RESEÑA DE JURISPRUDENCIA INTERESANTE A 27 DE MAYO DE 2025

PENAL

Órgano: Tribunal Supremo. Sala de lo Penal
Sede: Madrid
Sección: 1
Fecha: 22 de abril de 2025
Nº de Recurso: 2786 /2022
Nº de Resolución: 1197/2024
Procedimiento: Recurso de casación
Tipo de resolución: Sentencia
Id Cendoj: 28079120012025100394

MATERIA: Absolución al considerar que no se ha probado, fuera de toda duda razonable, la falta de consentimiento en las relaciones sexuales, elemento esencial para la configuración del delito de abuso sexual. Esta decisión subraya la importancia del principio de presunción de inocencia y la necesidad de una prueba contundente para desvirtuarlo en el ámbito penal.

El proceso judicial se inició con la Sentencia nº 137/2021, de fecha 21 de diciembre de 2021, dictada por la Sección Primera de la Audiencia Provincial de Palma de Mallorca. Esta sentencia condenó a P F como autor penalmente responsable de un delito de abuso sexual del art. 181 apartados 1, 2 y 4 del Código Penal, en continuidad delictiva (art. 74 CP), imponiéndole una pena de siete años y un día de prisión, además de las accesorias correspondientes.

Contra esta sentencia de primera instancia, el acusado interpuso un recurso de apelación. La Sentencia 7/2022, de 21 de marzo de 2022, dictada por la Sala Civil y Penal del Tribunal Superior de Justicia de las Illes Balears, desestimó dicho recurso de apelación, confirmando la condena inicial.

Ante esta situación, el acusado interpuso el presente recurso de casación ante el Tribunal Supremo, buscando la revisión de las decisiones judiciales previas.

El aspecto central y determinante de la Sentencia del Tribunal Supremo es la modificación del relato fáctico que había sido establecido en las instancias anteriores. De manera explícita, el Tribunal Supremo declara que:

"Modificamos el relato fáctico de la sentencia recurrida, en el sentido de no considerarse probado que PF mantuviese relaciones sexuales sin consentimiento de la denunciante, o al menos fuera de toda duda razonable."

Esta modificación reviste una importancia crucial, ya que el Tribunal Supremo establece que no existe prueba que permita afirmar con la certeza necesaria (más allá de toda duda razonable) que las relaciones sexuales se produjeron sin el consentimiento de la denunciante. Este principio de "duda razonable" es fundamental en el derecho penal y, si no se supera, debe conducir a la absolución.

En cuanto a los fundamentos de derecho, la sentencia es muy concisa. En su Fundamento Único, el Tribunal Supremo se remite a lo ya razonado en su "anterior Sentencia Casacional" (se entiende que se refiere a la primera sentencia dictada en este mismo recurso de casación, que abordaba otras cuestiones, como posiblemente el derecho de defensa, aunque el documento actual se centra en el fallo final y la modificación de hechos probados). En virtud de esta remisión y de la modificación del relato fáctico, el Tribunal llega a la conclusión de que la absolución es imperativa.

En consecuencia, el Tribunal Supremo decide absolver a PF del delito continuado de abuso sexual del que había sido acusado. Además, declara de oficio las costas procesales de ambas instancias anteriores (Audiencia Provincial y Tribunal Superior de Justicia), lo que significa que el acusado no deberá hacerse cargo de estos gastos judiciales.

SOCIAL

Órgano: Tribunal Supremo. Sala de lo Social
Sede: Madrid
Sección: 991
Fecha: 7 de abril de 2025
Nº de Recurso: 4716 /2023
Nº de Resolución: 289/2025
Procedimiento: Recurso de casación
Tipo de resolución: Sentencia
Id Cendoj: 28079149912025100008

Este caso trata sobre si el Instituto Nacional de la Seguridad Social (INSS) debe pagar intereses moratorios en una reclamación por el complemento de maternidad por aportación demográfica, tras reconocer el derecho del demandante a recibirlo desde 2017.

