Roj: **SAP GR 957/2022** - **ECLI:ES:APGR:2022:957**

Id Cendoj: **18087370052022100140**
Órgano: **Audiencia Provincial**
Sede: **Granada**
Sección: **5**
Fecha: **20/06/2022**
Nº de Recurso: **85/2022**
Nº de Resolución: **212/2022**
Procedimiento: **Recurso de apelación**
Ponente: **FRANCISCO SANCHEZ GALVEZ**
Tipo de Resolución: **Sentencia**

AUDIENCIA PROVINCIAL DE GRANADA

SECCIÓN QUINTA

[redacted]

JUZGADO DE PRIMERA INSTANCIA E INSTRUCCIÓN Nº 2 DE LOJA

ASUNTO: JUICIO ORDINARIO-OBLIGACIONES

PONENTE SR. D. [redacted]

S E N T E N C I A N Ú M.212/2022

ILTMOS. SRES.PRESIDENTAª [redacted] **MAGISTRADOSD.** [redacted] **D.** [redacted]

En la ciudad de Granada, a veinte de junio de dos mil veintidós.

La Sección Quinta de esta Audiencia Provincial constituida con los Iltmos. Sres. al margen relacionados ha visto en grado de apelación el recurso de apelación Nº 85/2022, dimanante de los autos con número 42/2021. Interpone recurso "CAJA RURAL DE GRANADA, SOCIEDAD COOPERATIVA DE CRÉDITO", representada por el Procurador D. [redacted]. Comparecen como apelados Dª [redacted] y D. [redacted], representados por la Procuradora Dª [redacted].

ANTECEDENTES DE HECHO

PRIMERO.- El Juzgado de Primera Instancia dictó sentencia el día 28 de diciembre de 2021, en cuya parte dispositiva se acuerda: *" Que **estimando** la demanda formulada por el Procurador de los Tribunales Dª* [redacted] *, en nombre y representación de D.* [redacted] *y Dª* [redacted] *, contra CAJA RURAL DE GRANADA SCC, debo declarar la responsabilidad de la demandada en la incorrecta ejecución de las operaciones de transferencia realizadas el 23 de Marzo de 2020 y, en consecuencia, debo condenar y condeno al demandado a abonar a los actores la cantidad de **siete mil ochocientos once con sesenta y ocho euros (7811,68 euros)** correspondientes a los cargos en cuenta por las operaciones ejecutadas así como a los intereses legales de dicha cantidad desde la fecha de su cargo en cuenta. Sin condena en costas procesales "*

SEGUNDO.- Interpuesto recurso de apelación y admitido a trámite, el Juzgado realizó los preceptivos traslados y una vez transcurrido el plazo elevó los autos a esta Sección de la Audiencia, donde se formó rollo y se ha turnado de ponencia. La votación y fallo ha tenido lugar el día 31 de mayo de 2022.

TERCERO.- En la tramitación del recurso se han observado las prescripciones legales.

Visto, siendo ponente el Ilmo. Sr. Magistrado D. [redacted] quien expresa el parecer del Tribunal.

FUNDAMENTOS DE DERECHO

[redacted]

PRIMERO.- En nombre de "Caja Rural de Granada Soc. Coop. de Crédito" se interpone recuso de apelación impugnando el pronunciamiento condenatorio dictado en su contra como consecuencia de la realización de varios pagos fraudulentos y transferencias efectuadas con el número de la tarjeta de débito de la actora, Dª [redacted] , con el código de verificación y la clave personal, que había sido obtenida mediante el procedimiento de phishing.

