Roj: **SAP PO 3078/2021** - **ECLI:ES:APPO:2021:3078**

Id Cendoj: **36057370062021100542**
Órgano: **Audiencia Provincial**
Sede: **Vigo**
Sección: **6**
Fecha: **21/12/2021**
Nº de Recurso: **346/2021**
Nº de Resolución: **539/2021**
Procedimiento: **Recurso de apelación**
Ponente: **JOSE FERRER GONZALEZ**
Tipo de Resolución: **Sentencia**

FONDO DOCUMENTAL CE

AUD.PROVINCIAL SECCION N. 6

PONTEVEDRA

SENTENCIA: 00539/2021

Modelo: N30090

C/LALÍN, NÚM. 4 - PRIMERA PLANTA - VIGO

Teléfono: 986817388-986817389 **Fax:** 986817387

Equipo/usuario: MB

N.I.G. 36057 42 1 2020 0009070

ROLLO: RPL RECURSO DE APELACION (LECN) 0000346 /2021

Juzgado de procedencia: XDO. PRIMEIRA INSTANCIA N. 2 de VIGO

Procedimiento de origen: JVB JUICIO VERBAL 0000714 /2020

Recurrente: Sabina

Procurador: MARIA JOSE TORO RODRIGUEZ

Abogado: OLALLA CARBALLO FIDALGO

Recurrido: ABANCA CORPORACION BANCARIA SA

Procurador: JOSE RAMON CURBERA FERNANDEZ

Abogado: FERNANDO BUA GIL

LA SECCIÓN SEXTA DE LA AUDIENCIA PROVINCIAL DE PONTEVEDRA, SEDE VIGO, constituida en Tribunal unipersonal por el Ilmo. MAGISTRADO Sr. **D. JOSE FERRER GONZALEZ**, ha pronunciado la siguiente

S E N T E N C I A Nº 539/2021

En VIGO, a veintiuno de diciembre de dos mil veintiuno.

VISTO en grado de apelación ante esta Sección 006, de la Audiencia Provincial de PONTEVEDRA, los Autos de JUICIO VERBAL 0000714/2020, procedentes del XDO. PRIMEIRA INSTANCIA N. 2 de VIGO, a los que ha correspondido el Rollo RECURSO DE APELACION (LECN) 0000346/2021, en los que aparece como parte apelante, Sabina , representado por el Procurador de los tribunales, Sra. MARIA JOSE TORO RODRIGUEZ, asistido por el Abogado Dª. OLALLA CARBALLO FIDALGO, y como parte apelada, ABANCA CORPORACION BANCARIA SA, representado por el Procurador de los tribunales, Sr. JOSE RAMON CURBERA FERNANDEZ, asistido por el Abogado D. FERNANDO BUA GIL, siendo el Magistrado Ponente - constituido como órgano unipersonal el Ilmo. Sr. D. JOSÉ FERRER GONZÁLEZ.

ANTECEDENTES DE HECHO

PRIMERO. El litigio en primera instancia.

1. La representación procesal de doña Sabina interpuso demanda frente a Abanca Corporación Bancaria S.A en la que terminó por solicitar que fuera condenada a abonarle 4.365,30 euros.

2. La demanda fue turnada al Juzgado de Primera Instancia número 2 de Vigo que incoó el Juicio 714/2020.

3. La representación procesal de Abanca Corporación Bancaria S.A solicitó la desestimación de la demanda.

4. La Magistrada Juez titular del Juzgado dictó sentencia de fecha 8 de febrero de 2021 desestimatoria de la demanda.

SEGUNDO. Trámite en segunda instancia.

5. La representación procesal de doña Sabina recurrió en apelación solicitando que se revocara la sentencia y se estimara su demanda.

6. La representación procesal de Abanca Corporación Bancaria S.A se opuso a la estimación del recurso.

FUNDAMENTOS DE DERECHO

PRIMERO. Controversia.

