AUDIENCIA PROVINCIAL DE ALICANTE
SECCIÓN NOVENA
SEDE EN ELCHE
[redacted]

NIG: [redacted]
Procedimiento: **RECURSO DE APELACION (LECN) Nº 000457/2023- PT -**
Dimana del Juicio Verbal Nº 000955/2022
Del JUZGADO DE PRIMERA INSTANCIA N° 3 DE ORIHUELA

Dª [redacted] LETRADA DE LA ADMINISTRACIÓN DE JUSTICIA CON DESTINO EN LA AUDIENCIA PROVINCIAL DE ALICANTE, SECCIÓN NOVENA CON SEDE EN ELCHE

DOY FE Y TESTIMONIO: Que en el rollo de apelación civil núm. 000457/2023, dimanante de Juicio Verbal - 000955/2022 del JUZGADO DE PRIMERA INSTANCIA Nº 3 DE ORIHUELA, se ha dictado la siguiente resolución:

SENTENCIA Nº45/2024

En ELCHE, a veintinueve de enero de dos mil veinticuatro

El Ilmo. Sr. Magistrado **D. José Manuel Calle de la Fuente**, ha visto los autos de Juicio Verbal 955/2022, seguidos en el Juzgado de Primera Instancia número 3 de Orihuela, de los que conoce en grado de apelación en virtud del recurso entablado por parte demandada, Caja Rural Central, SCC, habiendo intervenido en la alzada dicha parte, en su condición de recurrente, representada por la Procuradora Sra. [redacted] y dirigida por el Letrado Sr. [redacted] y como apelada Dª [redacted] representada por la Procuradora Sra. Mª [redacted] y dirigida por el Letrado Sr. Juan Pablo Palomar Pérez.

ANTECEDENTES DE HECHO

[redacted]

PRIMERO.- Por el Juzgado de primera instancia nº 3 de Orihuela en los referidos autos, se dictó sentencia con fecha 13 de octubre de 2022 cuya parte dispositiva es del tenor literal siguiente:

"*Debo estimar y estimo la demanda interpuesta por la Procuradora Dña.* [redacted] *en nombre y representación de Dña.* [redacted] *contra la mercantil Caja Rural Central Sociedad Cooperativa de Crédito, condenando a la misma al pago de 4.985 euros, intereses y costas procesales.*"

SEGUNDO.- Contra dicha sentencia, se interpuso recurso de apelación por la parte demandada, Caja Rural Central, SCC en tiempo y forma que fue admitido en ambos efectos, elevándose los autos a este Tribunal, donde quedó formado el Rollo número 457/2023, tramitándose el recurso en forma legal. La parte apelante solicitó la revocación de la sentencia de instancia y la apelada su confirmación. Para la deliberación y votación se fijó el día 25 de enero de 2024.

TERCERO.- En la tramitación de ambas instancias, en el presente proceso, se han observado las normas y formalidades legales.

FUNDAMENTOS DE DERECHO

PRIMERO.- Objeto del recurso

La sentencia recurrida, después de analizar la jurisprudencia y normativa que considera de aplicación, estima la demanda sobre la base de las siguientes consideraciones**: "...***Para la resolución del presente procedimiento, en base a la jurisprudencia citada en el anterior fundamento de derecho, debe señalarse como, para la desestimación de la demanda, es necesario que la entidad demandada acredite, no solo su actuación diligente, sino que la actora, además, actuó de forma negligente.*

En su declaración, que ha sido en todo momento coherente ordenada, sin incurrir en contradicción ni en otro elemento dato lleve negar credibilidad a la misma, indicó como nunca ha tenido un dispositivo IPhone 13, aportado junto con la demanda justificante de compra del dispositivo móvil empleado en el momento de los hechos, señalando incluso ser una marca que no le gusta usar dado la

complejidad de su sistema operativo.

