsabilidad de ese proveedor, de conformidad con los artículos 60 y 75 de dicha Directiva, en función de que la operación no haya sido autorizada, no haya sido ejecutada o haya sido ejecutada incorrectamente.

[...]

86. De este modo, existe un equilibrio entre, en primer lugar, la obligación de información que recae sobre el proveedor de servicios de pago, en segundo lugar, el deber de diligencia que incumbe al usuario del servicio de pago asociado a una obligación de notificación dentro de un plazo concreto y, en tercer lugar, la responsabilidad estricta del proveedor, sin que el usuario tenga que demostrar una falta o negligencia.»

La posterior sentencia del Tribunal de Justicia de 2 de septiembre de 2021 (C-337/20), tras indicar que, para interpretar una disposición del Derecho de la Unión, no solo debe tenerse en cuenta su tenor literal, sino también el contexto en el que se inscribe y los objetivos perseguidos por la normativa de la que forma parte, declara:

«32 En primer lugar, por lo que respecta, por una parte, al texto del apartado 1 del artículo 60 de la Directiva 2007/64 , titulado «Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas», conviene indicar que este artículo dispone que, sin perjuicio del artículo 58 de la citada Directiva, los Estados miembros velarán por que, en el caso de una operación de pago no autorizada, el proveedor de servicios de pago devuelva de inmediato al ordenante el importe de tal operación y, en su caso, por que restablezca en la cuenta de pago en la cual se haya adeudado el importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada.

[...]

39 En el sistema de este régimen de responsabilidad, la obligación de notificación por el usuario de servicios de pago de cualquier operación no autorizada es condición para que dicho régimen pueda aplicarse en favor del usuario, denominado también ordenante en determinadas disposiciones de la Directiva 2007/64 .

40 A continuación, el artículo 59 de esta Directiva incluye en el régimen de responsabilidad por operaciones no autorizadas un mecanismo de carga de la prueba favorable al usuario de servicios de pago. En esencia, la carga de la prueba recae sobre el proveedor de servicios de pago, que debe probar que la operación de pago fue autenticada, registrada con exactitud y contabilizada. En la práctica, el régimen de prueba establecido en dicho artículo 59 lleva, desde el momento en que la notificación prevista en el artículo 58 de la citada Directiva se ha efectuado dentro del plazo previsto en él, a someter al proveedor de servicios de pago a una obligación de devolución inmediata, de conformidad con el artículo 60, apartado 1, de dicha Directiva.

[...]

63 Así, como ha señalado, en esencia, el Abogado General en el punto 86 de sus conclusiones, el régimen de responsabilidad previsto en el artículo 60, apartado 1, de la Directiva 2007/64 se basa en un equilibrio entre la obligación de información que recae sobre el proveedor de servicios de pago y la obligación de notificación de cualquier operación no autorizada dentro de un plazo de trece meses que incumbe al usuario de servicios de

pago, que permite fundamentar la responsabilidad estricta del proveedor, sin que el usuario tenga que demostrar una falta o negligencia.»

6.-*Con arreglo a la normativa comunitaria y nacional aplicable y a la jurisprudencia comunitaria recaída en interpretación de la regulación de la que trae causa la primera, podemos concluir:*

1.º El usuario de servicios de pago debe adoptar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas y, en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, ha de notificarlo al proveedor de servicios de pago de manera inmediata, tan pronto tenga conocimiento de ello.

2.º En caso de que se produzca una operación de pago no autorizada o ejecutada incorrectamente, si el usuario de servicios de pago se lo comunica sin demora injustificada, el proveedor debe proceder a su rectificación y reintegrar el importe de inmediato, salvo que tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España.

3.º Cuando un usuario niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, incumbe al proveedor la carga de demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago.

4.º El mero hecho del registro por el proveedor de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones, correspondiendo al proveedor la prueba de que el usuario del servicio de pago cometió fraude o negligencia grave.

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.

7.- Según se avanzó antes, la aplicación de la normativa y jurisprudencia expuesta nos lleva a rechazar el motivo de recurso.