7. La señora Sabina solicitó la condena de Abanca Corporación bancaria, S.A., a reintegrarle la cantidad de 4365,30 euros como saldo de la cuenta asociada a la tarjeta de débito que tenía contratada con la entidad del que se habría dispuesto sin su consentimiento mediante el uso fraudulento de los datos del instrumento de pago en veinte operaciones realizadas los días 16 y 17 de mayo de 2020.

8. Abanca reconoció que la demandante había sufrido un fraude informático mediante la técnica del *phishing,* y alegó, en esencia, que la demandante habría de soportar las pérdidas pues *actuó con grave negligencia al recibir el correo fraudulento de phishing, lo que propició que el defraudador pudiera instalar su tarjeta en la aplicación Samsung Pay del terminal del defraudador y que éste pudiera una vez instalada realizar pagos con la tarjeta por importe de 4365,30 euros.*

9. En la sentencia dictada en primera instancia se desestimó la demanda al apreciarse, en resumen, que *queda acreditada la actuación negligente de la parte actora, debiendo el ordenante soportar todas las pérdidas derivadas de operaciones de pago no autorizadas de conformidad con el inciso final del artículo 46 del Real decreto ley 19/2018 de 23 de noviembre .*

10. El recurso de apelación de la demandante se articula en dos motivos. En el primero, invocando *error en la valoración de la prueba*, alega la *inexistencia negligencia grave en la conducta de la señora Sabina .* En el segundo, con carácter subsidiario, estima que no debió realizarse condena en costas al concurrir *serías y razonables dudas de hecho*.

1 1. La entidad bancaria demandada se opone al recurso de apelación reiterando que *la demandante actuó con grave negligencia y que, por lo tanto, no puede reclamar responsabilidad de Abanca con motivo del fraude informático sufrido.*

SEGUNDO. Marco normativo.

Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior

Considerando:

(72) A la hora de evaluar la posible negligencia o la negligencia grave del usuario de servicios de pago, deben tomarse en consideración todas las circunstancias. Las pruebas de una presunta negligencia, y el grado de esta, deben evaluarse con arreglo a la normativa nacional. No obstante, si el concepto de negligencia supone un incumplimiento del deber de diligencia, la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros. 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

FONDO DOCUMENTAL CENDOJ

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.

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 . En vigor desde el 14 de septiembre de 2019 (artículo 38)

Artículo 1 Objeto

El presente Reglamento establece los requisitos que deben cumplir los proveedores de servicios de pago a efectos de la aplicación de medidas de seguridad que les permitan hacer lo siguiente:

a) aplicar el procedimiento de autenticación reforzada de clientes, de conformidad con el artículo 97 de la Directiva (UE) 2015/2366 ;

b) eximir de la aplicación de los requisitos de seguridad de la autenticación reforzada de clientes, bajo determinadas condiciones limitadas y basadas en el nivel de riesgo, el importe de la operación de pago y la frecuencia con que se repite, y el canal de pago empleado para la ejecución de dicha operación;

c) proteger la confidencialidad y la integridad de las credenciales de seguridad personalizadas del usuario de servicios de pago;

d) establecer estándares abiertos comunes y seguros para la comunicación entre los proveedores de servicios de pago gestores de cuenta, los proveedores de servicios de iniciación de pagos, los proveedores de servicios de información sobre cuentas, los ordenantes, los beneficiarios y otros proveedores de servicios de pago en relación con la provisión y la utilización de servicios de pago en aplicación del título IV de la Directiva (UE) 2015/2366.

Artículo 2 Requisitos generales de autenticación.

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) 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.

Artículo 3 Revisión de las medidas de seguridad

1.La aplicación de las medidas de seguridad a que se refiere el artículo 1 deberá documentarse, probarse periódicamente, evaluarse y auditarse de conformidad con el marco jurídico aplicable al proveedor de servicios de pago por auditores con experiencia en el ámbito de la seguridad y los pagos informáticos y funcionalmente independientes, ya pertenezcan al organigrama del propio proveedor de servicios de pago o sean externos a él.

