Juzgado de Primera Instancia N°. 5 de Pamplona/Iruña, Sentencia 172/2023 de 3 Abr. 2023, Rec. 1566/2022

Ponente: Caballero García, Vanessa.

Nº de Sentencia: 172/2023

Nº de Recurso: 1566/2022

Jurisdicción: CIVIL

ECLI: ES:JPI:2023:707

14 min

Responsabilidad del Banco por las cantidades defraudadas mediante transferencias realizadas con el sistema de pago bizum

BANCA. Negligencia de la entidad bancaria en la prestación y uso de servicios de pago online. Transferencias mediante el sistema de pago bizum no autorizadas por el cliente. La falsedad de la transferencia es un riesgo a cargo del banco, por lo que si cumple una orden falsa habrá de reintegrar en la cuenta correspondiente las cantidades cargadas, salvo que el titular haya creado o elevado el riesgo de falsificación de forma imputable en el caso concreto. Falta de prueba de la recepción por el actor de los mensajes enviados por el banco a su teléfono móvil con la clave de seguridad que debía introducir para enviar el dinero. Además, se realizaron hasta 25 operaciones de bizum no autorizadas y el banco solo aporta 9 mensajes enviados al actor, de los que solo 7 contienen claves de seguridad.

El Juzgado de Primera Instancia nº 5 de Pamplona estima la demanda de reclamación de responsabilidad contra entidad bancaria por la realización de pagos por bizum sin autorización del cliente.

TEXTO

Juzgado de Primera Instancia nº 5 de Pamplona.

Procedimiento: Juicio Verbal 1566/22.

SENTENCIA Nº 000172/2023

En Pamplona, a 3 de abril de 2023.

Doña VANESSA CABALLERO GARCIA, Magistrada Titular del Juzgado de Primera Instancia nº 5 de Pamplona, habiendo visto y oído en juicio oral y público los presentes autos de JUICIO VERBAL 1566/22, en los que han sido parte, como DEMANDANTE, don Erasmo, asistida por el Letrado Don Iñaki Iribarren García y doña Arantxa Ros Gavilán y representados a través de la Procuradora Doña Natividad Izaguirre Oyarbide, y como DEMANDADA, la entidad UNICAJA BANCO S.A., asistida por la letrada doña Marta Roca Heres y representada a través del Procurador don Jaime Ubillos Minondo.

La presente resolución de ha dictado bajo el borrador realizado por el juez en prácticas Don Pedro Doria Sevine

ANTECEDENTES DE HECHO

PRIMERO.- La Procuradora Doña Natividad Izaguirre Oyarbide, en nombre y representación de Don Erasmo, en fecha de 30 de noviembre del 2.022, presentó DEMANDA DE JUICIO VERBAL contra UNICAJA BANCO S.A., en reclamación de la cantidad de 3.940 euros.

SEGUNDO.- En virtud de DECRETO de 15 de diciembre de 2.022, previa subsanación de los defectos de los que adolecía, fue admitida a trámite la demanda por los trámites del Juicio Verbal, emplazando a la entidad demandada para contestarla dentro del plazo de 20 días siguientes al de su notificación.

TERCERO.- El Procurador Don Jaime Ubillos Minondo, en nombre y representación de la entidad UNICAJA BANCO S.A. presentó escrito de CONTESTACIÓN a la demanda en fecha 24 de enero de 2.023, admitido a trámite en virtud de DILIGENCIA DE ORDENACION de 3 de febrero de 2023, convocándose a las partes para la celebración del juicio oral el día 23 de marzo del 2.023 a las 11:30 horas.

QUINTO.- Al acto de la vista comparecieron ambas partes, concurriendo en ellas los preceptivos requisitos de postulación.

La parte actora tras ratificarse en su escrito de demanda propuso como prueba la documental; la demandada tras ratificarse en su escrito de contestación a la demanda propuso como prueba la documental. Formuladas conclusiones por ambas partes, fueron declarados los autos vistos para sentencia.

En la presente resolución se han cumplido con todos los trámites legales.

FUNDAMENTOS DE DERECHO

PRIMERO.- La parte actora, el señor Erasmo, ejercita una acción de incumplimiento de las obligaciones contractuales, en reclamación de la cuantía de 3.940 euros, más los intereses legales conforme a la Ley de Servicios de Pago, correspondiente a 23 operaciones de cargo, realizadas mediante el sistema Bizum y no autorizadas, en su cuenta bancaria. Estas operaciones fueron realizadas entre el 19 de junio de 2022 y el 20 de junio de 2022, algunas con concepto yo y dirigidas a Rodolfo, Romulo y Maite, por un importe total de 3.940 euros.

