[redacted]

Sección Civil. Juzgado de Primera Instancia e Instrucción nº 1 de Gandesa (UPAD)
Avenida Joan Perucho, 2 - Gandesa - C.P.: 43780

TEL.: 977421626
FAX:
EMAIL:mixt1.gandesa@xij.gencat.cat

N.I.G.: [redacted]
Juicio verbal (250.2) (VRB) 291/2022 -A
-
Materia: Juicio verbal (resto de casos)

Entidad bancaria BANCO SANTANDER.
Para ingresos en caja. Concepto: 4182000003029122
Pagos por transferencia bancaria: [redacted]
Beneficiario: Sección Civil. Juzgado de Primera Instancia e Instrucción nº 1 de Gandesa (UPAD)
Concepto: [redacted]

Parte demandante/ejecutante: [redacted]
Procurador/a: [redacted]
Abogado/a: Juan Pablo Palomar Pérez

Parte demandada/ejecutada: BANCO SANTANDER, S.A.
Procurador/a: [redacted]
Abogado/a: [redacted]

SENTENCIA Nº 138/2022

Magistrada: Maria del Carmen Marcos Alvarez
Gandesa, 27 de noviembre de 2022

Antecedentes de hecho

Primero.- La procuradora de los Tribunales Dª [redacted] bajo la dirección letrada de D Juan Pablo Palomar Pérez, en representación de Dª [redacted] formula demanda de indemnización por daños y perjuicios por dolo o negligencia en incumplimiento de obligaciones, contra la entidad bancaria "Banco Santander SA", representada por el procurador de los Tribunales D [redacted] y con asistencia letrada de Dª [redacted] en la que, después de invocar los hechos y fundamentos jurídicos que estimó de aplicación, terminaba interesando se dictara sentencia en los términos consignados en la súplica, con expresa imposición de las costas del procedimiento al demandado.

Segundo.- La demanda se admitió y se tramitó conforme a la normativa procesal para este tipo de procedimiento y dada la oposición al mismo, el Decreto de fecha 6 de septiembre de 2022 admite la oposición al juicio monitorio y dispone la tramitación por las reglas del Juicio Verbal, finalmente, quedaron los autos para dictar la correspondiente sentencia.

Fundamentos de derecho

Primero.- La representación procesal de la parte actora ejercita acción de indemnización por daños y perjuicios al amparo del artículo 1101 del CC que establece que quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren el tenor de aquellas, en relación con los artículos 1902 y 1258 del mismo texto legal, el artículo 217 de la LEC, y los artículos aplicables de la DIRECTIVA 2015/2366, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior-reglamento delegado (UE) 2018/389, de la comisión, el Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera y el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la defensa de los consumidores y usuarios y otras leyes complementarias.

La representación procesal de la parte actora aduce que en fecha 14 de septiembre de 2020 Dª [redacted] suscribe el contrato de tarjeta de crédito con número [redacted] con la entidad bancaria "BANCO SANTANDER SA", estableciéndose en el mismo un límite de crédito de 3.500,00 €, y un límite de pérdida económica a su cargo hasta el momento en que se notifique la pérdida, sustracción o apropiación indebida al banco de 0,00 €. Adjunta como documento número UNO el contrato de tarjeta de crédito y como documento número DOS el extracto de movimientos de la tarjeta acreditativo de su utilización.

Así mismo, manifiesta que en fecha 20 de febrero de 2022 (domingo) a las 19,22.- horas se inició un ciberataque, con aplicación de una técnica de ingeniería social, sobre la plataforma de banca on-line de Dª [redacted] a través del envío a su dispositivo móvil de un mensaje SMS al que se dio la apariencia de haber sido remitido por la entidad bancaria "BANCO SANTANDER", entremezclándolo dentro del hilo de mensajes SMS auténticos provenientes de la referida entidad bancaria, que anexa como documento número TRES.

El referido mensaje, que burló la aplicación informática de mensajería propia del dispositivo móvil manifestaba lo siguiente: "Hemos detectado actividad sospechosa en su cuenta y ha sido bloqueada por seguridad. Acceda al enlace para desbloquearla hppts: // seguridad-particular.com." Dª [redacted] creyendo que tal mensaje provenía realmente de su entidad bancaria al constatar que el dominio de internet consistía en una extensión "https", y en la confianza de que estaría protegida ante a un acceso no autorizado a su cuenta, pulsó dicho enlace, que le redirigió a través de la web internet a un dominio que a su vez aparentaba la página web de BANCO SANTANDER. La página web fraudulenta le solicitó toda una serie de datos bajo el pretexto de solventar la incidencia de seguridad, los cuales fueron suministrados de buena fe por Dª [redacted] Pocos minutos después de introducir tales datos, y en el transcurso de

