Dosier jurídico

Derecho Civil
Derecho Penal

El phishing bancario y responsabilidad de las entidades financieras

tirant PRIME

El phishing bancario y responsabilidad de las entidades financieras

Miguel Alcalá, Autor

CONCEPTO Y CARACTERIZACIÓN GENERAL DEL *PHISHING* BANCARIO

El *phishing* bancario son un conjunto de técnicas variadas utilizadas por ciberdelincuentes para suplantar la identidad de una entidad o persona legítima, reconocida y de confianza (bancos, instituciones, etc.) con el objetivo de conseguir información personal y bancaria de sus víctimas, para posteriormente apoderarse de dinero de sus cuentas y tarjetas.

Se dice que el término *phishing* proviene de la palabra inglesa *"fishing"* (pesca), haciendo alusión a utilizar un cebo y esperar a que las víctimas «muerdan el anzuelo.» También se dice que el término *phishing* es la contracción de *password harvesting fishing* (cosecha y pesca de contraseñas). A quien practica el *phishing* se le llama *phisher*.

La mayoría de los casos de *phishing* se distribuyen a través del correo electrónico, pero también se utilizan las redes sociales, creando perfiles y páginas falsas; envío de mensajes SMS al teléfono móvil (smishing); o mediante llamadas telefónicas (vishing); webs falsas (Pharming); duplicados de SIM (SIM swapping); interceptación de comunicaciones entre cliente y banco (MITM); Software malicioso (malware, troyanos bancarios); ataques personalizados (Spear phishing); aplicaciones móviles falsas (fake apps); perfiles en redes sociales falsas (Spoofing de dominios o perfiles).

Pero esto son solo alguno de los medios conocidos, ya que cada día aparecen nuevos métodos y estrategias de intento de fraude digital, exponencialmente en crecimiento con la utilización de la Inteligencia Artificial.

No obstante, los ataques de *phishing* se pueden clasificar según el objetivo contra el que se dirige el ataque, el fin, el medio que se utiliza o según el modo de operación. Un caso concreto puede pertenecer a varios tipos de *phishing* a la vez.

El «phishing» es actuación fraudulenta de terceros, que implica 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, de la que debe de responder de acuerdo con el régimen legal resumido.

REGULACIÓN

a. **a. Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera ((TOL6.920.021)) regula las obligaciones de las entidades financieras en relación con el denominado *phishing* bancario**.

Concretamente el Artículo 45 que lleva por rúbrica **«Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas»** establece una responsabilidad «cuasi objetiva» de la entidad bancaria que le obliga a reintegrar al titular de la cuenta las cantidades dispuestas y no autorizadas por él.

«1. Sin perjuicio del artículo 43 de este real decreto-ley, en caso de que se ejecute una ***operación de pago no autorizada****,* ***el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación****, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada.*

La fecha de valor del abono en la cuenta de pago del ordenante no será posterior a la fecha de adeudo del importe devuelto.

2. Cuando la operación de pago se inicie a través de un proveedor de servicios de iniciación de pagos, el proveedor de servicios de pago

gestor de cuenta devolverá inmediatamente y, en cualquier caso, a más tardar al final del día hábil siguiente, el importe de la operación de pago no autorizada y, en su caso, restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada.

Si el responsable de la operación de pago no autorizada es el proveedor de servicios de iniciación de pagos, deberá resarcir de inmediato al proveedor de servicios de pago gestor de cuenta, a petición de este, por las pérdidas sufridas o las sumas abonadas para efectuar la devolución al ordenante, incluido el importe de la operación de pago no autorizada. De conformidad con el artículo 44.1, corresponderá al proveedor de servicios de iniciación de pagos demostrar que, dentro de su ámbito de competencia, la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable.

3. Podrán determinarse otras indemnizaciones económicas de conformidad con la normativa aplicable al contrato celebrado entre el ordenante y el proveedor de servicios de pago o el contrato celebrado entre el ordenante y el proveedor de servicios de iniciación de pagos, en su caso.»

b. **Código penal**

Artículo 249.

«1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:

a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.»

c. **Protección de datos**

1. **Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales TOL6.933.570**

Artículo 5. Deber de confidencialidad.

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

2. **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). TOL5.703.078**

Artículo 5. Principios relativos al tratamiento

1. Los datos personales serán:

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

JURISPRUDENCIA CIVIL

a. **A favor del cliente bancario**

Tribunal Supremo. Sala Primera, de 09/04/2025 RES:571/2025 TOL10.495.958

«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.»

Audiencia Provincial de Santander, de 01/04/2025 RES:242/2025, TOL10.507.374

« SEXTO.-El hecho de entrar en un enlace que recibe a través de una SMS que el propio terminal identifica como de Unicaja Banco, y la página abierta es idéntica a la de la entidad bancaria demandada, no puede considerarse una negligencia grave. Igualmente, el hecho de recibir la llama de un teléfono identificado como de Unicaja y leer los códigos que iba recibiendo a su interlocutor, identificado como empleado de Unicaja, quien le había informado que se estaba produciendo un acceso ilegítimo en su cuenta bancaria, misma información que la recibida por SMS, no puede calificarse como negligencia grave, la actora pensó que era necesario dar los códigos que recibía en su terminal para impedir un acceso ilegítimo en su cuenta bancaria. En ningún caso la actora fue consciente que al abrir el enlace recibido por SMS y dar por teléfono los códigos recibidos estaba autorizando al banco a realizar dos transferencias de 1.990 y 2990 Euros y cuatro bizum por el importe máximo de 490, 480, 470 y 460 Euros cada uno. Inmediatamente que comprueba que le han retirado fondos de su cuenta presenta denuncia ante el cuartel de la Guardia civil y al día siguiente presenta denuncia ante la entidad bancaria demandada.

Del relato fáctico anterior, quizás podría inferirse que la actora no agotó al máximo toda la diligencia que podría haber observado, al dar los códigos que recibía en su terminal. Dicha actuación aislada, cuyas consecuencias dañosas no están al alcance de ser previstas por una persona media en dicha fecha, habida cuenta el uso generalizado de la operativa bancaria online, no podemos conceptuarla como de negligencia grave.

A ello debe añadirse que la entidad bancaria debió activar un mayor sistema mayor de seguridad. El concepto de la transferencia era una serie de números y letras. No figuraba concepto alguno ni en las transferencias ni en los Bizum, cuando de la relación de movimientos que aporta la demandada resulta que todos los bizum realizados por el actor figura concepto. No había hecho nunca ni transferencias ni bizum por esos importes.

Cualquier procedimiento o sistema de seguridad anti-phising implantado por la entidad demandada debería haber detectado el carácter fraudulento de las operaciones y haber bloqueado las mimas.»

Audiencia Provincial de Zaragoza, de 04/03/2025 RES:87/2025, TOL10.519.435

«7. El usuario se limitó, por tanto, a seguir de forma razonable las pautas marcadas por la aparente plataforma informática de Ibercaja Directo que se le mostraba en la pantalla de su ordenador introduciendo unos

códigos de verificación que le fueron remitidos a su teléfono móvil. Tal actuación no nos parece que constituya una negligencia grave, dado que el usuario podía entender razonablemente que se trataba de un mecanismo reforzado de seguridad. Por consiguiente, un fallo de seguridad del sistema técnico empleado por la demandada pudo permitir la operativa fraudulenta, lo que solo es reprochable a esa parte, al no haber demostrado ninguna otra deficiencia o explicación técnica que pudiera exonerarle de responsabilidad, pese a que sobre ella recae la carga de demostrarlo, como ha quedado dicho.

8. De este modo, no cabe alegar el incumplimiento por el cliente de lo fijado en las condiciones generales, ni menos hasta el punto de alterar el régimen legal de la distribución de riesgos previsto en el RDL 19/2018, el cual solo encuentra sus excepciones cuando el usuario de servicios de pago no sea un consumidor ni una microempresa (artículo 34). Dentro de ese sistema legal imperativo, al prestador del servicio le corresponde la carga de probar que la operación no se vio afectada por un fallo técnico u otra deficiencia del servicio y que el usuario cometió fraude o incurrió en negligencia grave.»

Audiencia Provincial de Valladolid, de 04/03/2025 RES:85/2025, TOL10.497.518

« La aplicación de este sistema normativo y de responsabilidad a los hechos narrados por el demandante y que han resultado probados, conduce a la desestimación del recurso de apelación. Ninguna de las actuaciones que el banco apelante imputa al demandante y califica de gravemente negligentes, pueden tener ese calificativo. Como bien explica el Juez "*a quo* "para la realización del fraude que es objeto de litis se utilizan mensajes engañosos que entran en el teléfono móvil de la víctima, como verificados o autentificados con el ID de los SMS de la propia entidad bancaria (BANKINTER), resultando así prácticamente imposible que el terminal telefónico de la víctima les pueda catalogar como fraudulentos o "spam" dando credibilidad a que son enviados por la entidad bancaria, y también se utilizan llamadas al teléfono móvil de la víctima que entran como realizadas legítimamente por la propia BANKINTER al identificar el terminal telefónico el número de teléfono que realiza la llamada como del servicio de atención al cliente del banco figurando el mismo número que pertenece a dicho servicio, por lo que también se hace prácticamente imposible que la víctima desconfíe de la llamada facilitando el código de verificación enviado a su teléfono móvil y, más aún, teniendo en cuenta que desde dicho supuesto centro de llamadas de BANKINTER, se le alerta de que la actuación que se le

propone es necesaria para anular un cargo fraudulento que el propio servicio de banco ha detectado.