Funda su reclamación en los siguientes hechos; El día 20 de junio de 2022, al entrar en su cuenta de banca electrónica, el señor Erasmo, comprobó que, entre el 19 de junio y el 20 de junio de 2022, se habían cargado en su cuenta 25 bizums, 2 posteriormente anulados, que él no había realizado, ni autorizado, ni validado con clave de OTP.

Basa su reclamación en el artículo 41 y ss, 62 y 68 de la Ley 19/18 (LA LEY 11712/2018), de fecha de 23 de Noviembre, sobre Servicios de Pago y otras Medidas Urgentes en Materia Financiera, al entender que la entidad no se ha cerciorado de que las credenciales de seguridad personal únicamente hayan sido accesibles a la demandante, debiendo responsabilizarse del riesgo de su envío a otro usuario o de sus coordenadas, así como realizar las gestiones necesarias para verificar que se estuviera realizando una actividad ilícita con la tarjeta de su cliente. No ha procedió a la correcta autentificación de las operaciones. Ni acredita que fueran registradas con exactitud ni verifica el buen funcionamiento de su servicio de banca online en la fecha en la que produjo los cargos indebidos en la tarjeta de la actora; suplicando la integra estimación de la demanda con condena en costas a la parte demandada.

La parte demandada, la entidad UNICAJA BANCO S.A., se opone a las pretensiones formuladas de contrario alegando que, efectivamente, constan en la cuenta bancaria del señor Erasmo una serie de bizums pero no consta que estas operaciones sean fraudulentas, atendiendo a que debía de introducir multitud de datos para habilitar esos cargos ya que, la entidad demandada, envió al teléfono móvil del actor una serie de SMS, con la clave de seguridad que debía introducir para enviar el dinero por bizum. Entiende, que la banca electrónica cumplió con la normativa en materia de seguridad del pago por lo que los cargos indebidos realizados en la tarjeta de la actora se debieron a su propia negligencia dado que ambas operaciones fueron perfectamente registradas, validadas y autentificadas por la misma; suplicando la integra desestimación de la demanda con condena en costas a la parte actora.

SEGUNDO.- Partiendo de lo expuesto, la discrepancia fundamental que mantienen las partes, se centra en determinar si la entidad bancaria UNICAJA BANCO S.A. incurrió en un comportamiento negligente en el cumplimiento de las obligaciones derivadas de la prestación y uso de los servicios de pago online derivada del contrato de cuenta corriente concertado entre ambas partes.

Dada que la responsabilidad que se imputa a la entidad, derivada de la ejecución de una serie de operaciones no autorizadas por el titular de la cuenta de la cliente de UNICAJA BANCO S.A., la demandante, realizada a través del sistema de banca online, que la entidad pone a disposición de su cliente, he de hacer referencia a los siguientes aspectos, relacionados con la banca online;

1º.- El sistema bizum es un servicio al que voluntariamente pueden adherirse los clientes de una determinada entidad bancaria, siempre que cuente con una cuenta corriente activa en la misma, y que permite transferir dinero a la cuenta corriente de otra persona de forma instantánea y gratuita, sin necesidad de conocer su número de cuenta, requiriendo únicamente el conocimiento de su número de teléfono móvil.

2º.- Las transferencias mediante bizum se consideran incluidas dentro del concepto de transferencia de fondos de la Ley de Servicios de Pago y, por lo tanto, se regulan por el Real Decreto-Ley 19/18, 23 de noviembre (LA LEY 18608/2018). Esta normativa define la orden de pago como toda instrucción cursada por un ordenante o beneficiario a su proveedor de servicios de pago por la que se solicite la ejecución de una operación de pago. (art.3.28).

3º.- Desde un punto de vista contractual toda transferencia constituye una forma de ejecución de obligaciones contractuales previamente asumidas, ejecución obligada cuando se dan las condiciones pactadas, de ordinario, que haya provisión de fondos. Es por ello que se entiende

que la orden de transferencia constituye una declaración de voluntad o mandato (en el sentido del art. 254 Código de Comercio (LA LEY 1/1885)) en virtud del cual el banco asume la realización de transferencias por cuenta del cliente como parte del contrato de servicio de caja.