escasos segundos se sucedieron casi simultáneamente tres comunicaciones por SMS: el primero le comunicaba que BANCO SANTANDER no había autorizado una operación de pago a MEDIA MARKT con cargo a su tarjeta de crédito "por controles de seguridad", el segundo le comunicaba que no había autorizado una operación de 739.-€ con su tarjeta de débito por falta de saldo, y el tercero, precedido de la leyenda "SEGURIDAD", le indicaba que se habían registrado operaciones "poco habituales" con su tarjeta de crédito, instándole a contactar con la entidad bancaria para verificar la corrección de tal operativa, dichos mensajes se anexan como documento número SIETE.

Dª [redacted] al verificar el estado de sus cuentas en la banca on-line constata que había una orden de pago no autorizada a través de su tarjeta de crédito por importe de 2.577,00 €. Al contactar con el servicio de atención telefónica de la entidad bancaria se le confirma la operación de pago pese a no ser autorizada por ella, remitiéndole un correo electrónico con el alta de la incidencia. Adjunta como documento número OCHO el extracto de movimientos de la tarjeta de crédito del día 20 de febrero de 2022 y como documento número NUEVE el correo notificándole el número de incidencia nº 0001425229.

En fecha 21 de febrero de 2022 interpuso la correspondiente denuncia ante los Mossos d'Esquadra de Mora d'Ebre, y acudió a su oficina de la entidad bancaria para denunciar presencialmente los hechos. En fecha 1 de marzo de 2022 la entidad bancaria le comunica que no se procederá a la devolución del importe de 2.577,00 € al considerar que se trata de operaciones autorizadas correctamente y con el uso de las credenciales de seguridad personalizadas. Anexa como documento número ONCE la denuncia ante la autoridad policial, como documento número DOCE el formulario de denuncia ante la entidad bancaria, y como documento número TRECE en e-mail de respuesta de la entidad bancaria ante la denuncia efectuada. Así mismo, acude ante el Defensor del Cliente en fecha 11 de marzo de 2022 solicitando el reintegro de la cuantía sustraída, recibiendo el 31 de marzo de 2022 como respuesta que se inhibía de la reclamación por considerar que "excedía de su ámbito competencial".

La representación procesal de la parte actora expone que Dª [redacted] ha sufrido una pérdida patrimonial por importe de 2.577,00 €, pagado por la entidad bancaria sin su autorización y sin haber recibido ningún código de verificación por parte de la entidad bancaria, que da lugar a la responsabilidad extracontractual y contractual de la entidad bancaria.

La representación procesal de la parte demandada alega existencia de prejudicialidad penal al existir denuncia penal de los hechos y la continuación de estas actuaciones podría derivar en el dictado de resoluciones totalmente contradictorias con vulneración de Derechos Fundamentales de los intervinientes en este procedimiento.

Así mismo, manifiesta que efectivamente el objeto de este procedimiento es el daño sufrido por la parte actora al ser víctima de "phishing", que consiste en una actividad delictiva cuyo objeto es dar la apariencia frente a la víctima de ser un tercero, valiéndose incluso de emblemas y/o marcas comerciales similares, con ánimo de obtener datos personales y de seguridad provocando en la víctima un perjuicio patrimonial.

La representación procesal de la parte demandada aduce que la entidad bancaria "Banco Santander SA" ha cumplido escrupulosamente con sus deberes legales y contractuales en todo momento, siendo la parte actora quién actúa negligentemente al ceder sus credenciales de seguridad como consecuencia del engaño producido mediante técnicas de ingeniería social, conducentes a recabar datos bancarios sensibles, y que la falta de filtros en el envío y recepción de mensajes falsos sin un ID real o verificado no puede ser oponible a la entidad bancaria.

Anexa como documento número UNO el certificado REDSYS que acredita que la entidad bancaria en todo momento entendió que la operación estaba siendo producida por la parte actora al ser autorizada con sus claves de seguridad, y como documento número DOS el Registro de SMS/OTP enviados (autenticación PSD2) que demuestra que las operaciones fueron registradas correctamente y autenticadas pues, para realizar las mismas, no sólo el phiser o estafador tuvo acceso a las credenciales de seguridad de la parte demandante, porque así fueron cedidas a través del enlace malicioso del SMS, sino porque también tuvo acceso a los códigos SMS/OTP enviados al móvil del cliente para autenticar las operaciones, bien porque dicho terminal se encontrase hackeado o su SIM duplicada, o bien porque dicho códigos fueron igualmente cedidos al phiser por la parte demandante. Por tanto, el ciber-delincuente dispuso de los datos bancarios de la demandante (Número PAN, CVV...), del código OTP remitido mediante SMS por la entidad bancaria para autenticar la operación, así como de las claves de acceso a la Banca Digital.