Expuso igualmente como solo accedía a la aplicación bancaria desde su dispositivo móvil, sin usar otro dispositivo, sin que las claves de acceso a la aplicación las tuviese recogidas en algún papel o dispositivo, si que hubiese sufrido algún tipo de robo, hurto o pérdida de su móvil o bolso en los días previos.

La actora relató no tener conocimiento de los hechos por comunicación de la entidad demandada, sino que, al hacer una revisión de sus cuentas en el sofá de su casa tras comer, comprobó que habían desaparecido casi 5.000 euros, lo que le alarmó, dado que solo tenía unos 7.000 euros en cuenta. En ese momento llamó a la entidad bancaria, constando en autos el registro de la correspondiente llamada, recriminando la entidad demandada que no hubiese saltado ninguna alarma, informando esta de que había saltado una alarma momentos antes, constando en las actuaciones, tal como indicó el Letrado de la parte actora durante el interrogatorio, la anulación por parte de la entidad bancaria unas tres horas antes de la llamada de la demandante, sin que se hubiese informado a esta

De la prueba practicada no consta comunicación alguna de la demandada a la actora, sino al contrario, tuvo que ser la actora la que se pusiese en contacto al comprobar el saldo de su cuenta bancaria.

La demandante expuso igualmente no haber recibido sms o correo electrónico en el que se solicitasen datos, ni haber contestado a estos.

En la documentación aportada junto con el escrito de contestación a la demanda se aprecia como, en los días anteriores al bloqueo de la tarjeta, existieron conexiones empleando el número de teléfono y usuario de la demandada, pero desde un terminal diferente, iPhone 13, y con un sistema operativo diferente, IOS, constatando en la documentación aportada por la demandada como la actora empleaba siempre sistema Android y terminales Redmi, lo que corroboraría su versión de los hechos.

Así, en el documento cinco de la contestación, se recoge una activación del servicio push con sistema operativo IOS, o en el documento siente un registro de huella desde un IPhone13 con sistema operativo IOS, apareciendo en el resto de indicaciones el sistema operativo Android.

Es patente como otra persona, empleando las claves de la actora, desde un terminal diferente, sin que la demandante tuviese conocimiento ni provocase dicha circunstancia, consiguió burlar los diferentes sistemas de seguridad, sistemas que

eran responsabilidad de la demandada, sin que la actora actuase de una forma negligente, hecho este que debía acreditar la entidad demandada, por lo que, en base a lo expuesto en el anterior fundamento de derecho, solo cabe estimar la demanda presentada…". Todo ello en los términos que constan en la resolución recurrida.

Se alza la parte demandada recurrente frente a la sentencia de instancia alegando, en esencia, error en la valoración de la prueba, por cuanto que considera que de lo actuado resulta acreditado que fue la actuación negligente de la actora la que ocasiono el fraude y su pérdida patrimonial, dado que la entidad bancaria cumplió con todas sus obligaciones y que todas las operaciones fueron debidamente autenticadas mediante factor biométrico. Alude así mismo la recurrente, que la actora en algún momento también debió recibir este correo electrónico/sms y debió informar sus claves de ruralvía en su tarjeta, pero ella no lo reconoce ni en la denuncia que formulada ante la Policía Nacional, ni en la demanda, pero que tuvo que ser así por cuanto ello es así porque a CRC le consta que el día que se producen los cargos que está reclamando, 02/11/2021, el usuario de la cliente accede a ruralvía y a las 13:09h activa el servicio de biometría (para poder autorizar compras por internet únicamente con la huella/rostro). Para activar este servicio se envió un código de confirmación al número [redacted](número de móvil de la cliente), por lo que ella introduciendo ese código confirmó la activación de la biometría y permitió al ciberdelincuente autorizar los pagos por internet con huella.

Se alega asimismo que se infringe la valoración de prueba por cuanto no se han tenido en cuenta todas las pruebas solicitadas y que resultaron admitidas.

Todo ello en los términos que constan en su recurso.