El que ante este " modus operandi " el demandante hubiera dado veracidad a la llamada supuestamente de BANKINTER y facilitado las claves para operar, no puede calificarse de una actuación gravemente negligente dadas las características de entorno seguro y la apariencia de licitud en que la operación se produce, pues el defraudador está utilizando la identidad e identificación del propio banco, lo que razonablemente propicia el error del cliente haciéndole creer que realmente estaba operando con su banco cuando no es así ya que este ha sido suplantado (técnica conocida como *"phishing*"). No ha probado el banco por su parte, que hubiera adoptado o implementado aquellas medidas técnicas y de seguridad que fueran bastantes para detectar y evitar que se produjera esta clase de fraudes informáticos en su ámbito de actuación, ni en todo caso que las adoptadas fueran suficientes y eficaces para ello.»

Audiencia Provincial de Les Illes Balears, de 28/02/2025 RES:151/2025, TOL10.497.409

«Con base en ello, valorando las circunstancias concurrentes en el presente caso, no cabe apreciar negligencia grave por parte del demandante en el cumplimiento de su obligación de proteger sus credenciales de seguridad. No puede tacharse de gravemente negligente la conducta de quien, tras recibir en el mismo canal en el que recibe habitualmente las comunicaciones procedentes de su banco un mensaje de texto en el que se le informa que tiene que verificar su identidad facilitándole un enlace para ello, decide pulsar en ese enlace e introducir su usuario y contraseña, dado que, para una persona no experta, no es fácil detectar que el mensaje recibido es fraudulento o que la web a la que ha accedido a través del enlace facilitado es falsa.

No se niega que pudiera haber incurrido en falta de diligencia, o de exceso de confianza, cuando clickeó el mensaje autorizando el pago, no percatándose que no se trataba de un abono; provenía del mismo número de teléfono y desde el mismo hilo de mensajes que había dado inicio a toda la operación; no se estima que esto pueda ser llevado al extremo de ser tenido por una negligencia grave como la que invoca la recurrente, por lo que debe desestimarse el recurso de apelación interpuesto.»

Audiencia Provincial de Pontevedra, de 21/02/2025 RES:186/2025, TOL10.510.488

« Es al proveedor del servicio a quien incumbe la carga probatoria de demostrar su concurrencia, en el régimen de responsabilidad cuasi objetivo que ha quedado expuesto. Las sentencias de la Audiencia Provincial de Pontevedra de 1 de diciembre de 2022 y 23 de marzo de 2023 con cita de otras varias de diversas Audiencias, dando un paso más, señalan que "la negligencia que 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 haya podido ser inducido por un delincuente profesional. Como parámetro del actuar negligente también cabrá acudir al art. 1.104 CC (EDL 1889/1), que exige la diligencia asociada a la naturaleza de la obligación y a las circunstancias personales, de tiempo y lugar. Ello destacándose la complejidad y grado de perfección que presenta en la actualidad el método de "*phishing*" de difícil detección por persona de formación media, así como el deber de la proveedora del servicio de dotarse de tecnología suficiente y adecuada con exigencia de medidas implantadora activas, sin entenderse suficientes avisos generales o en página web de mero carácter informativo o divulgativo".»

Audiencia Provincial de Navarra, de 04/04/2025 RES:514/2025, TOL10.513.292

« Al limitarse la demandada a enviar las notificaciones PUSH a una aplicación, y no a un dispositivo concreto, sin cerciorarse de que las mismas llegan al teléfono móvil del cliente, ella misma pone de manifiesto que le resulta indiferente si ese mensaje lo recibe realmente el cliente u otra persona, lo que denota que su sistema de seguridad en absoluto es válido para evitar este tipo de fraudes. Al no incluir su sistema de verificación, información alguna relativa al concreto teléfono móvil al que se envían esas notificaciones, dando por sentado, que solo se pueden enviar a uno, cuando puede que no sea así, la entidad demandada de manera deliberada o culposa, decide ignorar si los PUSH se remiten a la persona legitimada para ello o no, a pesar de ser consciente de que, el único que tiene que validar una operación de pago es su concreto cliente. Cuando dicha operación se hace en persona, la entidad bancaria puede confirmar la identidad exigiendo la exhibición del D.N.I. donde se recogen datos suficientes para confirmar la identidad de la persona que pretende realizar la operación bancaria, entre otros, su propia imagen, y donde el empleado se puede cerciorar de que esa persona es la legitimada para realizar dicha operación. En la banca online se obvian estas cautelas y por ello la entidad financiera, que es la que más ventajas obtiene de dicho tipo de funcionamiento, por el ahorro de costes, entre otros motivos, debe extremar los

mecanismos de garantizar que las operaciones realizadas a través de dicho sistema sean seguras para el cliente." De lo expuesto, no puede sino compartirse la conclusión a la que llega la Juzgadora de Instancia, esto, es que no estamos ante dos operaciones debidamente autorizadas, así como la no acreditación ausencia de fallas en el sistema implementado por la demandada.»

Audiencia Provincial de Badajoz, de 19/02/2025 RES:71/2025, TOL10.507.682

« Ha de recordarse que ".. la **negligencia** que 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 haya podido ser inducido por un delincuente profesional. Como parámetro del **actuar negligente** también cabrá acudir al art. 1.104 CC , que exige la diligencia asociada a la naturaleza de la obligación y a las circunstancias personales, de tiempo y lugar. Ello destacándose la complejidad y grado de perfección que presenta en la actualidad el método de "*phishing*" de difícil detección por persona de formación media, así como el deber de la proveedora, del servicio de dotarse de tecnología suficiente y adecuada con exigencia de medidas implantadoras activas, sin entenderse suficientes avisos generales o en página web de mero carácter informativo o divulgativo"(entre otras, SAP de Pontevedra núm. 177/2023, de 23 de marzo y SAP de Pontevedra, Sección 3ª, núm. 364/2023, de 5 de octubre).»

Audiencia Provincial de Cáceres, de 18/02/2025 RES:204/2025, TOL10.491.382

« Desde lo expuesto, y por lo que hace al caso concreto, difícilmente puede calificarse de negligencia grave la conducta seguida por la demandante, en concreto, el haber atendido a aquel mensaje inicial en el que se le alertaba de que sus cuentas estaban bloqueadas por motivos de seguridad, accediendo al enlace con el que, tras introducir sus claves, permitió al delincuente la entrada a su cuenta en la *web*de la entidad. Con la técnica empleada (ya fuera "SMS spoofing" o cualesquiera otra de las modalidades de *phishing)*se generó una apariencia de veracidad del mensaje al ser recibido en el canal usual de comunicación de la entidad, y, a la vez, el desasosiego propio del anuncio o alerta de que las cuentas habían sido bloqueadas por motivos de seguridad, por lo que cualquier persona con formación media y con un uso ordinario de la banca digital hubiera reaccionado de igual manera en que lo hicieron el actor y su esposa, máxime cuando tras pinchar el enlace aparecían datos personales (DNI, número de

teléfono) y un requerimiento que le alentaba a continuar ("accede", "confirma") para solucionar la situación que ficticiamente había generado el ciberdelincuente.

Además, como advierte la sentencia de la Audiencia Provincial de Asturias (Sección 4ª) en su sentencia núm.- 450/2024, de 23 de octubre, *"la diligencia o negligencia del usuario no pueden ser confrontadas con el sesgo retrospectivo que da el conocimiento final de que las operaciones bancarias se cometieron con fraude. En otras palabras, el patrón de referencia debe ser el de quien toma decisiones en la confianza de que el entorno informático en el que se mueve es el propio de su entidad bancaria. Si no se ha incurrido en una negligencia grave en el primer paso, las decisiones ulteriores deben ser valoradas desde la óptica de quien se cree en un entorno lícito y seguro, y no desde el conocimiento final de que ese entorno resultó ser fraudulento".»*

Audiencia Provincial de Lleida, de 17/02/2025 RES:167/2025, TOL10.497.397

«CUARTO. - En base a los razonamientos expuestos, y que son plenamente aplicables al supuesto que ahora nos ocupa, no puede considerarse negligente, tal y como hace la sentencia de primera grado, que la demandante, usuaria de un medio de pago como cliente de BBVA, respondiera a un mensaje que aparentemente le había enviado su entidad bancaria y que le recondujo a una web o App que también tenía la apariencia de ser la auténtica de BBVA, sin que tampoco quepa efectuarle reproche alguno por introducir sus claves o credenciales cuando estaba en la creencia fundada de estar comunicándose con BBVA, de manera que su voluntad aparece claramente viciada por el engaño causado. En consecuencia, no puede considerarse que incida en una falta de cautela y de mínima precaución de la que puede derivarse responsabilidad alguna y menos que sean de tal entidad que permitan ser calificadas como negligencia grave a los efectos de los arts. 44 y 45 de la LSP.

Debe recordarse que el Reglamento Delegado 2018/389, de 27 de noviembre de 2017 , que complementa la DSP2 en lo relativo a las normas técnicas para la autenticación reforzada del cliente, establece la obligación de realizar un análisis de riesgo en tiempo real basado en el análisis de operaciones y en los elementos que caracterizan al usuario en un contexto de uso normal de las credenciales de seguridad. Ese análisis de riesgo debe tener en cuenta una serie de factores a los que nos hemos referido anteriormente y que sin duda fueron obviados por la entidad demandada, como también obvió que tanto la tarjeta de

crédito de la Sra. Marisol como la que obtuvo el defraudador tras suplantarla, tenían un límite cuantitativo de disposición diario de 1.000 €, a pesar de lo cual no puso impedimento alguno en la realización de disposiciones de 2.000 € cada una de ellas en cuatro días consecutivos. El establecimiento de límites cuantitativos diarios en el uso de tarjetas de crédito, además de por motivos de solvencia del usuario, obedece también a razones básicas de seguridad, que en este caso tampoco fueron respetadas por BBVA.»