.....

12. El RDL 19/2018 derogó la ley 16/2009 de 13 de noviembre de servicios de pago (disposición derogatoria única) y dispuso, en cuanto al régimen transitorio, que los contratos de servicios de pago suscritos con anterioridad a su entrada en vigor seguirían siendo válidos pero en todo caso habría de aplicarse las disposiciones de carácter imperativo que resulte más favorables para los consumidores y microempresas (Disposición Transitoria quinta). La Disposición Final 13ª estableció un régimen de entrada en vigor de la norma de manera escalonada que, partiendo de la general vigencia desde el día 25 de noviembre de 2018 (el siguiente a la fecha de publicación de la norma en el BOE, DF 13ª.1) culminó el 14 de septiembre de 2019 (18 meses desde la entrada en vigor del Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017, DF 131ª2.b) fecha desde la que habrían de aplicarse los artículos 37, 38, 39 y 68.

13. De las normas que en la legislación vigente regulan las obligaciones del proveedor y del usuario de los servicios de pago y el régimen de responsabilidad importa a efectos de este proceso considerar:

Artículo 41Obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas

El usuario de servicios de pago habilitado para utilizar un instrumento de pago:

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

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.

.....

Artículo 42. Obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago.

1. El proveedor de servicios de pago emisor de un instrumento de pago:

a) Se cerciorará de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento, sin perjuicio de las obligaciones que incumben al usuario de servicios de pago con arreglo al artículo 41.

b) Se abstendrá de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso de que deba sustituirse un instrumento de pago ya entregado al usuario de servicios de pago.

Esta sustitución podrá venir motivada por la incorporación al instrumento de pago de nuevas funcionalidades, no expresamente solicitadas por el usuario, siempre que en el contrato marco se hubiera previsto tal posibilidad y la sustitución se realice con carácter gratuito para el cliente.

c) Garantizará que en todo momento estén disponibles medios adecuados y gratuitos que permitan al usuario de servicios de pago efectuar una notificación en virtud del artículo 41.b), o solicitar un desbloqueo con arreglo a lo dispuesto en el artículo 40.4. A este respecto, el proveedor de servicios de pago facilitará, también gratuitamente, al usuario de dichos servicios, cuando éste se lo requiera, medios tales que le permitan demostrar que ha efectuado dicha comunicación, durante los 18 meses siguientes a la misma.

d) Ofrecerá al usuario de servicios de pago la posibilidad de efectuar una notificación en virtud del artículo 41.b), gratuitamente y cobrar, si acaso, únicamente los costes de sustitución directamente imputables al instrumento de pago.

e) Impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación en virtud del artículo 41.b).

2. El proveedor de servicios de pago soportará los riesgos derivados del envío de un instrumento de pago al usuario de servicios de pago o del envío de cualesquiera elementos de seguridad personalizados del mismo.

Artículo 44. Prueba de la autenticación y ejecución de las operaciones de pago.

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

Si el usuario de servicios de pago inicia la operación de pago a través de un proveedor de servicios de iniciación de pagos, corresponderá a éste demostrar que, dentro de su ámbito de competencia, la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable.

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

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

Artículo 45 Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas

FONDO DOCUMENTAL CENDOJ

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.

.....

Artículo 46Responsabilidad del ordenante en caso de operaciones de pago no autorizadas

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

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

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

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

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

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

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

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

.....

Artículo 64. Ausencia de responsabilidad cuando concurran circunstancias excepcionales e imprevisibles.

La responsabilidad establecida con arreglo a los Capítulos II y III de este Título no se aplicará en caso de circunstancias excepcionales e imprevisibles fuera del control de la parte que invoca acogerse a estas circunstancias, cuyas consecuencias hubieran sido inevitables a pesar de todos los esfuerzos en sentido contrario, o en caso de que a un proveedor de servicios de pago se le apliquen otras obligaciones legales.