La parte actora se opone al recurso e incide en el acierto de la resolucion

Reseñar que por auto de esta sala, de fecha 3 de noviembre de 2020 se inadmitió la prueba propuesta por la apelante, auto que no fue recurrido y que devino firme en derecho.

SEGUNDO.- Centrado el objeto de debate, en el supuesto objeto de recurso, estamos ante un fraude llamado " phishing", por el que se suplanta la identidad de la entidad bancaria para obtener información sobre las claves o credenciales de las cuentas bancarias o tarjetas de crédito/débito. Se envía un correo electrónico con la apariencia de ser remitido por la entidad bancaria, que contiene un enlace a una página que aparenta ser sitio oficial de ésta, pero que en realidad pertenece a un dominio bajo control del phiser. Es decir, el phishing que constituye una modalidad específica de fraude informático que visualiza las deficiencias de seguridad del sistema informático de una entidad y que trae causa en el uso de las redes telemáticas, a este respecto, la Agencia Española de Protección de Datos (Resolución DE 24 DE MAYO DE 2006) señaló: "*el objetivo de los ataques de " phishing" es la obtención de forma engañosa y fraudulenta de los códigos de usuarios y contraseñas de clientes de Banca Electrónica, al objeto de realizar transferencias no autorizadas...Su operatoria comienza con la adquisición en internet de un "paquete de herramientas", que incluyen programas informáticos e información necesaria para realizar los ataques. Esta información incluye "listas de equipos comprometidos" que pueden ser utilizados bien para mandar correos electrónicos, bien para alojar páginas web falsificadas. Incluyen además "bases de datos de direcciones de correo electrónico". Una vez en posesión del paquete, se remiten los correos electrónicos con carácter indiscriminado (buscando contactar con clientes de la entidad financiera) informando de la necesidad de conectarse a una página web que parece pertenecer a la citada entidad y portar los códigos de acceso y contraseñas de clientes. Dicha página web se suele alojar en un equipo conectado a Internet cuya seguridad se haya [visto] comprometida", sin conocimiento de su usuario, y que se encuentra normalmente en un país distinto al de los destinatarios del ataque. De esta forma se constituye un "fichero de datos personales con códigos de usuarios y contraseñas de clientes" recabados de forma engañosa y fraudulenta, que se ubica normalmente en el mismo "equipo remoto comprometido" en el que se aloja la página web falsificada. Con los datos obtenidos se realizan transferencias a cuentas de colaboradores situados en España los cuales a su vez retiran el dinero en efectivo y tras descontar una comisión realizan transferencias monetarias internacionales mediante entidades especializadas*".

Por otra parte, debemos tener presente que el RDL 19/2018, de 23 de

noviembre establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago.

Así, en caso de ejecutarse una operación de pago no autorizada, el artículo 45 señala que "...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..."

Este sistema de responsabilidad civil tan solo cesa cuando, conforme a lo establecido en el artículo 46, el ordenante ha actuado de manera fraudulenta o ha "incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41...", precepto este que impone al usuario la obligación de utilizar el instrumento de pago de conformidad con las condiciones que regulen la emisión y de tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas, y en caso de extravío, sustracción o apropiación indebida, notificarlos al proveedor de servicios de pago sin demora.

Dicho precepto puntualiza que "...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.".

Ahora bien, dicha norma, en el apartado 2 previene que, "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.".

De lo anterior resulta que, tratándose de operaciones no autorizadas, como es el caso, salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante, la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba a tal efecto. No debemos olvidar que la carga de la prueba sobre la implementación de medidas de seguridad adecuadas, suficientes, eficientes y actuales al nivel de riesgo modalidades de ataques informáticos en la red bancaria de banca *online* lo sea a cargo del usuario del sistema, pues el marco de responsabilidad establecido para el caso de operaciones de pagos hechos por proveedores de servicios no autorizadas o ejecutadas incorrectamente, es el de la cuasi-objetividad tal cual se desprende de la regulación específica sobre la materia a la que hemos hecho referencia anteriormente. Abunda en lo expuesto el principio de facilidad y disponibilidad probatoria al que se hace referencia en el art 217 de la lec, criterio este más que razonable, el cual resulta de aplicación en este tipo de supuestos, por cuanto que la propia seguridad y debida reserva de la red se contrapone al acceso por parte de un tercero distinto al titular de la misma que asume poner en la red pública un conjunto de comunicaciones para permitir operaciones bancarias que requiere de soluciones tecnológicas muy avanzadas que minimicen las amenazas contra la autenticidad, integridad y la confidencialidad de los datos que circulan a través de la red.