Audiencia Provincial de Valladolid, de 14/02/2025 RES:75/2025, TOL10.493.593

«La prueba exigible a la entidad financiera va mucho más allá de la mera afirmación de cumplimiento de los protocolos de seguridad previstos con carácter general, por lo que en el presente supuesto debería haber quedado acreditado de qué forma se pudo llevar a cabo la operación, examinando incluso el histórico con cargo a esa tarjeta o cuenta corriente, accesos por el usuario en banca electrónica, modificación de las claves de acceso con sus fechas y localización geográfica de quien lo hizo, o cuantas fuesen necesarias hasta esclarecer en qué momento y de qué forma se pudo apoderar de los datos de la parte demandante quien verificó la operación, pues, al no hacerlo, no se puede entender acreditada una negligencia por parte de ella.

En diversas resoluciones se ha atribuido la responsabilidad al cliente del banco o entidad financiera cuando se han facilitado los datos de forma gravemente negligente mediante una simple llamada telefónica, pero resulta necesario conocer exactamente de qué forma sucedió para poder determinar si concurre o no una grave negligencia por su parte. En la medida en que en este caso nada está acreditado, no puede saberse si hubo o no culpa de Dª Lorenza. De esa ausencia probatoria no puede derivarse, como pretende la apelante, atribuir la responsabilidad al usuario o cliente, sino, más bien al contrario, a la parte demandada, por lo que, ni ha existido un error en la valoración de prueba, ni se ha podido vulnerar lo dispuesto en el artículo 68 del citado Real decreto ley. Por tanto, debe desestimarse el recurso interpuesto, existiendo los incumplimientos recogidos en la sentencia de primera instancia, de modo que tampoco podría prosperar el segundo motivo del recurso, confirmándose en todos sus términos la sentencia dictada en primera instancia.»

Audiencia Provincial de Badajoz, de 14/02/2025 RES:137/2025, TOL10.497.726

«Ahora bien, el mencionado Real Decreto Ley establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago, con inversión de la carga probatoria, al presumirse la falta de autorización, si el titular lo niega. Este sistema de responsabilidad civil solo cesa cuando el cliente ha actuado fraudulentamente o con negligencia grave a la hora de aplicar los medios razonables de protección de seguridad personalizados de que haya sido provisto. También es responsable de comunicar a la entidad el pago no autorizado, en cuanto tenga conocimiento del mismo, siempre y cuando la entidad disponga de un sistema de comunicación adecuado, gratuito y disponible, en todo momento, que le permita al usuario del servicio efectuar la comunicación de la actuación fraudulenta.

Por otra parte, la normativa de consumo aplicable y la naturaleza adhesiva del contrato ampara de antemano al cliente. Desde el momento en que los medios digitales se han implantado en el negocio de la actividad bancaria, el riesgo de los fraudes debe ser soportado con carácter general por las entidades financieras. El auge económico de las entidades financieras se explica justamente por el abandono cada vez mayor de la presencialidad. La banca digital ha permitido un crecimiento exponencial de los servicios financieros con un enorme ahorro de costes. Las entidades bancarias tienen la doble condición de beneficiarias y de generadoras del riesgo. No basta con medidas genéricas de protección o avisos estereotipados de cuidado, sino que la seguridad de las operaciones bancarias precisa de soluciones tecnológicas avanzadas con el fin de garantizar tanto la autenticidad, como la integridad y confidencialidad de los datos.

Para los consumidores en general y más para los que sufren la brecha digital, es difícil detectar el fraude porque la delincuencia va perfeccionando el engaño. Por supuesto, desde el punto de vista jurídico, no podemos poner en el mismo plano a los clientes que a los bancos. Los clientes son las víctimas y las entidades financieras deben responder como depositarias y custodios de los ahorros. Por eso, el fraude digital, con carácter general, debe ser soportado por quienes se lucran con dicha actividad.

Hacen falta comunicaciones seguras, más formación a los clientes, más inversión en seguridad para evitar la clonación de las páginas y, si es necesario, bloquear las cuentas para la mejor protección de los clientes. No podemos olvidar que el depositante tiene derecho a la indemnidad de sus ahorros.

En este caso, discrepamos de lleno del recurso planteado por "Unicaja Banco, SA". Reconocemos que el estafador tiene como objetivo final

hurtar al cliente sus claves. Es verdad. Pero la responsabilidad de la banca no se agota con facilitar unas contraseñas y confiar en la Providencia. El banco no es un convidado de piedra.

No hay lugar también a una especie de sálvese quien pueda."Unicaja Banco, SA", cual, si fuera un crimen, achaca al usuario haber pinchado en el enlace. Ya lo hemos dicho, para llegar a ese hito, hay una cascada de recursos y medios que, al menos en este supuesto, "Unicaja Banco, SA" no agotó. El solo hecho de ser engañado, de ser víctima, no implica la comisión de una grave negligencia. Al contrario, una vez corroborado el fraude, se disipa cualquier negligencia, y menos grave, porque en general nadie tiene culpa del engaño, salvo que sea patente o burdo, que no es aquí el caso. Los ciberdelincuentes, cada vez más astutos, suplantan la identidad de la empresa y el ciudadano confía en que sus ahorros están más protegidos en los bancos que en sus domicilios.»

Audiencia Provincial de Les Illes Balears, de 17/09/2024 RES:577/2024 TOL10.291.541

«Este Tribunal debe tener en cuenta que **la negligencia a que se refiere el precepto ha de revestir la condición de grave, no siendo suficiente una negligencia leve ni media para la exclusión de la responsabilidad de la entidad bancaria.** En este sentido, el considerando 72 de la Directiva (UE) 2015/2366, sobre servicios de pago en el mercado interior, dispone que: «A la hora de evaluar la **posible negligencia** o la **negligencia** grave del usuario de servicios de pago, deben tomarse en consideración todas las circunstancias. Las pruebas de una presunta **negligencia**, y el grado de esta, deben evaluarse con arreglo a la normativa nacional. No obstante, si el concepto de **negligencia** supone un incumplimiento del deber de diligencia, la **negligencia** grave tiene que significar algo más que la mera **negligencia**, lo que entraña una conducta caracterizada por un grado significativo de **falta de diligencia**. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros» Además, en relación con el concepto de **negligencia** grave, con carácter general, cabe afirmar que la jurisprudencia viene entendiendo que linda con el dolo. Así, la sentencia de la Sala Primera del Tribunal Supremo de 30 de enero de 2003 revisa en profundidad el concepto, conectándolo con el de **falta de diligencia inexcusable**, por lo que su apreciación ha de ser restrictiva.»

Audiencia Provincial de Huesca, de 30/06/2024 RES:230/2024, TOL10.181.623

«Si el **usuario de servicios** de pago inicia la operación de pago a través de un proveedor de servicios de iniciación de pagos, corresponderá a éste demostrar que, dentro de su ámbito de competencia, la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable.

2. A los efectos de lo establecido en el apartado anterior, el registro por el proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, 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 con arreglo al artículo 41.

3. Corresponderá al proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, probar que el **usuario del servicio** de pago cometió fraude o negligencia grave (..)" Finalizando en el art. 45.1 que " Sin perjuicio del artículo 43 de este real decreto-ley, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada." Atendiendo a la normativa expuesta, corresponde a la demandada la carga de demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada y que la afectada ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 41. Pues bien, con base en ello, en este caso, se considera que no está debidamente acreditada esa negligencia grave por parte de la actora, es decir, no se ha demostrado ni que concurra fraude por parte de la demandante, al reconocerse que ha sido víctima de *phishing,* ni tampoco que concurra una negligencia grave en aquella, como se desprende de la prueba practicada, tal y como recoge en los argumentos de la sentencia recurrida, que se comparten, al indicar " El acceso se efectuó a lo que ella creía que era la web de Ibercaja y se realizó mediante una utilización

adecuada y habitual de sus datos y sus claves. En el documento de reclamación a Ibercaja se menciona que el acceso éste fue realizado a través del buscador Microsoft Edge, de lo que se infiere que cómo resultado de la búsqueda le dio la página web fraudulenta que se hizo pasar por la de la entidad. Una vez identificada, introdujo el código que le proporcionaron vía SMS. Respecto de éste, si bien es cierto que todavía no estaba realizando operación financiera alguna, no se aprecian motivos para que un ciudadano medio pudiera sospechar del carácter fraudulento del mismo, pues estamos ante un mensaje de texto que provenía del mismo número de Ibercaja. Pudiendo entenderse, además, que se le estaba exigiendo como un requisito adicional de identificación para poder acceder y operar en la banca electrónica".

