Audiencia Provincial de Asturias, Sección 7ª, Sentencia 285/2023 de 12 May. 2023, Rec. 787/2022

Ponente: Martínez-Hombre Guillén, Pablo.

Nº de Sentencia: 285/2023

Nº de Recurso: 787/2022

Jurisdicción: CIVIL

ECLI: *ES:APO:2023:1956*

8 min

Responsabilidad del Banco por el uso fraudulento por terceros de la tarjeta de crédito de una clienta tras bajarse esta en su móvil la aplicación del Banco

BANCA. TARJETAS DE CRÉDITO. Indemnización a cargo de la entidad bancaria por el uso fraudulento por terceros de la tarjeta de crédito de una clienta tras bajarse esta en su móvil la aplicación del Banco. No puede considerarse que los errores gramaticales del mensaje dirigido a la clienta, o la omisión de signos de puntuación, debieron alertarle del carácter fraudulento del mensaje, y desde luego no puede considerarse que un usuario medio sea conocedor de que la página web a la que accedió, con una dirección como la indicada en el mensaje donde se le piden las claves, tenía dominio de Rusia. Tampoco tiene por qué conocer que el servicio de biometría solo se activa si es expresamente solicitado, y por el contrario pudo pensar que la iniciativa obedecía al Banco, e introdujo el código que este le envió en un SMS por estar interesada en el sistema de seguridad reforzada. El sistema de pagos instaurado por el Banco no era totalmente seguro, sin que baste para eludir su responsabilidad la realización de campañas advirtiendo a sus clientes de los peligros del denominado "phishing", sino que será necesario reforzar los mecanismos de seguridad.
La AP Asturias confirma la sentencia de instancia que estimó la demanda de reclamación de indemnización contra entidad bancaria por el uso fraudulento de la tarjeta de crédito de la demandante.

TEXTO

AUD.PROVINCIAL SECCION SEPTIMA

GIJON

SENTENCIA: 00285/2023

Modelo: N30090

PZA. DECANO EDUARDO IBASETA, S/N - 2º. 33207 GIJÓN

-

Teléfono: 985176944-45 **Fax:** 985176940

Correo electrónico:

Equipo/usuario: RRN

N.I.G. 33076 41 1 2022 0000066

ROLLO: RPL RECURSO DE APELACION (LECN) 0000787 /2022

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

Procedimiento de origen: JVB JUICIO VERBAL 0000053 /2022

Recurrente: CAJA RURAL DE ASTURIAS

Procurador: LETICIA MARIA NORIEGA TRESPALACIOS

Abogado: MARLEN GONZALEZ PEREZ

Recurrido: María Rosario

Procurador: MARIA DEL PILAR LANA ALVAREZ

Abogado: DIEGO CUEVA DIAZ

SENTENCIA

Ilmos Magistrados-Jueces Sres/as.:

PABLO MARTINEZ-HOMBRE GUILLEN

En GIJON, a doce de mayo de dos mil veintitrés.

VISTO en grado de apelación ante esta Sección 007, de la Audiencia Provincial de GIJON, los Autos de JUICIO VERBAL 0000053 /2022, procedentes del JDO.1A.INST.E INSTRUCCION N.1 de VILLAVICIOSA, a los que ha correspondido el Rollo RECURSO DE APELACION (LECN) 0000787 /2022, en los que aparece como parte apelante, CAJA RURAL DE ASTURIAS, representado por la Procuradora de los tribunales, Sr./a. LETICIA MARIA NORIEGA TRESPALACIOS, asistido por la Abogada Dª. MARLEN GONZALEZ PEREZ, y como parte apelada, María Rosario, representado por la Procuradora de los tribunales, Sr./a. MARIA DEL PILAR LANA ALVAREZ, asistido por el Abogado D. DIEGO CUEVA DIAZ, siendo el Magistrado/a constituido como órgano unipersonal el/la Ilmo./Ilma. D./Dª PABLO MARTINEZ-HOMBRE GUILLEN.