Artículo 68. Autenticación.

1. Los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes, en la forma, con el contenido y con las excepciones previstas en la correspondiente norma técnica aprobada por la Comisión Europea, cuando el ordenante:

a) acceda a su cuenta de pago en línea;

b) inicie una operación de pago electrónico;

c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.

FONDO DOCUMENTAL CENDOJ

.....

6. No obstante, no será preciso aplicar la autenticación reforzada de clientes a la que se refiere el apartado 1 a los supuestos indicados en el artículo 98.1.b) de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 .

TERCERO. Responsabilidad por operaciones de pago fraudulentas.

14. El proveedor de servicios de pago se encuentra sujeto al cumplimiento de específicas obligaciones de protección en la emisión de los instrumentos de pago y en los procesos de autenticación de las operaciones de pago cuya finalidad es minimizar la probabilidad de ejecución de operaciones no autorizadas.

15. En relación con los instrumentos de pago ha de cumplir con las obligaciones sobre emisión y uso seguro que se establecen en el artículo 42.1 RDL 19/2018.

16. Los procesos o mecanismos de autenticación de las operaciones de pago deben cumplir con los requisitos que establece el Reglamento Delegado 2018/389 , lo que exige:

- a) Implementar las medidas de seguridad previstas en el artículo 1, que han de incluir el procedimiento de autenticación reforzada de clientes, con las salvedades específicamente señaladas.

- b)Incluir mecanismos de supervisión de las operaciones que permitan al proveedor de servicios de pago detectar operaciones de pago no autorizadas o fraudulentas. A tal efecto el proveedor de servicios de pago ha de tener en cuenta la totalidad de los factores de riesgo enumerados en el artículo 2, y, entre ellos, los *supuestos de fraude conocidos en la prestación de servicios de pago.*

- c) Auditar las medidas, en las condiciones del artículo 3.

17. El usuario de los servicios de pago deberá cumplir con las obligaciones que se establecen en el artículo 41 RDL 19/2010: a) Usar del instrumento de pago conforme a lo pactado y tomar las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas; b) En cuanto tenga conocimiento de haber perdido la posesión del instrumento de pago o de haber sido este utilizado sin su autorización, lo notificará sin demora indebida al proveedor de servicios de pago.

18. El régimen de la responsabilidad por las pérdidas derivadas de operaciones de pago por uso fraudulento de un instrumento de pago por un tercero se determina interpretando de manera integrada las previsiones del artículo 46 con la regulación general de las pérdidas por operaciones de pago no autorizadas del artículo 45 y con el régimen de la carga probatoria que se establece en el artículo 44 (todos del RDL 19/2018).

19. Será el proveedor de los servicios de pago quien habrá de responder de las pérdidas de importe superior a 50 euros por las operaciones de pago resultantes del uso fraudulento del instrumento de pago por un tercero; responderá de la totalidad de la pérdida cuando al ordenante no le hubiera sido posible detectar el posible uso fraudulento antes de que éste se hubiese materializado o cuando la pérdida se debiera a la acción u omisión de cualquier persona de la que el proveedor de servicios hubiera de responder.

20. El ordenante será quien soporte la totalidad de las pérdidas cuando concurran dos requisitos: a) La operación de pago fue autenticada y registrada con exactitud y no se vio afectada por ninguna deficiencia del servicio prestado por el proveedor de servicios de pago; b) El ordenante actuó de manera fraudulenta, o incumpliendo deliberadamente o por negligencia grave alguna de las obligaciones recogidas en el artículo 41 RDL 19/2018.

21. Al proveedor de servicios de pago le corresponde la carga procesal de acreditar tanto su propio comportamiento diligente en la autenticación de la operación de pago como el fraude o la negligencia grave del ordenante. La prueba de la diligencia en el procedimiento de autenticación deberá realizarse en relación a las exigencias del Reglamento Delegado 2018/389. La prueba del fraude del ordenante requerirá de la acreditación de hechos de los que pudiera llegar a inferirse que aquel actuó con engaño para beneficiarse de la operación de pago. La prueba de la negligencia grave del ordenante requerirá de la acreditación de las circunstancias concurrentes en la operación de pago de las que quepa inferir que la misma pudo realizarse porque aquel obró con una significativa falta de diligencia al usar del instrumento de pago o al proteger sus credenciales.