Incide en lo antes expuesto, la propia normativa de consumidores, condición que ostenta la actora, y no esta discutida en autos, al señalar que los prestadores de servicios serán responsables de los y perjuicios causados a los consumidores o usuarios, salvo que prueben que han cumplido las exigencias y requisitos reglamentariamente establecidos y demás cuidados y diligencias que exige la naturaleza del servicio, remarcando que se responderá de los daños originados en el correcto uso de los servicios, cuando por su propia naturaleza, o por estar así reglamentariamente establecido, incluyan necesariamente la garantía de niveles determinados de eficacia o seguridad, en condiciones objetivas de determinación, y supongan controles técnicos, profesionales o sistemáticos de calidad, hasta llegar en debidas condiciones al consumidor y usuario

En base a lo reseñado anteriormente, cabe concluir que si el fraude se

produce porque hay un déficit de la seguridad que no cabía esperar del servicio que se ofrece, el cual se encuadra en un ámbito que se halla bajo el control del hoy demandado, que es quien presta el servicio, y por tanto es el demandado quien cuenta con la información sobre las medidas de cuidado exigibles, y en su caso adoptadas, a fin de reducir el riesgo de riesgos, es el proveedor del servicio hoy demandado deviene responsable del daño, salvo que demuestre que fue la actora que actuó de forma negligente o fraudulenta y dicha prueba no se ha producido en el caso de autos, carga de la prueba de dicha negligencia de la actora que correspondía probar a la hoy demandada para eximirse de la responsabilidad reclamada, lo cual no ha acontecido en este supuesto.

Por otra parte, en cuanto al error en la valoración de la prueba que se denuncia, tampoco se aprecia por este tribunal, por cuanto que consideramos que la sentencia recurrida hace un análisis razonado y razonable del resultado probatorio, máxime cuando además se pretende atacar dicha valoración, sobre la base de una prueba que no fue practicada en primera instancia, y que fue inadmitida en esta segunda instancia por auto que ni siquiera fue recurrido por la parte apelante, por lo que al aludir que "... *en algún momento también debió recibir este correo electrónico/sms y debió informar sus claves de ruralvía en su tarjeta, pero ella no lo reconoce ni en la denuncia que formulada ante la Policía Nacional, ni en la demanda, pero que tuvo que ser así...*" **esa afirmación no pasa de ser una mera suposición de la parte recurrente, que no resulta avalada por medio probatorio alguno de los admitidos y practicados en autos.**

En conclusión, hallándonos ante un supuesto de responsabilidad cuasi objetiva y de riesgo, como indica la sentencia de la Audiencia Provincial Almería Sección 1ª, de 31 de enero de 2023 cuando dice*: "..., "es exigible a la apelante la responsabilidad patrimonial cuasi objetiva legalmente establecida, que, obviamente, supone un paso más en la protección al consumidor que el previsto en el art. 148 del Texto Refundido de la Ley para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, puesto que viene a excusar al consumidor de la negligencia en que pueda haber incurrido por facilitar sus datos personales y claves de confirmación o firma electrónica en virtud de la acción defraudatoria de terceros*", como

consecuencia de lo anterior, es a la demandada a quien corresponde acreditar que la operación ordenada sí fue auténtica y que no estuvo afectada por un fallo técnico o por otra deficiencia y/o que fue la actuación negligente de la actora la que hubiera ocasionado el fraude(fraude que no ha sido negado), y dicha prueba no la ha cumplimentado adecuadamente la parte demandada, por lo que debe correr la misma con las consecuencias negativas de dicha falta de prueba sobre tales extremos.