ANTECEDENTES DE HECHO

PRIMERO.- El Juzgado de Primera Instancia e Instrucción nº 1 de Villaviciosa dictó en los autos, Juicio Verbal nº 787/2022 Sentencia de fecha 26 de Agosto de 2022, cuya parte dispositiva es del tenor literal siguiente: "Que **estimando** la demanda interpuesta por la procuradora Sra. Sra. Lana Álvarez, en nombre y representación de María Rosario, contra Caja Rural de Asturias, S.C.C., **debo condenar y condeno** a la demandada a abonar a la actora la suma de **5.828,35 euros,** incrementada en el interés legal desde el requerimiento efecutado el día ocho de noviembre de 2021."

SEGUNDO.- Notificada la anterior Sentencia a las partes, por la representación de CAJA RURAL DE ASTURIAS, se interpuso recurso de apelación y admitido a trámite se remitieron a esta Audiencia Provincial, y cumplidos los oportunos trámites, se señaló para dictar la resolución en el presente recurso el día 9 de Mayo de 2023.

TERCERO.- En la tramitación de este recurso se han cumplido las correspondientes prescripciones legales.

FUNDAMENTOS DE DERECHO

PRIMERO.- *La sentencia apelada,* con fundamento, básicamente, en lo dispuesto en Real Decreto-Ley 19/2018, de 23 de noviembre (LA LEY 18608/2018), de Servicios de Pago y otras medidas urgentes en materia financiera, especialmente lo establecido en los artículos 41, 42, 44, 45, 46, 64 y 68, *condenó a la demandada Caja Rural de Asturias, S.C.C. al abono a la actora, doña María Rosario, al pago de la cantidad de 5.828,35 euros,* incrementada en el interés legal desde el requerimiento efectuado el día ocho de noviembre de 2021.

En la demanda se alegaba que el 6 de Noviembre de 2.021, la actora se dispuso bajar en su móvil la aplicación RURAL VIA, para poder acceder a información sobre su cuenta abierta en a la citada entidad, y una vez bajada y operativa, sobre las 15 horas recibe un SMS en el que consta identificado como remitente la propia Rural Vía, y que textualmente dice, "NOTIFICACION DE CAJA RURAL a partir de 6 de Noviembre de 2.201, no se puede utilizar su tarjeta, tienes que activar el nuevo sistema de seguridad de web", este mensaje le remite a un link de internet, que da entrada a una página de web con el logo y colores de RURALVIA en el que se recoge acceso a banca internet, debiendo identificarse el usuario con su nombre de usuario, NIF y contraseña, por lo que facilita tales datos sin sospechar nada. Sin embargo, a las 16.25 horas de la tarde contactan telefónicamente con ella responsables de la demandada para comunicarle

que se estaba operando con su tarjeta de forma sospechosa habiendo llegado a hacer cuatro cargos de diferentes cuantías y otros dos más que no llegaron a hacerse efectivos, todos ellos en el extranjero, por lo que van a proceder al bloqueo de dicha tarjeta. Y, cuando consulta la cuenta, observa que el referido 6 de Noviembre figuran cuatros operaciones cargadas, pese a que, en ningún momento, se le ha pedido la confirmación de tales cargos con la introducción de ninguna clave: una primera, por importe de 5.397 euros para una adquisición en la localidad de Saint Quen en Francia, a las 15:17; otra, por importe de 80,35 €, para una adquisición en Eindhoven, Holanda, a las 15:21; una tercera, por importe de 300,50 euros, para una adquisición de Bolougne, Francia, a las 15:2; y finalmente, una cuarta por importe de 50,50 €, para una adquisición en Bolougne, Francia a las 15:25.

La sentencia recurrida por la demandada consideró, en la aplicación de dicha normativa, *que era la entidad financiera quien debía asumir las consecuencias de dicha actuación fraudulenta,* sin que quepa extraer un comportamiento negligente de gravedad suficiente por parte de la actora para hacerla responsable de las operaciones de pago y el perjuicio sufrido. Siendo esta conclusión esencialmente cuestionada por la parte apelante, para quien la actora habría incurrido en negligencia grave por tales motivos.