Es verdad que el art. 36.1 del Real Decreto Ley 19/2018 establece que las operaciones de pago «se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución», así como que «[e]l ordenante y su proveedor de servicios de pago acordarán la forma en que se dará el consentimiento, así como el procedimiento de notificación del mismo». Como también es cierto que en la condición 4.ª del contrato de banca digital suscrito entre las partes se indica que «el usuario-titular se compromete a otorgar plena validez jurídica a

las operaciones realizadas mediante cualquier tipo de claves y/o códigos que permitan la identificación personal del mismo, dando como válidas y propias las operaciones realizadas empleando las claves o códigos previstos en este contrato», sin que se discuta que en el supuesto litigioso se emplearon las claves y/o códigos personales del demandante.

Pero no es menos cierto que, primero, estamos ante una regulación que se impone a las partes, sin que su aplicación quede al albur de la libertad o autonomía contractual, de modo que la condición 4.ª -como la cláusula 8.ª, de exoneración de responsabilidad de la entidad bancaria- han de respetar en todo caso el régimen de derechos, obligaciones y fórmulas de responsabilidad legalmente previstos; segundo, que, en el marco de esta regulación, el consentimiento no se entiende prestado por el solo hecho de que la operación de pago se haya realizado mediante la utilización de las claves personales, sino que es necesario que provenga del usuario o, en caso de que éste niegue su intervención, que se acredite fraude, incumplimiento deliberado o, al menos, negligencia grave por parte del usuario, cuya prueba recae sobre la entidad bancaria; y, tercero, cuando el usuario ha notificado de forma inmediata la existencia de una operación no autorizada, la entidad ha de proceder a su rectificación, salvo que demuestre que hubo fraude imputable al usuario.

En otras palabras, el que la entidad bancaria acredite que la operación fue autenticada, registrada con exactitud y contabilizada, no es suficiente para eximirle de responsabilidad. Ha de probar que la operación no resultó afectada por un fallo técnico u otra deficiencia del servicio prestado, y, dado que el cliente niega que la operación fuera consentida, que no hubo por parte de este último fraude, incumplimiento deliberado o negligencia grave."

Y sigue diciendo:

"1.- Formulación del motivo. La entidad recurrente denuncia la infracción de los arts. 44 y 45 del Real Decreto Ley 19/2018 , de servicios de pago, el primero porque la prueba practicada acredita que operación de pago fue autenticada, registrada con exactitud y contabilizada, y no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de los servicios de pago; y, el segundo, porque no es de aplicación al presente caso, ya que se trata de operaciones autorizadas, al haberse dado el consentimiento de conformidad con las condiciones contractuales conocidas y aceptadas por el actor mediante la firma de los contratos.

*En el desarrollo del motivo, la recurrente insiste en que no constan fallos de seguridad en los sistemas de Ibercaja Banca S.A., cuya responsabilidad se ciñe a sus propios sistemas informáticos y no a los dispositivos propiedad del usuario, que es quien debe velar y garantizar la seguridad tanto de su ordenador como de su dispositivo móvil. Es al cliente al que se le sustraen los datos y al que, con arreglo al contrato de banca digital «Ibercaja Directo», corresponde la obligación de guarda y custodia de las claves de usuario, por lo que el «robo o sustracción de las claves suponen una clara negligencia del usuario». Por otra parte, la entidad bancaria envía a los clientes, de forma personalizada, comunicaciones con advertencias, avisos y consejos sobre el modo en que deben actuar en el uso de la banca on line; el usuario se ha apartado consciente y voluntariamente de las indicaciones de la entidad que, en comunicados remitidos, relaciona las medidas que deben considerarse para evitar este tipo de fraudes mediante «**phishing**».*

2.- Decisión de la Sala. El motivo debe desestimarse por las razones que seguidamente se exponen.

La recurrente reitera que ha cumplido con rigurosidad sus obligaciones, la identificación del usuario, la autentificación de las operaciones realizadas y la aplicación del doble factor de autenticación impuesta por la normativa de servicios de pago, sin que haya sufrido ningún tipo de incidencia técnica como para que le fueran usurpados ningún tipo de datos de clientes que permitieran a terceros realizar las transferencias discutidas, por lo que de acuerdo con el art.44 RDL 19/2018 no debe responder.