En esta misma línea, la sentencia de la Sección 20ª de la Audiencia Provincial de Madrid de 20 de mayo de 2022, indica: "...l*a Directiva 2015/2036 la negligencia que le hace responder al cliente, es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que ha sido inducido por un delincuente profesional. Tampoco puede calificarse como grave dicho comportamiento conforme a la normativa del código civil, pues siendo exigible al demandante la diligencia que exija la naturaleza de la obligación y correspondan a las circunstancias de las personas, tiempo y lugar (art. 1.104 del cc), el método fraudulento empleado - phishing - es de una complejidad y grado de perfección, difícilmente detectable por un cliente de las características del demandante, ... Es cierto que dicho comportamiento no puede considerarse diligente, pero para hacer soportar al cliente las consecuencias, aún parciales como se concluye en la sentencia apelada, es preciso apreciar en él una negligencia y que además sea grave, que en la normativa europea antes referida se equipara a la comisión de un fraude, actuación en la que no se ha acreditado incurriese el demandante, por el hecho de haber pinchado el link que se le ofrecía y facilitar los datos y clave de la tarjeta..*

..la responsabilidad exigida a la entidad demandada, como proveedora del servicio, es la que se deriva de la naturaleza de tal prestación y de la posición contractual en la que se encuentran las partes, lo que le obliga a adoptar una serie de medidas de seguridad y dotarse de mecanismos de supervisión que permitieran detectar operaciones fraudulentas en la prestación de servicios de pago, tal como señala el artículo 2 del Reglamento Delegado 2018/389 , pues como se indica también en la sentencia citada de la Audiencia de Pontevedra, incluyendo la técnica del phishing, 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. Dicha actuación diligente no puede considerarse acreditada por la información que se facilita a los clientes a través de su página web, en cuanto la efectividad de esas obligaciones preventivas, lo que requerían era implementar en el sistema informático el mecanismo tecnológico adecuado para evitarlo; es decir mediante una con una conducta activa y no simplemente informativa o divulgativa".

Abunda en dicha postura, la SAP de Navarra 223/2023 de 9 de marzo que, en un supuesto similar al que nos ocupa, señaló: "*...Los hechos referidos por el demandante, y suficientemente contrastados tanto con la interposición inmediata de una denuncia ante cuerpo policial como con la también inmediata elevación de una reclamación ante la propia entidad por medio de su gestora y cancelación de la tarjeta -tal y como consta relatado en el documento nº 2 de la demanda-, son que ha sido víctima de una estafa en la modalidad de phishing (en inglés, "suplantación").*

Normalmente la realización de transferencias ordinarias con cargo a una cuenta vinculada es autenticada por el cliente mediante la introducción de las claves previamente facilitadas por la entidad de crédito con la que contrata, con respecto a las cuales tendrá unos deberes de custodia. Sin embargo, un ataque informático de phishing comporta la obtención por terceros de forma engañosa y fraudulenta de los códigos de usuarios y contraseñas de clientes de banca electrónica, al objeto de realizar transferencias no autorizadas. La técnica consiste, básicamente, en la suplantación de la identidad del banco o del proveedor del sistema de pago, a través de la cual se reclama al usuario los datos de tarjeta y credenciales bajo pretexto de necesidad de renovación o actualización de los mismos, para finalmente ejecutar transacciones fraudulentas con los datos obtenidos. Como describe la SAP Madrid 178/2015, de 4 de mayo, en un supuesto muy similar al que nos ocupa, "es

