Universidad de Valladolid

icava
Ilustre Colegio de Abogados de Valladolid

Colegio de Procuradores de Valladolid

Facultad de Derecho

MÁSTER en ABOGACÍA y PROCURA.

DICTAMEN SOBRE LA RESPONSABILIDAD CONTRACTUAL DE LAS ENTIDADES BANCARIAS EN SUPUESTOS DE FRAUDE A LOS USUARIOS DE LOS SERVICIOS DE PAGO.

Presentado por:

Tatiana Pereira Conde.

Tutelado por:

Francisco Javier Álvarez Hernando.

Valladolid, 16 de diciembre de 2024.

ÍNDICE

ABREVIATURAS

AP	Audiencia Provincial.
Art. /Arts.	Artículo/Artículos.
CC	Código Civil.
CP	Código Penal.
Etc.	Etcétera.
LEC	Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
LOPJ	Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
NÚM.	Número.
P./PP.	Página/Páginas.
RD-LSP	Real Decreto-ley 19/2018, de 23 de noviembre, de Servicios de Pago y otras medidas urgentes en materia financiera.
SAP	Sentencia de la Audiencia Provincial.
SAN	Sentencia de la Audiencia Nacional.
STS	Sentencia del Tribunal Supremo.
Ss.	Siguientes.
TRLGDCU	Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de Consumidores y Usuarios y otras leyes complementarias.
TS	Tribunal Supremo.
UE	Unión Europea.

-- La última línea de este Trabajo se ha incorporado en fecha 16 de diciembre de 2024. --

1. PRESENTACIÓN Y OBJETO DEL DICTAMEN.

En los últimos años, los servicios bancarios han experimentado una creciente digitalización, a través del uso de las nuevas tecnologías, convirtiéndose así en un nuevo instrumento para la comisión de delitos. Es por ello que, en su momento, el Consejo de Consumidores y Usuarios (CCU) ya advirtió que uno de los principales obstáculos al desarrollo del comercio electrónico era precisamente su desconfianza y la inseguridad que generaba a los usuarios[1].

No cabe duda de que los fondos que los usuarios tienen depositados en las entidades bancarias se han convertido en uno de los principales objetivos de la delincuencia. De ahí que autores como VELASCO NÚÑEZ[2], hayan señalado que la estafa se caracteriza por el modo comisivo activo de engañar o el pasivo de hacer sufrir un error que induzca a la víctima a realizar un acto perjudicial de disposición económica.

De este modo, son diversas las técnicas utilizadas por los ciberdelincuentes para estafar a sus víctimas, con el fin de sustraer su dinero o bien acceder a la información almacenada en sus dispositivos: el *"phishing"*, emplea correos electrónicos con enlaces o documentos que, tratan de infectar el dispositivo electrónico, una vez que se accede a los mismos; o el *"smishing"*, que en su lugar utiliza mensajes de texto o números de teléfono de entidades financieras haciéndose pasar por las mismas; etc.

En este sentido, el objetivo fundamental de este dictamen se basa en dar respuesta a algunas de las cuestiones y consecuencias que derivan directamente de los fraudes bancarios sufridos por los usuarios, como titulares de una determinada cuenta bancaria o tarjeta de crédito, señalando a su vez los mecanismos de defensa con los que cuentan a la hora de reclamar los daños y perjuicios ocasionados.

Asimismo, y en relación con este tema, se abordará la problemática existente respecto de la responsabilidad contractual de las entidades bancarias en estos supuestos, dada su obligación de garantizar en todo momento la seguridad en los medios de pago utilizados por los usuarios.

---

[1] C.C.U., *Banca on line y protección de los consumidores*, Madrid, 2001, p.21.
[2] VELASCO NÚÑEZ, E.: *Fraude digital y contra medios de pago. Defraudaciones mediante phishing, bizum; criptoactivos, tokens y otros medios de pago*, La Ley, Madrid, 2024, p.16.

2. ANTECEDENTES DE HECHO DEL CASO.

1º. Don José Antonio López García tiene suscrito, desde el 25 de octubre del año 2010, un contrato de cuenta corriente con n.º ES34 0182 4022 16 0123006433 y un contrato de tarjeta de crédito asociada a la misma, con n.º 4000 0014 3654 7899, con la entidad "Banco Bilbao Vizcaya Argentaria, S.A.", (en adelante, "BBVA").