Es decir, la facilidad y sencillez en el manejo de este tipo de datos conlleva el riesgo del fraude electrónico, sin que sea exigible al cliente medio un conocimiento informático sobre las eventuales técnicas de apropiación de sus datos personales, expuestos en la red en aras de posibilitar la agilidad y tratamiento masivo de transacciones electrónicas. Por el contrario, es incuestionable que las entidades bancarias se benefician de la extensión generalizada de este tipo de servicios de banca on-line, evitando los costes asociados a la atención de sus clientes en la red comercial mediante oficinas y personal y, por ello, la diligencia que es exigible a las mismas, se corresponde con la se exigiría a un "comerciante experto" y no la de un buen padre de familia, lo que le obliga, ante la realidad de prácticas delictivas como el referido "phising", a aumentar las medidas de seguridad específicas, por lo que no basta con medidas genéricas de protección o avisos estereotipados de cuidado, sino que "la seguridad de las operaciones bancarias precisa de soluciones tecnológicas avanzadas a los efectos de garantizar tanto la autenticidad como la integridad y confidencialidad de los datos", sin que se repute suficiente los avisos genéricos de los bancos, a través de su web, que ostentarían la calificación de " formulas predispuestas", vacías de contenido. Es decir, constatada la realidad de las operaciones defraudadoras y el conocimiento que cabe exigir a un consumidor medio en la adopción de medidas de cautela, para advertir y evitar las prácticas de captación de datos en el ámbito de la banca de particulares mediante los servicios de internet (que se conoce por sus siglas en inglés como "phissing"), **debe concluirse que no resulta suficiente, a los fines de eximir a la entidad prestadora del servicio, las advertencias que aparecen reflejadas en la página a través de la que operaba el cliente, como así se afirma, entre otras, en sentencias de las Audiencias Provinciales, como la SAP Navarra, sección 3ª de 9 de**

marzo del 2023 , SAP Rioja de 17 de febrero del 2023, de Málaga, sección 5ª de 23 de mayo del 2023 o de Madrid, sección 10 de 13 de enero del 2023 (que califica como responsabilidad cuasi-objetiva para la entidad financiera la prevista en la legislación ya expuesta salvo prueba de culpa grave del ordenante), Por ello, debe concluirse que la entidad demandada no ha probado, en este caso, que la conducta de la Sra. Teresa , víctima de un fraude, pueda ser calificada de grave en la custodia y uso de sus claves de seguridad en el sistema de servicios de pago on-line (sistema de pago que ofrece y pone a su servicio la entidad demandada), como pretende el recurrente, ya que la ley únicamente le exime de responsabilidad en supuestos de negligencia grave, fuera de los cuales, debe asumir la entidad recurrente el reintegro de los importes dispuestos y no autorizados que, en este caso, son 19.800 euros, desestimándose por ello este motivo de impugnación de la entidad demandada.»

Audiencia Provincial de Les Illes Balears, de 16/05/2024 RES:221/2024, TOL10.147.084

«Esta Sala debe tener en cuenta que la negligencia a que se refiere el precepto ha de revestir la condición de grave, no siendo suficiente una negligencia leve ni media para la exclusión de la responsabilidad de la entidad bancaria. En este sentido, el considerando 72 de la Directiva (UE) 2015/2366, sobre servicios de pago en el mercado interior, dispone que: «A la hora de evaluar la posible negligencia o la negligencia grave del usuario de servicios de pago, deben tomarse en consideración todas las circunstancias. Las pruebas de una presunta negligencia, y el grado de esta, deben evaluarse con arreglo a la normativa nacional. No obstante, si el concepto de negligencia supone un incumplimiento del deber de diligencia, la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros» Además, en relación con el concepto de negligencia grave, con carácter general, cabe afirmar que la jurisprudencia viene entendiendo que linda con el dolo. Así, la sentencia de la Sala Primera del Tribunal Supremo de 30 de enero de 2003 revisa en profundidad el concepto, conectándolo con el de falta de diligencia inexcusable, por lo que su apreciación ha de ser restrictiva.»

Audiencia Provincial de Asturias, de 07/10/2024 RES:460/2024, TOL10.286.780

« Este Tribunal se ha pronunciado, entre otras, en las sentencias de veinte de abril y 22 de junio de 2.023 sobre estos tipos de defraudaciones, en términos que ya se citan en la resolución recurrida. Así señalamos: "Y a partir de tal consideración, la única **negligencia** imputable al consumidor radica en haber confiado en el SMS recibido en su móvil, en la línea de mensajes de la demandada, y consignar en la página a la que resultó redireccionado las claves de acceso a su usuario, lo que esta Sala no ha considerado constitutivo de una **negligencia** grave en atención a la distribución de la responsabilidad regulado en la LSP. En la reciente sentencia de veinte de abril de dos mil veintitrés señalamos, en un supuesto análogo: "..la prueba allegada por el banco al respecto, que se redujo a una certificación del empleado de la demandada responsable del Departamento de Banca Digital aparece desmentido o, al menos, resulta insuficiente para probar, como le corresponde a la recurrente, aquella **actuación negligente** del cliente basada en la comunicación a terceros o cuidado de la clave de acceso. Como señala la sentencia de la Sec. 3ª de la AP de Burgos de 5 de diciembre de 2.022 a propósito del fraude por *phishing,* "la mayor parte de las AAPP han apreciado responsabilidad del proveedor de servicios de pago cuando lo único que ha hecho el usuario es descargarse estos programas maliciosos, sin introducir un segundo código de autenticación. Así, SSAP Zaragoza sección 5 del 1 de julio de 2.022 (ROJ: SAP Z 1482/2022), Granada sección 5 del 20 de junio de 2.022 (ROJ: SAP GR 957/2022), Valencia sección 6 del 13 de junio de 2022 (ROJ: SAP V 2622/2022), Madrid sección 20 del 20 de mayo de 2022 (ROJ: SAP M 7327/2022), y Pontevedra sección 6 del 21 de diciembre de 2021 (ROJ: SAP PO 3078/2021)".

En la sentencia de este Tribunal de trece de marzo del año en curso abordamos un supuesto análogo al presente y señalamos: "Se da la circunstancia en este caso de que el usuario sí facilitó el segundo código de autenticación, lo que, en principio sí podría calificase como de una actuación gravemente indiligente, que exoneraría de responsabilidad al proveedor de los servicios de pago. Pero, sin embargo, deben valorarse las concretas circunstancias concurrentes en el presente caso, que no aparecen discutidas en el litigio y aquél lo hizo tras recibir una llamada telefónica que figuraba en su terminal como procedente de una oficina local del banco y que así se lo indicó, lo que configura una puesta en escena del engaño basada en la confianza que proporcionaba la identificación del número telefónico y que produjo en la demandante el error de considerar como su interlocutor la entidad

bancaria. Y en este trance, no podemos calificar como **gravemente negligente** la actuación del usuario como **negligencia** grave, lo que conduce a la misma conclusión declarada en la sentencia recurrida". Y no es distinto este supuesto, en el que concurre el mismo ardid defraudador por el tercero y que impide calificar como grave la **negligencia** del usuario. Y la posterior operativa al vincular un sistema de pago de tal forma no es sino la consecuencia de lo anterior y merece el mismo tratamiento, que lleva, en suma, a la desestimación del recurso de apelación.»

Audiencia Provincial de Asturias, de 24/10/2024 RES:507/2024, TOL10.345.160

« TERCERO.-Así las cosas, en el caso enjuiciado, no es posible atribuir negligencia grave al cliente por la sola circunstancia de haber facilitado las claves a los ciberdelincuentes que le envían un enlace por SMS advirtiéndole de que se van a bloquear sus fondos, con el que se accede a una página que aparenta ser la de la entidad bancaria, por tanto con visos de ser auténtica, sobre la que la demandada no ha ejercido ninguna labor de control para evitar que esté abierta en la red; hecho que a la postre resulta ser común a todos los casos anteriores, pues el fraude se comete tras apoderarse los delincuentes de las claves del perjudicado, a las que han tenido acceso sin duda con al colaboración de éste , víctima del engaño, ni la negligencia grave del cliente se advera por el hecho de que, en el seno de la operación de los ciberdelincuentes, haya recibido un sms posterior que vinculaba la operación a un dispositivo que llegó a ejecutar, lo que es indicativo por el contrario, del complejo mecanismo empleado por quien cometió el delito para provocar el consentimiento del cliente , lo que tampoco fue detectado por la entidad , pese a que tenga constancia de tal actuación, como se desprende del documento 1 que ella aporta, todo lo cual obliga a confirmar la apelada por sus propios fundamentos.»

Audiencia Provincial de La Coruña, de 04/12/2024 RES:612/2024, TOL10.410.626

«9.- Una vez que no se discute que el cliente no es el defraudador, y que es evidente que fue engañado por un tercero, pero que cumplió con la posterior actuación exigible de comunicar la situación sin demora, recordamos que nuestro criterio, en reciente SAP de A Coruña Sección 4º de 22 de mayo de 2024 al respecto de la valoración de la negligencia grave del cliente engañado que que en particular el art. 44.3, dice que que corresponde al proveedor de servicios de pago, probar que el usuario del servicio de pago cometió fraude o negligencia grave, y que "..la propia Directiva (UE) 2015/2366 del Parlamento Europeo y del

Consejo, de 25 de noviembre de 2015 , sobre servicios de pago en el mercado interior, advierte en su considerando 72 que "si el concepto de negligencia supone un incumplimiento del deber de diligencia, la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros".

10.- Hemos de resolver en función de las circunstancias de cada caso concreto, y en aquel caso, incluso calificamos de negligente la conducta de quien había permitido el acceso a su banca móvil, pero hicimos ver que la conducta no era de negligencia grave, y que el caso no se asemejaba al de la SAP de A Coruña 17/2023 de la Sección Tercera de 25 de enero de 2023, en la que se lee: "No es una negligencia, son tres. Y si la primera aún pudiera ser más o menos comprensible (pinchar en un enlace), la segunda ya es grave (facilitar usuario y contraseña), y la tercera es totalmente temeraria (informar de la confirmación)". Dijimos que en el aquel caso, el elemento diferencial era el hecho de que al menos el paso último de confirmación se produjo en el contexto de una llamada telefónica que el usuario recibió desde un número de teléfono que, por la información que aparecía en su terminal, era efectivamente uno de los que el Servicio de Atención al Cliente de ABANCA tiene habilitado, y que llegamos a saber que el suplantador logró simular una llamada desde ese número de teléfono, y unos minutos antes, desde otro igual con prefijo de Pontevedra, y así las cosas, la valoración que merece la conducta del usuario, sin duda negligente, no alcanza el grado de gravedad exigible.»