La sentencia inicial del Juzgado de lo Social favoreció al demandante, condenando al INSS a pagar el complemento y los intereses desde la reclamación previa en 2021. Sin embargo, el INSS recurrió y el TSJ del País Vasco confirmó la decisión, pero posteriormente el recurso de casación del INSS fue estimado, anulando la condena a intereses.

El debate central radica en si, según la ley y la jurisprudencia, debe condenarse al INSS a pagar intereses moratorios en estos casos. La sentencia analiza varias cuestiones clave:

1. **Contradicción entre sentencias**: se comparan dos sentencias del TSJ que interpretan la ley de forma opuesta respecto a los intereses en casos similares. La sentencia recurrida condenaba a pagar intereses desde la fecha de efectos de la pensión, mientras que otra sentencia de contraste no lo hacía.

2. **Fundamentos jurídicos**:
    - La ley (LGSS y Ley General Presupuestaria) regula los intereses en relación con la relación de cotización, no en la relación de protección (prestaciones). La LGSS establece claramente cuándo se devengan intereses en cada caso.
    - La jurisprudencia del Tribunal Constitucional (STC 23/1997 y 209/2009) ha establecido que, en las relaciones de Seguridad Social, no se devengan intereses moratorios en la relación de protección, salvo en casos específicos como el fraccionamiento de pagos por prestaciones indebidas.

- La relación de cotización (entre empleador y la Seguridad Social) sí contempla intereses tanto a favor como en contra, pero esto no se aplica automáticamente a las prestaciones (relación beneficiario-Administración).

3. **Aplicación del artículo 1100 del Código Civil**:
   - La ley no obliga a pagar intereses moratorios en las prestaciones de la Seguridad Social, salvo excepciones muy concretas. La aplicación supletoria del CC (artículos 1100 y 1108) no es adecuada porque la LGSS regula expresamente los intereses y no hay laguna normativa.
   - Además, los intereses moratorios requieren una obligación líquida, vencida y exigible, y en las prestaciones públicas, generalmente, no se considera que exista esa exigibilidad inmediata, ya que la solicitud y reconocimiento de la prestación no funciona como una reclamación de deuda líquida y vencida.

4. **Normativa aplicable y jurisprudencia**:
   - La Ley General Presupuestaria (artículo 24) regula los intereses en casos de retraso en pagos de la Administración, pero su aplicación en prestaciones de Seguridad Social es limitada y requiere que se cumplan ciertos requisitos (resolución judicial, reclamación escrita, plazo de tres meses).
   - La jurisprudencia ha condenado a las Administraciones públicas al pago de intereses moratorios en casos de deudas salariales o indemnizaciones derivadas de contratos laborales, pero no en las prestaciones de la Seguridad Social, que tienen una naturaleza distinta y no contemplan intereses en su regulación.

5. **Discriminación y daños**: la sentencia también menciona que, tras una sentencia del TJUE, se reconoció que la negativa del INSS a reconocer el complemento de maternidad a los varones era discriminatoria. En estos casos, además de la condena a pagar el complemento, se condenó a pagar una indemnización por daños y perjuicios.

CIVIL

Órgano: Tribunal Supremo. Sala Primera de lo Civil
Sede: Madrid
Sección: 991
Fecha: 9 de abril de 2025
Nº de Recurso: 1151/2023
Nº de Sentencia: 571/2025
Procedimiento: Recurso de casación
Tipo de resolución: Sentencia
Ref. CJ 85950/2025
ECLI: ES:TS:2025:1671
Id Cendoj: 28079110012025100563

BANCA. Realización de quince transferencias bancarias no autorizadas, a través de la plataforma de banca electrónica. Supuesto de estafa "SIM phishing". Responsabilidad cuasi objetiva de la entidad bancaria.