Aduce la apelante, en síntesis, que se incurre en la sentencia en error en la valoración de la prueba y que se vulnera el art. 217 de la LEC, haciendo hincapié en que la Dª [redacted] es una joven que realiza compras diarias y transferencias en distintas páginas web, lo que motivó, precisamente, la ampliación del límite de compras de 600 a 6000 €, y que el mensaje recibido que le invitaba a pinchar en el enlace se trataba de un burdo email con links publicitarios de cocinas francesas, proveniente de spoex3@hotmail.com, mal redactado, con expresiones como "Gracias a no responder a este mensaje, usted no tendrá que responder" y en el que no aparecía dato alguno que le diera apariencia de ser la web de la entidad, habiendo introducido la actora los siguientes datos para activar la tarjeta que se le decía bloqueada en dicho mensaje:

- Usuario [redacted].
- NIF
- Contraseña [redacted].
- Clave Firma [redacted].
- Número de tarjeta.
- Fecha de Caducidad.
- CVV

Tras hacerlo la página se cerró, y sin verificación de ningún tipo, la actora dio por finalizada la activación de su tarjeta, por lo que mantiene que no observó el deber de diligencia exigible, similar al de custodia del número secreto de las tarjetas de crédito; y añade que Caja Rural de Granada alerta del peligro de phishing en su página web, invocando también la notoriedad y conocimiento del método phishing y que se trata de una usuaria habitual de internet, por lo que estima que cometió un grave imprudencia rellenando datos innecesarios para activar una tarjeta e incumpliendo, de una manera grave, las obligaciones que impone el artículo 27 de la Ley 16/2009 de utilizar el instrumento de pago de conformidad con las condiciones que regulan su emisión o utilización.

Considera errónea también la sentencia porque, tras reconocer que la cliente incurrió en negligencia, imputa la responsabilidad a la apelante porque se llegó a superar el límite de disposición diario de 6.000 euros, pero es un dato incorrecto porque los apuntes en cuenta muestran que las transferencias realizadas pertenecen a dos días distintos, concretamente la fecha de valor es del 21 y 22 de marzo de 2020, independientemente de que el apunte contable se realice el lunes, 23 de marzo (al ser 21 y 22, sábado y domingo), no llegando a superar el límite diario de compras con la tarjeta de débito de 6000 euros en ningún momento, a lo que se añade que además del uso de la tarjeta, se realizaron transferencias; al igual que considera que no le es reprochable que pusiera limitaciones al uso porque sí las hubo, y fue la propia clienta la que elevó de 600 a 6000 € diarios haciendo uso intensivo de la banca electrónica.

También rechaza la imputación de ausencia de control por la compra en páginas extranjeras de dudosa identificación, puesto que tanto el banco suizo al que se realizaron transferencias -Swiss Bankers-, como la web my.pocket.io de Reino Unido, son entidades legales con una identificación clara; y concluye que no se identifica un criterio de responsabilidad de la entidad; que no ha existido ninguna anomalía, déficit de seguridad, ni prueba de la causa concreta en este sentido, y sí de la negligencia de la actora.

Se opone al recurso la representación de la apelada, alegando que el email que le aparece en su móvil tiene apariencia de proceder de la entidad apelante, siendo el caso que la información relativa a los link publicitarios proviene de la investigación de la Guardia Civil, habiéndose recibido desde la dirección *"Ruralvia Caja Rural <spoex3@hotmail.com>",* siendo el caso que los hechos se producen durante el confinamiento por COVID 19 y que el email se recibe en fin de semana, estando las entidades bancarias cerradas, a pesar de lo cual se informó tan solo dos días después, lo que descarta que concurra negligencia grave; habiendo de tenerse en cuenta las técnicas utilizadas para ganarse su confianza, invocando a tal efecto el considerando 72 de la Directiva (UE) del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior, en relación con la valoración de la negligencia del usuario de servicios de pago; y sostiene que se obvia referir los requisitos que han de cumplir los proveedores de servicios de pago a efectos de aplicación de medidas de seguridad, que se encuentran regulados legalmente y detallados en la sentencia de instancia, concretamente sobre la autenticación reforzada, conforme al Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de

noviembre de 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo y al Real Decreto Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que lo incorpora a nuestra legislación, insistiendo en que el límite de la tarjeta fue sobradamente superado, y que se omite el hecho de que las transferencias fueron realizadas desde el terminal telefónico número NUM000 , que no se corresponde con ninguno de los teléfonos habilitados en los contratos de tarjeta de crédito que obran en las actuaciones ([redacted] en el caso de [redacted] ; y [redacted] en el caso de don [redacted]).