Audiencia Provincial de Lugo, de 14/11/2024 RES:454/2024, TOL10.352.537

«A la vista de la prueba practicada, concluimos que la conducta del demandante no puede calificarse de fraudulenta, o de incumplimiento deliberado o negligencia grave de las obligaciones que le impone el art. 41, que es "tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas".

La cesión a tercero de las credenciales de seguridad por parte del demandante (claves de acceso a su banca online y OTP para registro de otro dispositivo autorizado) propicia el acceso de un dispositivo ajeno a su banca electrónica y a las claves de acceso a la misma. Esta cesión y la negligencia del cliente debe ser valorada en el contexto en que se producen los hechos (art. 1.104 CC), mediante un comportamiento

fraudulento de tercero, constitutivo de infracción penal, con aparente procedencia de la entidad bancaria, que genera en el cliente la inseguridad de verse privado del uso de su cuenta bancaria, que oportunamente se le ofrece subsanar.

Este comportamiento no tiene la gravedad exigida por la normativa para pechar con las pérdidas de la transacción (art. 46.1 del Real Decreto Legislativo 19/2018).

Por el contrario, consideramos que el banco no cumple con las exigencias de la autenticación reforzada, por no adoptar medidas de seguridad para evitar que los códigos de autenticación de las transacciones llegan a manos de terceros distintos al cliente (arts. 5 y 6 del Reglamento Delegado 2018/389). La remisión de estos códigos OTP se realiza por un mensaje PUSH enviado a la propia página de banca online, en lugar de remitirse por sms al terminal del cliente; por lo que basta el acceso a la banca online para obtener el enlace que facilita el código, sin garantía de que el consentimiento lo presta el cliente.

Tampoco prueba la demandada la implementación de medidas de análisis y detección de operaciones fraudulentas, en los términos exigidos por el artículo 2 del Reglamento Delegado 2018/389; conocido como resulta la utilización de mecanismos como el que describe la demanda para captar los elementos de autenticación transmitidos al usuario, tal y como reconoce la demandada; siendo insuficiente la difusión de mensajes de prevención al usuario, cuya atención rigurosa por el usuario vendría a propiciar una desconfianza que impediría la normal utilización del servicio de banca electrónica. Y tampoco ha aportado dato alguno que permita considerar que la operativa usual del demandante incluya operaciones como las de litis.

En este orden de cosas, debe pechar la demandada con los riesgos derivados de la inseguridad del soporte facilitado para servicio de pago de sus clientes.»

Audiencia Provincial de Navarra, de 18/10/2024 RES:1217/2024, TOL10.413.193

« Alega la recurrente como motivo esencial de recurso que en ningún caso su actuación consistente en acceder al enlace y facilitar los datos de su tarjeta puede considerarse que supusiera una **negligencia** grave.

Dicho motivo de recurso debe ser estimado por entender que el Sr Federico actuó así en la creencia de que actuaba correctamente y no de que se trataba de un "tercero". Como también hemos recogido en otras resoluciones en supuestos similares, si el concepto de negligencia

supone un incumplimiento del deber de diligencia, la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia. Además, no podemos olvidar que la norma obliga al usuario a tomar "todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas"(art. 41.a LSP) y esa razonabilidad legalmente exigida no puede evaluarse a posteriori, sino en el momento del *phishing,* cuando el demandante fue engañado por medio de la suplantación, por el tercero estafador, de la identidad y aplicación informática de la entidad bancaria.

Por todo lo expuesto procede la estimación del recurso de apelación, toda vez que compete a la entidad bancaria que pone a disposición de su cliente instrumentos de pago y contratación electrónica el adoptar las medidas de seguridad necesarias para garantizar la plena autenticación de la operación, que ha de incluir la efectiva identidad del ordenante, debiendo asegurar y garantizar que la autorización de la operación provenía efectivamente del cliente titular de la tarjeta, lo que no demuestra haber supervisado ni verificado debidamente en este caso.»

Audiencia Provincial de Cáceres, de 04/12/2024 RES:798/2024, TOL10.388.481

« Así las cosas, valorando las circunstancias concurrentes en el presente caso, no cabe apreciar negligencia grave por parte de Doña Encarnación en el cumplimiento de su obligación de proteger sus credenciales de seguridad. No puede tacharse de gravemente negligente la conducta de quien, tras recibir en el mismo canal en el que recibe habitualmente las comunicaciones procedentes de su banco, un mensaje de texto en el que se le informa que se había bloqueado su cuenta por razones de seguridad, facilitándole un enlace para poder desbloquearla, decide pulsar en ese enlace e introducir su usuario y contraseña, dado que, para una persona no experta, no es fácil detectar que el mensaje recibido es fraudulento o que la web a la que ha accedido a través del enlace facilitado es falsa. En esas circunstancias, era preciso ser un experto en la materia para poder detectar que la comunicación obedecía a una estafa o fraude. Es cierto que dicho comportamiento no puede considerarse diligente, pero para hacer soportar al cliente las consecuencias, 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 Doña Encarnación, por el hecho de haber

pinchado el link que se le ofrecía y facilitar los datos y clave de la cuenta, y posteriormente autorizar la vinculación de otro dispositivo.»

Audiencia Provincial de Cáceres, de 03/09/2024 RES:378/2024, TOL10.261.298

«A lo dicho no es obstáculo las alegaciones de la demandada sobre la seguridad del sistema y la inexistencia de brechas de seguridad, pues si bien el sistema puede ser genéricamente seguro, no lo fue en el caso concreto. Así, el propio banco asume en su contestación que el actor fue objeto de un fraude mediante *phishing,* siendo la asunción de este engaño y/o fraude la constatación evidente de que el banco no había implementado todos las medidas o mecanismos necesarios para proteger a su cliente de ataques realizados por ciberdelincuentes, lo que comporta incumplimiento de su obligación de garantizar la seguridad de los servicios de pago efectuados a través de internet o dispositivos móviles. Responsabilidad de la que tampoco queda exenta con la remisión de avisos o advertencias genéricas a través de la web o en el propio contrato, manifestando en cuanto a esto la sentencia de la Audiencia Provincial de La Rioja de 17 de febrero de 2023 que *"es el banco quien ofrece este producto, en principio seguro, y es cierto que remite avisos y advertencias genéricas sobre su utilización; pero conociendo los distintos riesgos de los que avisa, le corresponde adoptar las medidas de seguridad o control necesarias, que en este caso no consta que se adoptaran. Y no basta con medidas genéricas de protección o avisos estereotipados de cuidado, pues tales avisos ostentarían la calificación de "formulas predispuestas", vacías de contenido. No son los clientes los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, o estar al tanto de los mismos, ni prevenir con su asesoramiento experto dichos riesgos".*

Audiencia Provincial de Madrid, de 13/01/2023, TOL9.410.719

«A tenor de lo expuesto, salvo la actuación fraudulenta, incumplimiento deliberado o negligencia grave del usuario, 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". La interpretación efectuada por la Juzgadora ad quem de la Ley 16/2009, de 13 de noviembre, de servicios de pago, es acorde no sólo con la literalidad de la norma, sino con el espíritu y finalidad de la misma (ex. art. 3 CC), lo que obligó a la determinación de la responsabilidad de la entidad bancaria a pesar de sus afirmaciones sobre la implementación de un modelo seguro de banca online, lo que no implica que el sistema fuera genéricamente seguro, pero como es evidente no lo fue en el presente

caso. Tampoco sirve de excusa a la entidad apelada la inclusión de avisos en web y otros medios de la entidad sobre el comportamiento seguro que en el uso de la plataforma había de tener el cliente, sino que la entidad bancaria debe dotar a la banca electrónica de las medidas de seguridad necesarias para prevenir unos tipos de fraude ya muy extendidos y que, como lo prueba el supuesto que nos ocupa, siguen produciéndose por falta de una medida adecuadas por la entidades bancarias, que ponen a disposición de sus clientes la banca online y la contratación electrónica como dotados de una seguridad que no garantizan.

Como se aduce en la sentencia apelada, **no podemos calificar la posible negligencia de la demandante en la conservación de sus claves como "grave" en ningún caso.** Estamos ante un tipo de fraude muy específico del que es fácil ser víctima, sin que ello implique una actuación negligente del cliente, dado lo bien articulada en su ejecución que está esta modalidad de fraude. Tanto de la declaración de la demandante en la vista, como de la declaración de los testigos, ha quedado acreditado que la Sra. Inocencia intentó varias veces hacer una transferencia a través de la banca electrónica y, al no poder hacerlo porque no recibía la clave en su teléfono móvil, acudió a la mañana siguiente a su oficina bancaria, explicando lo sucedido. La empleada no detecta ninguna irregularidad. Momento en que se debió detectar el fraude y bloquear las cuentas y tarjetas. Además, se dispuso de cantidades superiores al límite máximo pactado de disposición, sin control por la entidad bancaria, lo que fue posible por la modificación de los límites referidos, elevando los 1.200 iniciales a 6.000 euros por tarjeta, lo que realiza el tercero, al conocer sus claves como consecuencia del hackeo previo.»

