BASE DE DATOS DE Norma CEF.-
Referencia: NCJ067668

JUZGADO DE PRIMERA INSTANCIA Nº 7 DE LAS PALMAS DE GRAN CANARIA
Sentencia 08/2024, de 16 de octubre de 2024

Rec. n.º 1919/2023

SUMARIO:

Responsabilidad patrimonial bancaria. Contratos bancarios. Prestación del servicio de pago. Credenciales de seguridad. Obligaciones contractuales. Phishing. Suplantación en la identidad. Una clienta de la entidad bancaria movió todo su dinero a la cuenta de unos delincuentes tras ser engañada mediante mensajes al móvil que la llevaban a una réplica exacta de la web del banco.

Estimada la demanda de una vecina de la capital grancanaria que perdió todo su dinero al ser víctima de unos ciberdelincuentes que se hicieron pasar por la entidad bancaria en la que tenía su cuenta, y ha condenado al banco a abonar a la afectada la suma que le fue sustraída mediante phishing (4.902 euros) más los intereses legales devengados.

La entidad bancaria se oponía a la reclamación de la clienta, alegando que sólo ella era responsable de haber caído en la trampa. La autoridad judicial establece que existe responsabilidad patrimonial por parte del banco, ya que, expone, «siendo la demandada la que prestar el servicio de pago en un entorno tan tecnológico y susceptible cada vez más de ataques como el que ha sido objeto la actora, implica la responsabilidad patrimonial, dado que es el mismo el que debe de aumentar las medidas de seguridad específicas, y no meramente informativas, a la altura de los medios de pago que ofrece. Corresponde al proveedor del servicio acreditar que la operación fue autenticada, registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable. Asi como probar que el usuario del servicio de pago cometió fraude o negligencia grave. La demandada tan solo ha aportado la documentación referida a la forma de procesamiento de las transacciones. De los que no se puede concluir que la actuación en el caso de la actora infringiera gravemente sus obligaciones en cuanto a la salvaguarda y protección de los datos de seguridad personales sobre todo a la vista de la forma en la que se produjo las transferencias y en escenario de phishing previo.»

No puede pretenderse que la actora «desplegara una actitud sospechosa o inquisitiva en cuanto al mensaje remitido», que entendió legítimo «toda vez que incluso recibió llamadas de quien decía ser empleado de la demandada, que explicaban el motivo de los SMS remitidos (…) dentro de la línea de conversación que mantenía» con su banco. «No existen datos que supongan acreditar la existencia de una actuación imprudente por parte de la actora», teniendo en cuenta que se usó un sistema tecnológico complejo constando una serie de ataques mediante SMS a la confianza de la actora en quien creía ser la entidad financiera, remitiendo un enlace que le lleva a una página web de contenido idéntico, dando lugar de forma inmediata por parte de la clienta a denunciar los hechos y ponerlo en conocimiento de la entidad financiera tan pronto como fue consciente del resultado de las transferencias . La sentencia es susceptible de recurso de apelación ante la Audiencia Provincial de Las Palmas.

PRECEPTOS:

RD Ley 19/2018 (servicios de pago), arts. 41, 42, 43, 44.1, 45 y 46.1.

PONENTE:

D. José Ramón García Aragón,

JUZGADO DE PRIMERA INSTANCIA Nº 7

C/ Málaga nº2 (Torre 2 - Planta 3ª) Las Palmas de Gran Canaria Teléfono: 928 11 63 07

Fax.: 928 42 97 19

Email.: instancia7lpgc@justiciaencanarias.org

Procedimiento: Juicio verbal (250.2) Nº Procedimiento: 0001919/2023 NIG: 3501642120230035381

Materia: Sin especi?car

Resolución: Sentencia 000508/2024 IUP: LR2023191911

SENTENCIA

En Las Palmas de Gran Canaria a 16 de octubre de 2024 el Magistrado-Juez del Juzgado de Primera Instancia nº 7 de esta ciudad, D. José Ramón García Aragón, en los autos seguidos en este tribunal de Juicio Verbal 1919/2023 interpuesto por el Procurador D. Tomas Ramirez Hernandez en nombre y representación de D. ª Lidia contra la entidad Banco BBVA SA representado por el Procurador D. Francisco Ojeda Rodriguez en el que obran los siguientes:

ANTECEDENTES DE HECHO.

