Roj: **STS 1671/2025** - **ECLI:ES:TS:2025:1671**

Id Cendoj: **28079110012025100563**
Órgano: **Tribunal Supremo. Sala de lo Civil**
Sede: **Madrid**
Sección: **1**
Fecha: **09/04/2025**
Nº de Recurso: **1151/2023**
Nº de Resolución: **571/2025**
Procedimiento: **Recurso de casación**
Ponente: **MANUEL ALMENAR BELENGUER**
Tipo de Resolución: **Sentencia**

Resoluciones del caso: **SAP Z 1992/2022,**
ATS 14678/2024,
STS 1671/2025

T R I B U N A L S U P R E M O

Sala de lo Civil

Sentencia núm. 571/2025

Fecha de sentencia: 09/04/2025

Tipo de procedimiento: CASACIÓN

Número del procedimiento: 1151/2023

Fallo/Acuerdo:

Fecha de Votación y Fallo: 03/04/2025

Ponente: Excmo. Sr. D. Manuel Almenar Belenguer

Procedencia: AUD.PROVINCIAL DE ZARAGOZA, SECCIÓN 5.ª

Letrado de la Administración de Justicia: Ilmo. Sr. D. Juan Manuel Ávila de Encío

Transcrito por: ACV

Nota:

CASACIÓN núm.: 1151/2023

Ponente: Excmo. Sr. D. Manuel Almenar Belenguer

Letrado de la Administración de Justicia: Ilmo. Sr. D. Juan Manuel Ávila de Encío

TRIBUNAL SUPREMO

Sala de lo Civil

Sentencia núm. 571/2025

Excmos. Sres.

D. Ignacio Sancho Gargallo, presidente

D. Rafael Sarazá Jimena

D. Pedro José Vela Torres

D. Manuel Almenar Belenguer

En Madrid, a 9 de abril de 2025.

Esta Sala ha visto el recurso de casación interpuesto por Ibercaja Banco S.A., representada por el procurador D. Jorge Luis Guerrero Ferrández, bajo la dirección letrada de D.ª María Jesús Gracia Ballarín, contra la sentencia n.º 996/2022, de 17 de noviembre, dictada por la Sección 5.ª de la Audiencia Provincial de Zaragoza en el recurso de apelación n.º 20/2022, dimanante de las actuaciones de juicio ordinario n.º 505/2021 del Juzgado de Primera Instancia n.º 7 de Zaragoza. Ha sido parte recurrida D. Martin , representado por la procuradora D.ª Beatriz Utrilla Aznar y bajo la dirección letrada de D. Miguel Ángel Marqués Lafuente.

Ha sido ponente el Excmo. Sr. D. Manuel Almenar Belenguer.

ANTECEDENTES DE HECHO

PRIMERO.- *Tramitación en primera instancia*

1.- La procuradora D.ª Beatriz Utrilla Aznar, en nombre y representación de D. Martin , interpuso demanda de juicio ordinario contra Ibercaja Banco S.A. en la que solicitaba se dictara sentencia por la que se declare que:

«1.- La actuación de la demandada en la gestión del fraude sufrido por el actor supone un incumplimiento de las obligaciones contractuales asumidas por Ibercaja Banco S.A. en el contrato de banca a distancia y contrato de cuenta corriente y/o depósito detallados en el Hecho Primero de esta demanda.

2.- Que dicha actuación de la demandada ha ocasionado daños y perjuicios a los demandantes por importe de 56.474,63 euros (cincuenta y seis mil cuatrocientos setenta y cuatro euros y sesenta y tres céntimos), más los intereses dejados de percibir por dicha cantidad desde que se efectuaron las transferencias fraudulentas los días 17 y 18 de marzo de 2021, debiendo estar y pasar por las anteriores declaraciones y pagar al actor dicha cuantía.

3.- Todo ello con expresa imposición de costas a la parte demandada».

2.- La demanda fue repartida al Juzgado de Primera Instancia n.º 7 de Zaragoza, que incoó el procedimiento ordinario n.º 505/2021. Admitida a trámite, se procedió al emplazamiento de la parte demandada.

3.- El procurador D. Jorge Guerrero Ferrández, en representación de Ibercaja Banco S.A., contestó a la demanda mediante escrito en el que solicitaba la desestimación de la demanda con imposición de costas a la parte actora.