SEGUNDO.- Aunque se impugna por la apelante la valoración de la prueba, realmente vienen a asumirse los hechos que se declaran probados en la sentencia apelada, con arreglo los cuales:

1º.- En fecha 15 de octubre de 2019, doña [redacted] concertó con "Caja Rural de Granada Soc. Coop. de Crédito" contrato de tarjeta de débito para consumidores, con tarjeta número [redacted] , vinculada a la cuenta número [redacted] , cuyo titular es don [redacted] , padre de doña [redacted] .

2º.- El 21 de marzo de 2020 [redacted] recibió un correo electrónico en su teléfono móvil desde Ruralvia Caja Rural, con el hashtag "#estimadocliente", por el que se le informaba de que "por razones de seguridad hemos bloqueado su tarjeta temporalmente. Para activar su tarjeta nuevamente le invitamos a hacer clic en el enlace a continuación#". El correo electrónico fue recibido el sábado 21 de marzo a las 16,18 horas, desde una dirección identificada como *"Ruralvia Caja Rural <spoex3@hotmail.com>"* .

3º.- El límite diario para disponer en compras con la tarjeta de débito es de 6000 € , y la actora, tras recibir el correo electrónico, procedió a acceder a la página que le dirigió el enlace, identificándose y procediendo a dar todos sus datos de identificación, tales como número de usuario, DNI y contraseña y firmar el cambio con la clave de firma.

4º. Finalmente fueron sustraídas de la cuenta asociada las cantidades de 1.500 €, 500 €, 1.016,47 €, 1.016,47 €, 1.016,47 € y 965,65 € sucesivamente. El beneficiario de las dos primeras operaciones es MYPOCKET.IO, y en las cuatro restantes SWISS BANKERS AG. Posteriormente volvieron a realizar otra transferencia desde la cuenta de don [redacted] a la de doña [redacted] , por importe de Mil Trescientos Euros (1.300 €), así como dos nuevas compras a través de internet por importe de 1.539,96 € y 256,66 €, cuyo beneficiario volvió a ser SWISS BANKERS AG. El total defraudado asciende a la cantidad de 7.811,68 €.

5º. La actora explicó que "pinchó" el enlace y le pidieron sus datos, rellenando los mismos un domingo y que no se dio cuenta del fraude hasta el martes.

Respecto a estos hechos solo aclararemos que los defraudadores accedieron a la cuenta bancaria de Don [redacted] , desde la que realizaron una transferencia por importe de seis mil Euros (6.000 €) hasta la cuenta de su hija Dª [redacted] , y posteriormente las seis compras a través de internet referidas; y una segunda transferencia de 1300 € y dos nuevas comparas por importe de 1.539,96 € y 256,66 €, cuyo beneficiario volvió a ser SWISS BANKERS AG.

En dicha sentencia se considera cuestiones nucleares la concurrencia o no de negligencia por la usuaria y el cumplimiento o no de las obligaciones contractuales exigibles a proveedora del servicio de pago por internet, siendo indiscutida la existencia de una actuación defraudatoria por un tercero; y acaba imputándose a la entidad demandada falta de control exigible al materializar hasta ocho transferencias en las que se procedía a realizar supuestas compras en páginas extranjeras de dudosa identificación, considerando que lo lógico hubiera sido aceptar la primera o segunda de las operaciones, pero al observar la continuidad de las mismas suspender o paralizarlas evitando la sangría de las operaciones de transferencia inconsentidas, por lo que concluye que, aunque también concurra negligencia de la cliente, debe responder la entidad bancaria, porque, si bien no está obligada a controlar todos y cada una de las operaciones bancarias que a través de internet o por cualquier otro medio se realicen, sí que es exigible ese control en aquellas que resulten más evidentes, como es el caso, en el se le permitió al defraudador realizar numerosas transferencias o pagos llegando a superar el límite de disposición de 6000 euros, lo que se dice que a " *todas luces revelaba una operación defraudatoria*".