2º. En fecha 20 de noviembre de 2024, el Sr. López García se encontraba en su domicilio de Valladolid, sito en calle Madre de Dios, núm. 6 - 2º Izda, cuando recibió un correo electrónico de Doña Laura Pérez Martínez, su gestora de la entidad bancaria, en el cual le indicaba que debía hacer acceder al enlace facilitado a fin de bloquear una serie de cargos que estaban intentando hacer en su cuenta bancaria. Este link le trasladó a una página *web* que el Sr. López García reconoció efectivamente como la de la entidad, en la cual le pedían cumplimentar sus datos, tanto personales como referentes a claves bancarias de su cuenta con esta entidad.

3º. Tras lo ocurrido, el Sr. López García decidió acceder a la banca *online* para consultar el estado de su cuenta corriente. En ese mismo instante, se percató de que efectivamente se habían realizado, **de forma indebida y sin su consentimiento**, los cargos en cuestión. En concreto, los movimientos realizados a través de la tarjeta bancaria arriba referenciada, ascendían a un total de TRES MIL TRESCIENTOS SESENTA Y CUATRO EUROS CON CINCUENTA Y SEIS CÉNTIMOS (3.364,56€), distribuidos del siguiente modo:

I. En fecha 20/11/2024, por un importe de MIL QUINIENTOS SESENTA Y CUATRO EUROS (1.564€), bajo el concepto "*ALIEXPRESS*".

II. En fecha 20/11/2024 por un importe de MIL OCHOCIENTOS EUROS CON CINCUENTA Y SEIS CÉNTIMOS (1.800,56€), bajo el concepto "*AMAZON*".

4º. Tan pronto como D. José Antonio fue consciente de estos movimientos en su cuenta bancaria no autorizados ni realizados por él, acudió a la oficina más cercana a fin de **ponerlo en conocimiento de su entidad bancaria**. Esta intentó exculparse afirmando que el mismo *"seguramente"* habría hecho "click" en algún enlace malicioso o que *"probablemente"*

habría introducido sus datos personales y bancarios en algún sitio fraudulento, todas estas afirmaciones sin ningún tipo de prueba o fundamento real u objetivo.

5º. Tras lo ocurrido, D. José Antonio asegura que no solo no recibió mensaje alguno por parte de la entidad BBVA a fin de confirmar las diferentes operaciones realizadas, sino que tampoco recibió ningún tipo de alerta por la que pudiese confirmar las mismas, con carácter previo a su tramitación, dado que por parte de la referida entidad bancaria no se llevó a cabo ningún sistema de autenticación de doble factor respecto de ninguna de las transacciones.

6º. A la vista de los hechos acontecidos, el día 22 de noviembre de 2024 D. José Antonio acudió a la Comisaría de la Policía Nacional de las Delicias para interponer la correspondiente denuncia, dado que había sido víctima de un fraude.

7º. En fecha 25 de noviembre de 2024, D. José Antonio presentó por escrito la oportuna **reclamación extrajudicial** ante la entidad bancaria BBVA, por importe de TRES MIL TRESCIENTOS SESENTA Y CUATRO EUROS CON CINCUENTA Y SEIS CÉNTIMOS (3.364,56€), correspondiéndose con la cantidad que fue sustraída a consecuencia de las acciones fraudulentas no autorizadas por él.

8º. El día 8 de enero de 2025, BBVA dio contestación a la reclamación, desestimando totalmente la solicitud de reembolso de la cantidad sustraída de la cuenta bancaria del Sr. López García. El resultado desfavorable de dicha reclamación se basa, por parte de la entidad bancaria, en una serie de argumentos que dan a entender que lo sucedido es consecuencia de una serie de actitudes negligentes llevadas a cabo por D. José Antonio, escudándose en una serie de artículos del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

9º. A día de hoy, la entidad bancaria no ha procedido a la restitución de dicho importe puesto que no se considera responsable de todo lo ocurrido, de ahí que el Sr. López García no haya podido recuperar la cantidad de dinero correspondiente a los cargos realizados en su cuenta sin su consentimiento. Es por ello que el Sr. López García acude a la letrada abajo firmante a fin de conocer cuál sería en este caso la responsabilidad de la entidad BBVA, dadas las condiciones que figuran en el contrato de cuenta corriente suscrito entre ambas partes, así como las acciones que se podrían ejercitar a fin de recuperar el dinero sustraído a consecuencia del *phishing* del que ha sido víctima.