Mas ya hemos visto que, de conformidad con el art. 44 RDL, en caso de que el usuario niegue haber autorizado una operación de pago ya autorizada, el cumplimiento de las obligaciones relativas a la autenticación, registro y contabilización de la operación de pago fue autenticada, 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 el supuesto enjuiciado fallan ambos presupuestos. En primer lugar, la entidad demandada debía probar, no solo que la operación no se vio afectada por un fallo técnico, sino que no se ha producido una prestación defectuosa del servicio, cuestión que ya ha sido objeto de análisis con ocasión de examinar el anterior motivo, concluyendo que el servicio no se prestó correctamente.

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."

Un nuevo examen de las actuaciones a la luz de la doctrina jurisprudencial contenida en la sentencia transcrita nos lleva a revocar la sentencia impugnada y estimar la demanda.

En particular no podemos compartir la conclusión alcanzada por la Juzgadora de instancia cuando considera acreditado que fue el actor quien actuó sin la debida diligencia, debiendo hacer las consideraciones siguientes.

1) En primer lugar, cabe indicar que el demandante comunicó a la entidad bancaria lo ocurrido tan pronto tuvo conocimiento de ello. Así, el Sr. Amadeo afirma en su demanda que inmediatamente después de haber recibido la llamada telefónica del supuesto empleado de Deutsche Bank contactó con el Banco, extremo que no es negado por la demandada; el mismo día de los hechos, 1 de marzo de 2024, presentó denuncia ante los Mossos d'Esquadra; también el mismo día 1 de marzo cumplimentó los formularios de reclamación de operaciones con tarjeta de Deutsche Bank en los que se consignan las operaciones no autorizadas y se hace constar que la tarjeta ha estado en poder del actor todo el tiempo; en fecha 7 de marzo de 2024 el Sr. Amadeo dirigió un burofax a la entidad bancaria relatando lo sucedido el día 1 y reclamando el reintegro del dinero sustraído; en fecha 18 de marzo de 2024 el actor remitió un correo electrónico al banco reiterando su reclamación. No consta que Deutsche Bank contestara ninguna de estas comunicaciones a excepción del último correo electrónico que generó una respuesta automática (documento 3 a 8 de la demanda). Aunque el banco manifiesta haber procedido a una investigación, lo cierto es que no hay prueba alguna de ello y menos aún que con ella se hubiera verificado que no se había comprometido la seguridad de los datos registrados en la entidad. Nada se ha aportado al respecto y nada se comunicó al cliente. Parece evidente que si hubiera existido tal investigación se habría traído a los autos y se habría comunicado su resultado al actor, y nada de eso ha sucedido.

2) Hay que recordar que no basta con una mera falta de diligencia del cliente sino que es necesario probar la existencia de fraude o negligencia grave, correspondiendo a la entidad bancaria en todo caso la carga de la prueba. En el supuesto enjuiciado la entidad bancaria no ha apuntado en ningún momento la existencia de fraude por parte del actor, habiéndose limitado a afirmar que el Sr. Amadeo no actuó con la diligencia debida y así lo ha entendido también la sentencia de instancia, consideración que la Sala no comparte.

3) La demandada considera relevante que el actor siguiera las indicaciones de un supuesto empleado del banco sin sospechar nada cuando desde la entidad se indica a los clientes que nunca se va a poner en contacto con ellos por vía telefónica para solicitar datos bancarios. Aun siendo ciertas las campañas publicitarias de las entidades bancarias alertando de los riesgos de fraude, no lo es menos que en el presente caso el actor afirma que quien se identificó como empleado del banco no le pidió ningún dato, sino que contaba con su nombre, apellidos, DNI, dirección, número de cuenta y números de sus tarjetas, por lo que el Sr. Amadeo no facilitó ningún dato personal, bancario ni credencial o contraseña.

4) La juzgadora de instancia concluye que el actor actuó sin la debida diligencia *"al recibir varios SMS en su teléfono móvil solicitándole unas claves para activar su tarjeta en otro dispositivo",*refiriéndose en varias ocasiones a mensajes y SMS. Sin embargo, el actor no dice en ningún momento haber recibido un mensaje o un SMS; lo que relata es que el supuesto empleado le explicó que para proceder a la anulación de las tarjetas debía confirmar el procedimiento y que para ello le aparecería en la aplicación un aviso para aceptar la operación, añadiendo que cuando el aviso apareció, confirmó. Según el actor, todo lo sucedido fue en el aplicativo del banco y la demandada no ha probado que no fuese así.