Por todo ello, expone que la entidad bancaria puede demostrar el correcto funcionamiento del proceso de autenticación reforzada en las operaciones realizadas, llegando a la conclusión que fue la parte actora quién perdió el control sobre sus credenciales de seguridad.

Segundo.- En relación a la prejudicialidad penal, el artículo 40 de la Ley de Enjuiciamiento Civil establece que cuando en un proceso civil se ponga de manifiesto un hecho que ofrezca apariencia de delito o falta perseguible de oficio, el Tribunal Civil, mediante providencia, lo pondrá en conocimiento del Ministerio Fiscal, por si hubiere lugar al ejercicio de la acción penal.

Hay que decir que con carácter general la existencia de una cuestión prejudicial penal no suspende el curso del proceso civil. En este sentido, la STS 209/13 de 4

[redacted] abril, Roj: STS 1569/2013 - ECLI:ES:TS:2013:1569, declaró que «para que resulte procedente la suspensión por prejudicialidad penal, el artículo 40.2 LEC no sólo exige, en el apartado 1º, la existencia de una causa criminal por unos hechos de apariencia delictiva que fundamenten las pretensión del proceso civil, sino también, en el 2º, que la decisión del tribunal penal acerca del hecho por el que procede la causa criminal pueda tener un influencia decisiva en la resolución sobre el asunto civil». Evidentemente, la carga de la prueba tanto de la existencia de la cuestión prejudicial penal como de la concurrencia de las circunstancias que posibilitan la suspensión del procedimiento civil, corresponde al litigante que la solicita.

En el caso que nos ocupa, queda acreditado y demostrado que la parte actora ha interpuesto la correspondiente denuncia ante los Mossos d'Esquadra de Mora d'Ebre en fecha 21 de febrero de 2022, pero en cambio no se ha demostrado el estado actual de las actuaciones policiales, ni que haya derivado en un procedimiento penal en el Juzgado de Instrucción correspondiente.

Ello permite concluir que entre ambos pleitos no media la vinculación causal que podría justificar la suspensión de las presentes actuaciones por causa de prejudicialidad penal, por ende, la petición de suspensión no puede tener acogida.

Tercero.- A la luz de las normas generales sobre la distribución del onus probandi, ha de entenderse que incumbe a la parte actora, según el tenor del párrafo 1º del artículo 217 de la Ley de Enjuiciamiento Civil, el deber de probar los hechos que permanezcan inciertos y fundamenten sus pretensiones, así como aquellos otros de los que ordinariamente se desprenda, según las normas jurídicas a ellos aplicables, el efecto jurídico correspondiente a las pretensiones deducidas en el escrito de demanda (párrafo 2º de la norma citada). Demostrados por el demandante, en su caso, los hechos que fundamentan su pretensión, se asigna a la demandada, conforme al párrafo 3º del precitado artículo 217 de la Ley Procesal, la carga de probar los hechos que, conforme a las normas que les sean aplicables, impidan, extingan o enerven la eficacia jurídica de los hechos a que se refiere el apartado anterior.

De la prueba documental queda demostrado y acreditado que en fecha 20 de febrero de 2022 (domingo) a las 19,22.-horas se inició un ciberataque, con aplicación de una técnica de ingeniería social, sobre la plataforma de banca on-line de Dª [redacted] a través del envío a su dispositivo móvil de un mensaje SMS al que se dio la apariencia de haber sido remitido por la entidad bancaria "BANCO SANTANDER", a través del cual le sustrajeron la cuantía total de 2.577,00 €. Así mismo, queda demostrado que posteriormente la entidad bancaria demandada a través del servicio de SMS notifica a la parte actora el intento de dos compras no autorizadas con la tarjeta de crédito y el registro de operaciones no habituales.

Dª [redacted] declara ante esta sede judicial que en el momento en que recibe un SMS en su teléfono móvil comunicándole que había un problema de seguridad con su cuenta bancaria, lo da por veraz y procede a realizar todas las maniobras que le demandan a fin de solucionar dicho problema. Manifiesta que todo tenía apariencia que provenía de la entidad bancaria "Banco Santander SA", Manifiesta que ella es usuaria de un teléfono IPhone, el cual está identificado en la entidad bancaria, pero es curioso que la compra de 2.577,00 € se realice con un dispositivo Xiaomi que nunca ha utilizado ni tenido, y que la entidad bancaria no lo detectara, dado que con el único dispositivo que se conecta a la banca electrónica es con su IPhone. A preguntas de la letrada de la parte demandada reitera que la entidad bancaria le avisa de actividad sospechosa una vez ya se ha realizado la primera compra, bloqueando una segunda, y que en ningún momento recibe un SMS solicitando la verificación o validación del pago, viendo el cargo directamente en su cuenta corriente.

Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita o "suplanta la identidad" de una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.

La normativa aplicable en estos casos es el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera y de la legislación de consumidores y usuarios. Según el artículo 36 de dicha norma, a falta del consentimiento del usuario de la operación de pago, la misma se considera no autorizada. El artículo 43 manifiesta 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. Establece la norma en su artículo 45 que, en caso de que se ejecute una operación no autorizada, el banco devolverá al usuario el importe de la operación de inmediato y a más tardar al final del día hábil siguiente a la notificación de la operación. La excepción a lo anterior es que el banco sospeche de la existencia de fraude, en cuyo caso debe comunicar dichos motivos al Banco de España. Pero también restituirá al usuario el adeudo, pues su obligación es actuar con la diligencia de un buen comerciante.

La responsabilidad del banco descansa sobre el hecho de que la tecnología que implementa son fuentes generadoras de riesgo a través de lo que se denominan «fugas del sistema». Y entiende la jurisprudencia menor que deben responder de ellas porque son los bancos quienes imponen el uso en masa de sus tarjetas, con sus reglas de funcionamiento y seguridad (Sentencia nº 428/2021 de la Audiencia Provincial de Salamanca). Es decir, que la falsedad de una transferencia es un riesgo a cuenta del banco. Máxime cuando la eficacia del sistema de autenticación del banco exonera de responsabilidad al mismo. Por tanto, 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.

La Sentencia nº 74/2022, de 28 de febrero, de la Audiencia Provincial de Madrid (Sección 11ª) expone, "en cuanto la responsabilidad cuasiobjetiva del banco en el supuesto de operaciones de pago no autorizadas por el usuario, que "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.", "La responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse 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.", "La resolución planteada ente esta Sala debe tener un carácter revocador teniendo en cuenta el contenido de la anterior sentencia, pudiéndose añadir el conocido "riesgo operacional", que debe ser asumido por los bancos en virtud de su posición de garante al ser una pieza clave para evitar la comisión de fraudes. Así mismo, existe una obligación genérica de las entidades financieras por buenas prácticas profesionales, gestión de riesgos y defensa frente a fraudes, estableciendo procedimientos que garantizan el principio "Conoce a tu Cliente", que incluye que los bancos deben conocer el tipo de operaciones que estos realizan e identificar posibles operaciones irregulares y/o fraudes de los que puedan ser víctimas. En conclusión, salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante (Art.32), la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago "no se vio afectada por un fallo técnico o cualquier otra deficiencia" (art. 30). La interpretación efectuada por la Juzgadora ad quem de la Ley 16/2009, de 13 de noviembre, de servicios de pago, no es acorde no sólo con la literalidad de la norma, sino con el espíritu y finalidad de la misma (ex. art. 3 CC), en función de lo previsto, en los artículos 30 y 32 de la mentada Ley 16/2009, de 13 de noviembre, de servicios de pago, pudiendo concluir con la determinación de la responsabilidad

de la entidad bancaria a pesar de sus afirmaciones sobre la implementación de un modelo seguro de banca online, siendo lo cierto que ninguna prueba objetiva se aporta, lo que no implica que el Tribunal niegue que el sistema fuera genéricamente seguro, porque es consustancial al propio sistema, sino porque no consta qué medidas en particular constituían el modelo de actuación progresivo y de respuesta ante las distintas formas fraudulentas de actuar"

Analizada la responsabilidad de la entidad de pago, resta hacer lo propio con la del usuario. Y es que, el único caso en que la norma obliga al usuario a soportar las pérdidas es si él mismo ha actuado en fraude o incumpliendo deliberadamente o por negligencia grave alguna de sus obligaciones.

La jurisprudencia es unánime a la hora de considerar que el banco debe restituir las cantidades antijurídicamente sustraídas por un tercero en tanto que como depositaria de los fondos tiene la obligación legal de conservar y devolver el dinero depositado. Únicamente se le podrá exonerar de dicha obligación cuando pudiera acreditar que el cliente ha actuado fraudulentamente o con negligencia grave a la hora de proteger sus datos personales y confidenciales, no pudiéndose considerar como negligencia o culpa haber caído en el fraude de un correo o página web aparentemente verídicos.