Con arreglo a las sentencias a la que remite y al marco jurídico desde el que, en línea con éstas, enfoca la cuestión, hay que deducir que considera concurrente una negligencia no grave por parte de la cliente y un déficit de medidas de seguridad por parte de la apelante, quedando identificados en dicha sentencia, en cualquier caso y contrariamente a lo que se sostiene en el recurso, los criterios de imputación de responsabilidad a "CAJA RURAL DE GRANADA", tal y como ha quedado expuesto; siendo el caso que se declara expresamente que no se superó el límite diario de disposición de 6000 €, si bien sí se estima concurrente la especial exigibilidad de control porque se superarse esa cantidad con la sucesiva realización de operaciones en un corto espacio de tiempo.

TERCERO.- Esta sala, siguiendo la pauta de las sentencias precedentes, invocadas en la propia apelada, singularmente de la sentencia núm. 107/2018, de 12 de marzo de la Sección 8ª de la Audiencia Provincial de Alicante, que compendia otros pronunciamientos, ha de partir de la consideración de que, con arreglo al marco jurídico en el que se desenvuelve la actividad de servicios de pago a través de banca on line, el régimen de la responsabilidad de la prestadora del servicio ha de reputarse cuasi-objetivida, en la medida en que sólo se excluye en unos casos por culpa grave del cliente y en otros por únicamente por fraude imputable al mismo, lo que implica, además, que la carga de la prueba de esas circunstancias exoneratorias y la paralela inexigibilidad de otra conducta a la referida entidad incumba a ésta en todo caso.

Así resulta de la siguiente reglamentación:

* El artículo 147 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, dispone: " *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* ", siendo indiscutido que los demandantes merecen la consideración de consumidores.

* El art. 148 de la misma norma, según el cual " *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*".

* El art. 44 del Real Decreto-ley 19/2018, de 23 de noviembre, de regulación de los servicios de pago y otras medidas urgentes en materia financiera, que deroga la Ley 16/2009, de 13 de noviembre, de servicios de pago, con arreglo al cual " 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, conforme a su apartado tercero " *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*".

* El art. 45 de la misma norma establece " *Sin perjuicio del artículo 43 de este real decreto -ley, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine*".

* Art. 46.2 de la misma norma, conforme al cual " *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*"; teniendo en cuenta que, conforme al art. 2.5 se considera autenticación reforzada: " *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*".

A tales efectos se ha de tener en cuenta que, conforme al art. 41 de la misma Ley, en vigor cuando se perfeccionó el contrato de tarjeta, constituyen obligaciones del usuario de servicios de pago habilitado para utilizar un instrumento de pago, hacerlo en las que se establezcan y tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas; así como en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, habrá de notificarlo al proveedor de servicios de pago o a la entidad que este designe, sin demora indebida en cuanto tenga conocimiento de ello.

Con arreglo a este régimen jurídico de la responsabilidad del prestador de servicios de pago, hemos de concluir a la vista de los hechos acreditados que la apelante no había establecido un sistema de autorización de pagos con autenticación reforzada, lo que implica que la reglamentación expuesta, concretamente el citado art. 46.2 presuponga que el prestador de servicios asume la responsabilidad patrimonial por un riesgo perfectamente descrito tanto para el usuario como para el prestador de servicios como es la defraudación con el procedimiento de phising, descrito por la Agencia Española de Protección de Datos (Resolución del Expediente Nº [redacted], DE 24 DE MAYO DE 2006): " 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 ".