3. CONCEPTOS PREVIOS.

3.1. El *Phishing*.

Dada la relevancia que ha ido adquiriendo el *phishing* en los últimos años, definir sus notas caracterizadoras no resulta sencillo. Pese a esto, son muchos los autores que se han pronunciado, proyectando así sus ideas fundamentales, lo que contribuye a su vez al esclarecimiento de las técnicas de "ingeniería social", como práctica de obtener información a través de la manipulación de los usuarios[3].

Con carácter general, RIBÓN SEISDEDOS[4] se refiere al *phishing* como la "pesca de datos" que tienen como objetivo provocar un daño patrimonial a un tercero, sin su consentimiento, mediante la utilización fraudulenta de sus claves. En este sentido, la Audiencia Provincial de Barcelona (Sección 14ª) señaló en su Sentencia núm. 151/2013, de 7 de marzo, que " […] el denominado *phising* que proviene del inglés pescar, *phishing* es la contracción de *password harvesting fishing*: cosecha y pesca de contraseñas, y, en el que se utiliza, como se indica en la demanda, a unas personas llamadas "muleros", que son personas que abren una cuenta corriente a la que se transfieren los fondos, y después éste los transfiere a otra o dispone de los mismos, cobrando por ello una comisión […]".

Asimismo, la Sentencia núm. 405/2023, de 23 de octubre, de la Audiencia Provincial de Valladolid (Sección 1ª), se refiere al *phishing* como el conjunto de "técnicas que determinan revelación de información confidencial haciendo un *click* en un enlace a través del engaño a una persona, cliente o usuario de servicios de pago, ganando su confianza y suplantando su identidad ante un tercero, en este caso, la entidad bancaria (proveedora de los servicios de pago), lo que da lugar a que se lleven a cabo unas acciones que no fueron realmente autorizadas por el cliente y que la entidad bancaria materializó de forma inmediata".

Por su parte, PIQUERES CASTELLOTE[5] señala que consiste en la captación ilícita de datos personales, principalmente relacionados con claves para el acceso a servicios bancarios y financieros a través de correos electrónicos o páginas *web* que imitan y copian la imagen o apariencia de una entidad bancaria o financiera.

---

[3] BANCO DE ESPAÑA: *¿Qué es el phishing y cómo evitarlo? ¡No piques!* <https://clientebancario.bde.es/pcb/es/blog/que-es-el-phishing-y-como-evitarlo.html> [Fecha de consulta: 15/12/2024].

[4] RIBÓN SEISDEDOS, E.: *Fraudes bancarios y defensa del afectado. Nuevas tendencias defraudatorias. Especial referencia al phishing bancario*, Tirant lo Blanch, Valencia, 2024, p.31.

[5] PIQURES CASTELLOTE, F.: "Conocimientos básicos en Internet y utilización para actividades ilícitas" en *Delitos contra y a través de las nuevas tecnologías ¿Cómo reducir su impunidad?*, Madrid, 2006, p.71.

Por tanto, a la vista de las meritadas definiciones y de los diferentes argumentos esgrimidos por las Audiencias, cabe deducir que es habitual que el *phishing* se origine por medio de la **suplantación de la identidad** del banco por parte del delincuente, denominado *phisher*, con el fin de adquirir **información confidencial** relativa a las contraseñas de las cuentas bancarias o tarjetas de crédito, que le permita acceder a las cuentas de los usuarios de banca electrónica.

En palabras de FERNÁNDEZ CABRERA[6], el modus operandi habitual consiste en utilizar la imagen corporativa, el lenguaje y el formato de una entidad bancaria para solicitar a la víctima a través del correo electrónico que incorpore sus datos bancarios en la *web* indicada, y todo ello, sin sospecha alguna.

Respecto a los motivos alegados a la hora de llevar a cabo este proceso, pueden ser de muy diversa naturaleza. Lo más habitual es que el usuario reciba una notificación en su dispositivo de uso personal en la que se le requiere para cambiar sus claves bancarias por la concurrencia de problemas técnicos, o bien bloquear una serie de cargos que se van a hacer efectivos en su cuenta, proporcionándole un enlace que "supuestamente" le redirigirá de forma directa al que aparenta ser el sitio *Web* oficial de su entidad bancaria. Sin embargo, la realidad es muy distinta. En todo caso, los delincuentes tratan de redirigir a los usuarios a páginas *web* fraudulentas, adjuntando a su vez archivos que contienen *malwares* que infectan el sistema receptor de dicha notificación, una vez que la misma ha sido abierta.