4º.-Dado el carácter negocial de la orden de pago, ésta puede pactarse que tenga lugar en cualquier forma, incluida la electrónica. En particular, el consentimiento a operaciones de pago por el usuario en el ámbito de la banca electrónica supone que el cliente deba haber firmado un contrato de adhesión a los servicios de banca electrónica. La LSP establece al respecto que el ordenante y su proveedor de servicios de pago acordarán la forma en que se dará el consentimiento, así como el procedimiento de notificación del mismo, negocio jurídico que determina que la transferencia se entienda autorizada por el ordenante de acuerdo con el mismo precepto de la LSP. El consentimiento del ordenante se prestará, según el medio utilizado para prestar dicho consentimiento, mediante, o la firma de la autorización y orden de transferencia correspondiente, o verbalmente a través de la vía telefónica o a través de banca por internet o electrónica.

5º.- Tanto en la 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. Por ello y para su ejecución, el banco debe comprobar en todo caso la autenticidad de la orden y, salvo pacto en contrario, que existe saldo suficiente.

6º.- De ordinario, para la realización de transferencias ordinarias con cargo a una cuenta vinculada es preciso que el cliente haya de autenticar la operación mediante la introducción de las claves previamente facilitadas por la entidad de crédito con la que contrata, con respecto a las cuales tendrá unos deberes de custodia.

7º.- La falsedad de la transferencia (que el ordenante no sea el titular de la cuenta) es un riesgo a cargo del banco porque, en principio, el deudor sólo se libera pagando al verdadero acreedor por lo que, si el banco cumple una orden falsa, habrá de reintegrar en la cuenta correspondientes las cantidades cargadas. Una excepción a esta distribución de riesgos se produce en el caso de que el titular haya creado o elevado el riesgo de falsificación de forma imputable en el caso concreto. Así lo prevé el alto Tribunal Supremo en la sentencia de fecha de julio de 1988.

8º.- La ley cambiaria se ampara en el principio general de que el daño que resulte del pago de un cheque falso o falsificado será imputado al librado, a no ser que el librador haya sido

negligente en la custodia del talonario de cheques, o hubiere procedido con culpa. Este es el principio se recoge hoy la LSP, articulo 36 y siguientes, pues 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 a su proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud, y que no se vio afectada por un fallo técnico o cualquier otra deficiencia. El registro por el proveedor de servicios de la utilización del instrumento de pago no bastará necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que este actuó de manera fraudulenta o incumplió deliberadamente o por negligencia grave una o varias de sus obligaciones previstas en la propia ley.

En este sentido, el artículo 41 de la Ley de Servicios de Pago, establece que es obligación del usuario: " a) utilizará el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago que deberán ser objetivas, no discriminatorias y proporcionadas y, en particular, en cuanto reciba un instrumento de pago, tomará todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas;b) en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, lo notificará al proveedor de servicios de pago o a la entidad que este designe, sin demora indebida en cuanto tenga conocimiento de ello".

El art. 42 de la LSP, establece que el proveedor de servicios deberá;" a ) 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.

b) Se abstendrá de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso de que deba sustituirse un instrumento de pago ya entregado al usuario de servicios de pago.

Esta sustitución podrá venir motivada por la incorporación al instrumento de pago de nuevas funcionalidades, no expresamente solicitadas por el usuario, siempre que en el contrato marco se hubiera previsto tal posibilidad y la sustitución se realice con carácter gratuito para el cliente.

c) Garantizará que en todo momento estén disponibles medios adecuados y gratuitos que permitan al usuario de servicios de pago efectuar una notificación en virtud del artículo 41.b), o solicitar un desbloqueo con arreglo a lo dispuesto en el artículo 40.4. A este respecto, el proveedor de servicios de pago facilitará, también gratuitamente, al usuario de dichos

servicios, cuando éste se lo requiera, medios tales que le permitan demostrar que ha efectuado dicha comunicación, durante los 18 meses siguientes a la misma.

d) Ofrecerá al usuario de servicios de pago la posibilidad de efectuar una notificación en virtud del artículo 41.b), gratuitamente y cobrar, si acaso, únicamente los costes de sustitución directamente imputables al instrumento de pago.

e) Impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación en virtud del artículo 41.b)

2. El proveedor de servicios de pago soportará los riesgos derivados del envío de un instrumento de pago al usuario de servicios de pago o del envío de cualesquiera elementos de seguridad personalizados del mismo".

El art. 43 respecto a operaciones de pago no autorizadas, establece que;" El usuario de servicios de pago obtendrá la rectificación por parte del proveedor de servicios de pago de una operación de pago no autorizada o ejecutada incorrectamente únicamente si el usuario de servicios de pago se lo comunica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 60, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo.

Los plazos para la notificación establecidos en el párrafo primero no se aplicarán cuando el proveedor de servicios de pago no le haya proporcionado ni puesto a su disposición la información sobre la operación de pago con arreglo a lo establecido en el título II.