Cuando un cliente niegue haber autorizado una operación de pago ya ejecutada o alegue que se ejecutó de manera incorrecta, recae sobre el proveedor de servicios de pago la carga de probar que la operación fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado. La expresión "deficiencia del servicio" abarca cualquier falta de diligencia o mala praxis en la prestación del servicio. Las buenas prácticas pasan por adoptar las medidas de seguridad necesarias para garantizar el correcto funcionamiento del sistema de servicios de pago, entre las cuales destacan las orientadas a detectar de forma automática la concurrencia de indicios de que puede tratarse de una operación anómala y generar una alerta o un bloqueo temporal y las dirigidas a incrementar el control y vigilancia cuando se han recibido noticias o alertas de un posible aumento del riesgo.
(...)

FUNDAMENTOS DE DERECHO
PRIMERO.- *Resumen de antecedentes.*

1.- Son antecedentes fácticos no discutidos o declarados acreditados en la instancia y de interés para la resolución del recurso los siguientes:

i) D. Martin es titular, junto con sus padres, D. Torcuato y D.ª Raquel, de la cuenta corriente y/o depósito n.º NUM000, y, con su esposa Dña. Sonia, de la cuenta corriente n.º NUM001, ambas abiertas en la entidad Unicaja Banco S.A. Asimismo, D. Martin y Unicaja Banco S.A. suscribieron en fecha 31 de agosto de 2004 un contrato de banca a distancia nº NUM002***.

(...)

iii) El mismo 24 de febrero, a las 06:37, D. Martin recibió en su teléfono móvil, n.º NUM003*****, varios mensajes SMS con códigos para la materialización a través del sistema digital de transferencias que no obedecían a órdenes emitidas por él, lo que puso en conocimiento del personal de la sucursal del banco.

*iv) En fechas 27 de febrero y 2 y 12 de marzo de 2021, Google Play y Google Ads realizaron varios cargos no autorizados en la cuenta n.º NUM001, por valor de 464,98 €, utilizando su tarjeta VISA n.º NUM004 ****, lo que D. Martin comunicó a la entidad bancaria, reiterando su preocupación por los SMS recibidos,* al tiempo que presentaba la pertinente reclamación a Google, que la rechazó el 15 de marzo, al no haber podido confirmar que se hubiera producido algún tipo de actividad fraudulenta.

(...)

vi) Entre la noche del 17 y la mañana del 18 de marzo de 2021 se realizaron quince transferencias bancarias desde la cuenta corriente n.º NUM000, de las cuales diez lo fueron a través de la plataforma Bizum (por importe de 500 € cada una) y cinco a través de la plataforma de banca electrónica «Ibercaja Directo» (por importes de 28.970 €, 19.870 €, 9.876 € y dos de 9.870 € cada una -78.456,20 € en total-), devengando 236,53 € en comisiones, lo que suma un cargo total de 83.692,73 €.

vii) La mayoría de las mencionadas transferencias se efectuaron a favor de delincuentes conocidos por la Policía, a través de la línea de móvil NUM003*****, titularidad de D.ª Estefanía, para lo cual se utilizó una tarjeta SIM que había sido duplicada el 17 de marzo, a las 17:29 horas, sin autorización de la titular, en el distribuidor Remedios (Murcia), lo que permitió al autor/es acceder a la información almacenada en la tarjeta, y recibir y utilizar el código solicitado para las sucesivas operaciones.

viii) El demandante no supo lo sucedido hasta la mañana del día 18 de marzo, cuando el personal de la sucursal, alertado por una llamada del personal del Banco Santander S.A., que había detectado el ingreso realizado en una cuenta sospechosa, le preguntó si durante la noche había hecho transferencias por valor de 83.000 €, a lo que respondió que no. Al acceder a la banca electrónica y comprobar la realidad de la información, el mismo día 18 presentó la correspondiente denuncia en la comisaría

de la Policía Nacional, lo que motivó la incoación de las diligencias previas n.º 1017/21021 por el Juzgado de Instrucción n.º 11 de Zaragoza.

ix) En atención a la reclamación del actor, Ibercaja Banco S.A. solicitó la restitución de las cantidades dispuestas a las distintas entidades de destino, consiguiendo la devolución de 27.218,10 €, que fueron reintegrados al actor.

