ADMINISTRACION DE JUSTICIA

JDO.1A.INST.E INSTRUCCION N.4
AVILES
SENTENCIA: 00[redacted]/2024
C/ MARCOS DEL TORNIELLO 27 AVILES -
Teléfono: 985127829-28-27, Fax: 985127830
Correo electrónico: juzgado4.aviles@asturias.org
Equipo/usuario: LRI
Modelo: 0030K0
N.I.G.: 33004 41 1 2023 0006215
JVB JUICIO VERBAL 0000[redacted] /2023
Procedimiento origen: /
Sobre OTRAS MATERIAS
DEMANDANTE D/ña. [redacted]
Procurador/a Sr/a. [redacted]
Abogado/a Sr/a. [redacted]
DEMANDADO D/ña. UNICAJA BANCO S.A.
Procurador/a Sr/a. [redacted]
Abogado/a Sr/a.

SENTENCIA Nº [redacted]/2024

En Avilés, a dieciocho de abril de dos mil veinticuatro.

Vistos por mi, Dña. Lucia Rodríguez-Vigil Iturrate, Magistrada Juez del Juzgado de Primera Instancia nº 4 de los de Avilés y su Partido, los autos de Juicio Verbal con nº [redacted]/2023 sobre reclamación de cantidad, seguidos a instancia de D. [redacted], representado por la Procuradora de los Tribunales Dª [redacted] y asistido de la Letrada Dª [redacted], contra la entidad UNICAJA BANCO S.A, representada por la Procuradora de los Tribunales Dª [redacted] y asistida del Letrado D. [redacted], procedo a dictar Sentencia según los siguientes,

ANTECEDENTES DE HECHO

PRIMERO.- El día 10 de noviembre de 2023 se presentó ante el Decanato de esta localidad por la Procuradora de

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

los Tribunales Dª [redacted], en nombre y representación de D. [redacted], demanda de juicio verbal frente a la entidad UNICAJA BANCO S.A, que por turno de reparto correspondió a este Juzgado, en la que, con fundamento en los hechos y consideraciones legales que cita, se concluía suplicando se dictase sentencia por la que "*se condene a la entidad "UNICAJA BANCO, S.A." a abonar a mi mandante la cantidad de DOS MIL SEISCIENTOS TREINTA EUROS (2.630 €), en concepto de daños y perjuicios sufridos por el incumplimiento de la demandada de sus obligaciones contractuales, con más los intereses legales desde la fecha de la reclamación extrajudicial efectuada al Servicio de atención al cliente de la entidad bancaria (12/08/2022), todo ello con imposición a de costas a la demandada".*

SEGUNDO.- Admitida a trámite la demanda, se dio traslado de la misma a la parte demandada para que se personara y la contestase en el plazo de 10 días, habiendo evacuado este trámite en tiempo y forma.

TERCERO.- A continuación se citó a las partes para la celebración de vista, que tuvo con la presencia de todas ellas. Practicada la prueba declarada admitida, se dio por concluido el acto, quedando los autos en la mesa de su SSª para Sentencia.

FUNDAMENTOS DE DERECHO

PRIMERO.- La representación de D. [redacted] ejercita una acción de reclamación de cantidad, alegando, en esencia, los siguientes hechos, que la parte actora es

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

cliente de la entidad demandada desde hace años, como "cliente minorista".

D. [redacted], el día 5 de agosto de 2023 recibe un SMS dentro de la cadena de SMS que habitualmente utiliza la entidad UNICAJA para enviarle información. En dicho mensaje se le advertía que *"su cuenta estaba desactivada, por seguridad le rogamos que complete la siguiente verificación https://unicaja.es-area-privada.com/login".* A continuación recibió una llamada de un supuesto empleado del banco, en la que se le decía que se estaban efectuando movimientos de dinero desde Alicante en sus cuentas, y que residiendo en Asturias podían haberle hackeado las cuentas, por lo que para anular esos movimientos ilícitos debía facilitar las claves temporales que le irían llegado a su terminal móvil mediante tres SMS siendo que efectivamente en breves instantes (20:58 h) recibió los mismos facilitando las claves correspondientes como se le había solicitado.

A continuación D. [redacted] llama a las 21:03 horas al Servicio de Atención al Cliente de UNICAJA (952 076 263) para comprobar que los cargos se habían anulado, y se le contesta que desde UNICAJA BANCO no le habían requerido para nada pudiendo tratarse de una estafa.

La parte demandada se opuso a la pretensión de la parte actora. Asumiendo que el mismo había sido víctima de una estafa, niega cualquier tipo de responsabilidad, y sostiene que existe negligencia de la propia parte actora, que facilitó las claves a extraños para que pudieran ordenar las transferencias. Alego igualmente la existencia de prejudicialidad penal.