4.- Previos los trámites correspondientes, el Juzgado de Primera Instancia n.º 7 de Zaragoza dictó sentencia n.º 292/2021, de 29 de octubre, con la siguiente parte dispositiva:

«Que estimo la demanda presentada por la Procuradora de los Tribunales D.ª Beatriz Utrilla Aznar, actuando en representación de D. Martin , frente a Ibercaja Banco SA y en su virtud se declara que:

1.- La actuación de la demandada en la gestión del fraude sufrido por el actor supone un incumplimiento de las obligaciones contractuales asumidas por Ibercaja Banco S.A. en el contrato de banca a distancia y contrato de cuenta corriente y/o depósitos detallados en el fundamento de derecho primero de esta sentencia.

2.- Que dicha actuación de la demandada ha ocasionado daños y perjuicios al demandante por importe de 56.474,63 euros (cincuenta y seis mil cuatrocientos setenta y cuatro euros y sesenta y tres céntimos), más los intereses dejados de percibir por dicha cantidad desde que se efectuaron las transferencias fraudulentas los días 17 y 18 de marzo de 2021, debiendo estar y pasar por las anteriores declaraciones y pagar al actor dicha cuantía.

3.- Todo ello con expresa imposición de costas a la parte demandada».

SEGUNDO.- *Tramitación en segunda instancia*

1.- La sentencia de primera instancia fue recurrida en apelación por la representación de Ibercaja Banco S.A.

2.- La resolución de este recurso correspondió a la sección 5.ª de la Audiencia Provincial de Zaragoza, que lo tramitó con el número de rollo n.º 20/2022, en el que, tras los oportunos trámites, en fecha 17 de noviembre de 2022 se pronunció sentencia, cuya parte dispositiva, literalmente copiada, decía:

«1 Desestimamos el recurso de apelación interpuesto por IBERCAJA BANCO S.A. y confirmamos la sentencia apelada dictada en estas actuaciones por el Ilmo. Magistrado-Juez del Juzgado de Primera Instancia Nº 7 de Zaragoza.

2 Con condena en costas a la parte apelante.

3 Dese al depósito el destino legal».

TERCERO .- *Interposición y tramitación del recurso de casación*

1.- El procurador D. Jorge Guerrero Ferrández, en representación de Ibercaja Banco S.A., interpuso recurso de casación, que se fundamenta en los siguientes motivos:

«Primero.- Fundado en infracción del art. 36 del Real Decreto Ley 19/2018, de servicios de pago, relativo a la Autorización de operaciones de pago, en relación con los arts. 2 y 3 del Reglamento Delegado UE 2018/389 de la Comisión Europea, 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.

»Segundo.- Infracción de los artículos 44 y 45 del Real Decreto Ley 19/2018, de servicios de pago.».

2.- Las actuaciones fueron remitidas por la Audiencia Provincial a esta Sala, y las partes fueron emplazadas para comparecer ante ella. Recibidas las actuaciones y personadas las partes por medio de los procuradores mencionados en el encabezamiento, se dictó auto de fecha 27 de noviembre de 2024, cuya parte dispositiva es como sigue:

«Admitir el recurso de casación interpuesto por la representación procesal de Ibercaja Banco SA presentó contra la sentencia dictada el 17 de noviembre de 2022 por la Audiencia Provincial de Zaragoza (Sección Quinta) en el rollo de apelación nº 20/2022, dimanante del juicio ordinario nº 505/2021 del Juzgado de Primera Instancia nº 7 de Zaragoza.»

3.- Se dio traslado a la parte recurrida para que formalizara su oposición, lo que hizo mediante la presentación del correspondiente escrito

4.- Al no solicitarse por las partes la celebración de vista pública, se señaló para votación y fallo el 3 de abril de 2025, en que ha tenido lugar con el resultado que seguidamente se expone.