22. Cuando el proveedor de servicios de pago no acredite el cumplimiento de los deberes de diligencia propios en la autenticación habrá de responder de la pérdida resultante del uso fraudulento del instrumento de pago por un tercero salvo que concurra el fraude del ordenante.

CUARTO. Decisión.

23. No se discutía ya en la instancia que las operaciones de pago mediante las que se detrajeron de la cuenta bancaria que la señora Sabina tenía en la entidad Abanca la suma de 4365,30 euros respondieron a órdenes

de pago realizadas por un tercero que usó de manera fraudulenta de los datos de una tarjeta de débito de aquella. Los hechos relevantes que dieron lugar a los pagos fraudulentos son los siguientes:

- El 16 de mayo de 2020 la señora Sabina recibió un correo electrónico en el que figuraba simulado el emblema del Servicio Estatal Correos y Telégrafos, y en el que se le pedía que para confirmar la recepción de un pedido realizase un pago de 2,99 euros mediante un botón de enlace que, tras ser pulsado, le llevó a una página que simulaba ser de la entidad Abanca, pero que en realidad estaba bajo el dominio de un tercero, en la que se le solicitaba el número de tarjeta, la fecha de caducidad y la clave CVV2, datos que introdujo.

- Usando de los datos obtenidos el tercero instaló la tarjeta en la aplicación Samsung Pay de su propio teléfono móvil, y solicitó el alta a la entidad Abanca.

- Abanca remitió al teléfono móvil la señora Sabina cinco *sms* con el mismo contenido siguiente: *Atención! Usa el código NUM000 para instalar tu tarjeta acabada en NUM001 en Samsung Pay. Válido 30min. No lo compartas. Si tienes dudas llama al 981 910 522 (24h).*

- La señora Sabina introdujo la clave recibida en la página que simulaba ser de Abanca.

- Con la clave obtenida el tercero completó la instalación de la tarjeta en la aplicación Samsung de su terminal.

- Abanca remitió al teléfono móvil la señora Sabina , a las 19:16 horas del día 16 de mayo de 2020, un *sms* con el contenido siguiente: *Tu tarjeta acabada en NUM001 ha sido activada en Samsung Pay. Si no es correcto llámanos al 981 910 522 (24h).*

- Entre las 17:24:54 horas del día 16 y las 15:16:42 horas del día 17 de mayo de 2020 el tercero realizó, con cargo a la tarjeta de la señora Sabina y mediante la aplicación Samsung Pay, 20 órdenes de pago que tenían como beneficiarios a establecimientos de dos localidades de Francia, que supusieron que finalmente se detrajera de la cuenta bancaria de la primera la suma total de 4365,30 euros.

- La señora Sabina comunicó telefónicamente a Abanca, a las 23:35 horas, que había descubierto en su cuenta bancaria la retención de la cantidad de 4200 euros para pagos con su tarjeta de débito que ella no había efectuado, solicitando la baja del instrumento de pago y de la banca electrónica.

24. Se alega en el recurso que *la sentencia recurrida no sólo no razona, sino que ni siquiera sostiene que dicha negligencia sea grave tal y como exigen la ley y la jurisprudencia*. Y se añade, como segundo argumento, que *aunque se apreciase que concurrió negligencia en la conducta de la actora (cuestión que dejamos negada), en ningún caso puede sostenerse que esta pudiese calificarse como grave, único supuesto de que la entidad proveedora de servicios de pago quedaría exonerada de responsabilidad*, terminando por alegar que *es el banco quien ha cumplido órdenes de pago falsas, siendo él el responsable de comprobar la veracidad de la autorización de la ordenante.*