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

SEGUNDO.- Con carácter previo, y antes de entrar a resolver sobre el fondo del asunto, reiterando lo ya motivado de forma oral en el acto de la vista, corresponde el oportuno pronunciamiento sobre la alegada cuestión prejudicial penal al amparo del art. 40 de la LEC, concluyendo que no cabe apreciar la misma, pues no concurren los requisitos del art. 40 de la LEC. Como recuerda el AAP de Jaén, Secc. 1ª, de 22 de octubre de 2015, *Sobre la prejudicialidad penal, se exige, para que proceda su admisión, que conllevaría la suspensión del proceso civil mientras se tramite el proceso penal, los requisitos que se señalan en el artículo 40 de la Ley de Enjuiciamiento Civil. En concreto:*

a) que se acredite plenamente la existencia de un proceso penal.

b) que los hechos investigados en el proceso penal, con apariencia de delito sirvan de fundamento a las pretensiones de las partes en el proceso civil.

c) que la decisión del tribunal penal acerca del hecho por el que se procede en la causa criminal pueda tener una influencia decisiva en la resolución sobre el asunto civil.

En definitiva, se exige una especial coincidencia y conexión de los procesos, de ahí que se pregone esa nota de la imprescindibilidad de la causa penal, recogida en el artículo 40 de la Ley de Enjuiciamiento Civil y en el artículo 10 de la Ley Orgánica del Poder Judicial, en orden a evitar que, por el perjuicio que se produciría a la seguridad jurídica, nos pudiéramos encontrar con Sentencias contradictorias dictadas por órganos de distintos órdenes jurisdiccionales. En este sentido, la Sentencia de 5 de diciembre de 1.996 declara que "la relación existente entre los mencionados artículos 114 (L.E.Cri.) y 10 (L.O.P.J.) evidencia que la medida de suspensión está vinculada a la imposibilidad de prescindir de la existencia de la cuestión penal para la debida decisión de

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

la planteada en el civil o de que esta venga condicionada por el contenido de aquélla". En parecidos términos declara la Sentencia de 21 de septiembre de 1.998 que: "Y ello, por la sencilla razón - añade esta Sala del Tribunal Supremo - de que, mientras subsista el proceso penal , la existencia misma del "hecho histórico" que motiva las actuaciones están "sub judice", con el efecto, además, de vincular absolutamente al Tribunal de lo civil, en lo establecido por la jurisdicción penal -(artículo 116 de la Ley de Enjuiciamiento Criminal), a diferencia, de lo que ocurre si reconocida la existencia del hecho básico, el juez de lo civil formula con arreglo a las normas sustantivas y procesales civiles, cuya aplicación le corresponde, enfoque y consecuencias inculpatorias distintas de las penales". En idénticos términos se pronuncian las Sentencias de 20-4-79, 21-6-85, 31-1-86, 21-9-98 y 19-12-01".

En nuestro caso, ni consta que haya un proceso penal abierto (sólo una denuncia), ni cabe apreciar la imprescindibilidad de la causa penal para resolver el presente asunto. Máxime cuando la propia parte demandada viene a reconocer que el demandante pudo ser víctima de un engaño por tercero/s.

Y ello porque, una cosa es que la investigación penal lleve a determinar el destino último del dinero y el autor o autores del engaño, y otra diferente es valorar si hay responsabilidad por parte de la demandada en sus obligaciones para con la demandante, precisamente porque terceros pudieron hacer que la misma accediera a su banca online y, bajo engaños, le llevaran a ordenar varias transferencias. Aun cuando las diligencias penales dieran lugar a una causa penal en un Juzgado, y en el seno de la misma una persona fuera identificada como autor, ello ni incide ni condiciona la

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

resolución de la controversia planteada en vía civil. No hay posibilidad de sentencias contradictorias, y la demandada siempre podría reclamar como perjudicada (si tiene que responder de esas transferencias fraudulentas) al autor de la infracción penal.

TERCERO.- Sentado lo anterior, aunque ninguna de las partes lo hace constar así expresamente, no cabe duda de que media entre los mismos sendos contratos de cuenta corriente. Ello no es controvertido.