FUNDAMENTOS DE DERECHO

PRIMERO.- *Resumen de antecedentes.*

1.- Son antecedentes fácticos no discutidos o declarados acreditados en la instancia y de interés para la resolución del recurso los siguientes:

i) D. Martin es titular, junto con sus padres, D. Torcuato y D.ª Raquel , de la cuenta corriente y/o depósito n.º NUM000 , y, con su esposa Dña. Sonia , de la cuenta corriente n.º NUM001 , ambas abiertas en la entidad Unicaja Banco S.A. Asimismo, D. Martin y Unicaja Banco S.A. suscribieron en fecha 31 de agosto de 2004 un contrato de banca a distancia nº NUM002 ***.

ii) En fecha 24 de febrero de 2021, a las 06:31 horas, D. Martin recibió un aviso de Google, en el que se le informaba que se había detectado una vulneración de su cuenta de correo electrónico @gmail, comprobándose un acceso no autorizado, ante lo cual, minutos después y como medida de prevención, a las 06:37 horas procedió al cambio de contraseña de la cuenta de correo.

iii) El mismo 24 de febrero, a las 06:37, D. Martin recibió en su teléfono móvil, n.º NUM003 *****, varios mensajes SMS con códigos para la materialización a través del sistema digital de transferencias que no obedecían a órdenes emitidas por él, lo que puso en conocimiento del personal de la sucursal del banco.

iv) En fechas 27 de febrero y 2 y 12 de marzo de 2021, Google Play y Google Ads realizaron varios cargos no autorizados en la cuenta n.º NUM001 , por valor de 464,98 €, utilizando su tarjeta VISA n.º NUM004 ****, lo que D. Martin comunicó a la entidad bancaria, reiterando su preocupación por los SMS recibidos, al tiempo que presentaba la pertinente reclamación a Google, que la rechazó el 15 de marzo, al no haber podido confirmar que se hubiera producido algún tipo de actividad fraudulenta.

v) El 16 de marzo, D.ª Estefanía recibió un email de Google en su dirección de correo de @gmail con el siguiente mensaje: «Alerta de seguridad crítica, se ha bloqueado un intento de inicio de sesión. Alguien acaba de usar tu contraseña para intentar iniciar sesión en tu cuenta». Inmediatamente, procedió a cambiar la contraseña, y, al día siguiente, 17 de marzo, el actor acudió a la oficina bancaria, donde informó sobre lo sucedido y solicitó la cancelación de la tarjeta y la emisión de otra nueva.

vi) Entre la noche del 17 y la mañana del 18 de marzo de 2021 se realizaron quince transferencias bancarias desde la cuenta corriente n.º NUM000 , de las cuales diez lo fueron a través de la plataforma Bizum (por importe de 500 € cada una) y cinco a través de la plataforma de banca electrónica «Ibercaja Directo» (por

importes de 28.970 €, 19.870 €, 9.876 € y dos de 9.870 € cada una -78.456,20 € en total-), devengando 236,53 € en comisiones, lo que suma un cargo total de 83.692,73 €.

vii) La mayoría de las mencionadas transferencias se efectuaron a favor de delincuentes conocidos por la Policía, a través de la línea de móvil NUM003 *****, titularidad de D.ª Estefanía , para lo cual se utilizó una tarjeta SIM que había sido duplicada el 17 de marzo, a las 17:29 horas, sin autorización de la titular, en el distribuidor Remedios (Murcia), lo que permitió al autor/es acceder a la información almacenada en la tarjeta, y recibir y utilizar el código solicitado para las sucesivas operaciones.

viii) El demandante no supo lo sucedido hasta la mañana del día 18 de marzo, cuando el personal de la sucursal, alertado por una llamada del personal del Banco Santander S.A., que había detectado el ingreso realizado en una cuenta sospechosa, le preguntó si durante la noche había hecho transferencias por valor de 83.000 €, a lo que respondió que no. Al acceder a la banca electrónica y comprobar la realidad de la información, el mismo día 18 presentó la correspondiente denuncia en la comisaría de la Policía Nacional, lo que motivó la incoación de las diligencias previas n.º 1017/21021 por el Juzgado de Instrucción n.º 11 de Zaragoza.

ix) En atención a la reclamación del actor, Ibercaja Banco S.A. solicitó la restitución de las cantidades dispuestas a las distintas entidades de destino, consiguiendo la devolución de 27.218,10 €, que fueron reintegrados al actor.

