ADMINISTRACION DE JUSTICIA

AUD.PROVINCIAL SECCION CUARTA
OVIEDO

SENTENCIA: 00163/2024

Modelo: N10250
C/ CONCEPCIÓN ARENAL Nº 3 - 3

-

Teléfono: 985968737 **Fax:** 985968740
Correo electrónico:

Equipo/usuario: PBG

N.I.G. 33004 41 1 2023 0001390
ROLLO: RPL RECURSO DE APELACION (LECN) 0000113 /2024
Juzgado de procedencia: JDO.1A.INST.E INSTRUCCION N.7 de AVILES
Procedimiento de origen: ORD PROCEDIMIENTO ORDINARIO 0000192 /2023

Recurrente:
Procurador: NURIA ARNAIZ LLANA
Abogado: CELESTINO GARCIA CARREÑO
Recurrido: UNICAJA BANCO S.A.
Procurador: [redacted]
Abogado: [redacted]

Rollo: RECURSO DE APELACION (LECN)

NÚMERO 163

En OVIEDO, a once de abril de dos mil veinticuatro, la Sección Cuarta de la Ilma. Audiencia Provincial de Oviedo, compuesta por D. Francisco Tuero Aller, Presidente, D. Javier Alonso Alonso y Dª. Raquel Blázquez Martín, ha pronunciado la siguiente:

S E N T E N C I A

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

En el recurso de apelación número 113/2024, en autos de JUICIO ORDINARIO Nº 192/2023, procedentes del Juzgado de Primera Instancia número 7 de los de Avilés, promovido por **DOÑA** [redacted], demandante en primera instancia, contra **UNICAJA BANCO S.A.**, demandada en primera instancia, siendo Ponente el Ilmo. Sr. Magistrado D. Francisco Tuero Aller.

ANTECEDENTES DE HECHO

PRIMERO.- Que por el Juzgado de Primera Instancia nº 7 de Avilés se ha dictado sentencia de fecha 21 de noviembre de 2023 cuya parte dispositiva es del tenor literal siguiente: "Que debo desestimar como desestimo íntegramente la demanda formulada por doña [redacted] frente a la entidad UNICAJA BANCO, S.A.

Con expresa imposición de costas a la demandante".

SEGUNDO.- Contra la expresada resolución se interpuso por la parte demandante recurso de apelación, del cual se dio el preceptivo traslado, y remitiéndose los autos a esta Audiencia Provincial se sustanció el recurso, señalándose para deliberación y fallo el día nueve de abril de dos mil veinticuatro.

TERCERO.- Que en la tramitación del presente recurso se han observado las prescripciones legales.

FUNDAMENTOS DE DERECHO

PRIMERO.- No es discutido que la demandante, Doña [redacted], fue víctima de una estafa informática durante unos breves minutos sobre las 21 horas del día 2 de julio de 2022 y sobre las 00 horas del día siguiente, ni tampoco, en lo sustancial, el medio como se llevó a cabo, a través de los siguientes pasos: En primer término Doña [redacted] recibió una llamada a su terminal telefónico de quien dijo ser empleado del Banco del que era cliente, aquí demandado, comunicándole que alguien le estaba realizando un hackeo en su cuenta bancaria, que le estaban retirando dinero de ella y que para evitarlo debía desactivar su tarjeta de crédito y volver a activarla, así como repetir unas claves que le iban a llegar vía SMS; y así hizo con las claves de los diversos SMS que le llegaron en esos instantes,

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

en los que se hacía mención a múltiples operaciones bancarias (una transferencia por importe de 1.900 € que conllevó una comisión de 9,50 €, seis cargos de Bizum, cuya aplicación autorizó en esos momentos, por 500 € cada uno, 13 compras con tarjeta de débito, once cargos de 180 €, un cargo de 150 € y otro de 100 €). El mismo día 3 de julio comprobó que se habían cargado en su cuenta esos movimientos bancarios, por un total de 7.139,50 € que en realidad habían sido transferidos a un tercero defraudador, que se había valido de ese proceder para obtener la autorización para realizar tales operaciones. Tras denunciar ante la policía el mismo día estos sucesos, Doña [redacted] reclama en este juicio la restitución de la indicada suma que le fue sustraída, con sus intereses.