Como viene recordando la jurisprudencia, estamos ante un contrato atípico que en los últimos años ha ido adquiriendo autonomía respecto del contrato de depósito que le servía de base, y que encuentra su singularidad en el "servicio de caja" que, también según la jurisprudencia, ha de ser encuadrado en nuestro sistema dentro del marco general del contrato de comisión mercantil (Sentencias de 15 de julio de 1993 , de 19 de diciembre de 1995 , de 9 de octubre de 1997) que, en definitiva pertenece al que pudiéramos llamar "género del mandato ": una relación gestoría, un contrato de gestión, en utilidad del cliente que implica un servicio (un facere útil, caracterizado por la alienidad del resultado) por cuyo desarrollo la entidad bancaria o financiera percibe una remuneración.

De tal relación derivan los deberes de rendición de cuentas, de información (artículos 263 CCom y 1720 CC , un deber reforzado por la Ley 26/1988 de 29 de julio, de Ordenación bancaria e intervención de las Entidades de Crédito), y entre ellos los deberes de actuar conforme a las instrucciones recibidas y, en todo caso, con la diligencia quam in suis (artículo 255 CCom), pues se responde por culpa,

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

cuyo rigor será medido por el parámetro de que se trate o no de un mandato retribuido (artículo 1726 CC).

Dentro de estos deberes adquiere especial relevancia el deber de diligencia de la entidad depositaria y gerente del "servicio de caja", que no se trata de la diligencia de un buen padre de familia, sino la que corresponde a un "comerciante experto", pues actúa en virtud de la relación de depósito y comisión y "encuentra buena parte de su fundamento en lucro que en tales cometidos obtiene la entidad bancaria, como señala la STS de 15 de julio de 1998." (En tal sentido, además, de la SAP de Alicante ya citada, la SAP de Sevilla, Secc. 6ª, de fecha 27 de julio de 2022, o la SAP de Jaén, Secc. 1ª, de 26 de enero de 2022).

En este marco contractual, lo que no hay duda es que la transferencia es un servicio que forma parte del servicio de caja, es un medio de pago consistente en una orden dada al banco por el cliente a fin de que, con cargo a su cuenta abone un determinado importe a un beneficiario o al propio ordenante. Y es hecho no controvertido, y que en cualquier caso se infiere de la documental aportada por las partes, que en fecha 5 de agosto de 2022, D. [redacted] recibe un mensaje (fraudulento) en el que se le informa de que "Le informamos que su cuenta está desactivada, por seguridad le rogamos que complete la siguiente verificación aquí:https://unicaja.es-area-privada.com/login"", pinchó el enlace que contenía el mismo SMS, recibiendo posteriormente una llamada , supuestamente del banco, para informarle que había movimientos extraños en su cuenta, y que para bloquearlos tendría que facilitar unas claves que le mandarían, acto seguido por SMS, facilitando las mismas a su interlocutor.

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

Tras ello, y al llamar al servicio de atención al clienta para verificar que se habían anulado unas supuestas transferencia se dio cuenta que había sido víctima de una estafa

CUARTO.- Con carácter previo conviene referirse al marco normativo existente, y aplicable a supuestos como el de autos, en especial la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior, que en su considerando 72 dispone 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. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros. Se deben considerar nulas las cláusulas contractuales y las condiciones de prestación y utilización de instrumentos de pago mediante las cuales aumente la carga de la prueba sobre el consumidor o se reduzca la carga de la prueba sobre el emisor. Además, en situaciones específicas y, más concretamente, cuando el instrumento de pago no esté presente en el punto de venta, como en el caso de los pagos en línea, resulta oportuno que el proveedor de servicios aporte pruebas de la presunta negligencia, puesto que los medios a disposición del ordenante son limitados en esos casos.*

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

Esta Directiva se complementa con el Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 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. En su artículo 1° el citado Reglamento establece cuales son 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.

Su artículo 2° establece los requisitos los generales de autenticación, disponiendo que "*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*

PRINCIPADO DE ASTURIAS

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.

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.

En la normativa nacional hay que remitirse al RDL 19/2018, de 23 de noviembre se regulan las obligaciones del proveedor y del usuario de los servicios de pago y el régimen de responsabilidad de ambos, así como la carga de la prueba de tales circunstancias que, en lo que aquí respecta, son:

- art. 41 (obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas): utilizar el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago y, en particular, en cuanto reciba un instrumento de pago, tomar todas las medidas

ADMINISTRACION DE JUSTICIA

razonables a fin de proteger sus credenciales de seguridad personalizadas;

- art. 42 (obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago): El proveedor de servicios de pago emisor de un instrumento de pago 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;

- art. 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

PRINCIPADO DE ASTURIAS

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".