2.- En el presente procedimiento y con base en los mencionados hechos, D. Martin ejercita una acción de responsabilidad contractual frente a Ibercaja Banco S.A., en reclamación de 56.474,63 €, por los daños y perjuicios causados por el incumplimiento de las obligaciones asumidas por la demandada en el contrato de banca a distancia y en el contrato de cuenta corriente y/o depósito nº NUM000, titularidad de D. Martin y de sus padres, D. Torcuato y D.ª Raquel, al haberse realizado quince transferencias bancarias no autorizadas, a través de la plataforma de banca electrónica «Ibercaja Directo».

(...)

4.- La sentencia de instancia estima la demanda y condena a la demandada a abonar al actor la cantidad reclamada.

(...)

5.- La entidad Ibercaja Banco S.A. presentó recurso de apelación, que fue desestimado por la Audiencia Provincial.

(...)

6.- La entidad demandada Ibercaja Banco S.A. formula recurso de casación contra la expresada sentencia, que fundamenta en dos motivos que seguidamente se analizarán.

SEGUNDO.- *Primer motivo de recurso de casación*.

2.-*Decisión de la Sala*. El motivo debe ser desestimado por las razones que seguidamente se exponen.

La controversia radica en determinar quién debe responder por las operaciones de pago no autorizadas, en tanto que realizadas por un tercero que, utilizando las credenciales del usuario que ha obtenido por cualquier medio, suplanta su identidad y accede electrónicamente a su cuenta sin su consentimiento. O, dicho de otra manera, qué debe entenderse por «operaciones de pago no autorizadas», si, en general, las que han sido realizadas por un tercero sin el consentimiento del usuario titular de la cuenta, o, exclusivamente, las efectuadas sin seguir el procedimiento legal y contractualmente fijado.

Con carácter previo, es preciso significar que *la Audiencia ha declarado probado que las operaciones de pago se ejecutaron por terceras personas, ajenas y sin el consentimiento del demandante,* lo que comporta rechazar de plano las dudas sugeridas por la recurrente.

[...]

6.- Con arreglo a la normativa comunitaria y nacional aplicable y a la jurisprudencia comunitaria recaída en interpretación de la regulación de la que trae causa la primera, podemos concluir:

1.º El usuario de servicios de pago debe adoptar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas y, en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, ha de notificarlo al proveedor de servicios de pago de manera inmediata, tan pronto tenga conocimiento de ello.

2.º En caso de que se produzca una operación de pago no autorizada o ejecutada incorrectamente, si el usuario de servicios de pago se lo comunica sin demora injustificada, el proveedor debe proceder a su rectificación y reintegrar el importe de inmediato, salvo que tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España.

3.º Cuando un usuario niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, incumbe al proveedor la carga de 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.

4.º El mero hecho del registro por el proveedor de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones, correspondiendo al proveedor la prueba de que el usuario del servicio de pago cometió fraude o negligencia grave.

En suma, la responsabilidad del proveedor de los servicios de pago, en los casos de operaciones no autorizadas o ejecutadas incorrectamente, tiene carácter cuasi objetivo, en el doble sentido de que, primero, notificada la existencia de una operación no autorizada o ejecutada incorrectamente, el proveedor debe responder salvo que acredite la existencia de fraude; y, segundo, cuando el usuario niegue haber autorizado la operación o alegue que ésta se ejecutó incorrectamente, corresponde

al proveedor acreditar 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, sin que el simple registro de la operación baste para demostrar que fue autorizada ni que el usuario ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave.

Profundizando en este último punto, la expresión «operaciones no autorizadas» incluye aquellas que se han iniciado con las claves de usuario y contraseña del usuario -necesarias para acceder al sistema de banca digital- y confirmado mediante la inserción del SMS enviado por el propio sistema al dispositivo móvil facilitado por el usuario, siempre que éste niegue haberlas autorizado, en cuyo caso el banco deberá acreditar 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 que presta.