En este sentido, la propia Audiencia Nacional hace alusión al "*phishing bancario*" en la Sentencia de la Sala de lo Penal, núm. 7/2020, de 25 de marzo, como una modalidad de estafa que "consiste en el envío de un enlace, normalmente de una entidad bancaria, al correo electrónico o al teléfono móvil de la víctima, de manera que cuando el receptor pincha sobre el mismo, cree estar en la página oficial correspondiente y al poner las claves personales de acceso, las mismas son extraídas y utilizadas con posterioridad por terceros, […], para realizar transferencias no queridas por la víctima".

En definitiva, el *phisher* utiliza una serie de técnicas engañosas como, por ejemplo, el propio código fuente del programa del banco (HTML) y su dirección (URL) [7], generando la

[6] FERNÁNDEZ CABRERA, M.: "La tutela penal del comercio electrónico" en: MADRID PARRA, Agustín (director) y BLANCO SÁNCHEZ, María Jesús (coordinadora) *Derecho Mercantil y Tecnología*, Aranzadi, Navarra, 2018, capítulo 21, pp. 607-630.
[7] USERA, L.: "Desfalcos por *phishing*", *Revista Dialnet*, núm. 46, 2007, pp. 24-26.

confianza necesaria en la víctima (usuario) a la hora de ceder sus datos, puesto que consigue que el sitio *web* adquiera la verdadera apariencia de la entidad bancaria en cuestión.

3.2. El sistema de autenticación de doble factor.

En palabras del Instituto Nacional de Ciberseguridad (INCIBE), el sistema de autenticación de doble factor, también conocido como "autenticación en dos pasos", consiste en una medida de seguridad adicional a la contraseña que se utiliza para proteger el acceso no autorizado a las cuentas de los usuarios *online*[8].

Por su parte, las propias entidades bancarias se comprometen a implementar este sistema de autenticación reforzada, el cual fue introducido por la Directiva (UE) 2015/2366 del Parlamento y del Consejo, de 25 de noviembre, sobre Servicios de Pago en el Mercado Interior, también conocida como "Directiva Europea de Servicios de Pagos Digitales" (PSD2). En cuanto a su objetivo, fundamentalmente se basa en el aumento de la seguridad de las transacciones digitales en las cuales se utiliza la tarjeta como medio de pago.

A modo de ejemplo, la entidad BBVA[9] en su página *web* hace referencia al aumento de protección que dicho sistema proporciona en los pagos *online* con tarjeta ya que, al confirmar la identidad de la persona en dos pasos, permite asegurarse de que efectivamente la misma es la titular de la tarjeta que utiliza.

Generalmente, esta verificación se lleva a cabo en dos etapas diferenciadas: en primer lugar, el usuario deberá acceder mediante el primer factor que se corresponde con su patrón biométrico (huella dactilar, rasgos faciales…etc.) o bien la contraseña de acceso a la *web* o *APP*, que el mismo conoce con carácter previo; y, tras ello, deberá introducir el código único temporal que le será enviado en ese instante a su dispositivo móvil o bien generado para autenticar la operación. De ahí, la importancia de que este sistema de autenticación de doble factor se encuentre activo en todo momento, impidiendo así a los ciberdelincuentes acceder a la cuenta del usuario, aunque sean conocedores de la contraseña, ya que no disponen del código de verificación que es enviado en el segundo paso.

---

[8] INSTITUTO NACIONAL DE CIBERSEGURIDAD: *Autenticación de dos factores* (2FA). <https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras/autenticacion-de-dos-factores> [Fecha de consulta: 17/11/2024].

[9] BANCO BILBAO VIZCAYA AREGENTARIA, S.A.: *PSD2: la autenticación reforzada.* <https://www.bbva.es/general/seguridad/herramientas/doble-autenticacion.html> [Fecha de consulta: 23/11/2024].

4. CUESTIONES PLANTEADAS.

Una vez examinados los conceptos previos necesarios para una mejor comprensión del supuesto de hecho expuesto en el apartado núm. 2 del presente Trabajo Fin de Máster, se plantean una serie de cuestiones jurídicas sobre el mismo:

PRIMERA. – Obligaciones de la entidad BBVA, como proveedora de los servicios de pago, y del Sr. López García, como usuario de los mismos, en supuestos de operaciones no autorizadas.