2 5. Para impugnar el recurso la entidad demandada estima que la demandante *actuó con grave negligencia*, pues *no debió pinchar el* link del *correo recibido, no debió facilitar los datos completos su tarjeta en la página falsa a la que le remitió el link, debió leer y comprobar los SMS que le envió Abanca durante la instalación de la tarjeta en la aplicación Samsung Pay del terminal del defraudador, no debió facilitar la clave para la finalización de la instalación de la tarjeta en la aplicación Samsung Pay.* Y añade que *Abancatiene una posición muy activa y un nivel muy alto de exigencia en la defensa de la seguridad informática sus clientes y en la persecución de posibles defraudadores informáticos que puedan utilizar su nombre.*

2 6. En la sentencia dictada en primera instancia se estima acreditada *la actuación negligente de la parte actora debiendo el ordenante soportar todas las pérdidas derivadas de las operaciones de pago*, pero no se llega a realizar la expresa valoración de la gravedad de la negligencia. Habrá de considerarse, por tanto, si con los elementos fácticos que se dicen considerados podría llegarse a entenderse correctamente realizada tal ponderación. Tales elementos son los siguientes: se consideró, en primer lugar, que *el correo electrónico supuestamente enviado por Correos en el que se le exigía el pago de 2,99 euros para entregar el paquete era impreciso,* pues *no se identifica el número de pedido y el nombre del remitente,* y además *no está bien redactado pues emplea palabras como "aquí" o "verificaciún" sin que ello fuese advertido por la parte actora;* en segundo lugar se dice que *cuando la señora Sabina pulsó en el recuadro este le redirigió a lo que ella identificó como la página de la entidad demandada e introdujo el número de tarjeta para el pago de 2,99 euros, a pesar de los correos de advertencia enviados por Abanca en diferentes ocasiones en los que recordaba que Abanca nunca solicitaba claves ni otra información relevante por correos electrónicos o enlaces* ; y en tercer lugar, se indica que *a pesar de los SMS que le envió Abanca durante la instalación de la tarjeta en la aplicación de Samsung Pay, y una vez instalada procediera a insertar el código para completar la operación sin leer ni comprobar lo expuesto en los SMS enviados* .

27. Determinar si la señora Sabina , al abrir el enlace del correo electrónico que le llevó a una página que no era la oficial de la entidad emisora de su tarjeta de débito en la que introdujo los datos de su instrumento de pago y el código de seguridad, incurrió en negligencia grave al usar de instrumento de pago o al cumplir su obligación adoptar las medidas razonables para proteger sus credenciales de seguridad personalizadas requiere considerar la totalidad de las circunstancias concurrentes y en particular la técnica de la que se valió el tercero defraudador para hacerse con las citadas credenciales; el *phishing*.

28. El *phishing* aparece configurado, en el caso, por dos elementos; a) Envío de un correo electrónico con la apariencia de ser remitido por una entidad con la que el receptor puede tener alguna relación de servicios; b) El correo contiene un enlace a una página que aparenta ser del sitio oficial de la entidad emisora de la tarjeta pero que en realidad pertenece a un dominio bajo el control del *phisher*.

29. El deber de diligencia de la demandada para asegurar la correcta autenticación de las operaciones de pago exigía de dotarse de mecanismos de supervisión que permitieran detectar operaciones de fraudulentas a cuyo efecto habría de considerar *los supuestos del fraude conocidos en la prestación de servicios de pago* (artículo 2 del Reglamento Delegado 2018/389). Es por ello que conocido que la técnica del *phishing* incluye, a menudo, la creación y puesta en la red de páginas que clonan las del sitio oficial de las entidades emisoras de instrumentos de pago, el deber de diligencia de la entidad demandada exigía dotarse de la tecnología *antiphishing* precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas, lo que, de producirse, impediría que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace del correo electrónico haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor.