Primero.

Se interpuso demanda que por turno de reparto correspondió a esta Juzgado. En ella se interponía demanda contra la entidad demandada solicitando la condena del demandado en la forma solicita en el suplico de la demanda.

Admitida la demanda mediante Decreto de fecha 19 de enero de 2024 se procede por la demandada a contestar a la misma . Citando a las partes al acto de la vista que se celebró el 15 de octubre de 2024 con el resultado que consta en los autos

Segundo.

Que en la tramitación del presente procedimiento se han observado los preceptos legales.

FUNDAMENTOS DE DERECHO.

Primero.

La actora interesa la condena de la demanda a la cantidad de 4902€ € con base en los diversos cargos y disposiciones que se efectuaron por la actora en la cuenta que tenía abierta en la entidad demandada por vulneración del RD Ley 19/2018 y de forma subsidiaria se condene a la demandada por incumplimiento de los niveles de garantía y seguridad adecuados en la prestación del servicio debiendo restituir la demandada la cantidad de 4902 € .

La demandada niega toda responsabilidad en cuanto al cargo que se le reclama por la actora toda vez que dado las circunstancias del mismo y los mecanismos de veri?cación y autenticación que se llevaron a cabo actuó con toda la diligencia que le es exigible aportando datos en cuanto a campañas de concienciación frente a los fraudes telemáticos que pueden producirse .Atribuyendo a la actora la responsabilidad por haber dado a conocer a terceros datos y claves de seguridad .

Segundo.

La normativa aplicable al caso de autos se cifra en los artss 41 y ss del Real Decreto Ley 19/2018 de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia ?nanciera que se reproduce a los efectos de clari?car el supuesto de autos .

En el articulo 41 se regulan las obligaciones 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 ?n 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 noti?cará al proveedor de servicios de pago o a la entidad que este designe, sin demora indebida en cuanto tenga conocimiento de ello.

Por su parte en cuanto al articulo 42 referido a las 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

En cuanto a la prueba el artículo 44. 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 de?ciencia 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 de?ciencias 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.4. El proveedor de servicios de pago conservará la documentación y los registros que le permitan acreditar el cumplimiento de las obligaciones establecidas en este Título y sus disposiciones de desarrollo y las facilitará al usuario en el caso de que así le sea solicitado, durante, al menos, seis años. No obstante, el proveedor de servicios de pago conservará la documentación relativa al nacimiento, modi?cación y extinción de la relación jurídica que le une con cada usuario de servicios de pago al menos durante el periodo en que, a tenor de las normas sobre prescripción puedan resultarles conveniente para promover el ejercicio de sus derechos contractuales o sea posible que les llegue a ser exigido el cumplimiento de sus obligaciones contractuales.Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la ?nanciación del terrorismo, así como en otras disposiciones nacionales o de la Unión Europea aplicables.

Y en cuanto a la responsabilidad el artículo 45. 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 ?nal del día hábil siguiente a aquel en el que haya observado o se le haya noti?cado 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.

Si el responsable de la operación de pago no autorizada es el proveedor de servicios de iniciación de pagos, deberá resarcir de inmediato al proveedor de servicios de pago gestor de cuenta, a petición de este, por las pérdidas sufridas o las sumas abonadas para efectuar la devolución al ordenante, incluido el importe de la operación de pago no autorizada. De conformidad con el artículo 44.1, corresponderá al proveedor de servicios de iniciación de pagos 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 de?ciencias vinculadas al servicio de pago del que es responsable.

Si bien la responsabilidad del ordenante se regula en el articulo 46 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 noti?cado 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 bene?ciario o el proveedor de servicios de pago del bene?ciario no acepten la autenticación reforzada del cliente, deberán reembolsar el importe del perjuicio ?nanciero 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 noti?cación a que se re?ere el artículo 41.b), de un instrumento de pago extraviado o sustraído.