SEGUNDA. – Límites de la responsabilidad entre el BBVA y el Sr. López García.

TERCERA. – La carga de la prueba: ¿existe negligencia grave por parte del Sr. López García?

CUARTA. – Posibilidad de recuperar la cantidad sustraída.

QUINTA. – Acción de responsabilidad frente a la entidad BBVA por las operaciones no autorizadas: procedimiento, órgano competente, cuantía y plazo para su ejercicio.

SEXTA. – Prejudicialidad penal y la falta de litisconsorcio pasivo.

SÉPTIMA. – Intereses que resultan de aplicación.

OCTAVA. – Condena en costas.

5. FUNDAMENTOS JURÍDICOS.

5.1. Sobre las obligaciones de la entidad BBVA, como proveedora de los servicios de pago, y del Sr. López García, como usuario de los mismos, en supuestos de operaciones no autorizadas.

La entrada en vigor del Real Decreto-Ley 19/2018, de 23 de noviembre, de Servicios de Pago y otras medidas urgentes en materia financiera (en adelante, RD-LSP), mediante el cual se incorporó a nuestro ordenamiento jurídico la Directiva (UE) 2015/2366 del Parlamento y del Consejo, de 25 de noviembre, sobre Servicios de Pago en el Mercado Interior, supuso fundamentalmente la creación de un entorno de **mayor seguridad** para los usuarios. De este modo, se pretendía, por el legislador, facilitar y mejorar la seguridad en el uso de sistemas de pago a través de Internet, reforzando a su vez el nivel de protección de los usuarios frente a los posibles fraudes que pudieran originarse.

A la hora de analizar las implicaciones que puede llegar a tener un supuesto de estafa como el que viene siendo objeto de análisis en el presente Trabajo Fin de Máster, claramente se pueden diferenciar las obligaciones existentes, por un lado, para la entidad bancaria, como proveedora de los servicios de pago y, por otro, para el consumidor, como usuario de los mismos.

A) Las obligaciones de la entidad bancaria.

En primer lugar, cabe señalar que la entidad bancaria debe facilitar en todo momento un sistema de banca telemática segura[10], surgiendo así la obligación de contar con **sistemas de seguridad adecuados** que le permitan detectar las transferencias y disposiciones no autorizadas por los usuarios, lo que garantiza la seguridad de las operaciones, como recuerda la reiterada SAP de Barcelona (Sección 14ª), núm. 151/2013, de 7 de marzo ("dicha modalidad fraudulenta de movimientos de cuenta es una práctica extendida, por lo que, exige por ello que la entidad bancaria o crediticia deba adoptar medidas de seguridad específicas").

[10] CALVO SAN JOSÉ, M. J.: "La responsabilidad civil de los bancos en los delitos de estafa por "*phishing*", *Actualidad Jurídica Iberoamericana*, núm. 18, 2023, pp. 1788-1809.

En este sentido, la Audiencia Provincial de Valladolid (Sección 1ª) viene a señalar en la ya mencionada Sentencia núm. 405/2023, de 23 de octubre, que ante este tipo de prácticas delictivas no resulta suficiente implementar 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", siendo insuficientes, por tanto, los avisos genéricos que proporcionan los bancos en sus sitios *web*, los cuales podrían ser considerados como "fórmulas predispuestas", carentes de contenido.

De ahí, la importancia de que las órdenes de pago sean llevadas a cabo mediante una **autenticación reforzada**, tal y como se indicaba en el epígrafe tercero. Gracias a este sistema, la entidad se encontraría habilitada para detectar de forma automática si los elementos de autenticación han podido ser objeto de una posible sustracción respecto del titular de los mismos, evitando así que entidades extrañas accedan a la cuenta corriente del usuario.

Sin embargo, en este caso el Sr. López García asegura que no recibió mensaje alguno por parte de la entidad BBVA de forma que pudiese confirmar los cargos en cuestión, lo cual podría llevar a pensar que el sistema de autenticación de la entidad se vio afectado por un fallo técnico, impidiendo así lograr su principal cometido.

Por otra parte, el art. 42 del RD-LSP, recoge un amplio catálogo de **obligaciones del proveedor de servicios de pago**, como emisor de un instrumento de pago, entre las que se encuentran las siguientes:

a) Asegurarse de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento.