imprescindible proporcionar una definición del phishing, para determinar ante qué abuso informático nos encontramos. En el presente caso, el phishing se origina con la suplantación de la identidad del banco por parte del phisher con la finalidad de adquirir información confidencial sobre contraseñas de cuentas bancarias, tarjetas de crédito o cualquier otra información en relación con el banco, que permita entrar en las cuentas de los usuarios en Internet de banca electrónica. El internauta recibe un correo electrónico o cualquier mensaje instantáneo, a través del cual se le informa de que debe cambiar sus claves bancarias, proporcionándole un link a través del cual pueda acceder a la página Web de la supuesta entidad bancaria y allí realizar la modificación aconsejada. En la mayoría de los métodos de phishing se utilizan técnicas de engaño, a través de las cuales el phisher utiliza contra la víctima el propio código de programa del banco o servicio similar, adquiriendo la página Web la verdadera apariencia de la entidad bancaria. Igualmente, resulta muy habitual que el internauta reciba un correo en el que se le informe de que debe verificar sus cuentas, seguido por un enlace que parece la página Web oficial de la entidad bancaria" .

En tal escenario, la operación no se encuentra completamente "autenticada" en términos de la LSP, porque falta la certificación de la identidad del usuario ordenante de la operación. No resulta suficiente, por sí solo, haber completado los mecanismos reforzados de autenticación establecidos por la entidad, debido a que si no se han implementado otros sistemas para restringir sólo al usuario el acceso al canal de banca electrónica que autentifica, no puede descansar automáticamente toda la responsabilidad en dicho usuario, dado que al proveedor del servicio de pago le compete la responsabilidad respecto del buen funcionamiento y la seguridad del mismo y es obligación esencial de las entidades prestadoras del servicio de banca on line el dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones por lo que, en el supuesto de insuficiencia o mal funcionamiento de las adoptadas, deben ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema. Por ello la previsión legal contempla, como excepción que impide la reclamación del usuario, la posibilidad de fraude o negligencia grave imputable al mismo, con expresa exigencia normativa de que la demostración de tales factores recae en el proveedor: "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" (art. 44.3 LSP).

Este es el verdadero fondo esencial del presente recurso de apelación. Defiende la entidad demandada que en el caso que nos ocupa el Sr. Desiderio incurrió en una grave negligencia por el hecho de que accedió al enlace y facilitó en la aplicación desplegada con el mismo tanto los datos de su tarjeta como sus credenciales para autenticar, cuando por el contrario la aplicación oficial de Caixabank nunca reclama estos elementos a sus usuarios. Y más todavía ante la condición del demandante de agente de la Policía Foral y las recomendaciones y alertas del cuerpo ante este tipo de fraudes. Subraya el recurso de apelación que si la propia normativa considera como negligencia grave el hecho de guardar las credenciales junto con el instrumento de pago en un formato abierto y fácilmente detectable (Directiva 2015/2366), con mayor fundamento es, también, una negligencia grave facilitar esos datos a tercero. No obstante, en realidad la Directiva se limita a poner tal supuesto como ejemplo de negligencia grave en el punto nº 72 de su Considerando o Introducción, donde se explica que "A la hora de evaluar la posible negligencia o la negligencia grave del usuario de servicios de pago, deben tomarse en consideración todas las circunstancias. 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".

En el caso que nos ocupa el demandante facilitó "a tercero" los datos y credenciales de su tarjeta bajo fraude por suplantación de la entidad demandada. Es decir, en tal momento, en la creencia de que no se trataba de ningún "tercero". La norma obliga al usuario a tomar "todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas" (art. 41.a LSP), y esa razonabilidad legalmente exigida no puede evaluarse a posteriori, sino en el momento del phishing, cuando el demandante fue engañado por medio de la suplantación, por el tercero estafador, de la identidad y aplicación informática de la entidad bancaria.