5) La sentencia justifica la falta de diligencia del actor acogiendo plenamente la versión ofrecida por la demandada en su escrito de contestación a la demanda, copiando párrafos enteros de dicho escrito sin que hayan sido validados por prueba alguna.

6) Contrariamente a la consideración de la juez a quo, no podemos calificar de negligencia grave el hecho de confirmar lo que se presenta como una operación de anulación de tarjetas cuando el cliente se limita a confirmar la operación en la propia aplicación informática del banco.

Llegados a este punto conviene retomar la **STS 571/2025**, cuando señala que:

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."

El Tribunal Supremo no considera *"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 tampoco la Sala puede considerar normal que en un solo día, y en espacio de pocos minutos, se realicen catorce operaciones de importes elevados (siete de ellas por la misma cantidad de 863,14 €) sin que salten las alarmas de la entidad bancaria. El proveedor de servicios de pago, dice el Tribunal Supremo, ha de adoptar las medidas de seguridad que garanticen su correcto funcionamiento y minimicen los riesgos y los efectos nocivos de su materialización.

7) Por último, cabe recordar que el hecho de que la entidad bancaria acredite que la operación fue autenticada, registrada con exactitud y contabilizada, no es suficiente para eximirle de responsabilidad.

Así pues, procede afirmar la responsabilidad de la entidad bancaria y, consecuentemente, la obligación de la demandada de reintegrar el importe de las operaciones no autorizadas por el actor que asciende a 12.786,16 €, más el interés legal desde la fecha de los cargos que además coincide con la de la primera reclamación extrajudicial.

El demandante reclama también la suma de 2.000 € en concepto de daño moral alegando que su boda debía celebrarse el día 17 de mayo de 2024, con un coste aproximado de 14.000 €, y que como consecuencia de lo acaecido su saldo bancario llegó a ser negativo y su novia se vio obligada a solicitar un préstamo.

La jurisprudencia viene admitiendo la posibilidad de indemnizar el daño moral, entendiendo por tal el sufrimiento o padecimiento psíquico o espiritual, comprendiendo situaciones tales como la impotencia, zozobra, inquietud, ansiedad, angustia, pesadumbre, temor o presagio de incertidumbre (SSTS 7 marzo 2005, 11 noviembre 2003, 31 mayo 2000). La Sentencia del Tribunal Supremo de 9 de septiembre de 2021 establece que *"el daño moral indemnizable incluye padecimientos psíquicos como impacto, ansiedad, incertidumbre o quebranto emocional, y no requiere prueba objetiva directa cuando deriva de hechos suficientemente graves."*

En el caso enjuiciado estimamos razonable la petición formulada pues es comprensible la situación de inquietud, angustia e incertidumbre que debió sufrir el demandante cuando se vio despojado de sus ahorros dos meses antes de su boda y ante los gastos que debía afrontar, situación que fue provocada por la entidad demandada al no atender la reclamación formulada ni proceder a la restitución del dinero sustraído.

En atención a lo expuesto procede revocar la sentencia de instancia, acordando en su lugar estimar la demanda y condenar a Deutsche Bank a abonar al actor la cantidad de 12.786,18 €, más el interés legal desde la fecha de los cargos y la cantidad de 2.000 € en concepto de daño moral más el interés previsto en el art. 576 LEC.

TERCERO.-De conformidad con lo dispuesto en el art. 398 LEC, no se hace especial pronunciamiento respecto de la costas de esta alzada.

FALLO

ESTIMOel recurso de apelación interpuesto por Amadeo contra la sentencia dictada por el Juzgado de Primera Instancia nº 13 de Barcelona en fecha 8 de julio de 2024, que revoco, acordando en su lugar estimar la demanda formulada por Amadeo contra DEUTSCHE BANK SAE, condenando a la entidad demandada a abonar al actor la cantidad de 12.786,18 €, más el interés legal desde la fecha del cargo y la cantidad de 2.000 € en concepto de daño moral más el interés previsto en el art. 576 LEC, así como al pago de las costas.

No se hace especial pronunciamiento respecto de las costas de esta alzada.

Procede reintegrar a la parte recurrente el depósito constituido, devolver las actuaciones al órgano judicial de instancia y archivar el presente procedimiento.

Contra esta resolución no cabe interponer recurso alguno.

Así por esta sentencia, lo pronuncio, mando y firmo.

La Magistrada

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.