Sentencia Audiencia Provincial de Asturias de 20/05/2021 TOL8.530.519

«SEGUNDO. - La parte apelante reitera que la única causa de las operaciones fraudulentas base de la reclamación deducida en la demanda, es el incumplimiento por parte del demandante de su obligación de observar la debida diligencia en la custodia de sus contraseñas "Pin" y no compartir dicha información con terceros, obligación contractual contraída por aquel a tenor de los doc. 2 y 3 adjuntados con su contestación y también legal al amparo del art. 41.1.a) del Real Decreto- Ley 19/2018, declinando su responsabilidad en los hechos acaecidos. Si bien, sustenta la errónea valoración de la prueba en la que habría incurrido la recurrida al declarar su responsabilidad, en el hecho de que el propio demandante habría reconocido que había

facilitado los datos de su tarjeta a tenor del contenido de la denuncia presentada ante la Policía (doc.2), denuncia referida a la utilización fraudulenta de la tarjeta de débito número NUM001 en fecha 8 de junio de 2020.

Sin embargo, del contenido de la denuncia en cuestión no se extrae otra cosa, que el demandante ha sido objeto de una estafa vía internet, mediante el envío de un e-mail de "Correos" con relación a un burofax por el remitido, advirtiéndole de que la dirección es errónea, indicándole los pasos a seguir para solventarlo, lo que verifica, derivándole a la entidad Santander para abonar un importe de 1,60 euros; acción con la cual suplantando a la entidad bancaria logran hacerse con sus credenciales, es decir, el conocimiento del número secreto "Pin" por terceros no autorizados lo ha sido por causas ajenas a la voluntad del demandante y que no obedecen a una negligencia grave en el cumplimiento de su obligación de custodia de sus credenciales, máxime cuando obedece a una actuación por el realizada en Correos que, en principio, no tiene por qué hacerle dudar de su certeza y fiabilidad, hecho que, por otra parte, no es extraño, ni ajeno a la propia dinámica del funcionamiento del sistema, correspondiéndole a la entidad bancaria asumir los riesgos que conlleva la tarjeta en sí porque ella se lleva los beneficios, como así se recoge en la recurrida con cita dela SAP Madrid, Sección 10ª, de 25 de noviembre de 2011. **De ahí que, como acertadamente se recoge en la recurrida, el art. 44 del Real Decreto- Ley contenga un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago, con inversión de la carga de la prueba,** al presumirse la falta de autorización si el titular lo niega, salvo que se pruebe que el cliente haya actuado fraudulentamente o con negligencia grave a la hora de aplicar los medios razonables de protección de que haya sido provisto o cuando no haya comunicado a la entidad el pago no autorizado en cuanto tenga conocimiento del mismo; prueba inexistente en este supuesto, por lo que debe decaer el recurso.

TERCERO. - Tampoco cabe acoger la pretensión deducida en el recurso, con carácter subsidiario, para el supuesto de ser desestimado el recurso, cual es, la no imposición de costas por concurrir dudas de hecho y de derecho, simple alegato sin concretar qué dudas de hecho concretas son las que plantea el supuesto enjuiciado y, por ende, que sean serias, objetivas, fundadas y que supongan un plus de incertidumbre al que normalmente se suscita en toda contienda judicial. Otro tanto cabe afirmar de las dudas de derecho al no especificar que sobre estos hechos exista doctrina jurisprudencial contradictoria. Procediendo, por

tanto, al ser desestimado el recurso, imponer las costas de esta alzada a la apelante (art. 398.1 de la LEC).»

SAP de Murcia n.º 414/2022, de 19 de diciembre TOL9.389.886

«6.- Partiendo de estos hechos, es necesario fijar, como bien hace la sentencia apelada, el **régimen jurídico correspondiente a estos servicios de pago por banca electrónica.** Sobre esta cuestión existe una abundante jurisprudencia menor, pudiéndose citar, a tal efecto, y como alguna de las últimas resoluciones que analizan la responsabilidad de la entidad de crédito emisora las SSAP de Alicante (8ª) 107/18, de 12 de marzo; Pontevedra (6ª) 539/21, de 21 de diciembre; Madrid (11ª) 74/22, de 28 de febrero; Madrid (20ª) 184/22, de 20 de mayo; Valencia (6ª) 254/22, de 13 de junio; Badajoz (3ª) 159/22, de 16 de junio; o Granada (5ª) 212/22, de 20 de junio. La conclusión común de estas resoluciones, como señala la SAP Granada 212/22 citada es que "...

ha de partir de la consideración de que, con arreglo al marco jurídico en el que se desenvuelve la actividad de servicios de pago a través de banca on line, **el régimen de la responsabilidad de la prestadora del servicio ha de reputarse cuasi-objetiva,** en la medida en que sólo se excluye en unos casos por culpa grave del cliente y en otros por únicamente por fraude imputable al mismo, lo que implica, además, que la carga de la prueba de esas circunstancias exoneratorias y la paralela inexigibilidad de otra conducta a la referida entidad incumba a ésta en todo caso".

10.- Como se deriva del régimen señalado en el fundamento de derecho anterior, en lo que respecta a la responsabilidad por operaciones de pago fraudulentas o no autorizadas, el proveedor de servicios de pago se encuentra sujeto al cumplimiento de específicas obligaciones de protección en la emisión de los instrumentos de pago y en los procesos de autenticación de las operaciones de pago cuya finalidad es minimizar la probabilidad de ejecución de operaciones no autorizadas, respondiendo por las operaciones de pago resultantes del uso fraudulento del instrumento de pago por un tercero, ordenante actuara de manera fraudulenta, o incumpliendo deliberadamente o por negligencia grave alguna de las obligaciones recogidas en el art. 41 RDLSP. Por ello, , como señala la SAP Badajoz (3ª) 159/22, "... al proveedor de servicios de pago le corresponde la carga procesal de acreditar tanto su propio comportamiento diligente en la autenticación de la operación de pago como, en su caso, el fraude (requerirá de la acreditación de hechos de los que pudiera llegar a inferirse que aquel actuó con engaño para beneficiarse de la operación de pago) o la negligencia grave del ordenante (requerirá de la acreditación de las circunstancias

concurrentes en la operación de pago de las que quepa inferir que la misma pudo realizarse porque aquel obró con una significativa falta de diligencia al usar del instrumento de pago o al proteger sus credenciales)".

11.- **Por tanto, lo importante a los efectos de la resolución del presente recurso, no es tanto la existencia de diligencia en la actuación de la entidad de crédito demandada, sino sí esta ha probado que la actora incurrió en fraude, incumplimiento deliberado o negligencia grave en relación a las operaciones no autorizadas cuya devolución reclama** a través de la presente demanda. Hay que partir de que, como señala la SAP Madrid (11ª) 74/22, "... 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...". Y tal como señala la sentencia apelada, cuyos acertados razonamientos hacemos nuestros e integramos como parte de esta resolución, tal prueba no se ha logrado en las presentes actuaciones.

17.- Señalado lo anterior, deben de ser desestimados los tres motivos iniciales y, por extensión, **debe de ser desestimado también la alegación sobre la concurrencia de culpas** entre la proveedora y el usuario del servicio de pago. Lo primero que es preciso señalar es que, dados los términos del RD Ley 19/2018, **no parece posible admitir la existencia de concurrencia de culpas dado que fija dicha norma claramente las responsabilidades únicas de la entidad proveedora del servicio y del propio usuario del servicio**, de forma que si aquella no prueba, como no ha probado, la existencia de fraude, incumplimiento o negligencia grave de éste, tiene la obligación legal de devolver íntegramente las cantidades correspondientes a las operaciones no autorizadas.

Y si concurre en el usuario cualquiera de dichas circunstancias, el mismo está obligado a soportar los pagos realizados sólo imputables al mismo, lo que deja poco margen a la concurrencia de culpas. En segundo lugar, hay que indicar que, como se ha razonado en los apartados anteriores, no existe causa alguna que permita justificar que la actora incurrió en ningún tipo de negligencia, ni leve ni grave, por lo que no podría imputarse a la misma culpa alguna a los efectos de su concurrencia.»

Sentencia Audiencia Provincial de Badajoz, de 16/06/2022, TOL9.174.667

«No ha de olvidarse que en el *phishing* se usan técnicas para ganarse la confianza del usuario del instrumento de pago y aprovecharse de una simulación cada vez más perfeccionada. A ello debiera responderse por la entidad bancaria también con mecanismos de protección cada vez mayores y mejores. Así, no podía la entidad desconocer que frecuentemente mediante esta técnica el tercero defraudador utiliza los datos de la tarjeta para activarla en una aplicación de pago, por lo que debiendo conocer que el teléfono desde el que se le había solicitado la activación no se encontraría entre los que hubiera registrado su nombre el actor, la comunicación del número de terminal telefónico devenía exigible para que aquélla pudiera conocer que era un tercero quien podría disponer de los datos de la tarjeta mediante la aplicación de pago que se activaría.»