La sentencia de primer grado, tras hacer un detenido análisis de la normativa aplicable, la establecida en el Real Decreto-Ley 19/2018, de 23 de noviembre, desestimó la demanda por cuanto, a su entender, concurrió en el caso negligencia grave por parte de la usuaria, que exime de responsabilidad al Banco demandado. No conforme con esa decisión, la demandante interpone el presente recurso en el que defiende en especial que medió un fallo de seguridad en el proveedor del servicio de pago en orden a prevenir y evitar este tipo de órdenes fraudulentas

SEGUNDO.- Se está, pues, ante un tipo de estafa informática cometida mediante la captación de datos bancarios, induciendo a error a la víctima tras hacerse pasar por la propia entidad bancaria, a la que suplantan a través de correos electrónicos (técnica conocida como "phishing"), a través de SMS fraudulentos ("smishing") o de llamadas telefónicas (vishing) como sucedió en este caso, con el objetivo final de que los clientes proporcionen sus datos de carácter personal y claves bancarias para acceder así a sus cuentas y lograr que le sean transferidas sumas más o menos importantes de dinero. La excusa frecuentemente utilizada, como ocurrió en este caso, es la de informar sobre un acceso no autorizado o un comportamiento fraudulento en las cuentas online, de tal modo que los clientes alertados ante esa circunstancia, intentan comunicar con el Banco cuando en realidad lo que hacen es facilitar sus datos bancarios al defraudador.

TERCERO.- Como decíamos en sentencias de 13 de diciembre de 2023 y 21 de marzo de 2024, al abordar un caso similar, "*El marco normativo que sirve para dar respuesta a la controversia se contiene en la actualidad en el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que sustituyó a la precedente Ley 16/2009, de 13 de noviembre, de servicios de pago, y en el que, por lo que aquí importa, se recogen las obligaciones esenciales que incumben al usuario de servicios de pago y a las entidades que los prestan.*

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

Así, y por lo que concierne al primero, el usuario está obligado (art. 41 a) a utilizar el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del mismo, y, en particular, "tomará todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas". En tanto el proveedor de esos servicios está obligado (art. 42.1 a) a cerciorarse que 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…".

A su vez, y en relación a los supuestos de operaciones no autorizadas o ejecutadas incorrectamente, el usuario está obligado (art. 43.1) a comunicar su existencia "sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones…". Y está llamado, además, a soportar (art. 46.1.3º) "todas las pérdidas derivadas de operaciones de pago no autorizadas si … 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".

Fuera de esos supuestos –ausencia de comunicación en tiempo de las operaciones, actuación fraudulenta del usuario, o negligencia grave- la proveedora del servicio está obligada a realizar la rectificación del cargo (art. 43.1) y devolución del importe (art. 45.1), bajo la premisa de que, ante la negación por el usuario de haber autorizado la operación o la afirmación de que la misma fue realizada de manera incorrecta, corresponde a aquella (art. 44.1º) "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…", al igual que tiene la carga de acreditar (art. 44.3º) "que el usuario del servicio de pago cometió fraude o negligencia grave", sin que, a la par, el registro de la utilización del instrumento por el proveedor baste por si solo y 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…" (art. 44.2º).

Y esa responsabilidad se acentúa aún más cuando el proveedor no exige "autenticación reforzada" del cliente, supuesto en que éste último únicamente responde de haber actuado de forma fraudulenta (art. 46.2º). Concepto ese que se corresponde con (art. 2.5) "la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), que son independientes -es decir, que la vulneración de uno no compromete la fiabilidad de los demás-, y concebida de manera que se proteja la confidencialidad de los datos de identificación".

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

Con todo, pues, lo que resulta de esas previsiones es el establecimiento a cargo de la proveedora de los servicios de pago de un riguroso régimen de responsabilidad ante disposiciones no autorizadas, que solo cede con la demostración de la actuación fraudulenta o gravemente negligente del usuario. Régimen sin duda inspirado en la idea de que los beneficios que comporta (tanto para el tráfico económico, como para la actividad del proveedor de los servicios) el avance tecnológico en los instrumentos de pago, debe estar justamente compensado con la protección reforzada de quien los emplea y se ve expuesto a actuaciones fraudulentas como la que hubo en el caso de autos. Con razón dice, por ello, la sentencia de instancia que se trata de una responsabilidad cuasi objetiva, que es la calificación que le otorgan, además de las resoluciones que en ella se citan, otras del mismo sentido como las sentencias de las Audiencias Provinciales de Lleida, Sec. 2ª, de 29 de junio de 2023; La Rioja, Sec. 1ª, de 17 de febrero de 2023; Almería, Sec. 1ª, de 31 de enero de 2023; o Madrid, Sec. 10ª, de 13 de enero de 2023, además de cuantas en ellas se mencionan, en las que, con las variaciones propias de cada caso, se abordan supuestos de fraude similares al que nos ocupa. Al igual que lo hace también la sentencia de la Sec. 5ª de esta Audiencia de 22 de junio de 2023".