SEGUNDO.- *Cuestiona en primer lugar la apelante dicha conclusión argumentado que el mensaje SMS que fue recibido, que a su vez determinó que la actora proporcionara al delincuente su nombre de usuario, NIF y contraseña, permitía de una forma claramente detectable por su redacción y dirección de la pagina web a la que se reenviaba, conocer el carácter fraudulento de la operación,* a cuyos efectos debe indicarse que el marco normativo regulador de la prestación de los servicios de pago es el Real Decreto-ley 19/2018, de 23 de noviembre (LA LEY 18608/2018), de servicios de pago y otras medidas urgentes en materia financiera, y en el supuesto aplicable al case de autos rigen fundamentalmente los arts.. 41, 42 nº 1 a), 44 y 46, cuyo contenido damos por reproducido, que, en la interpretación de las Audiencia Provinciales, suponen la cuasi-objetivación de la responsabilidad del proveedor del servicio, y así, como indica la sentencia de la Audiencia Provincial de Granada 212/2022 (LA LEY 202852/2022), Sección 5ª, y citada por la de Almería Sección 1ª, de 31 de enero de 2023 (LA LEY 56711/2023), "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 (LA LEY 11922/2007), 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".

En esta misma línea, la sentencia de la Sección 20ª de la Audiencia Provincial de Madrid de 20 de mayo de 2022 (LA LEY 167264/2022), indica en "la Directiva 2015/2036 la negligencia que le hace responder al cliente, es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que ha sido inducido por un delincuente profesional. Tampoco puede calificarse como grave dicho comportamiento conforme a la normativa del código civil, pues siendo exigible al demandante la diligencia que exija la naturaleza de la obligación y correspondan a las circunstancias de las personas, tiempo y lugar (art. 1.104 del cc (LA LEY 1/1889)), el método fraudulento empleado -phishing- es de una complejidad y grado de perfección, difícilmente detectable por un cliente de las características del demandante,..... Es cierto que dicho comportamiento no puede considerarse diligente, pero para hacer soportar al cliente las consecuencias, aún parciales como se concluye en la sentencia apelada, es preciso apreciar en él una negligencia y que además sea grave, que en la normativa europea antes referida se equipara a la comisión de un fraude, actuación en la que no se ha acreditado incurriese el demandante, por el hecho de haber pinchado el link que se le ofrecía y facilitar los datos y clave de la tarjeta".

Así las cosas *debe tenerse presente que la actuación de la demandada se produce tras bajarse la aplicación Rural Vía, lo que por mucho que ahora se cuestione, resulta de forma acreditada por la propia documental aportada por la apelante,* pues resulta evidente que, aunque la apelada la tenía instalada en otros dispositivos móviles, lo que consta es que a las 15,55 horas el día 6 de noviembre de 2021, se instaló en un dispositivo distinto, y con un sistema operativo diferente al anterior dispositivo móvil. *Siendo por ello creíble la versión de la actora de que fue, tras dicho hecho cuando recibe un mensaje con el contenido "Notificación de Caja Rural Partir del 06/11/2021, No se puede utilizar su tarjeta. Tienes que activar el nuevo sistema de seguridad web: https://bit.ly/2WDUwm4", sin que en este contexto quepa considerar que la falta de coherencia en la persona gramatical, en que se dirige al cliente, o en el que se omiten los signos de puntuación e incluso algunas palabras, puede considerarse que debió conducir a la actora del carácter fraudulento del mensaje, máxime cuando esta una circunstancia usual en este tipo de mensajes telemáticos, y ni que decir tiene*

que, desde luego no puede considerarse que un usuario medio sea conocedor de que la página web con una dirección como la indicada en el segundo de los mensajes donde se le piden las claves, tenia dominio de Rusia.

TERCERO.- *La apelante argumenta además que la actuación de la actora propició que el ciberdelincuente pudiera salvar el mecanismo de seguridad reforzada establecido, al permitir al activar el servicio de biometría cuando no lo había solicitado, pues la entidad envió un SMS con un código a la Sra. María Rosario cuando el "ciberdelincuente" activó el registro de biometría, y a pesar de no haber solicitado la activación de este servicio, la ahora demandante, de forma absolutamente incomprensible - y, lógicamente, negligente- introdujo el código recibido confirmando la activación de este servicio.* Así, en el Anexo VI consta enviado un SMS a la Sra. María Rosario el día 6 de noviembre a las 16:02 que decía lo siguiente "para finalizar el registro biométrico que permite firmar con huella/Face ID sus compras por internet introduzca el código NUM000".