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

c) Garantizar la disponibilidad de medios adecuados y gratuitos que permitan al usuario de servicios de pago efectuar una notificación o solicitar un desbloqueo.

d) Ofrecer al usuario de servicios de pago la posibilidad de efectuar una notificación, gratuitamente y cobrar, si acaso, únicamente los costes de sustitución directamente imputables al instrumento de pago.

e) Impedir cualquier utilización del instrumento de pago una vez efectuada la notificación.

En definitiva, a la vista de todas estas obligaciones legales, son evidentes las exigencias que en este caso recaen sobre la entidad BBVA, por el hecho de ser la proveedora de los servicios de pago. Por ello, resulta inevitable el deber general que tiene de mantener la seguridad en las operaciones realizadas debido a la responsabilidad de riesgo que asume al suministrar estos servicios, tal y como se analizará más adelante.

B) Las obligaciones del usuario.

Adentrándonos ya en el ámbito de actuación del usuario de los servicios de pago, una vez que el mismo haya tenido conocimiento de la utilización no autorizada del instrumento de pago, lo primero que ha de hacer es **comunicarlo sin demora a su entidad financiera**. Precisamente, esto fue lo que hizo el Sr. López García, a fin de intentar bloquear el ataque sufrido con la mayor celeridad posible, solicitando al banco BBVA, al mismo tiempo, la retrocesión de los cargos no autorizados. Asimismo, es recomendable dejar siempre **constancia fehaciente** de dicha notificación, lo cual se acredita con la reclamación extrajudicial efectuada por el mismo el día 25 de noviembre de 2024.

En concreto, sobre el grado de diligencia exigible al usuario de los servicios bancarios, como titular del medio de pago, se pronuncia el art. 41 del mencionado RD-LSP. Además, este precepto señala que el usuario debe hacer uso del instrumento de pago de acuerdo con las condiciones que regulen la emisión y utilización del mismo, las cuales deben ser objetivas, no discriminatorias y proporcionadas. Claramente, se puede deducir que la diligencia que se espera del mismo se corresponde con la de un **consumidor medio**, conforme a unos principios de razonabilidad y buena fe, puesto que está obligado a adoptar *"todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas"*.

Por otra parte, también es preciso determinar si se origina un **deber de autoprotección**, puesto que es habitual que en este tipo de supuestos se lleve a cabo, por

parte de la víctima (usuario), determinadas actuaciones, mediante las cuales se proporcionan al delincuente una serie de claves, facilitando así la comisión del delito.

En este sentido, la STS 854/2014, de 2 de diciembre, señalaba que "En lo relativo a las obligaciones de autoprotección que serían exigibles a la víctima, la jurisprudencia ha aceptado excepcionalmente en algunos casos la atipicidad de la conducta cuando el engaño es tan burdo, tan fácilmente perceptible, que hubiera podido ser evitado por cualquier sujeto pasivo con una mínima reacción defensiva, o, al menos, por un sujeto pasivo cualificado obligado a ciertas cautelas.

Ahora bien, una cosa es la exclusión del delito de estafa en supuestos de "engaño burdo", o de "absoluta falta de perspicacia, estúpida credulidad o extraordinaria indolencia ", y otra que se pretenda desplazar sobre la víctima de estos delitos la responsabilidad del engaño, y se le exija un modelo de autoprotección o autotutela que no está definido en el tipo ni se reclama en otras infracciones patrimoniales.

En palabras de la STS 482/2008 de 28 de junio, el principio de confianza o de la buena fe negocial que rige como armazón en nuestro ordenamiento jurídico, no se encuentra ausente cuando se enjuicia un delito de estafa. La ley no hace excepciones a este respecto, ni obliga al perjudicado a estar más precavido en este delito que en otros, de forma que la tutela de la víctima tenga diversos niveles de protección".

Asimismo, según la Sala de lo Penal del Tribunal Supremo, "[…] la aplicación del delito de estafa no puede quedar excluida mediante la culpabilización de la víctima con específicas exigencias de autoprotección, cuando la intencionalidad del autor para aprovecharse patrimonialmente de un error deliberadamente inducido mediante engaño pueda estimarse suficientemente acreditada, y el acto de disposición se haya efectivamente producido, consumándose el perjuicio legalmente previsto." (STS 162/2012, de 15 de marzo).