- art. 45.1 (Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizada:"*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 (...) 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*"

- art. 46 (Responsabilidad del ordenante en caso de operaciones de pago no autorizadas): *"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 (...)"*

- art. 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. 2. En lo que se refiere a la iniciación de las operaciones de pago electrónico mencionada en el apartado 1, letra b) respecto de las operaciones remotas de pago electrónico, los proveedores de servicios de pago aplicarán una autenticación reforzada de clientes que incluya elementos que asocien dinámicamente la operación a un importe y un beneficiario determinados. 3. En los casos a los que se refiere el apartado 1, los proveedores de servicios de pago contarán con medidas de seguridad adecuadas para proteger la confidencialidad y la integridad de las credenciales de seguridad personalizadas de los usuarios de los servicios de pago. 4. Los apartados 2 y 3 se aplicarán asimismo cuando los pagos se inicien a través de un proveedor de servicios de iniciación de pagos. Los apartados 1 y 3 se aplicarán asimismo cuando la información se solicite a través de un proveedor de servicios de pago que preste servicios de información sobre cuentas. (...)".

De esta manera, 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, en su caso, el fraude (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) o 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).

ADMINISTRACION DE JUSTICIA

QUINTO.- Pues bien, de la prueba practicada, consta acreditado que la parte demandante recibió un SMS dentro de la cadena de SMS que habitualmente utiliza la entidad UNICAJA para enviarle información. En dicho mensaje se le advertía que "*su cuenta estaba desactivada, por seguridad le rogamos que complete la siguiente verificación https://unicaja.es-area-privada.com/login*"

Dicho enlace llevaba a una "App espejo", idéntica a la de la entidad bancaria donde habría que introducir todas las claves de acceso a la banca on line por parte del cliente. Hecho que consta en la documental aportada junto con el escrito de demanda.

Consta igualmente que ese mismo día recibió una llamada de un supuesto empleado del banco en la que se le decía que se estaban efectuando movimientos de dinero desde Alicante en sus cuentas, y que residiendo en Asturias podían haberle hackeado las cuentas, por lo que para anular esos movimientos ilícitos debía facilitar las claves temporales que le irían llegado a su terminal móvil mediante tres SMS siendo que efectivamente en breves instantes (20:58 h) recibió los mismos facilitando las claves correspondientes como se le había solicitado. No consta que en esa llamada el actor hubiera facilitado su usuario y contraseña.

A continuación D. [redacted] llama a las 21:03 h al Servicio de Atención al Cliente de UNICAJA (952 076 263) para comprobar que los cargos se habían anulado y se le contesta que desde UNICAJA BANCO no le habían requerido para nada pudiendo tratarse de una estafa. Hechos estos que quedan corroborados con el cronograma de las llamadas y mensajes recibidos por la parte actora.

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

No se observa por quien suscribe, fraude, negligencia grave ni incumplimiento por parte del demandante en el comportamiento que sostuvo.

No hay duda, y así lo reconoce el propio banco, que pudiéramos estar ante un supuesto de estafa. El método utilizado puede enmarcarse dentro del phishing (o alguna variante del mismo conocidas como Smishing y/o Vishing). El primero de ellos es un tipo de ataque de ingeniería social que se realiza a través de la mensajería del teléfono móvil o por SMS. El objetivo es obtener información personal, contraseñas, números de tarjetas de crédito y/o números de cuentas bancarias y en general cualquier tipo de información sensible o confidencial que permite a los ciberdelincuentes cometer estafas o fraudes electrónicos. Para conseguir su propósito, el atacante utilizará la suplantación de identidad de personas y organizaciones. De forma que en el caso de que quieran obtener la información bancaria de sus víctimas para cometer una estafa o fraude, los atacantes enviarán mensajes SMS haciéndose pasar por la entidad bancaria de la víctima (SMS Spoofing) para obtener las credenciales de acceso a su banca electrónica (usuario y contraseña) y el código de un solo uso que se envía al móvil de usuario para confirmar el acceso. En el Vishing, el contacto se realiza a través de llamadas telefónicas, donde el atacante suplanta la identidad de una empresa, organización o incluso de una persona de confianza, con el fin de obtener información personal de sus víctimas.

Es decir, si D. [redacted] accedió al enlace y/o facilitó las claves recibidas por SMS con las que se hicieron efectivas las operaciones bancarias, es porque previamente había recibido una alerta en su móvil sobre la desactivación de su cuneta, y se le advirtió desde la cuenta

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

suplantada que para cancelar las disposiciones debía introducir la clave recibida vía SMS. Así las cosas, no puede sostenerse falta de prudencia por parte del consumidor.

Es más, establece el art. 44.1 que 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.

Y es claro que en nuestro caso sí que hubo un fallo por el proveedor del servicio de pago, pues personas ajenas al banco, vulnerando sus sistemas de seguridad, fueron los que mandaron el supuesto enlace para desbloquear la cuenta, origen de la estafa.