2. Cuando intervenga un proveedor de servicios de iniciación de pagos, el usuario de servicios de pago deberá obtener la rectificación del proveedor de servicios de pago gestor de cuenta en virtud del apartado 1, sin perjuicio de lo dispuesto en el artículo 45.2, y el artículo 60.1

9º.- Los servicios que prestan las entidades de crédito a sus clientes a través de su oficina virtual se desenvuelven en redes TCP/IP (Internet) o WAP (comunicaciones móviles).

10º.- Siendo Internet una red pública de comunicaciones, la seguridad de las operaciones bancarias precisa de soluciones tecnologías avanzadas a los efectos de garantizar tanto la

autenticidad como la integridad y la confidencialidad de los datos. Por estos motivos las entidades prestadoras del servicio de banca online deben dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones. Consecuencia derivada de la omisión, insuficiencia o defectuoso funcionamiento de las adoptadas es que han de ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema.

11º.- La banca electrónica está siendo objeto de transferencias no autorizadas por el cliente y que vienen antecedidas por el método delictivo conocido como phishing que constituye una modalidad específica de fraude informático que visualiza las deficiencias de seguridad del sistema informático de una entidad y que trae causa en el uso de las redes telemáticas. En este sentido la propia actora ha sido víctima de tale hechos, denunciados ante la Comisaria de Policía Nacional, que no ha podido, a día de hoy, averiguar su autoría, al no haber obtenido ninguna línea de investigación viable.

De acuerdo con la Agencia Española de Protección de Datos (R Expediente Nº : NUM000, 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 ".

La responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse que ésta autorizada al haberse realizado de acuerdo con los sistemas de autenticación del banco.

Los sistemas de autenticación se establecen por los proveedores de servicios de pago y si un banco no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante víctima de esta práctica fraudulenta sea el único responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo. Por tanto, en el caso de órdenes de pago y transferencias fraudulentas puede afirmarse que sin dicha declaración de voluntad la operación de pago o transferencia de fondos, presuntamente realizada por la titular de los fondos, se considerará no autorizada.

Las medidas de seguridad no solamente están destinadas a proteger la seguridad de las órdenes de pago emitidas por los clientes, sino que su eficacia exonera a las entidades de crédito de sus responsabilidades frente a las órdenes de pago no emitidas por sus clientes de tal forma que el incumplimiento de este específico deber de vigilancia da lugar a una responsabilidad por " culpa in vigilando" o responsabilidad objetiva por el mal funcionamiento de los servicios de banca electrónica. Y en este sentido, la Audiencia Provincial de Zaragoza de fecha 14 de mayo de 2013 (LA LEY 68774/2013), condenó a Barclays Bank a reintegrar 20.947 euros al cliente víctima de phishing. La Sentencia señala que;" la Ley de Servicios de Pago expresa con claridad que, salvo una tardanza injustificada del usuario del servicio de banca electrónica en comunicar la irregularidad de las operaciones, será el banco quien deberá devolverle de inmediato el importe de la operación no autorizada y, en su caso, restablecerá la cuenta de pago en que haya adeudado dicho importe al estado que habría existido de no haberse efectuado la operación de pago no autorizada. Por ello y salvo actuación fraudulenta o negligencia grave del titular de la cuenta, la responsabilidad de la operación es del banco al que corresponde además probar el correcto funcionamiento del sistema informático".

En consecuencia, a lo expuesto, hay responsabilidad bancaria por los defectos de seguridad del sistema que determina la ejecución de órdenes de pago no autorizadas por su cliente, con la única excepción de que el banco acredite la culpa o negligencia de la víctima. Constituye por tanto obligación esencial de las entidades prestadoras del servicio de banca online el dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones por lo que, en el supuesto de insuficiencia o mal funcionamiento de las adoptadas, deben ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema.

En el caso de autos, la entidad bancaria aporta como documental (documento nº 7) una serie de SMS que, según la entidad demandada, fueron enviados a la parte actora con la clave de seguridad necesaria para realizar las operaciones, lo que acreditaría que el señor Erasmo, conocía las claves de seguridad y las introdujo voluntariamente, por lo que no habría un negligente funcionamiento de los medios de seguridad en el pago. Sin embargo, no ha quedado acreditado que dichos mensajes fueran recibidos, y aun cuando se hubiera admitido la solicitud extemporánea realizada por la parte demandada de oficio a la compañía telefónica, ello únicamente habría permitido probar el envío y en su caso recepción de los mensajes en el teléfono móvil de la parte demandante, no su validación o introducción por el señor Erasmo,

teniendo la carga de probar este hecho la parte demandada por cuanto es la entidad bancaria la que se entiende que posee los documentos y registros necesarios para ello.

