BASE DE DATOS DE Norma CEF.-
Referencia: NCJ067354

AUDIENCIA PROVINCIAL DE OVIEDO

Sentencia 142/2024, de 21 de marzo de 2024
Sección 4.ª
Rec. n.º 89/2024

SUMARIO:

Contratos bancarios. Servicios de pago. Estafa informática mediante la apropiación de datos personales (correos electrónicos y SMS suplantando a la proveedora de servicios de pago). Spoofing. Transferencia. Obligaciones y responsabilidad del proveedor de servicios de pago.
Condenada a la entidad bancaria a pagar 6.000 euros a un usuario que fue víctima de una estafa de suplantación de identidad conocida como «SMS spoofing». El perjudicado recibió un SMS, aparentemente del banco del que era cliente, que decía: AVISO: un acceso no autorizado está conectado a su cuenta online. Si no reconoce este acceso verifique inmediatamente: tras pinchar en el enlace le llegó un nuevo mensaje con el texto: «Unicaja Banco: Introduce la clave de seguridad para finalizar con la vinculación de dispositivo de Banca Digital». Poco después le informaba que había ejecutado una transferencia por importe de 6.000 euros, que en realidad no había sido ordenada por él sino por un tercero que había obtenido sus datos bancarios y la autorización para realizarla. La entidad admite que el primer paso de facilitar las claves de usuario y contraseña cuando recibió el primer mensaje pudiera no ser suficiente para calificarlo de negligencia grave. No obstante, mantiene que el segundo paso que dio el perjudicado cuando autorizó la vinculación de otro dispositivo es el que permitió llevar a cabo la operación fraudulenta.
El magistrado destaca que, según el informe policial, la modalidad de fraude utilizado es la más avanzada, conocida como «SMS spoofing» mediante la cual el autor de la estafa suplanta el ID de los SMS de la entidad bancaria, de forma que es prácticamente imposible que el teléfono del perjudicado catalogue tales mensajes como fraudulentos o spam, generando la confianza de la víctima en su autenticidad.
Esa responsabilidad se acentúa aún más cuando el proveedor no exige una «autenticación reforzada del cliente, supuesto en que éste último únicamente responde de haber actuado de forma fraudulenta». El Banco no solo no ha demostrado que el cliente hubiera incurrido en negligencia grave en el proceso que desembocó en la estafa, sino que todo apunta a un déficit del sistema de seguridad de la propia entidad bancaria para evitar esta clase de ataques informáticos. Se establece por tanto 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.
La actuación del usuario no puede calificarse de «temeraria ni gravemente negligente» a la vez que no puede exigirse a quien resultó engañado mayor precaución que a quien debía poner los medios necesarios para evitarlo. Condena al banco tras razonar que existió un incumplimiento contractual por su parte al no haber comprobado la autorización de la orden de pago y no disponer de un adecuado sistema de seguridad que previniera este tipo de órdenes fraudulentas. 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.

PRECEPTOS:

RDL 19/2018 (Servicios de pago), arts. 41, 42.1 a), 43.1, 44, 45.1 y 46.1.3.º.

PONENTE:

Don Francisco Tuero Aller.

AUD.PROVINCIAL SECCION CUARTA

OVIEDO

SENTENCIA: 00142/2024

Modelo: N10250

C/ CONCEPCIÓN ARENAL Nº 3 - 3

Teléfono: 985968737 Fax: 985968740

Correo electrónico:

Equipo/usuario: CRR

N.I.G. 33037 41 1 2023 0001135

ROLLO: RPL RECURSO DE APELACION (LECN) 0000089 /2024

Juzgado de procedencia: JDO.1A.INST.E INSTRUCCION N.3 de MIERES

Procedimiento de origen: JVB JUICIO VERBAL 0000370 /2023

Recurrente: UNICAJA, S.A.