1. Si el proveedor de servicios de pago no tiene disponibles medios adecuados para que pueda noti?carse 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.

Tercero.

Con este escenario normativo se somete a la consideración del Tribunal las operaciones llevada a cabo por la propia actora como fueron sendas transferencias de fecha 1 de junio de 2023 por valor de 1152€ y 3750€ desde la cuenta legítima de la misma con la entidad demandada a una cuenta que se fue suministrada en el curso de un engaño o ardid en la que la actora trans?rió todos los fondos de que disponía . Operativa que se llevó a cabo mediante la remisión por el canal habitual de comunicación con la demandada de SMS en el que se le informaba de una alerta de seguridad en su tarjeta . Formando parte este SMS del hilo de mensajes de la entidad ?nanciera . Remitiendo para su subsanación a un link . Link que fue accionado por la demandante desde su teléfono movil . Lo que le llevó a una web con todos los rasgos identi?cadores de la web del banco . En ella la actora insertó clave y contraseña para acceder no lográndolo.

De esta forma al día siguiente recibe una llamada telefónica de quien dijo ser empleado de la demandada con conocimiento de datos personales de la actora , nombre , apellido , ultimas operaciones … informándole que se habría producido una situación de grave riesgo de seguridad informática y que debía de transferir todos sus fondos a una nueva cuenta con un IBAN que se le remitió por el hilo de SMS de la entidad ?nanciera . Llevando a cabo la actora las dos operaciones que se indican en su demanda a una cuenta con el IBAN de la entidad demandada perdiendo toda disponibilidad sobre las referidas cantidades dando lugar a la denuncia de la actora ante el Cuerpo Nacional de Policía .

De tal forma que el juego de cargas , responsabilidades y obligaciones que cifra de un lado en que corresponde al proveedor del servicio acreditar que la operación fue autenticada , registrada con exactitud y no se vio afectada por un fallo técnico u otras de?ciencias vinculadas al servicio de pago del que es responsable. Asi como probar que el usuario del servicio de pago cometió fraude o negligencia grave. Siendo la contrapartida la responsabilidad del ordenante la actuación de forma fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41.

De esta forma la demandada entiende que a la vista de la documentación aportada a los autos y la declaración de la actora consta acreditado que efectivamente no se produjo ningún problemas en cuanto a la dimensión técnica de la operación . Relacionada con su registro y ejecución técnica.

Otro extremos es que la demandada entiende que la vista del sistema usado para llevar a cabo la operación se debe de deducir la existencia de una actuación negligente de la ordenante al haber incumplido gravemente sus obligaciones en cuanto a la conservación y sigilo de sus credenciales , numero secreto (PIN) y acceso a su teléfono móvil . No obstante ello se basó en la recepción de un SMS malicioso en el que se informaba de una limitación temporal de su tarjeta , que la derivó mediante a un enlace a una hacía una pagina web ?cticia con apariencia de verosimilitud a la de la entidad ?nanciera . En la que introdujo datos personales de la misma. Recibiendo mensajes y llamadas de quien decía ser empleados de la entidad ?nanciera a los facilitó datos personales . Ocasionando con toda seguridad el acceso a sus elementos biométricos y sistemas propios de veri?cación . Tal y como consta en el SMS remitido a la actora pero que la misma interpretó dentro del conglomerado de mensajes referidos y relacionados con la situación de limitación provisional de la tarjeta tal y como consta los pantallazos aportados con la demanda .