Otras sentencias favorables al cliente bancario: Audiencia Provincial de Zaragoza, de 11/10/2024 RES:621/2024, TOL10.322.081; Audiencia Provincial de Lleida, de 30/07/2024 RES:575/2024, TOL10.221.200; Audiencia Provincial de Asturias, de 18/02/2025 RES:78/2025, TOL10.498.709; Audiencia Provincial de Madrid, de 13/02/2025 RES:68/2025, TOL10.495.163; Audiencia Provincial de Asturias, de 12/02/2025 RES:69/2025; TOL10.494.051; Audiencia Provincial de Guadalajara, de 10/02/2025 RES:39/2025, TOL10.478.930;

b. **En contra del cliente bancario**

Audiencia Provincial de Madrid, de 07/10/2024 RES:407/2024, TOL10.351.996

« Pues bien en este caso, en efecto existió una conducta negligente del demandante que consistió en instalar la aplicación push bullet que permitió el control de su teléfono y el facilitar los códigos OTP para las transferencias del día 15 y enviar un correo a la dirección facilitada que le indicaron por teléfono, que debe calificarse como negligencia grave. Ciertamente el sr Salvador, como relató en su denuncia y es declarado hecho probado en la sentencia , recibió la llamada del número que en apariencia provenía de OPENBANK , entidad que opera con sus clientes ,entre otros medios, por vía telefónica como explicó el testigo sr Carlos José. Además como señala el recurrente las operaciones para poder ser llevadas a cabo requerían el previo acceso a la banca online, y el sr Salvador no facilitó su identidad ni su clave . Es preciso remarcar que los controles de fraude del banco -sistema BioCatch - resultaron por completo ineficaces. Se dijo por el testigo que no existió ninguna brecha de seguridad que diera lugar a que se expusieran las claves de acceso de la banca online, pero también explicó que los estafadores se

sirven de medios fraudulentos para obtener las claves sin el concurso del cliente. Ahora bien , no se puede entender sino como una negligencia grave , esto es como una conducta que no llevaría a cabo ni el sujeto menos diligente , la actuación del demandante. En efecto, si las operaciones de transferencia -dos transferencias inmediatas de 6.000 euros y otras dos no inmediatas de 18.000 y 19.000 euros- se pudieron llevar a cabo fue debido a que el sr Salvador recibió los mensajes sms con los códigos OTP el día 15 y ,pese a que el texto de los mensajes era inequívoco de modo que cualquier persona podí comprender que al facilitar los códigos se iba a proceder a autorizar las transferencias de importes superiores a la supuesta transferencia de 5.000 euros que se pretendía evitar, facilitó los códigos. En cuanto a las transferencias del día 16 , también recibió los códigos por vía sms con mensajes inequívocos en los términos expresados, códigos de autorización de sendas transferencias , aunque este día no fuera necesario ya comunicarlo verbalmente a los estafadores porque había procedido a instalar la aplicación que permitía el control de su teléfono , acto este también que denota una negligencia grave. En todo caso recibidos los sms de autorización de transferencia el sr. Salvador no se puso en contacto inmediato con Open Bank como resulta su obligación conforme al dictado del artículo 41 LSP.

En conclusión, no se disiente de la conclusión de la sentencia apelada. En este caso puede reprocharse a la entidad bancaria , que no ha incumplido ninguna normativa que resulte aplicable, la ineficacia del sistema de detección preventiva de fraude, pero frente a ello resulta que en este caso el fraude se ha consumado por la negligencia activa del cliente . El engaño de los delincuentes no fue complejo sino burdo , no pudiendo llevarse a cabo si el ahora demandante hubiera prestado una atención mínima a los mensajes acompañados a los códigos OTP o no hubiera instalado la aplicación que permitió el control de sus mensajes .Tal conducta no puede sino tenerse por una grave falta de diligencia que impide la apreciación de responsabilidad en la entidad demandada.»

Audiencia Provincial de La Coruña, de 25/01/2023, TOL9.445.258

«Todo el planteamiento de la demanda, y ahora del recurso, se fundamenta en la aplicación del artículo 46 del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que regula la «responsabilidad del ordenante en caso de operaciones de pago no autorizadas», en el cual se exonera a la entidad pagadora si don Carmelo incurrió en **negligencia** grave. Como se dijo, la primera obligación del usuario

es adoptar «todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas». Y la más elemental es no facilitar esos datos a terceros. Suministrar de forma reiterada e imprudente esos datos es una **negligencia** grave, contra la que nada puede hacer la entidad bancaria. Si toda medida de seguridad, incluso reforzada, es vulnerada por el propio cliente, nada puede hacerse [nemo propiam turpitudinem allegare potest (Nadie puede alegar su propia torpeza)].

Negligencia grave que se agrava cuando, recibiendo un mensaje donde "Abanca Corporación Bancaria, S.A." -esta vez sí- le notifica que se está pidiendo autorización para una transferencia de 9.132 euros, en lugar de leer el SMS con un mínimo detenimiento para así percatarse del engaño, procede a trasladar el código de verificación a su interlocutor. No es una negligencia, son tres. Y si la primera aún pudiera ser más o menos comprensible (pinchar en un enlace), la segunda ya es grave (facilitar usuario y contraseña), y la tercera es totalmente temeraria (informar de la confirmación).»

Audiencia Provincial de Madrid, de 01/07/2022, TOL9.223.750

«...En este sentido este tribunal en supuestos en los que la utilización ilícita de datos bancarios obtenidos mediante sistema fraudulentos, como el denominado *phishing* y otros, hemos apreciado responsabilidad en la entidad proveedora del servicio.

Ahora bien en el supuesto concreto aquí analizado, no consta acreditado, ni siquiera se alega, que se hubiera podido obtener las claves o datos de acceso mediante procedimientos de ese tipo, ni que la demandada hubiera denunciado o puesto en conocimiento de la demandada la sustracción o utilización de métodos ilícitos para conseguir las claves que permitieran realizar las operaciones banca on line, por lo que gestionada de manera satisfactoria, según admite la propia demandante, **la situación derivada de la sustracción de que fue víctima la demandante en el mes de mayo de 2017, ninguna responsabilidad cabe atribuir a la demandada en las operaciones realizadas en el mes de abril de 2018, con base en la sustracción anterior, por lo que la obtención de las mismas únicamente pudo haberse debido al descuido o ausencia de adopción de las medidas que razonablemente le eran exigibles al usuario a fin de proteger debidamente los elementos de seguridad personalizados**, máxime si previamente había sido objeto de sustracción de idénticos instrumentos de pago, a los que sustituyeron las tarjetas y claves nuevas, mediante los cuales se realizaron las operaciones no asumidas por su parte.»

Audiencia Provincial de Barcelona, de 15/09/2011, TOL2.254.882

«CUARTO. - Sentado lo anterior, hemos de constatar también que sin la descuidada actuación de la entidad actora no se hubiera podido consumar el perjuicio. Así:

-Es cierto que la operativa de banca por internet supone un ahorro de costes (materiales y humanos) y puede constituir una importante fuente de ingresos para los bancos. Pero no lo es menos que proporciona también una indudable comodidad al cliente, en este caso, una sociedad mercantil, evitando desplazamientos y la consiguiente pérdida de tiempo y, en definitiva, de dinero. No podemos aceptar, por tanto, la conclusión del Juzgado de que, siendo Banco de Santander el principal beneficiario del contrato, es quien debe asumir las consecuencias de la fraudulenta utilización del sistema por terceros.

-Incurrió Oclusiones Peláez SL en una indiscutible negligencia en la custodia de las claves al seguir las indicaciones de un inhabitual correo electrónico cuya autenticidad no había comprobado previamente. Y ello constituye un positivo incumplimiento de la cláusula cuarta del contrato que le obligaba a custodiar las claves de acceso y ejecución, así como a dar inmediato conocimiento al banco de cualquier incidencia que al respecto pudiera detectar.

-Tampoco parece que cumpliera la actora la obligación prevista en el pacto séptimo del repetido contrato ("realizar una comprobación diaria, a través de su terminal de ordenador, del movimiento de su/s cuenta/s ..."). Nótese que, habiendo quedando reflejadas de forma inmediata en el extracto informático las discutidas transferencias (así lo ratificó el testigo Sr. Avelino y no hay prueba en otro sentido en los autos), por tanto, el propio 17 de octubre de 2006, no se percató Oclusiones Peláez SL de los movimientos, dando el correspondiente aviso al banco, hasta el siguiente día 18, retraso que impidió realizar la correspondiente retrocesión antes de que los defraudadores dispusieran ya irremediablemente de los fondos.

Valorando, en consecuencia, la concurrencia de las respectivas conductas y, haciendo uso de la facultad que contempla el artículo 1103 del CC (v. SSTS de 28 de noviembre de 2007, 6 de febrero de 2008, 16 de diciembre de 2009), **se moderará en un cincuenta por ciento la responsabilidad exigida en la demanda.** Así pues, acogiendo parcialmente el recurso, fijaremos en 5.176'84 euros la suma a cuyo pago será condenada la entidad demandada, suma que devengará los intereses dispuestos en la sentencia apelada.»

CONCLUSIÓN

Tras el análisis de los pronunciamientos de los tribunales civiles puede concluirse los **criterios esenciales para valorar las reclamaciones por phishing bancario**.

1. Responsabilidad cuasi objetiva del banco

- El régimen legal aplicable (RD-L 19/2018, de servicios de pago, y normativa europea PSD2) impone una responsabilidad cuasi objetiva al proveedor de servicios de pago, de forma que:
    - Se presume la falta de autorización de la operación si el cliente la niega.
    - El banco solo se exonera si prueba que hubo negligencia grave o actuación fraudulenta del usuario.
    - La carga de la prueba recae exclusivamente en el banco, conforme al artículo 45 del RD-L 19/2018 y jurisprudencia consolidada.

2. Concepto estricto de “negligencia grave”

- La negligencia grave no puede confundirse con la mera imprudencia o descuido común. Requiere una conducta cualificada, próxima al dolo, y se interpreta de forma restrictiva.
- Se descarta la negligencia grave en supuestos como:
    - Clicar en un enlace recibido por SMS aparentemente enviado por el banco.
    - Introducir datos en una web que simula ser la del banco.
    - Proporcionar códigos de verificación por teléfono a quien se identifica falsamente como empleado del banco.
- Según el considerando 72 de la Directiva (UE) 2015/2366, y la jurisprudencia nacional, el entorno simulado por el delincuente es cada vez más sofisticado, lo que refuerza la conclusión de que la víctima actúa de buena fe y razonablemente engañada, sin incurrir en negligencia grave.