Por ello, el Tribunal Supremo niega que se pueda culpabilizar a la víctima ni oponerse un deber de protección[11], de modo que resulta necesario examinar en cada caso la **idoneidad de la maniobra engañosa**, como posible causa de la percepción errónea de la realidad por parte del usuario, aun cuando los sistemas de autoprotección disponibles pudieran haberlo evitado por medio de una actuación especialmente cautelosa.

[11] *Análisis jurisprudencial de estafas por phishing.* IBERLEY. <https://www.iberley.es/temas/analisis-jurisprudencial-estafas-phishing-67281> [Fecha de consulta: 10/11/2024].

Respecto al supuesto práctico que es objeto de análisis en este Trabajo, el engaño producido podría ser calificado como idóneo en lo que a la causa del error se refiere. Prueba de ello es que, haciéndose pasar por la entidad BBVA, le son proporcionadas al Sr. López García una serie de indicaciones con el fin de bloquear una serie de cargos que se estaban intentando hacer en su cuenta bancaria, lo que resulta ser un tanto verosímil en atención al contexto en el que se produce.

5.2. Sobre los límites de la responsabilidad del BBVA y del Sr. López García.

A la vista del análisis efectuado en el epígrafe anterior, es evidente que la entidad bancaria está obligada a garantizar el control técnico adecuado de todos y cada uno de los servicios prestados, así como los debidos niveles de seguridad, respondiendo por los daños y perjuicios ocasionados en caso de incumplimiento.

En este sentido, autores como HERAS HERNÁNDEZ[12] y MARTÍNEZ DE SALAZAR BASCUÑA[13] consideran que la mayor diligencia exigida a las entidades de crédito, en relación con las exigencias de buena fe, y acorde con la naturaleza de las relaciones contractuales bancarias, originan una especial responsabilidad, próxima a la **responsabilidad por riesgo del profesional**, derivada de los hechos que las mismas realizan dentro del ámbito de su actividad y que únicamente cesará en los supuestos de negligencia probada del cliente.

Dicho esto, resulta ser de aplicación lo dispuesto en el art. 147 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de Consumidores y Usuarios y otras leyes complementarias (en adelante, TRLGDCU), en el cual se contempla el régimen general de responsabilidad, considerando a los prestadores de servicios como responsables de los daños y perjuicios causados a los consumidores o usuarios, *"[…] salvo que prueben que han cumplido las exigencias y requisitos reglamentariamente establecidos y los demás cuidados y diligencias que exige la naturaleza del servicio."*

[12] HERAS HERNÁNDEZ, Mª M.: "El modelo de responsabilidad civil de las entidades financieras en función de su profesionalidad", *Cuadernos de Derecho y Comercio,* núm. 27, Madrid, 1998, p. 215.
[13] MARTÍNEZ DE SALAZAR BASCUÑANA, L.: "Protección de particulares frente a malas prácticas bancarias", *Estudios de Derecho Judicial,* núm. 55, CGPJ, Madrid, 2005, pp. 186 y ss.

A su vez, el artículo 45 RD-LSP señala que *"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. […]"*, aun siendo posible determinar otro tipo de indemnización económica en atención a la normativa aplicable al contrato suscrito entre el usuario y el proveedor de los servicios, conforme señala el apartado tercero del citado precepto.

Dicho esto, en atención a lo dispuesto en el art. 36.1 RD-LSP, cabe señalar que únicamente se considerarán autorizadas las operaciones de pago en el supuesto de que el ordenante haya otorgado su consentimiento para la ejecución, considerándose, por tanto, no autorizadas a falta del mismo. Sin embargo, cabe señalar que, en los supuestos de fraude por *phishing*, aunque el usuario ingrese en la página *web* de la entidad bancaria o bien facilite las claves de forma voluntaria, lo cierto es que ningún caso lo realiza con ánimo de autorizar la operación fraudulenta por lo que el delincuente no dispone de un consentimiento por parte del titular de la cuenta, sino que se vale del engaño o mecanismos para obtener las claves[14]. Es por ello que, GÓMEZ-LINACERO[15] puso de manifiesto que la falta de consentimiento debe completarse, indefectiblemente, con el consentimiento viciado, según los principios básicos de nuestro derecho contractual y obligacional, erigidos sobre el consentimiento como piedra angular del acto perfeccionador del negocio.

Por consiguiente, la responsabilidad del titular de la banca *online* es de **naturaleza cuasi-objetiva**, derivada de la exigencia a la entidad titular del servicio *online* de adoptar medidas de seguridad necesarias y renovables ante los distintos modos de fraude informático, de forma que, salvo que se acredite la **negligencia grave** por parte del usuario de la banca electrónica (artículo 46 RD-LSP), la entidad financiera debe responder del reintegro de los importes obtenidos de forma fraudulenta.