CUARTO.- Y partiendo de estas premisas el recurso debe ser estimado, por cuanto si bien es de observar una comportamiento descuidado o negligente por parte de Doña en el proceso que desembocó en esa estafa, esa negligencia no merece el calificativo de grave si se pone en relación con las circunstancias concurrentes en el caso concreto y, en especial, con la falta de diligencia del propio Banco en orden a evitar esta clase de ataques informáticos como a continuación se razonará.

Efectivamente cabe reprochar a la demandante que hubiera confiado en lo que se le decía a través de una llamada efectuada por persona desconocida ya que, por más que su interlocutor manifestara que era un empleado de la entidad bancaria, nada aparecía que refrendase esa afirmación. No se está ante un caso de los conocidos como CALLER ID SPOOFING, mediante la cual el autor de la estafa utiliza el propio ID de la entidad bancaria, pues la propia Doña reconoció en el acto del juicio que en las llamadas no aparecia reflejado que provenían del Banco. A lo que se añade que también admitió que no leyó detenidamente los mensajes que le iban llegando, sino que se limitaba a facilitar las claves al defraudador. Esta actuación de la usuaria resulta más entendible ante la alerta, que creía enviada por el Banco, de que alguien había realizado movimientos fraudulentos en su cuenta, y de esta forma intentaba neutralizarlos. En esos momentos, a últimas horas de la tarde, la demandante viajaba en autobús hacia su centro de trabajo, lo que hacía más

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

difícil aún que se concentrara en lo que estaba sucediendo y guardara la necesaria tranquilidad y prudencia ante el ataque informático del que se le informaba; aún más si se observa la dificultad que supone atender simultáneamente desde el mismo terminal a la llamada telefónica y a los sucesivos mensajes que aparecían en su pantalla.

El hecho de facilitar las claves de seguridad que le iban siendo requeridas en los sucesivos SMS para autorizar las operaciones venía precedido y motivado, como se dice, por el engaño ya consumado con la primera llamada, y estaba sin duda guiado por el ánimo de evitar lo que, desgraciadamente, se perseguía con él, por lo que esa actuación, por sí misma, no puede calificarse de temeraria ni gravemente negligente, sin que, como decíamos en la sentencia citada de 13 de diciembre de 2023, *"pueda exigirse a quien resultó engañada mayor precaución que a quien debía poner los medios necesarios para evitar el engaño".*

Y si bien ha de admitirse que una lectura detenida y atenta del contenido de esos SMS podían haber alertado a Doña [redacted] del error que cometía, en cuanto indicaban que estaba autorizando operaciones bancarias en favor de terceros, no puede obviarse, ha de insistirse, que la conducta seguida por ella ha de enmarcarse en el ámbito del engaño que estaba sufriendo, en el que era pieza clave la introducción de esas claves para, precisamente, evitar el fraude que creía fundadamente estar sufriendo. Y es en ese marco, en las circunstancias indicadas, y en el del normal nerviosismo y precipitación que produce en cualquier persona esta clase de alertas, en el que ha de valorarse la expresada conducta.

En este contexto difícilmente puede atribuirse la calificación de negligencia grave al actuar de la demandante. Es al proveedor del servicio a quien incumbe la carga probatoria de demostrar su concurrencia, en el régimen de responsabilidad cuasi objetivo que ha quedado expuesto. Las sentencias de la Audiencia Provincial de Pontevedra de 1 de diciembre de 2022 y 23 de marzo de 2023 con cita de otras varias de diversas Audiencias, dando un paso más, señalan que *"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 implantadora activas, sin*

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

entenderse suficientes avisos generales o en página web de mero carácter informativo o divulgativo".

En definitiva, aunque pudiera apreciarse cierto grado de precipitación o descuido en la conducta de la demandante, lo que no se observa, a la vista de las circunstancias expuestas, es la grave negligencia que le imputa el Banco.

Pero, además, concurren otros datos que apuntan claramente a la responsabilidad de la demandada en lo sucedido, decisiva en este caso. Ella misma señala en el escrito de contestación que el Banco de España ya se había hecho eco de esta clase de delitos, informando de las nuevas modalidades de suplantación de la identidad del Banco. Y, sin embargo, no adoptó las técnicas o medidas de seguridad que fueran bastantes para evitar que se produjeran esta clase de fraudes en su ámbito de actuación, o, al menos, de haberlas adoptado, fueron insuficientes como lo demuestra que siguieran teniendo lugar.