Procurador: NURIA MARIA ALVAREZ-TIRADOR RIERA

Abogado: ISABEL ALVAREZ GARCIA

Recurrido: UNIÓN DE CONSUMIDORES DE ASTURIAS

Procurador: TOMAS GARCIA-COSIO ALVAREZ

Abogado: JOSE ANTONIO BALLESTEROS GARRIDO

NÚMERO 142

En OVIEDO, a veintiuno de marzo de dos mil veinticuatro, el Ilmo. Sr. D. FRANCISCO TUERO ALLER , Magistrado de la Sección Cuarta de la Ilma. Audiencia Provincial de Oviedo, actuando como órgano unipersonal designado para el conocimiento del presente recurso, ha pronunciado la siguiente

SENTENCIA

En el recurso de apelación número 89/2024, en autos de JUICIO VERBAL Nº 370/2023, procedentes del Juzgado de Primera Instancia número tres de los de Mieres, promovido por UNICAJA, S.A., demandada en primera instancia, contra UNIÓN DE CONSUMIDORES DE ASTURIAS, quien actúa en representación de su socio D. Federico, demandante en primera instancia.

ANTECEDENTES DE HECHO

Primero.

Por el Juzgado de Primera Instancia número tres de los de Mieres se dictó Sentencia con fecha 21 de diciembre de 2023, cuya parte dispositiva es del tenor literal siguiente:

"Que estimo íntegramente la demanda presentada por UNIÓN DE CONSUMIDORES DE ASTURIAS, en representación de su socio D. Federico contra UNICAJA BANCO S.A., condenando a esta a abonar a aquel la cantidad de 6.000 euros a la parte actora, junto con los intereses legales de dicha cantidad desde la fecha de la reclamación extrajudicial (6/7/2022); todo ello con expresa condena en costas a la parte demandada.".

Segundo.

Contra la expresada resolución se interpuso por la parte demandada recurso de apelación, del cual se dio el preceptivo traslado, y remitiéndose los autos a esta Audiencia Provincial se sustanció el recurso, y constituido el

Tribunal con un solo Magistrado, se señaló para la decisión del presente recurso el día diecinueve de marzo 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 el demandante, D. Federico, fue víctima de una estafa informática en junio de 2022, ni tampoco el medio como se llevó a cabo, a través de los siguientes pasos: En primer término D. Federico recibió un SMS, aparentemente del Banco del que era cliente, aquí demandado, en los siguientes términos "AVISO: un acceso no autorizado está conectado a su cuenta online. Si no reconoce este acceso verifique inmediatamente: https:/is.gd/Clientes_Unicaja"; a continuación clicó en el enlace y le llegó otro nuevo SMS del siguiente tenor: "Unicaja Banco: Introduce la clave de seguridad NUM000 para finalizar con la vinculación de dispositivo de Banca Digital"; pocos minutos después el Banco le informaba que había ejecutado una transferencia por importe de 6.000 €, que en realidad no había sido ordenada por él sino por un tercero defraudador, que había obtenido los datos bancarios del demandante y la autorización para realizar la operación en la forma indicada. Reclama D. Federico en este juicio la restitución de la indicada suma que le fue sustraída, con sus intereses.

La sentencia de primer grado, partiendo de la normativa establecida en el Real Decreto-Ley 19/2018, de 23 de noviembre, estimó la demanda tras razonar que existió un incumplimiento contractual por parte del Banco al no haber comprobado la autorización de la orden de pago y no disponer de un adecuado sistema de seguridad que previniera este tipo de órdenes fraudulentas.

A través del presente recurso el Banco admite que el primer paso dado por el demandante, al facilitar las claves de usuario y contraseña de su Banca a Distancia cuando recibió el primer mensaje fraudulento, pudiera no ser suficiente para calificarlo de negligencia grave, aunque no fuera "la mejor de las decisiones". Pero sostiene que sí merece ese calificativo el segundo paso dado por D. Federico, cuando tras recibir la clave de seguridad, autorizó la vinculación de otro dispositivo, que permitió llevar a cabo la operación fraudulenta mediante la clave OTP.

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") o bien a través de SMS fraudulentos como en este caso ("smishing"), con el objetivo final de que los clientes proporcionen sus datos de carácter personal y claves bancarias para acceder así a sus cuentas de forma fraudulenta. La excusa frecuentemente utilizada, como sucedió en este caso, es la de informar sobre un acceso no autorizado a 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. Según informe policial obrante en autos, la modalidad utilizada en este caso fue la más avanzada conocida como SMS SPOOFING, mediante la cual el autor de la estafa suplanta el ID de los SMS de la entidad bancaria, de forma que es prácticamente imposible que el terminal telefónico del perjudicado catalogue tales mensajes como fraudulentos o spam, generando la confianza de la víctima en su autenticidad.