A mayor abundamiento, y como nos recuerda la SAP de Zaragoza, Secc. 5ª, de fecha 1 de julio de 2022, hay que hacer hincapié en las medidas de seguridad que debe adoptar la entidad oferente del servicio de pago online (banca online). Así, por referencia a la SAP Alicante, secc.8ª 107/2018, de 12 de marzo, recuerda que:

Parte del R.D. legislativo 1/2007 en su art. 147 (responsabilidad de los prestadores de servicios, salvo prueba de cumplimiento de exigencias reglamentarias y demás cuidados que exige la naturaleza del servicio). Precepto interpretado por la S.T.S. 185/2016, de 18 de marzo que llama a ponderar la causa del evento dañoso, si había o no un déficit de la seguridad que legítimamente cabía esperar y la facilidad probatoria correspondiente a cada una de las partes (art. 217.7 LEC)

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

Se trata, pues, de una responsabilidad cuasi-objetiva del proveedor de los servicios de pago.

[…]"Tanto en banca telefónica como por internet, el proveedor de servicios de pago, o lo que es lo mismo, el banco emisor, debe implementar las medidas necesarias para asegurar la autenticación e identidad del ordenante a la hora de prestar su consentimiento"

En caso contrario, le corresponde a dicha entidad la devolución de lo ilícitamente obtenido de la cuenta del cliente (arts. 30 y 31 LSP, actualmente Arts. 36 y siguientes del R.D. ley 19/2018, de 23 de noviembre, trasposición de la Directiva UE 2015/2366, del Parlamento y del Consejo de 25 de noviembre 2015 sobre servicios de pago).

No basta, pues, con medidas genéricas de protección o avisos estereotipados de cuidado, sino que -sigue razonando la SAP Alicante 8ª, 107/2018 - la seguridad de las operaciones bancarias precisa de soluciones tecnológicas avanzada a los efectos de garantizar tanto la autenticidad como la integridad y confidencialidad de los datos.

Considera que los avisos genéricos de los bancos, a través de su web, no suplen los deberes contractuales de las partes, ni la implementación de medidas de seguridad eficaces. Tales avisos ostentarían la calificación de " formulas predispuestas", vacías de contenido.

No son los clientes los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, ni prevenir con su asesoramiento experto dichos riesgos. No se puede objetar al usuario que debía conocer aspectos técnicos tales como identificar una web falsa (salvo supuestos de evidentes falsedad) u otros fallos técnicos)".

Haciendo propias dichas conclusiones, estando claro que la parte demandante fue víctima de un fraude, y por todo lo

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

expuesto, debe estimarse la pretensión de la misma , condenando a la entidad demandada a que abone las cantidades reclamadas, más los correspondientes intereses legales devengados por dichas cantidades hasta su completo pago. Ello por aplicación del art. 1.100 del CC, y el art. 45 del Real Decreto-ley más arriba citado (constando la reclamación fehaciente al banco el día 14 de diciembre).

Por todo lo anteriormente expuesto procede estimar la pretensión ejercitada por la parte actora, debiendo la parte demandada devolver al cliente la suma de las operaciones no autorizadas, y que ascienden a 2630 euros.

QUINTO.- *Costas*.- Conforme a lo dispuesto en el art. 394.1 de la LEC, en los procesos declarativos, las costas de la primera instancia se impondrán a la parte que haya visto rechazadas todas sus pretensiones, salvo apreciación de serias dudas de hecho o de derecho.

Dado que no se han apreciado en este proceso serias dudas de hecho ni de derecho, y que las pretensiones de la parte actora han sido íntegramente estimadas corresponde imponer las costas a la demandada.

Vistos los preceptos legales invocados, y demás normas de general y pertinente aplicación,

FALLO

ESTIMANDO INTEGRAMENTE la demanda de juicio verbal interpuesta por D. [redacted] contra la entidad UNICAJA BANCO S.A, debo **CONDENAR y CONDENO** a esta última a que abone a la parte actora la cantidad de dos mil seiscientos treinta euros (2.630 €), más el interés legal

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

desde la reclamación extrajudicial de fecha agosto de 2023), así como al pago de las costas causadas en el procedimiento.

Notifíquese esta resolución a las partes haciéndoles saber que la misma es firme y que contra ella no podrán interponer recurso alguno de conformidad con lo dispuesto en el artículo 455 y siguientes de la Ley de Enjuiciamiento Civil.

Así por esta mi Sentencia, la pronuncio, mando y firmo.

PRINCIPADO DE ASTURIAS