3. Exigencia de altos estándares de diligencia al banco

- El banco no puede limitarse a implantar medidas genéricas o formularios informativos estereotipados.
- Se le exige un estándar de diligencia superior al del “buen padre de familia”; debe actuar como un ordenado y experto comerciante.
- Esto implica:

- Análisis de riesgos en tiempo real (Reglamento Delegado 2018/389).
- Verificación efectiva del consentimiento del cliente.
- Detección de patrones anómalos de operación (horarios, importes, ausencia de conceptos, frecuencia...).
- Sistemas de alerta y bloqueo automático de operaciones sospechosas.

4. Importancia del entorno fraudulento y apariencia de veracidad

- La apariencia de legitimidad del entorno (web, app, llamadas, SMS), especialmente si utiliza canales habituales del cliente o simula datos del banco, impide considerar que el cliente incurrió en negligencia grave.
- Los tribunales reiteran que el conocimiento ex post del fraude no puede contaminar la valoración de la actuación del cliente en el momento del engaño (principio contra el sesgo retrospectivo).

5. Medidas adoptadas por el cliente tras el fraude

- La diligencia del cliente en la reacción al fraude (como denunciarlo ante la Guardia Civil o notificar al banco con rapidez) es valorada positivamente.
- Esta reacción contribuye a excluir la negligencia grave y refuerza la posición jurídica del usuario como víctima y no como corresponsable.

6. Ineficacia de la alegación de "sistema seguro" por parte del banco

- Que el banco declare su sistema como "seguro" no prueba su eficacia concreta en el caso enjuiciado.
- No basta con probar la existencia teórica de mecanismos de seguridad, sino que debe acreditarse su funcionamiento efectivo y adecuado en el caso concreto.

JURISPRUDENCIA PENAL

Audiencia Provincial de Asturias, de 26/01/2023, TOL9.437.133

«Estima esta Sala, como acertadamente se indica en la instancia, que el supuesto objeto de estos autos constituye una **estafa *informática*** de las denominadas *"phishing"*, mediante la cual se accedió de modo *fraudulento* a la cuenta de la entidad gestoría Alberca, tras tener

conocimiento de la entidad bancaria con la que operaba y de los clientes, y simulando ser el titular se ordenaron transferencias bancarias en su perjuicio, utilizando para dificultar la localización, se emplean lo que se denomina en dicho argot como mulas o muleros, personas los hoy recurrentes, que, a cambio de una remuneración y comisión, facilitan mediante su cuenta corriente, el desvío del dinero propiedad de los perjudicados a la misma.

La jurisprudencia ha tenido ocasión de manifestarse sobre este **delito de estafa** *informática,* tipificado en el precepto citado, señalando la STS 845/2014, de 2 de diciembre que: abrir una cuenta corriente con el exclusivo objeto de ingresar el dinero del que se desapodera a la víctima, encierra un hecho decisivo para la consumación del **delito de estafa**. No basta con disponer de las claves que permitan realizar la operación, es necesaria una cuenta corriente que no levante sospechas y que, mediante la extracción de las cantidades transferidas pueda llegar a obtener el beneficio económico perseguido. Precisamente por ello, la contribución de quien se presta interesadamente a convertirse en depositario momentáneo de los fondos sustraídos integrará de ordinario el **delito de estafa**, y sin que a ello se oponga el hecho de que no conste participaran en el mecanismo previo por el que se consiguieron las claves de acceso al correo y se efectuó la orden de transferencia desde la cuenta de la Gestoría pues consta la participación de los recurrentes en los hechos comprendida en el art. 28 b), al tratarse de una cooperación necesaria.»

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Teniendo en cuenta que una modalidad del fraude bancario (phishing) se comete por el infractor obteniendo un duplicado de la tarjeta SIM de la víctima facilitada por el operador de telefonía, la Agencia Española de Protección de Datos ha tenido ocasión de pronunciarse sobre tales infracciones, desde el punto de vista administrativo, por vulneración de los datos personales que ha contribuido a la comisión de los hechos por el infractor.

Expediente N.º: PS/00046/2021, Agencia Española de Protección de Datos, Resolución de 01/02/2022, TOL8.771.308

«Como ha quedado acreditado en la instrucción de este procedimiento, la imposición de la sanción deriva de unos Hechos Probados que constituyen una infracción muy grave del RGPD. Los hechos se imputan a SIMYO como responsable del tratamiento de la expedición de duplicados de tarjetas SIM, por lo que, debe rechazarse rotundamente la afirmación realizada relativa a que “no se puede

tomar en consideración supuestos de hecho no examinados en el presente procedimiento, donde no se ha calificado las responsabilidades derivadas y los tratamientos y conducta, por lo tanto, dichos supuestos no pueden utilizarse para perjudicar, en ningún supuesto, a SIMYO, en tanto no se ha acreditado infracción o incumplimiento alguno»

Procedimiento N.º: PS/00046/2021 Recurso de reposición N.º RR/00777/2021, Agencia Española de Protección de Datos 02/02/2022, TOL8.771.306

«La Agencia no se descuelga de ningún razonamiento ni tampoco achaca toda la responsabilidad a SIMYO. Le atribuye la responsabilidad que le corresponde como responsable de ese tratamiento específico "Emisión de un duplicado de tarjeta SIM", toda vez que conforme a la definición del artículo 4.7 del RGPD es quién determina la finalidad y medios del tratamiento realizado. SIMYO en su condición de operador deber ser más exigente a la hora de proporcionar un duplicado de una tarjeta SIM. Las verificaciones de identidad deben ser exhaustivas para evitar problemas de suplantación de identidad. En el momento en el que se logra la tarjeta SIM duplicada se tiene también acceso a este segundo factor de autenticación y, por tanto, desde ese instante, se podrían materializar fraudes bancarios»

BIBLIOGRAFÍA

Falsificación de documentos y de tarjetas bancarias, Emiliano Borja Jiménez, TOL10.521.278

CHAVELI DONET, E.A. et al. (2015) "Fraude Electrónico su Gestión Penal y Civil." Tirant Lo Blanch. Available at:

https://www.tirantonline.com/cloudLibrary/ebook/info/9788490865576 (https://www.tirantonline.com/cloudLibrary/ebook/info/9788490865576).

2. Guzmán Rodríguez, H.E. et al. (2021) "Derecho de la Contratación Electrónica y Comercio Electrónico en la Unión Europea y en España." Tirant lo Blanch. Available at: https://www.tirantonline.com/cloudLibrary/ebook/info/9788413782270 (https://www.tirantonline.com/cloudLibrary/ebook/info/9788413782270).

3. Rincón Cárdenas, E. (2020) "Derecho del Comercio Electrónico y de Internet." Tirant lo Blanch. Available at:

https://www.tirantonline.com/cloudLibrary/ebook/info/9788413369051 (https://www.tirantonline.com/cloudLibrary/ebook/info/9788413369051).

4. Christian Kersting et al. (2019) "Daños, Comercio Electrónico y Derecho Europeo de la Competencia." Tirant lo Blanch. Available at:

https://www.tirantonline.com/cloudLibrary/ebook/info/9788413362137 (https://www.tirantonline.com/cloudLibrary/ebook/info/9788413362137).

5. SANCHIS CRESPO, C. and Eloy Velasco Núñez (2019) "Delincuencia Informática." Tirant lo Blanch. Available at:

https://www.tirantonline.com/cloudLibrary/ebook/info/9788413133577 (https://www.tirantonline.com/cloudLibrary/ebook/info/9788413133577).

6. FLORES PRADA, I. (2012) "Criminalidad informática." Tirant Lo Blanch. Available at:

https://www.tirantonline.com/cloudLibrary/ebook/info/9788490335703 (https://www.tirantonline.com/cloudLibrary/ebook/info/9788490335703).

7. Campañas de *phishing* sobre el COVID-19. Agencia Española de Protección de datos. Campañas de *phishing* sobre el COVID-19 | AEPD (https://www.aepd.es/es/prensa-y-comunicacion/blog/campanas-de-phishing-sobre-el-covid-19)

TARJETAS

- **Phishing**
  https://www.tirantonline.com/base/tol/bin_card/phishing?token_id=6822d8915313e0000eeda322&search_token=phishing
- **Phishing bancario**
  https://www.tirantonline.com/base/tol/bin_card/phishing%20bancario?token_id=6822d9205313e0000a946df3&search_token=phishing+bancario

FORMULARIOS

<< Formularios civiles >>

1. Reclamación extrajudicial a la entidad bancaria exigiéndole responsabilidad por las cantidades dispuestas sin su autorización. *Phishing* bancario TOL9438606

2. Demanda de juicio ordinario reclamando la devolución de los cargos indebidos en tarjeta de crédito. *Phishing* bancario TOL8.648.355
3. Demanda de juicio ordinario contra entidad bancaria en reclamación de cantidad por responsabilidad en *phishing* bancario TOL9.357.362
4. Demanda de juicio verbal contra entidad bancaria en reclamación de cantidad por su responsabilidad en *phishing* bancario TOL9.362.191
5. Demanda de juicio ordinario reclamando la devolución de los cargos por ejecución de transferencias no autorizadas (phishing) TOL8.648.356
6. Interposición de recurso de apelación contra la sentencia que desestima la demanda reclamando la devolución de los cargos no autorizados en tarjeta de crédito. *Phishing* bancario TOL9449225

<< Formularios penales >>

1. Denuncia por delito de estafa informática. *Phishing* bancario TOL9.403.207


tirant
PRIME