Esto nos lleva a la forma o mecanismos usado para la adquisición que dio lugar a la operación cuestionada. Del contenido de la documentación aportada a los autos consta que las dos transferencias se llevaron a cabo por la propia actora y que fue ella misma la que suministró todos los pasos , datos y claves en orden a llevar a cabo estas transferencias de la cuenta de la actora o otra cuenta maliciosa de la propia entidad demandada . Pero ello no puede desligarse del hecho de que tal cadena de sucesos ha sido motivada y puesta en marcha por la remisión en el hilo de mensajes SMS , en uno de los canales habitual de comunicación, de un mensajes que la actora entendió legítimo . Con?ando en la procedencia y con?ando en la esfera de con?anza que se desprende del referido medio de comunicación. No pudiendo pretenderse , y menos de forma revisionista , que la actora desplegara una actitud

sospechosa o inquisitiva en cuanto al mensaje remitido . A entender que las operaciones que la misma llevó a cabo y que superaron todas las operativas y mecanismos técnicos se ejecutaron por la actora con base en una serie de mensajes maliciosos que la misma entendía que procedían de la entidad ?nanciera . Y que entendió legítimo toda vez que incluso recibió llamadas de quien decían ser empleados de la demandada que explicaban el motivo de los SMS remitidos que procede dentro de la linea de conversación que mantenía con el BBVA .

Que en el curso de las referidas actuaciones se produjeron las operaciones fraudulentas puesto que estan basadas en la convicción errónea de la cliente de estar operando en el entono seguro de la entidad ?nanciera .

Con una alta dosis de credibilidad dado los medios empleados por los defraudadores . Dando lugar de forma inmediata por parte de la clienta a denunciar los hechos y ponerlo en conocimiento de la entidad ?nanciera tan pronto como fue consciente del resultado de las transferencias .

No constando , dado la forma en la que se habría aportado los medios de prueba por parte de la demandada en cuanto al supuesto informe , que el sistema de autenticación se llevara a cabo de una manera más precisos o compleja . Pero incluso admitiendo que el sistema usado fuera el biométrico , a la vista de la propia operativa que se habría desplegado por parte de los terceros maliciosos no resulta difícil entender que se habría podido superar los mismos de forma sencilla al haber tenido acceso con las claves de la actora a sus datos y elementos sensibles .

De tal forma que ya consta la existencia de un importante dé?cit probatoria por parte de la demandada en orden a la acreditación de la actuación negligente de la actora . En cuanto a que no se ha especi?cado en modo alguno cual es el standar de seguridad del que se debe de partir y que se habría dado lugar al fraude o negligencia grave por su parte en el cumplimiento de sus obligaciones de custodia del instrumento de pago y las credenciales de seguridad.

Por otro lado no consta ni explicado ni acreditado a que motivo obedecían la alertas recibida por la actora desde números relacionados con los de la entidad BBVA. O que ha sido de la identidad del IBAN de la cuenta de destino a las que se remitieron las transferencias .

Con estos elementos las trasferencias se llevaron a cabo por la suplantación de la demandada en cuanto a la web , SMS , llamadas telefónicas ...de tal forma que las mismas (transferencias) se produjeron en un entorno de con?anza de que estaba llevándolo a cabo en el entorno seguro de la entidad bancaria . Dado la procedencia de los SMS y las llamadas telefónicas . Asi como de la redireción a una web suplantadora de la de la entidad ?nanciera.

Pues bien desde esta perspectiva a la vista de la documentación bancaria y policial aportada no se puede suponer la existencia de una negligencia grave de la ordenante . Sino que la demandada debe de probar precisamente la existencia de tal imprudencia grave como es el eventual falta de diligencia en cuanto a la conservación y custodia de sus credenciales de seguridad . O en sentido estricto que la actora no ha desplegado las medidas razonables a ?n de proteger estos datos actuando de forma negligente habiendo actuado de forma inmediata al detectar el fraude tanto respecto de la entidad demandada como ante la FFCCSSEE .

La demandada tan solo ha aportado la documentación referida a la forma de procesamiento de las transacciones . De los que no se puede concluir que la actuación en el caso de la actora infringiera gravemente sus obligaciones en cuanto a la salvaguarda y protección de los datos de seguridad personales sobre todo a la vista de la forma en la que se produjo las transferencias y en escenario de phishing previo .