30. A ese mecanismo *antiphishing* parece referirse la entidad demandada cuando en la impugnación del recurso, y antes en la contestación a la demanda, alegaba tener *una posición muy activa y un nivel muy alto de exigencia en la defensa de la seguridad informática de sus clientes;* pero resulta que no se acreditó por medio alguno su implementación en el sistema informático de las operaciones de pago al momento de los hechos objeto del proceso, limitándose la prueba aportada en relación a su actuación en la prevención del phishing a la remisión de correos a los usuarios de los instrumentos de pago que había emitido, entre ellos la demandante, en los que explicaba aquella técnica defraudatoria y realizaba recomendaciones y advertencias que el usuario habría de observar para evitar el conocimiento de las credenciales de su instrumento de pago por el defraudador, correos explicativos insuficientes para entender observada la diligencia propia pues supondría dejar únicamente al cuidado del usuario la evitación de un fraude que debía prevenirse con una conducta activa propia mediante el mecanismo tecnológico adecuado.

31. La señora Sabina al introducir los datos de su tarjeta de débito en la página que aparentaba ser de la entidad Abanca para abonar el precio de un servicio que aparentemente le habría de prestar la entidad Correos y Telégrafos estaba haciendo uso del instrumento de pago conforme a su propia finalidad, por lo que en relación a las obligaciones que le imponía el artículo 41 del RDL 19/2018 restaría por determinar si al haber accedido a la página que simulaba ser de la entidad bancaria emisora de la tarjeta desde un enlace de un correo electrónico *impreciso y con dos faltas de ortografía* y haber introducido en aquella no sólo los datos de su tarjeta sino también la clave de activación de una aplicación de pago que un tercero había instalado en un terminal propio habría de determinarse que incurrió en negligencia grave en el deber de protección de sus credenciales de seguridad personalizadas. La lectura atenta del correo electrónico le hubiera permitido a la señora Sabina percatarse tanto de su contenido impreciso, al no identificar el pedido al que se refería, como de las dos faltas de ortografía, datos relevantes para adoptar su decisión de aceptar o no el pago electrónico que se le solicitaba, por lo que en ausencia de tal lectura reflexiva habría de considerarse su falta de diligencia en la protección de las credenciales del instrumento de pago. Pero han de tenerse en cuenta las circunstancias en las que tal decisión se adoptó, previo el engaño premeditado de un tercero para ganarse su confianza, lo que, estimo, debe llevar a que no haya de apreciarse una negligencia grave en la omisión de la lectura atenta del correo electrónico. En el phising se usan técnicas de ingeniería social para ganarse la confianza del usuario del instrumento de pago y aprovecharse de los sesgos cognitivos en la toma de decisiones, lo que, en el caso se habría concretado en la simulación del envío a nombre de una entidad de confianza para la usuaria (Correos y Telégrafos), y en el aprovechamiento del sesgo de confirmación por el cual se tiende a favorecer la información que confirma las opiniones que ya se tenían o que resulta consistente con los hechos ya conocidos (la señora Sabina explicó que estando esperando un pedido de mascarillas creyó que a él se refería la entrega del paquete que se le anunciaba en el correo electrónico).

32. Los SMS que la entidad demandada envió a la señora Sabina comunicándole el código que había de utilizar para instalar su tarjeta en la aplicación de pago Samsung Pay, y el que le envío después de su activación no proporcionaban información sobre el número del terminal telefónico en el que se había solicitado y después activado la citada aplicación de pago. Tal omisión supone un incumplimiento de los deberes de diligencia en