A este respecto, la mención «deficiencia del servicio» no significa error o fallo del sistema informático o electrónico -posibilidad que estaría prevista en el concepto de «fallo técnico»-, sino que abarca cualquier falta de diligencia o *mala praxis* en la prestación del servicio, en el entendimiento de que el grado de diligencia exigible al proveedor de los servicios de pago no es el propio del buen padre de familia, sino que la naturaleza de la actividad y los riesgos que entraña el servicio que se presta, sobre todo en una relación empresario/consumidor, obliga a elevar el nivel de diligencia a un plano superior, como es el del ordenado y experto comerciante.

Lógicamente, las buenas prácticas pasan por adoptar las medidas de seguridad necesarias para garantizar el correcto funcionamiento del sistema de servicios de pago, entre las cuales destacan las orientadas a detectar de forma automática la concurrencia de indicios de que puede tratarse de una operación anómala y generar una alerta o un bloqueo temporal (v.gr. reiteración de transferencias sin solución de continuidad, horario en que se producen, importe de las mismas, destinatarios, antecedentes en el uso de la cuenta...), o las dirigidas a incrementar el control y vigilancia cuando se han recibido noticias o alertas de un posible aumento del riesgo.

7.- Según se avanzó antes, la aplicación de la normativa y jurisprudencia expuesta nos lleva a rechazar el motivo de recurso.

(...)

En otras palabras, *el que la entidad bancaria acredite que la operación fue autenticada, registrada con exactitud y contabilizada, no es suficiente para eximirle de responsabilidad. Ha de probar que la operación no resultó afectada por un fallo*

técnico u otra deficiencia del servicio prestado, y, dado que el cliente niega que la operación fuera consentida, que no hubo (sic) por parte de este último fraude, incumplimiento deliberado o negligencia grave. Sin embargo, lejos de haber acreditado tales extremos, la prueba practicada evidencia lo contrario.

(...)

Estos precedentes ponían de manifiesto, para cualquier observador medio, razonablemente atento y perspicaz, y más aún, para un empleado de banca, que alguien había conseguido acceder a las cuentas del actor, y, por ende, que disponía de sus claves de usuario y contraseña, lo que hubiera debido motivar una reacción inmediata, que pasaba cuando menos por la modificación de las claves y/o códigos. Nada se hizo. Al no adoptarse medida de protección alguna, tan solo restaba que los autores encontraran la manera de eludir el último obstáculo, esto es, la vía para recibir directamente el código de confirmación de la operación.

Por otra parte, los avances de la tecnología actual hacen relativamente sencillo diseñar sistemas o aplicaciones informáticas idóneas para detectar ciertas anomalías en la prestación de los servicios de pago. Operaciones que, tratándose de empresas o sociedades con un concreto objeto social, pueden calificarse como ordinarias, deben inmediatamente levantar sospechas y dar lugar a una respuesta cuando afectan a personas físicas ajenas a tales actividades. A este respecto, sería suficiente un control automático de determinados factores, como el número y sucesión de operaciones, el intervalo en que se ejecutan, la hora del día, su importe, entidades de destino..., para generar un aviso que reforzara los requisitos de confirmación y minimizara los posibles riesgos. No puede considerarse como normal e irrelevante que una persona que jamás efectúa operaciones de madrugada, de repente, proceda a llevar a cabo hasta diecisiete operaciones seguidas y por un importe tan elevado. Del mismo modo que el sistema rechazó dos de Bizum por exceder del máximo diario, el proveedor de servicios de pago ha de adoptar las medidas de seguridad que garanticen su correcto funcionamiento y minimicen los riesgos y los efectos nocivos de su materialización.

Llegado este punto, nos encontramos, de un lado, ante una conducta diligente del titular de la cuenta, que informó, inmediata y reiteradamente, al personal de entidad de lo que estaba sucediendo, cumpliendo la obligación que expresamente le imponía la normativa comunitaria y nacional; y, de otro lado, ante un servicio que se presta defectuosamente por el proveedor, tanto por no tomar en consideración la información recibida pese a su gravedad, como por omitir la adopción de medidas que posibilitaran la detección de eventuales maniobras fraudulentas.