Teniendo en cuenta que se usó un sistema tecnológico complejo constando una serie de ataques mediante SMS a la con?anza de la actora en quien creía ser la entidad ?nanciera remitiendo un enlace que le lleva a una pagina web de contenido idéntico . Recibiendo llamadas de personal que decía ser de la entidad ?nanciera . Lo que que permite concluir que no existen datos que suponga acreditar la existencia de actuación imprudente por parte de la actora .

Constando serios indicios de que en el presente caso se han visto comprometidas elemento de ciberseguridad . De tal forma que este grado de complejidad y coordinación implican de un lado la eventual atenuación en cuanto a la diligencia exigida al ordenante al referirse a una actuación razonable . Y por otro lado que la demandada debía de desplegar mayor actividad probatoria en orden a poder veri?car los sistema de contacto con sus clientes mediante meros SMS . Sin que se puede imputar a la actora una carga diabólica en cuanto a la acreditación de los hechos para exonerarse de la responsabilidad .

Que la operación se hubiera realizado por la propia actora creyendo que estaba actuando en el marco de la entidad ?nanciera y por ende protegida permite veri?ca el alto grado de complejidad cibertecnológíca que se ha desplegado por los defraudadores . No constando que la actora tuviere conocimientos mas allá de los de la mera usuaria que le permitiera conocer o poder conocer el riesgo ante el que se encontraba . No quedando acreditado una actuación negligente de la actora o un incumplimiento de sus deberes . Exigiendo acreditación por parte de la demandada en orden a la obligación de la carga probatoria de que se ha producido una infracción grave de las medidas razonables de protección de sus credenciales cuando el ataque se ha producido mediante la suplantación de su propio entorno corporativo de la parte demandada .

Que en el caso que nos ocupa ante la falta de prueba de la gravedad en cuanto a la negligencia de la actora procediendo a estimar la demanda debiendo la demandada devolver la cantidad de 4.902 € , ex art 44 y 45 del RDL 19/2018. No siendo controvertida por la demandada en cuanto a su cuanti?cación .

Además la SAP, Civil sección 2 del 13 de marzo de 2024 (ROJ: SAP S 233/2024 Pues bien, resolviendo conjuntamente los motivos fáctico y jurídico de la apelación es oportuno señalar que son reiteradas las decisiones de las Audiencias Provinciales que atribuyen a las entidades prestadoras de servicios de pago, responsabilidad patrimonial cuasi objetiva por el riesgo que el propio sistema de pagos conlleva y de la que sólo puede exonerarse mediante la prueba de la culpa grave del ordenante, correspondiendo a la entidad acreditar que la operación ordenada fue auténtica y no estuvo afectada por un fallo técnico o por otra de?ciencia como pudiera ser un supuesto de phishing, tal y como establece el art. 44.1. del Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia ?nanciera ("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 de?ciencia del servicio prestado por el proveedor de servicios de pago").

En este sentido la SAP de Pontevedra de 23 de marzo de 2023 señala que "A la hora de estudiar la concurrencia de negligencia grave del usuario del servicio de pago online, partiendo del admitido criterio de responsabilidad cuasi objetiva de la entidad en la prestación del servicio de banda virtual respecto a operaciones de pago como la transferencia, reiterada jurisprudencia considera que dicha negligencia debe ser grave en atención a las circunstancias demostradas del caso, atribuyéndose en todo caso la carga probatoria de la misma al proveedor del servicio con arreglo a art. 217 LEC . En interpretación de directiva 2015/2366 , la negligencia que hace responder al cliente es la que se deriva de una conducta caracterizada por un grado signi?cativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que haya podido ser inducido por un delincuente profesional. Como parámetro del actuar negligente también cabrá acudir al art. 1.104 CC , que exige la diligencia asociada a la naturaleza de la obligación y a las circunstancias personales, de tiempo y lugar. Ello destacándose la complejidad y grado de perfección que presenta en la actualidad el método de " phishing" de difícil detección por persona de formación media, así como el deber de la proveedora del servicio de dotarse de tecnología su?ciente y adecuada con exigencia de medidas implantadoras activas, sin entenderse su?cientes avisos generales o en página web de mero carácter informativo o divulgativo - por todas, SS. AP Pontevedra (Secc. 6ª) 21.12.21 y Madrid (20ª) 20.5.2022 , en la línea de lo razonado en SS. AP Valencia (6ª) 13.6.2022 , Granada (5ª) 20.6.2022 y Badajoz (3ª)
21.6.2022 -".