la prevención del fraude mediante phising, pues no podía la entidad desconocer que frecuentemente mediante aquella el tercero defraudador utiliza los datos de la tarjeta para activarla en una aplicación de pago de la que tiene dominio, por lo que debiendo conocer que el teléfono desde el que se le había solicitado la activación no se encontraría entre los que hubiera registrado su nombre la señora Sabina en su ficha de cliente, la comunicación del número de terminal telefónico devenía exigible para que aquélla pudiera conocer que era un tercero quien podría disponer de los datos de la tarjeta mediante la aplicación de pago que se activaría. En tales circunstancias no cabe observar negligencia grave en el acto de la señora Sabina introduciendo la clave de activación de la obligación de pago en la página que simulaba ser de Abanca, pues para que pudiera ponderarse su error (explicó que había entendido que los mensajes se referían al pago que realizaba con su propio teléfono móvil que era de la marca Samsung) como inexcusable le faltaba el dato del número de teléfono en el que la aplicación se activaría, con el que podría haber conocido que el pago no se realizaría mediante el teléfono propio sino mediante el de un tercero.

33. De lo expuesto se concluye que la entidad demandada no habría acreditado la observancia de los deberes de diligencia que le eran exigibles en la autenticación de las operaciones de pago, pues ni habría probado haber implementado un mecanismo antiphising de protección de los usuarios de los instrumentos de pago por ella emitidos frente al uso fraudulento por un tercero de páginas imitativas de las propias para hacerse con las credenciales del instrumento, ni habría puesto en conocimiento del usuario los datos necesarios para que este conociera que se trataba de instalar su tarjeta en una aplicación de pago de un terminal de un tercero. Se concluye, también, que no cabría observar negligencia grave de la demandante de los deberes de conducta al usar del instrumento de pago y al introducir las credenciales de uso personal en una página que imitaba las del sitio oficial de la entidad emisora de su tarjeta. Habrá de ser, en consecuencia, la entidad demandada como proveedora de los servicios de pago usados de manera fraudulenta por un tercero logrando con ello acceder a la cuenta bancaria de la demandante quien haya de responder las pérdidas sufridas por esta con tales operaciones.

34. La responsabilidad se extenderá a la totalidad de la pérdida pues en momento alguno anterior a que se realizase la última de las operaciones fraudulentas de pago la entidad demandada había informado a la demandante del número del terminal telefónico desde el que se estaban realizando las órdenes de pago fraudulentas ni de circunstancia alguna (las localidades en las que se ubicaban los establecimientos en los que se realizaban los pagos, que la entidad proveedora de servicios debía analizar si se correspondían con los patrones habituales de las operaciones de la usuaria de la tarjeta) que hubiera permitido conocer tal uso fraudulento, conocimiento que esta solo adquirió tras examinar los movimientos de su cuenta bancaria.

35. No solicitándose en la demanda intereses de naturaleza distinta, únicamente se aplicarán los procesales previstos en el artículo 576 de la Ley de Enjuiciamiento Civil.

QUINTO. Costas procesales y depósito para recurrir.

36. Al estimarse el recurso no se hará una especial imposición de las costas de la segunda instancia, en atención a lo dispuesto en el artículo 398 de la Ley de Enjuiciamiento Civil. Y habrá de devolverse el depósito en su día realizado para recurrir (Disposición Adicional 15 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial).

37. La estimación de la demanda supone que, en aplicación del criterio vencimiento objetivo, las costas de la primera instancia habrán de ser impuestas a la parte demandada (artículo 394 de la Ley de Enjuiciamiento Civil).

Por lo expuesto, y haciendo uso de la potestad de juzgar que confiere el artículo 117 de la Constitución Española.

FALLO

1. Estimar el recurso de apelación interpuesto por la representación procesal de Dª. Sabina frente a la sentencia de 8 de febrero de 2021 , que se revoca.

2. Estimar la demanda interpuesta por la representación procesal de Dª. Sabina frente a Abanca Corporación Bancaria S.A, condenando a la demandada a abonar a la demandante la cantidad de 4365,30 euros, con los intereses por mora procesal del artículo 576 LEC , y al pago de las costas procesales de la primera instancia.

3. No hacer especial imposición de las costas de la segunda instancia.

MODO DE IMPUGNACIÓN: Contra esta resolución no cabe recurso alguno.

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

FONDO DOCUMENTAL CENDOJ