2.- En el presente procedimiento y con base en los mencionados hechos, D. Martin ejercita una acción de responsabilidad contractual frente a Ibercaja Banco S.A., en reclamación de 56.474,63 €, por los daños y perjuicios causados por el incumplimiento de las obligaciones asumidas por la demandada en el contrato de banca a distancia y en el contrato de cuenta corriente y/o depósito nº NUM000 , titularidad de D. Martin y de sus padres, D. Torcuato y D.ª Raquel , al haberse realizado quince transferencias bancarias no autorizadas, a través de la plataforma de banca electrónica «Ibercaja Directo».

3.- La demandada Ibercaja Banco S.A. se opone a la demanda y solicita su desestimación. Alega que, en las fechas indicadas y al amparo del contrato de banca electrónica «Ibercaja Directo» suscrito por ambas partes, se efectuaron por el titular cinco transferencias a través de la banca digital y otras doce operaciones de Bizum, dos de las cuales se anularon al superar el máximo diario.

Según afirma, todas las transferencias realizadas cumplen las exigencias impuestas en la normativa aplicable, constituida por el Real Decreto-ley 19/2018 de 23 de noviembre, de servicios de pago, que adaptó la normativa de servicios de pago para trasponer la Directiva 2015/2366 y el Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa dicha Directiva, en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos seguros, ya que se ejecutaron con identificación correcta del titular o usuario de las cuentas de origen y empleo de un doble factor de autentificación, consistente en el envío mediante SMS de un código/clave, que debía incorporar el usuario-titular del servicio «Ibercaja Directo», para continuar, consentir, confirmar y hacer efectiva la operación (el SMS se envía de forma exclusiva y con validez temporal limitada al teléfono móvil facilitado por el titular para este tipo de comunicaciones y autorizaciones a fin de operar a través de la banca on-line). Y, en cuanto a las operaciones vía Bizum, se llevan a cabo a través de una aplicación Ibercaja Pay, a la que se accede con el mismo usuario y clave de Ibercaja Directo, comprobándose que el dispositivo es el mismo que se usó para efectuar el alta en el servicio.

En el supuesto enjuiciado, el actor introdujo sus claves en reiteradas ocasiones para acceder al sistema, así como los códigos que se le enviaron por SMS para dar conformidad a las operaciones que realizaba, por lo que ningún incumplimiento cabe imputar a la entidad bancaria.

El control y las medidas de seguridad que la normativa impone a la entidad bancaria -continúa- no debe alcanzar a la falta de seguridad o vulnerabilidad que pueda tener el actor en sus dispositivos o a la falta de cautela en el uso o actuaciones que puedan facilitar a un tercero el uso de sus claves o de las contraseñas recibidas, mediante el acceso a páginas web o click en enlaces que puedan permitir a terceros el acceso a los datos de su dispositivo o de sus contactos, o datos o informaciones extraídos de sus propios correos electrónicos, que puedan comprometer sus claves de Google o la duplicidad o clonación de su tarjeta, o datos bancarios, que posibilitaran el control de su dispositivo por terceros. Por el contrario, sí que es responsabilidad del titular o usuario el mantenimiento actualizado de los dispositivos que utilice para operar en el servicio «Ibercaja Directo» (ordenador, móvil...), con los adecuados niveles de seguridad.

En este caso, posiblemente se ha producido una suplantación de identidad o «phishing», pero las operaciones se autorizaron al haber cumplido el doble factor de autenticación, sin detectarse incidencia alguna, y, por tanto, conforme a lo dispuesto en el art. 44 del RD-ley 19/2018. Acreditada dicha circunstancia (la doble autenticación), no corresponde a la entidad bancaria demandada 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.

En última instancia, en los contratos de banca digital y de cuenta corriente y/o depósitos se prevé expresamente (cláusula 8ª) que la demandada 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 Ibercaja Banco.

4.- La sentencia de instancia estima la demanda y condena a la demandada a abonar al actor la cantidad reclamada.