Lo cierto es, además, que la parte demandada aporta una serie de mensajes enviados a la parte demandante (documento nº 7) pero solo 9 de ellos corresponden a los días 19 y 20 de junio, y de esos 9, solo 7 contienen claves de seguridad para operaciones realizadas el día 19 de junio. Además, los extractos bancarios que constan en el documento nº 4 aportado por la parte, no nos permiten comprobar las horas de los bizums, por lo que no se pueden comparar con los SMS aportados. Por otra parte, los SMS contienen cantidades diferentes a los bizums enviados pues dos de ellos comunican que se va a realizar un bizum de 500 euros cuando de dichos extractos bancarios se constata que las operaciones de transferencia no superaron los 200 euros, por lo que las cantidades no cuadran.

Por todo ello, teniendo en cuenta que se realizaron hasta 25 operaciones de bizum no autorizadas, como se acredita del documento nº 4 aportado por la parte demandada, y que solo se aportan por la parte demandada 7 mensajes con claves de seguridad, es claro que existió un deficiente funcionamiento de la normativa sobre seguridad en el pago y, por lo tanto, le corresponde al banco la responsabilidad de abono de la cantidad defraudada.

Por consiguiente, acreditado el incumplimiento por la entidad bancaria demandada de sus obligaciones en los sistemas de pago online o a distancia, la demanda debe ser estimada.

TERCERO.- De acuerdo con la petición formulada, procede acceder a la pretensión de la actora, respecto a su petición de intereses, condenando a la demandada al abono del interés legal del dinero desde la fecha del cargo, e incrementados en dos puntos desde la fecha de ésta resolución y hasta su completo pago, a tenor de lo establecido en el artículo 1.108 del Código Civil (LA LEY 1/1889) y 576.1 de la Ley de Enjuiciamiento Civil (LA LEY 58/2000).

CUARTO.- .- En virtud de lo dispuesto en el artículo 394.1 LEC (LA LEY 58/2000), al ser estimada la demanda, se imponen a la parte demandada las costas procesales causadas.

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

FALLO

Que ESTIMANDO la demanda formulada por Don Erasmo frente la entidad UNICAJA BANCO S.A., y debo DECLARAR y declaro que la demandada incumplió el contrato de cuenta corriente con nº NUM001 junto con sus anexos de servicios de pago y contrato de Banca a Distancia;

Que ESTIMANDO la demanda formulada por Don Erasmo frente la entidad UNICAJA BANCO S.A., y debo DECLARAR y declaro la responsabilidad de la entidad UNICAJA BANCO en la incorrecta ejecución de las 23 operaciones no autorizadas realizadas mediante Bizum entre el 19 de junio y el 20 de junio de 2022 por un importe total de 3.940 euros.

Que ESTIMANDO la demanda formulada por Don Erasmo frente la entidad UNICAJA BANCO S.A., y debo DECLARAR y declaro que se han producido para la actora unos daños y perjuicios por importe de TRESMIL NOVECIENTOS CUARENTA EUROS (3.940 euros) correspondiente al cargo en cuenta por las operaciones no autorizadas.

Que ESTIMANDO la demanda formulada por Don Erasmo frente la entidad UNICAJA BANCO S.A., debo CONDENAR y condeno a la entidad demandada abonar a la actora el importe de los daños y perjuicios causados, valorados en la cantidad de TRESMIL NOVECIENTOS CUARENTA EUROS (3.940 euros), junto con los intereses legales de dicha cantidad desde la fecha de su cargo en cuenta, incrementados en dos puntós desde la fecha de ésta resolución y hasta su completo pago.

Todo ello con expresa imposición a la parte demandada de las costas procesales causadas.

Notifíquese esta resolución a las partes, haciéndoles saber que contra la misma cabe interponer RECURSO DE APELACIÓN ante este Juzgado dentro de los veinte días siguientes al de su notificación.

Llévese el original al Libro de sentencias y expídase testimonio para su unión a los autos.

Así lo acuerda, manda y firma Doña VANESSA CABALLERO GARCIA, Magistrada Titular del Juzgado de Primera Instancia nº 5 de Pamplona, y su Partido. Doy fe.-

La difusión del texto de esta resolución a partes no interesadas en el proceso en el que ha sido dictada sólo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran y con pleno respeto al derecho a la intimidad, a los derechos de las

personas que requieran un especial deber de tutela o la garantía del anonimato de las víctimas o perjudicados, cuando proceda. Los datos personales incluidos en esta resolución no podrán ser cedidos, ni comunicados con fines contrarios a las leyes.