Por consiguiente, no se aprecia infracción del art. 36.1 del Real Decreto Ley 19/2018, lo que comporta la desestimación del motivo.

TERCERO.- *Segundo motivo de recurso.*

2.-*Decisión de la Sala*. El motivo debe desestimarse por las razones que seguidamente se exponen.

La recurrente reitera que ha cumplido con rigurosidad sus obligaciones, la identificación del usuario, la autentificación de las operaciones realizadas y la aplicación del doble factor de autenticación impuesta por la normativa de servicios de pago, sin que haya sufrido ningún tipo de incidencia técnica como para que le fueran usurpados ningún tipo de datos de clientes que permitieran a terceros realizar las transferencias discutidas, por lo que de acuerdo con el art.44 RDL 19/2018 no debe responder.

(...)

Mas ya hemos visto que, *de conformidad con el art. 44 RDL, en caso de que el usuario niegue haber autorizado una operación de pago ya autorizada, el cumplimiento de las obligaciones relativas a la autenticación, registro y contabilización de la operación de pago fue autenticada, no exime de responsabilidad al proveedor de servicio, sino que deberá acreditar además que la operación no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado, sin que mero registro de la utilización del instrumento de pago baste para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones*.

En el supuesto enjuiciado fallan ambos presupuestos. En primer lugar, la entidad demandada debía probar, no solo que la operación no se vio afectada por un fallo técnico, sino que no se ha producido una prestación defectuosa del servicio, cuestión que ya ha sido objeto de análisis con ocasión de examinar el anterior motivo, concluyendo que el servicio no se prestó correctamente.

Asimismo, el hecho de que la filtración o el conocimiento de las claves por el tercero no sea imputable a la entidad bancaria tampoco la libera de obligación de responder ni traslada al usuario la obligación de soportar las pérdidas, ya que el proveedor de servicios de pago, además de demostrar que el servicio se prestó correctamente -lo que no sucedió-, debía acreditar la concurrencia de fraude o incumplimiento deliberado o gravemente negligente por parte del usuario, y, en relación con este extremo, las sentencias de instancia

y de apelación coinciden en que no se ha probado fraude ni incumplimiento doloso o por negligencia grave de las obligaciones que correspondían al demandante, y, en concreto, las de tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas y de notificar al proveedor de servicios de pago la utilización no autorizada del instrumento de pago, tan pronto tuvo conocimiento de ello, lo que así hizo, participando las tentativas de acceso a su cuenta con una antelación de tres semanas.

Obsérvese que, contra lo que mantiene por la recurrente, *el que un tercero hubiera podido acceder a las claves de acceso a la banca digital del demandante no supone per se que haya incurrido en negligencia alguna, pudiendo existir múltiples explicaciones, muchas de las cuales resultan difícilmente atribuibles a título de negligencia, y menos aún, de negligencia grave*.

FALLO

Por todo lo expuesto, en nombre del Rey y por la autoridad que le confiere la Constitución, esta sala ha decidido:

1.º- Desestimar el recurso de casación interpuesto por Ibercaja Banco S.A., representada por el procurador D. Jorge Luis Guerrero Ferrández, bajo la dirección letrada de D.ª María Jesús Gracia Ballarín, contra la sentencia n.º 996/2022, de 17 de noviembre, dictada por la Sección 5.ª de la Audiencia Provincial de Zaragoza en el recurso de apelación n.º 20/2022, que confirmamos.

2.º- Imponer a Ibercaja Banco S.A. las costas del recurso de casación.

3.º- Ordenar la pérdida del depósito constituido para interponer el recurso de casación.

Líbrese al mencionado tribunal la certificación correspondiente, con devolución de los autos y del rollo de Sala.

Notifíquese esta resolución a las partes e insértese en la colección legislativa.

Así se acuerda y firma.