La sentencia repasa la legislación aplicable, con especial hincapié en los arts. 36 y 41 a 46 del Real Decreto Ley 19/2018, de 13 de noviembre, que establecen un régimen de responsabilidad cuasi objetiva del proveedor de los servicios de pago, y las Directrices de la Autoridad Bancaria Europea (EBA/GL/2017/09), que coinciden en la necesidad, por razones de seguridad, de sustituir el modo tradicional de acceder a los servicios on-line a través de unas credenciales basadas exclusivamente en usuario y contraseña, por un sistema de autenticación fuerte, basado en al menos dos factores, el segundo de los cuales puede ser un certificado digital, un dispositivo criptográfico que genera un número único, una línea de telefonía para recibir SMS o una app en un dispositivo móvil. En la entidad demandada se estaría produciendo el paso del sistema antiguo en que el segundo factor consistía en una tarjeta de coordenadas, al nuevo, mediante envío de un SMS, lo que se acomoda a la normativa vigente.

Expuesto el régimen aplicable, la sentencia analiza la actuación del demandante y de la demandada. Por lo que se refiere al primero, razona que, de acuerdo con los preceptos apuntados, el usuario solo responde cuando haya incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones, por lo que, al no existir ningún elemento del que se deduzca la existencia de un fraude o incumplimiento deliberado, la cuestión se reconduce a dilucidar si es posible hablar de negligencia grave, cuya prueba incumbe a la demandada y que la jurisprudencia comunitaria relaciona con el incumplimiento del deber de notificación del art. 58 de la Directiva 2007/64/CE. Después de examinar la prueba practicada, la sentencia descarta una conducta en el actor que se pudiera calificar como negligencia grave, antes al contrario, consta que un mes antes de los hechos ya advirtió expresamente y de forma inmediata de la recepción de los SMS con claves de confirmación de transferencias que él no había ordenado, lo que revela un obrar diligente, pues incluso en caso de haber sido víctima de phishing y proporcionado inconscientemente sus datos, hizo lo correcto, como es ponerse en contacto con Ibercaja Banco, que debía hacer reaccionado proporcionando un nuevo número de usuario, clave de acceso y firma electrónica -datos que ya obraban en poder de terceros-. Y lo mismo sucedió con la problemática planteada con la Tarjeta Visa, que sí fue reemplazada.

Por esta razón, aunque el sistema de banca electrónica de la demandada y la operativa del mismo se adecúa a la legislación aplicable, lo cierto es que, al no haberse acreditado negligencia grave del usuario, la entidad bancaria debe responder del reintegro de las cantidades dispuestas de forma fraudulenta, sin que corresponda a los clientes/usuarios prevenir ni averiguar las modalidades de riesgos que el sistema conlleva.

Conclusión que, según destaca la sentencia, se refuerza, teniendo en cuenta que, por un lado, en el último párrafo de la cláusula 3ª del contrato «Ibercaja Directo», se prevé que, por seguridad, el banco podrá solicitar del titular la confirmación por escrito de determinadas operaciones cuando existieren dudas sobre la identidad del ordenante, como aquí ocurrió, ya que las operaciones que dan lugar a la reclamación, por sus características, deberían haber sido detectadas por los sistemas técnicos de Ibercaja Banco; y, por otro lado, esta detección no solo no se produjo de manera tempestiva, sino que la alerta provino de una fuente externa, a saber, una llamada del Banco Santander que avisó de la recepción de una transferencia en una cuenta sospechosa de la entidad.

5.- La entidad Ibercaja Banco S.A. presentó recurso de apelación, que fue desestimado por la Audiencia Provincial.

En síntesis, la Audiencia declara probado que las transferencias fueron realizadas por delincuentes, que duplicaron la tarjeta SIM de la esposa del perjudicado, accediendo a la información confidencial almacenada en ella y tomando el control de su banca digital, en lo que se conoce como una modalidad de estafa denominada «SIM swapping».

Con esta base fáctica, la sentencia recuerda que la Ley de Servicios de Pago establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora de los servicios de pago, conforme al cual, tratándose de operaciones no autorizadas, salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante, la responsabilidad será del proveedor del servicio de pago, lo que implica que recae sobre él la carga de probar que la orden de pago «no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado», expresión esta última que implica que el banco debe actuar con la diligencia exigible en atención a las circunstancias de las personas y operaciones realizadas.