No obstante, de forma previa a la reclamación la víctima del engaño deberá poner en conocimiento del banco que se ha realizado una operación de pago no autorizada o ejecutada incorrectamente, según establece el artículo 43 de la misma Ley. Se entenderá que dicha comunicación se realizó de manera diligente siempre y cuando se efectuase en el plazo de 3 meses desde la fecha del acto delictivo.

Es criterio constante de la Jurisprudencia que la valoración de la prueba practicada por el órgano a quo ha de ser libre y racional conforme a las reglas de la sana crítica. En este sentido la Ley exige, para fundamentar la emisión de sentencia en la prueba practicada en el juicio, no sólo la existencia de una mínima actividad probatoria, sino que su contenido tenga entidad suficiente para construir enlace racional y ajustado a las reglas de la lógica deductiva entre el contenido del elemento probatorio seleccionado para sustentar el Fallo y la convicción a la que llega el órgano sentenciador. La convicción de éste debe asentarse sobre una firme y sólida base fáctica y un lógico proceso argumental para obtener, aun por las vías indirectas de la deducción valorativa de los hechos, un juicio fundado que no rompa con la necesaria armonía que debe presidir todo proceso deductivo (STS 19/09/90). Ha de reiterarse que la resolución del debate radicaba únicamente en calibrar la valoración probatoria de las pruebas practicadas, y que en el trance de acometer tal tarea, en función de las consideraciones expuestas y los indicios aportados a las actuaciones, se han reputado todas ellas dotadas de la virtualidad suficiente para fundamentar la sentencia condenatoria.

Cuarto.- En cuanto a las costas procesales por imperio de los artículos 32 y 394 y siguientes de la Ley de Enjuiciamiento Civil, ha lugar a su imposición a la parte demandada.

En relación a los intereses moratorios del artículo 1100 y siguientes del CC, solicitados por la parte actora, corresponden desde la reclamación extrajudicial o judicial. En este caso, corresponden desde la interposición de la demanda dada la materia que nos ocupa.

Fallo

Estimo la demanda formulada por la procuradora de los Tribunales Dª [redacted] en representación de Dª [redacted] contra la entidad bancaria "Banco Santander SA", y en su consecuencia, declaro a la entidad bancaria "Banco Santander SA" como responsable de los daños y perjuicios causados a través del "phishing", y **condeno** a la entidad bancaria "Banco Santander SA" a indemnizar a Dª [redacted] en la cuantía total de 2.577,00 € más los correspondientes intereses moratorios desde la interposición de la demanda, y del artículo 576 de la LEC, con expresa imposición de las costas procesales a la parte demandada.

Modo de impugnación: recurso de APELACIÓN ante la Audiencia Provincial de Tarragona (art.455 de la LEC). El recurso se interpone mediante un escrito que se debe presentar en este Órgano dentro del plazo de VEINTE días, contados desde el siguiente al de la notificación, en el que se debe exponer las alegaciones en que se base la impugnación, citar la resolución apelada y los pronunciamientos que impugna. Además, se debe constituir, en la cuenta de Depósitos y Consignaciones de este Órgano judicial, el depósito a que se refiere la DA 15ª de la LOPJ reformada por la LO 1/2009, de 3 de noviembre. Sin estos requisitos no se admitirá la impugnación (arts. 458.1 y 2 de la LEC).

Así lo mando y firmo.
La Juez en sustitución Mª del Carmen Marcos Álvarez

responsabilidad de la misma, dónde serán tratados con la máxima diligencia.

Quedan informados de que los datos contenidos en estos documentos son reservados o confidenciales y que el tratamiento que pueda hacerse de los mismos, queda sometido a la legalidad vigente.

Los datos personales que las partes conozcan a través del proceso deberán ser tratados por éstas de conformidad con la normativa general de protección de datos. Esta obligación incumbe a los profesionales que representan y asisten a las partes, así como a cualquier otro que intervenga en el procedimiento.

El uso ilegítimo de los mismos, podrá dar lugar a las responsabilidades establecidas legalmente.

En relación con el tratamiento de datos con fines jurisdiccionales, los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación en el proceso en que los datos fueron recabados. Estos derechos deberán ejercitarse ante el órgano judicial u oficina judicial en el que se tramita el procedimiento, y las peticiones deberán resolverse por quien tenga la competencia atribuida en la normativa orgánica y procesal.

Todo ello conforme a lo previsto en el Reglamento EU 2016/679 del Parlamento Europeo y del Consejo, en la Ley Orgánica 3/2018, de 6 de diciembre, de protección de datos personales y garantía de los derechos digitales y en el Capítulo I Bis, del Título III del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.