Lo cierto es que, al margen de que, ciertamente lo argumentado en orden a la forma de obtener las claves por parte del ciberdelincuente, no es tan claro como la parte pretende, pues efectivamente en el anexo IV referido el login de banca a distancia, de su informe se infiere que existen desde las 15,55 horas numerosas operaciones con errores por lo que no es descartable que se haya logrado por el tercero mediante un sistema de generación de código, en realidad, si ello fue realmente como lo asegura la apelante, *teniendo presente que la actora lo que pretendía era dar de alta la aplicación en su teléfono, no tiene porqué conocer que tal mecanismo de seguridad solo se activa si es expresamente solicitado, y por el contrario pudo pensar que la iniciativa obedecía a la entidad financiera, e introdujo el código por estar interesada en este sistema de seguridad reforzada, que, es notorio, es un mecanismo que se está generalizando por los usuarios de este tipo de productos.*

CUARTO.- *Los dos últimos motivos del recurso se asiente en la argumentación de que la apelante habría sido quien advirtió del fraude, bloqueando así el resto de las operaciones que se intentaron, y que su actuación en todo caso ha sido diligente, tanto implementando los mecanismos de seguridad preciso para dar el servicio de pago, como mediante la realización de campañas advirtiendo a sus clientes de los peligros del denominado "phishing", argumentos que están abocados al fracaso, desde el momento en que tales sistemas de seguridad no funcionaron en cuanto a las operaciones que son las que determinan la reclamación de la actora, y que ponen de manifiesto que en sistema de pagos instaurado por la apelante no es totalmente seguro, sino que está*

expuesto a fraudes como el de autos, sin que base para eludir su responsabilidad con la realización de las campañas a las que alude, sino que será necesario reforzar los mecanismos de seguridad, pues en definitiva, y como señala la citada sentencia de la Sección 20ª de la Audiencia Provincial de Madrid de 20 de mayo de 2022 (LA LEY 167264/2022) "la responsabilidad exigida a la entidad demandada, como proveedora del servicio, es la que se deriva de la naturaleza de tal prestación y de la posición contractual en la que se encuentran las partes, lo que le obliga a adoptar una serie de medidas de seguridad y dotarse de mecanismos de supervisión que permitieran detectar operaciones fraudulentas en la prestación de servicios de pago, tal como señala el artículo 2 del Reglamento Delegado 2018/389, pues como se indica también en la sentencia citada de la Audiencia de Pontevedra, incluyendo la técnica del phishing, la creación y puesta en la red de páginas que clonan las del sitio oficial de las entidades emisoras de instrumentos de pago, el deber de diligencia de la entidad demandada exigía dotarse de la tecnología antiphishing precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas, lo que, de producirse, impediría que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace del correo electrónico haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor. Dicha actuación diligente no puede considerarse acreditada por las información que se facilita a los clientes a través de su página web, en cuanto la efectividad de esas obligaciones preventivas, lo que requerían era implementar en el sistema informático el mecanismo tecnológico adecuado para evitarlo; es decir mediante una con una conducta activa y no simplemente informativa o divulgativa".

CUARTO.- Lo expuesto conduce a la desestimación del recurso, lo que determina que se impongan a la demandada las costas causadas tanto en la instancia como en la apelación (arts. 394 nº 1 y 398 nº 1 de la Ley de Enjuiciamiento Civil (LA LEY 58/2000)), sin que en el caso de autos se aprecien serias dudas de hecho que justifiquen eludir el criterio del vencimiento objetivo que en esta materia rige, puesto que con arreglo a las conclusiones fácticas sentadas, y el régimen de responsabilidad cuasiobjetiva que rige en la materia, aquellas no se dan.

FALLO

SE DESESTIMA el recurso de apelación interpuesto por la Procuradora Sra. LETICIA MARIA **NO**RIEGA TRESPALACIOS, en nombre y representación de CAJA RURAL DE ASTURIAS, contra la sentencia dictada el día 26 de Agosto de 2022, por el Juzgado

de Primera Instancia e Instrucción nº 1 de Villaviciosa, en los autos de Procedimiento, Juicio Verbal nº 53/2022, y, que se confirma en todos sus pronunciamientos, con imposición de costas a la parte apelante.

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