Al no haber acreditado la entidad recurrente qué negligencia pudo cometer el demandante que permitiera que unos delincuentes le duplicaran la tarjeta SIM -sin que el mero hecho del robo o sustracción de las claves suponga negligencia del usuario ni las advertencias genéricas o avisos estereotipados que puedan hacer los bancos sirvan para imputar tal negligencia-, la Audiencia concluye que debe responder, máxime atendidas las deficiencias observadas en el servicio prestado, como son que un hecho tan inusual como la ejecución de quince transferencias en una noche, por importe superior a 80.000 €, no hiciera saltar las alarmas en ese mismo momento y no al día siguiente y ni siquiera por iniciativa propia, o que, a pesar de las advertencias del actor en fechas inmediatamente anteriores de que había recibido varios SMS de transferencias no solicitadas y de los alertas de seguridad comunicadas por Google, la demandada no extremara las precauciones.

Finalmente, la sentencia descarta tanto el supuesto incumplimiento por parte del cliente de las cláusulas 1ª, 4ª y 5ª del contrato al realizar la operación, ya que no fue el demandante quien la efectuó, sino unos delincuentes que duplicaron la tarjeta SIM, como la aplicación de la cláusula 8ª, de exoneración, al entender que, como señala la sentencia de instancia, dicha cláusula «no puede entenderse válida en tanto en cuanto vaya contra el régimen normativo imperativo derivado de los preceptos antes reseñados».

6.- La entidad demandada Ibercaja Banco S.A. formula recurso de casación contra la expresada sentencia, que fundamenta en dos motivos que seguidamente se analizarán.

SEGUNDO.- *Primer motivo de recurso de casación.*

1.- *Formulación del motivo*. La recurrente denuncia que la sentencia de apelación infringe el art. 36 del Real Decreto Ley 19/2018, de servicios de pago, en relación con los arts. 2 y 3 del Reglamento Delegado (UE) 2018/389 de la Comisión Europea, al presumir, por la sola declaración del actor, que las transferencias controvertidas deben ser consideradas operaciones no autorizadas, por haber sido realizadas por terceros que habrían utilizado las credenciales del usuario Sr. Martin -extremo no acreditado-, cuando lo cierto es que habían sido correctamente autorizadas y registradas en los sistemas informáticos de la entidad, en cumplimiento y conforme a las condiciones contractuales pactadas con el actor en sendos contratos de cuenta y de servicio «Ibercaja Directo».

En el desarrollo del motivo alega que, con arreglo al citado art. 36, las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución, debiendo el ordenante y el proveedor de servicios acordar la forma en que se dará el consentimiento, así como el procedimiento de notificación del mismo. Según la condición 4ª del contrato celebrado entre las partes, «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». Así, con la introducción de todos los datos de forma correcta, debe entenderse dado el consentimiento para la operación.

La forma de otorgar el consentimiento era conocida y aceptada por ambas partes, admitiendo el actor que se diera validez a las operaciones si se utilizaban las claves que le habían sido facilitadas por la entidad. Con tal consentimiento quedó validada y autorizada la operación reclamada. La demandada efectuó las comprobaciones oportunas sobre las credenciales del actor, para validar las operaciones, habiendo quedado acreditado, además de la identificación del usuario, la doble autenticación, en cumplimiento de las normas técnicas de seguridad reforzada impuesta por la normativa comunitaria y nacional.

En el presente caso -insiste la recurrente-, en todas transferencias se llevó a cabo la identificación correcta del usuario con un doble factor de autenticación, que consistió (i) en que el titular accede al sistema digital con su clave de usuario y contraseña o clave de firma, y (ii)se envía mediante SMS, de forma exclusiva y con validez temporal «por unos momentos», un código para confirmar la operación, al teléfono móvil que el titular ha facilitado en la oficina para operar a través de la banca on line. Si tales credenciales eran conocidas por terceros y las emplearon para, a través del móvil del actor, ejecutar las operaciones en la banca digital, no cabe imputar responsabilidad alguna a la demandada.

Por último, los sistemas de detección se basan en anomalías; si se introduce usuario y contraseñas correctas, el sistema no da error. Las operaciones efectuadas, inicialmente, no suponen evidencias o indicios de simulación o fraude, ya que se realizaron de forma correcta por el usuario correspondiente al actor, identificándose debidamente con las claves y contraseñas que la entidad le había facilitado en la contratación de los distintos servicios de banca electrónica.

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

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.