Singular relevancia tienen las especiales particularidades del caso: Son numerosísimos los apuntes bancarios que tuvieron lugar en muy pocos minutos, algunos de los cuales no llegaron a buen fin, sin que el Banco explique la causa de porqué unos tuvieron resultado y otros no. Varias horas antes, a las 13.38 horas del mismo día 2 de julio aparece ya un mensaje sobre vinculación de dispositivo que se repite a las 21.05, sin que tampoco se aclare mínimamente esa duplicidad de anotaciones pese a que parece presumible que fuera ésta la vía de acceso del ciberdelincuente a la cuenta de Doña [redacted], que permitió llevar a cabo la estafa. Todos los movimientos se producen a horas poco habituales y resultan sumamente inusuales, como la gran cantidad de operaciones tipo Bizum en una persona que hasta entonces no disponía de la aplicación, direcciones de IP ubicadas en terceros países, compras en entidades tan poco entendibles en una persona que carece de un particular perfil financiero –al menos nada consta en sentido contrario- como las realizadas a Verse o a Rebellon Pay. Ese elevado número de desplazamientos de dinero a favor de terceros en condiciones tan peculiares, ajenos totalmente a la "pauta de gasto" que seguía la actora según declaró en el acto del juicio, en manifestaciones que no aparecen desvirtuadas en modo alguno, debieron alertar y permitir al Banco detectar que se estaba ante un posible fraude, de contar con el necesario sistema de seguridad para prevenir esta clase de actuaciones, ya entonces conocida como se ha visto.

Debe añadirse a lo anterior que, como argumenta la apelante, es sabido que en esas fechas la entidad demandada, con motivo de la fusión de la banca digital con otras entidades, sufrió un gran número de ataques informáticos, que por su repetición difícilmente pueden imputarse a los usuarios y no a una quiebra de sus sistemas de seguridad. De esa situación ya nos hacíamos eco en la repetida sentencia de 21 de marzo de 2024, y no deja de constituir un hecho notorio, al menos en el ámbito de esta Comunidad en tanto fue objeto de

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

importante divulgación en los medios de comunicación que, en cuanto tal, está exento de prueba (art. 281.4 LEC).

En resumen, como también señalábamos en las repetidas sentencias de 13 de diciembre de 2023 y 21 de marzo de 2024, el usuario procedió como con "*toda probabilidad habría realizado gran parte de la población, por más que sea usuaria de esos canales tecnológicos, en los que el refinamiento en el desarrollo de la actividad delictiva parece ir un paso por delante de las barreras que se ponen para evitarla, pese a que, sin duda, es a la entidad a quien corresponde implementar todos los medios precisos para anticiparse a esa actividad, que es de lo que, sin embargo, aquí no hay prueba alguna*".

QUINTO.- La estimación de demanda y recurso comporta la imposición a la demandada de las costas ocasionadas en la instancia, sin que proceda hacer expresa declaración de las aquí causadas (arts. 394 y 398 LEC)

Por lo expuesto, la Sala dicta el siguiente:

F A L L O

Estimar el recurso de apelación interpuesto por Doña [redacted] frente a la sentencia dictada por el Juzgado de Primera Instancia nº 7 de Avilés en juicio ordinario seguido con el nº 192/23, la que revocamos y, en su lugar, acordamos:

1º) Estimar íntegramente la demanda interpuesta por dicha recurrente frente a Unicaja Banco S.A., a la que condenamos a que abone a la anterior la cantidad de 7.139,50 €, más sus intereses desde la fecha de la previa reclamación extrajudicial. Y

2º) Condenamos a la entidad bancaria demandada al pago de las costas causadas en primera instancia, sin hacer expresa declaración de las generadas por el recurso.

Devuélvase a la apelante el depósito constituido para recurrir.

Contra esta sentencia podrá interponerse recurso de casación, en los casos, por los motivos y con los requisitos prevenidos en los arts. 477 y ss. L.E.C., debiendo interponerse en el plazo de **VEINTE DÍAS** ante este Tribunal, con constitución del depósito de 50 euros en la cuenta de consignaciones de este Tribunal en el Banco Santander e identificación del procedimiento al que se refiere.

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

Así, por esta nuestra Sentencia, lo pronunciamos, mandamos y firmamos.

PRINCIPADO DE ASTURIAS

FIRMA (1): Fco. Arturo Tuero Aller (11/04/2024 13:09)
FIRMA (2): Javier Alonso Alonso (12/04/2024 13:51)
FIRMA (3): Raquel Blazquez Martin (12/04/2024 14:02)