Es de destacar, por otra parte, que según ese informe policial, en fechas coincidentes con la del acto aquí enjuiciado se produjeron numerosísimas denuncias por hechos similares con relación a la misma entidad bancaria, que pocos días antes había procedido a la integración tecnológica y operativa, o fusión informática, como consecuencia del proceso de fusión y absorción de otras entidades.

Tercero.

Como decíamos en sentencia de 13 de diciembre de 2023, 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.

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".

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 desestimado, por cuanto el Banco no solo no ha demostrado que el cliente hubiera incurrido en negligencia grave en el proceso que desembocó en la estafa, sino que todo apunta a un déficit del sistema de seguridad de la propia entidad bancaria para evitar esta clase de ataques informáticos. Y así:

1º) Ya se ha dicho que ni siquiera el apelante califica de negligencia grave la primera actuación del demandante, al clicar sobre el enlace que aparecía en el primer mensaje. Y que ello es así se desprende sin lugar a dudas por la imposibilidad para el cliente, o para su terminal telefónico, de percibir que se estaba ante un SMS fraudulento, dada la técnica utilizada de SPOOFING, pues el estafador utilizaba el propio ID de la entidad bancaria. Actuación la del cliente, por lo demás lógica ante la alerta, que se suponía enviada por el Banco, de que alguien no autorizado había entrado en su cuenta online.

2º) En coherencia con lo anterior, introdujo a continuación la clave de seguridad que le fue facilitada por el Banco con el fin de "finalizar con la vinculación de dispositivo a Banca Digital". No se advertía entonces, como pretende la apelante, de que se trataba de vincular otro dispositivo distinto, circunstancia que podría haber generado desconfianza en el cliente, sino que se hablaba solo de dispositivo, sin indicar cual fuera, de tal modo que lo que hubo de presumir éste es que se trataba del propio, que había que vincular de nuevo dado el acceso no autorizado del que había sido informado. No es cierto, en consecuencia, que el demandante hubiera introducido la clave OTP necesaria para llevar a cabo la concreta operación, la transferencia indicada, sino que, una vez vinculado el dispositivo que utilizaba el ciberdelincuente, a éste le serían remitidas las claves necesarias para las nuevas operaciones que deseara realizar, y no a quien aquí acciona.

En definitiva, este segundo paso venía precedido y motivado por el engaño ya consumado con el primer SMS, y estaba sin duda guiado por el ánimo de evitar lo que, desgraciadamente, se perseguía con él, por lo que esa actuación 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

3º) Concurren, además, otros datos que apuntan a la responsabilidad de la demandada en lo sucedido. Ella misma señala en el escrito de contestación que seis meses antes, el 11 de enero de 2022, el Banco de España se había hecho eco de esta clase de delitos, informando de las nuevas modalidades de smishing y spoofing. Y, sin embargo, no adoptó las técnicas o medidas de seguridad que fueran suficientes para evitar que se produjeran esta clase de fraudes en su ámbito de actuación, al menos hasta que sucedieron los hechos controvertidos, como lo demuestra que siguieran teniendo lugar. Es más, el gran número de estafas cometidas por este medio en pocos días con relación a esta misma entidad bancaria evidencia la falta de medidas o la quiebra de las que pudiera haber tomado, pues difícilmente puede sostenerse que un gran número de usuarios hubieran incidido casi simultáneamente en una conducta gravemente negligente en sus interacciones con el Banco.

Incluso las particularidades del caso (transferencia con carácter inmediato, por importe de relativa importancia, desde un nuevo dispositivo que acaba de vincularse a la banca digital, a favor de una financiera extranjera de dinero electrónico), tan poco usuales en la práctica, debía haber permitido al Banco detectar que se estaba ante un posible fraude.

En resumen, como también señalábamos en la repetida sentencia de 13 de diciembre de 2023, 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 desestimación del recurso comporta la imposición al apelante de las costas aquí causadas (art. 398 LEC).

En atención a lo anteriormente expuesto,

FALLO

Desestimar el recurso de apelación interpuesto por UNICAJA S.A. frente a la sentencia dictada el 21 de diciembre de 2023 por el Juzgado de Primera Instancia número tres de Mieres en autos de Juicio Verbal núm. 370/2023, que se confirma íntegramente, con expresa imposición de costas a la parte recurrente.

Dese el destino legal al depósito constituido para recurrir.

Contra esta resolución no cabe recurso (art. 477.1º de la Ley de Enjuiciamiento Civil).

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