Con carácter previo, es preciso significar que la Audiencia ha declarado probado que las operaciones de pago se ejecutaron por terceras personas, ajenas y sin el consentimiento del demandante, lo que comporta rechazar de plano las dudas sugeridas por la recurrente.

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.

Sin embargo, lejos de haber acreditado tales extremos, la prueba practicada evidencia lo contrario.

La secuencia fáctica permite observar que (i) tres semanas antes, el demandante informó a la entidad de la recepción en su dispositivo móvil de diversos mensajes SMS en los que se indicaban otros tantos códigos para validar transferencias desde su cuenta y que él no había solicitado; (ii) en fechas 27 de febrero y 2 y 12 de marzo de 2021, Google Play y Google Ads realizaron varios cargos no autorizados en la cuenta titularidad de D. Martin y su esposa en Ibercaja Banco S.A., utilizando su tarjeta VISA, lo que el demandante comunicó a la entidad bancaria; (iii) el 16 de marzo, D.ª Estefanía recibió un email de Google en la que se alertaba de que «Alguien acaba de usar tu contraseña para intentar iniciar sesión en tu cuenta», por lo que procedió a cambiar la contraseña, y, al día siguiente, 17 de marzo, el actor acudió a la oficina bancaria, donde informó sobre lo sucedido y solicitó la cancelación de la tarjeta y la emisión de otra nueva; y (iv) en la noche del 17 al 18 de marzo de 2021, se realizaron quince transferencias bancarias desde la cuenta corriente titularidad de D. Martin y sus padres, de las cuales diez lo fueron a través de la plataforma Bizum (por importe de 500 € cada una) y cinco a través de la plataforma de banca electrónica «Ibercaja Directo» (por importes de 28.970 €, 19.870 €, 9.876 € y dos de 9.870 € cada una).

Estos precedentes ponían de manifiesto, para cualquier observador medio, razonablemente atento y perspicaz, y más aún, para un empleado de banca, que alguien había conseguido acceder a las cuentas del actor, y, por ende, que disponía de sus claves de usuario y contraseña, lo que hubiera debido motivar una reacción inmediata, que pasaba cuando menos por la modificación de las claves y/o códigos. Nada se hizo. Al no adoptarse medida de protección alguna, tan solo restaba que los autores encontraran la manera de eludir el último obstáculo, esto es, la vía para recibir directamente el código de confirmación de la operación.

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.

Llegado este punto, nos encontramos, de un lado, ante una conducta diligente del titular de la cuenta, que informó, inmediata y reiteradamente, al personal de entidad de lo que estaba sucediendo, cumpliendo la obligación que expresamente le imponía la normativa comunitaria y nacional; y, de otro lado, ante un servicio que se presta defectuosamente por el proveedor, tanto por no tomar en consideración la información recibida pese a su gravedad, como por omitir la adopción de medidas que posibilitaran la detección de eventuales maniobras fraudulentas.

Por consiguiente, no se aprecia infracción del art. 36.1 del Real Decreto Ley 19/2018, lo que comporta la desestimación del motivo.

TERCERO.- *Segundo motivo de recurso.*

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.

CUARTO.- *Costas procesales y depósito*.

1.- La desestimación del recurso de casación implica que deban imponerse a la recurrente las costas procesales por él causadas (art. 398.2 LEC), así como la pérdida del depósito constituido (disposición adicional 15.ª, apartados 8 y 9, LOPJ).

FALLO

Por todo lo expuesto, en nombre del Rey y por la autoridad que le confiere la Constitución, esta sala ha decidido

1.º- Desestimar el recurso de casación interpuesto por Ibercaja Banco S.A., representada por el procurador D. Jorge Luis Guerrero Ferrández, bajo la dirección letrada de D.ª María Jesús Gracia Ballarín, contra la sentencia n.º 996/2022, de 17 de noviembre, dictada por la Sección 5.ª de la Audiencia Provincial de Zaragoza en el recurso de apelación n.º 20/2022, que confirmamos.

2.º- Imponer a Ibercaja Banco S.A. las costas del recurso de casación.

3.º- Ordenar la pérdida del depósito constituido para interponer el recurso de casación.

Líbrese al mencionado tribunal la certificación correspondiente, con devolución de los autos y del rollo de Sala.

Notifíquese esta resolución a las partes e insértese en la colección legislativa.

Así se acuerda y firma.