La realidad de las prácticas delictivas como el mencionado phising, hace exigible aumentar las medidas de seguridad especí?cas, como ya señaló la SAP de Barcelona de 7 de marzo de 2013, ya que el banco no puede ofrecer un sistema on line sin adoptar las medidas de seguridad necesarias.

En el mismo sentido, cabe citar entre otras muchas, las SSAP de Valladolid de 23 de octubre de 2023, Huelva 16 de octubre de 2023, o Pontevedra de 18 de septiembre de 2023, o la de esta misma sección segunda de la Audiencia Provincial de Cantabria de 10 de octubre de 2023 (ROJ: SAP S 1267/2023), y todas las que en ellas se citan.

Como consecuencia de lo hasta aquí expuesto, ha de concluirse que la entidad demandada, como prestadora de servicios de pago, debe asumir la responsabilidad patrimonial que se le exige por el riesgo que el propio sistema de pagos conlleva, tal como se interesó por la actora.

Por lo que constando que parte de las actuaciones se debieron a una suplantación en la identidad de la entidad ?nanciera , unido a una suerte de responsabilidad cuasi-objetiva , siendo la demandada la que presta el servicio de pago en un entorno tan tecnológico y susceptibles , cada vez mas de ataques , como el que ha sido objeto la actora , implica la responsabilidad patrimonial dado que es el mismo el que debe de aumentar las medidas de seguridad especí?cas, y no meramente informativas, a la altura de los medios de pago que ofrece .

Cuarto.

Con relación a los intereses, se devengarán los intereses de demora calculados al tipo del interés legal y desde la fecha de interposición de la demanda iniciadora del presente procedimiento, conforme a lo establecidos en los artículos 1100, 1101 y 1108 del Código Civil.

Quinto.

Conforme al artículo 394.1 de la Ley de Enjuiciamiento Civil , que expresa el principio del vencimiento objetivo, las costas se imponen a la parte demandada ante la estimación de la demanda.

Por todo lo cual:

FALLO

Debo estimar y estimo la demanda interpuesta por el Procurador D. Tomas Ramirez Hernandez en nombre y representación de D. ª Lidia contra la entidad Banco BBVA SA representado por el Procurador D. Francisco Ojeda Rodriguez debiendo condenar a la demandada a abonar a la actora la cantidad de4902€ € mas los intereses legales ?jados en la forma del Fundamento de derecho Cuarto , con expresa condena en costas a la parte demandada.

Así lo pronuncio, mando y ?rmo.

Notifíquese a las partes la presente resolución haciéndoles saber que esta resolución no es ?rme y contra ella podrá interponerse recurso de apelación que se interpondrá ante el tribunal que haya dictado la resolución que se impugne dentro del plazo de veinte días contados a partir del día siguiente la de la noti?caron de la presente resolución, debiendo en todo caso la parte que cumplir lo dispuesto en la Disposición Adicional Decimoquinta de la LO 1/2009 de 3 de noviembre conforme a lo apartados 2 , 3.b) respecto del deposito para recurrir en los términos y con las prevenciones contenidas en los apartados 6 y ss de la referida disposición.
onal Decimoquinta de la LO 1/2009 de 3 de noviembre conforme a lo apartados 2 , 3.b) respecto del deposito para recurrir en los términos y con las prevenciones contenidas en los apartados 6 y ss de la referida disposición.

PUBLICACIÓN.- Leída y publicada fue la anterior resolución por el Juez que la dictó estando celebrando audiencia pública el mismo día de su fecha. Doy fe.

EL/LA MAGISTRADO