Destaca el recurso de apelación que el propio Sr. Desiderio reconoció en juicio su "negligencia", pero es que como ha quedado visto en palabras de la Directiva, no basta con cualquier falta de diligencia o precaución en la custodia de las credenciales personales, sino que debe darse una conducta significativamente negligente. De esta forma, "grave" sería la negligencia de quien toma la iniciativa a la hora de desproteger sus credenciales, o la negligencia de quien hace entrega de los datos y credenciales a un tercero que se muestra claramente como tal, como ajeno a la entidad bancaria mediante signos y evidencias suficientes de tal ajenidad. Pero no ostenta la misma "gravedad" relevante la negligencia de quien no actúa por iniciativa propia sino arrastrado por comportamiento fraudulento de tercero, mediante un mecanismo de fraude muy específico y complejo, y de difícil detección, en el que es fácil ser víctima de un engaño ante la apariencia y creencia de oficialidad de la entidad, sin embargo fraudulentamente aparentada por suplantación, sin que se aprecie en ello una cualificada negligencia. Como afirma la SAP Pontevedra 623/2022, de 1 de diciembre, "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 significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que 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 suficiente y adecuada con exigencia de medidas implantadoras activas, sin entenderse suficientes 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-"

En la misma línea, SAP de Asturias 285/2023 de 12 de mayo.

En el caso que nos ocupa, los sistemas de autenticación se establecen por la propia entidad demandada, y si no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante, víctima de esta

práctica fraudulenta, sea el responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo, por lo que la omisión, insuficiencia o defectuoso funcionamiento de las adoptadas es que han de ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema, con las excepciones antes analizadas, y que no han resultado probadas en las presentes actuaciones, lo que da lugar a una responsabilidad por "culpa in vigilando" o responsabilidad cuasi objetiva por el mal funcionamiento de los servicios de banca electrónica, máxime cuando no consta probado por la demandada, que es a quien correspondía la prueba por las razones expuestas, que se hiciera un uso indebido del sistema por parte de la actora ni que incumpliera con sus obligaciones básicas, puesto que no consta prueba directa o indiciaria que revele que hubo extravío ni un uso claramente imprudente o no diligente del sistema por parte de la actora.

Por otra parte, ni se alega de forma expresa, ni se acredita que la actora actuara de forma diligente, por el contrario la actora, una vez que advirtió la existencia de una operación fraudulenta, como dice la sentencia recurrida, fue la actora la que dio aviso al Banco, y no al revés.

En definitiva, en base a los argumentos que se contiene en la sentencia recurrida, unidos a los que han sido expuestos por esta sala, procede la desestimación del recurso.

TERCERO.- Se imponen a la recurrente las costas de la apelación, al haberse producido la desestimación del mismo, de conformidad con lo dispuesto en el art 398 de la lec.

VISTAS las disposiciones citadas y demás de general y pertinente aplicación, en nombre del Rey y por la autoridad conferida por el Pueblo Español.

FALLO: Que desestimo el recurso de apelación interpuesto por la representación procesal de Caja Rural Central, SCC contra la sentencia del juzgado de primera instancia número 3 de Orihuela, de fecha 13 de octubre de 2022, que confirmo. Se imponen a la recurrente las costas de la apelación.

Con pérdida del depósito constituido.

Notifíquese esta sentencia conforme a la Ley y, en su momento, devuélvanse los autos originales al Juzgado de procedencia, de los que se servirá acusar recibo, acompañados de certificación literal de la presente resolución a los oportunos efectos de ejecución de lo acordado, uniéndose otro al rollo de apelación.

Contra la presente resolución no cabe recurso alguno.

Así, por esta mi sentencia definitiva que, fallando en grado de apelación, lo pronuncio, mando y firmo.

PUBLICACIÓN.-La anterior resolución ha sido leída y publicada en el día de su fecha por el Ilmo. Sr. Ponente, estando la Sala reunida en audiencia pública. Doy fe.

CONCUERDA lo precedentemente transcrito bien y fielmente con su original al que me remito y refiero. Y para que así conste, expido el presente en Elche a, uno de febrero de dos mil veinticuatro.

LA LETRADA DE LA ADMON. DE JUSTICIA