Este procedimiento fue el utilizado en el caso, propiciando las dos transferencias o traspasos no autorizadas entre las cuentas de los demandantes, al hallarse asociada la de D. [redacted] a la de su hija, Dª [redacted], e igualmente las compras tampoco autorizadas y las transferencias de los importes del precio a las entidades referidas; sin que conste ni se haya alegado por la apelante que dichas operaciones fuesen sometidas a un procedimiento de autenticación reforzada, a pesar de que, como se dice en la sentencia apelada, suponen una sucesión de operaciones singulares por su cuantía en el contexto de lo que venía siendo habitual en la operativa de dichas cuentas asociadas al uso de la tarjeta, puesto que, si bien no superaban el límite diario, sí se distanciaban notablemente de lo que era la media de reiteradas transacciones anteriores, y, además, se realizaron desde un teléfono también distinto a los designados en el contrato de tarjeta, por lo que, siendo evidente que los actores no concurren como partícipes dolosos en la defraudación, 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, habida cuenta que el propio recurso de apelación se sustenta en la consideración de que concurre negligencia grave por parte de Dª [redacted], lo que no excusa dicha responsabilidad en el caso de ausencia de autenticación reforzada; teniendo en cuenta que, por otra parte, tampoco se opone ni concurre demora en la comunicación y denuncia del fraude por parte de los clientes.

Procede, por tanto, la confirmación de la sentencia apelada y la desestimación del recurso.

CUARTO.- Las costas del recurso se imponen a la apelante, en aplicación de los artículos 394.1 y 398.1 de la LEC, y de conformidad con lo establecido en la Disposición Adicional Decimoquinta de la Ley Orgánica del Poder Judicial aprobada por la Ley Orgánica 1/09 de 3 de noviembre, procede acordar la pérdida del depósito constituido por la recurrente, al que el Juzgado de Primera Instancia dará el destino legal correspondiente.

Vistos los preceptos legales citados y demás de general y pertinente aplicación,

FALLAMOS

Desestimando el recurso de apelación interpuesto en nombre de "CAJA RURAL DE GRANADA, SOCIEDAD COOPERATIVA DE CRÉDITO", se confirma la sentencia núm. 219/2021, de 28 de diciembre, del Juzgado de Primera Instancia e Instrucción nº 2 de Loja, con imposición a la apelante de las costas del recurso de apelación y pérdida del depósito constituido para recurrir.

MODO DE IMPUGNACIÓN: Contra esta Sentencia no cabe recurso ordinario alguno, sin perjuicio de que contra la misma pueden interponerse aquellos extraordinarios de casación o infracción procesal, si concurre alguno de los supuestos previstos en los artículos 469 y 477 de la Ley de Enjuiciamiento Civil, en el plazo de veinte días y ante esta misma Sala, previa constitución del/los depósito/s en cuantía de 50 euros por cada recurso que se interponga, debiendo ingresarlo/s en la cuenta de esta Sala abierta en Banco Santander nº [redacted] indique nº cuenta-expediente judicial [redacted] utilizando para ello el modelo oficial, debiendo indicar en el campo "Concepto" que se trata de un recurso seguido del código "[redacted]" y "Recurso Extraordinario por infracción procesal"/"Recurso de Casación", de conformidad con lo establecido en la Disposición adicional Decimoquinta de la L.O. 6/1985 del Poder Judicial, salvo concurrencia de los supuestos de exclusión previstos en el apartado

5 de la misma y quienes tengan reconocido el derecho de asistencia jurídica gratuita. A los efectos previstos en los artículos 471 y 481.2 de la Ley de Enjuiciamiento Civil se hace saber a las partes que, de necesitarla, podrán solicitar de este Tribunal la certificación de la sentencia que previenen tales preceptos. De no verificarlo así se entregará al recurrente, en su caso con el emplazamiento para ante el Tribunal Supremo.

Así, por esta nuestra sentencia, definitivamente juzgando, lo pronunciamos, mandamos y firmamos.

DILIGENCIA DE PUBLICACIÓN

En el día de su firma, la extiendo yo el/la Letrado/a de la Administración de Justicia para hacer constar que, firmada la anterior Sentencia nº 212/22 por el/los Iltmo/s Magistrados que la dictan, se procede a su publicación de conformidad con lo previsto en los arts. 120.3 CE, 204.3 y 212.1 LEC, se incorpora al libro de su clase numerada por orden correlativo a su fecha, remitiendo las correspondientes notificaciones.

EL/LA LETRADO/A DE LA ADMINISTRACIÓN DE JUSTICIA