[14] RODRÍGUEZ ALMIRÓN, F.: "El delito de estafa informática. ¿Es posible determinar la responsabilidad civil de la entidad financiera en base al artículo 120.3 del Código Penal como consecuencia del «*phishing*»?", *Revista de Derecho Penal y Criminología*, núm. 30, 2023, pp. 273-304.
[15] GÓMEZ-LINACERO CORRALIZA, A.: "Responsabilidad civil de los bancos frente a la estafa informática: preguntas y respuesta en clave práctica", *Diario La Ley*, núm. 10590, Sección Tribuna, 2024.

El mayor grado de objetivación en la responsabilidad de la entidad bancaria se encuentra fuertemente marcado por el llamado "*bonus argentarius*" del deber de diligencia de las entidades bancaria, de acuerdo con lo razonado en al SAP Madrid (Sección 20ª) núm. 184/2022, de 20 de mayo: "La responsabilidad exigida a la entidad demandada, como proveedora del servicio, es la que se deriva de la naturaleza de tal prestación y de la posición contractual en la que se encuentran las partes, lo que le obliga a adoptar una serie de medidas de seguridad y dotarse de mecanismos de supervisión que permitieran detectar operaciones fraudulentas en la prestación de servicios de pago, tal como señala el artículo 2 del Reglamento Delegado 2018/389, pues como se indica también en la sentencia citada de la Audiencia de Pontevedra, incluyendo la técnica del *phishing*, la creación y puesta en la red de páginas que clonan las del sitio oficial de las entidades emisoras de instrumentos de pago, el deber de diligencia de la entidad demandada exigía dotarse de la tecnología *antiphishing* precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas, lo que, de producirse, impediría que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace del correo electrónico haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor"

En este sentido es reiterada jurisprudencia del Tribunal Supremo, el hecho de que la responsabilidad "ha sufrido un proceso de progresiva objetivación, basada especialmente en la teoría de la creación del riesgo, conforme a la que, quien se beneficia de actividades que de alguna forma puedan generar un riesgo para terceros, debe soportar las eventuales consecuencias negativas de orden civil respecto de esos terceros cuando resultan perjudicados" (STS 49/2020, de 12 de febrero); declarando, a su vez, que "conforme a la naturaleza y función del contrato de cuenta corriente bancaria, el cercioramiento o comprobación de la veracidad de la firma del ordenante constituye un presupuesto de la diligencia profesional exigible a la entidad bancaria con relación a sus obligaciones esenciales de gestión y custodia de los fondos depositados por el titular de la cuenta, cuyo incumplimiento da lugar a la indemnización de daños y perjuicios, conforme a lo dispuesto en los artículos 1101 y 1106 del Código Civil" (STS 311/2016, de 12 de mayo).

Se trata del denominado "riesgo operacional", cuya asunción le corresponde en su integridad a la entidad bancaria en supuestos de conductas fraudulentas que afectan a los fondos de sus clientes, debiendo tener, por tanto, conocimiento del mismo y de su operativa habitual.

Por otra parte, en lo relativo a la responsabilidad del usuario, el apartado primero del artículo 46 RD-LSP dispone que existe la posibilidad de que el usuario quede obligado a soportar las pérdidas originadas a consecuencia de las operaciones no autorizadas, estableciendo así un máximo de 50 euros, a menos que no le sea posible detectar la pérdida, la sustracción o la apropiación indebida del instrumento de pago (salvo cuando el propio ordenante haya actuado fraudulentamente), o en el hipotético caso de que la pérdida se debiera a la acción o inacción de empleados o de cualquier agente, sucursal o entidad de un proveedor de servicios de pago al que se hayan externalizado actividades.

Sin embargo, es preciso tener en cuenta que *"el ordenante soportará todas las pérdidas derivadas de operaciones de pago no autorizadas si el ordenante ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave de una o varias de las obligaciones establecidas en el artículo 41."*, no siendo de aplicación dicho límite.

Así este precepto continúa diciendo que *" […] En todo caso, el ordenante quedará exento de toda responsabilidad en caso de sustracción, extravío o apropiación indebida de un instrumento de pago cuando las operaciones se hayan efectuado de forma no presencial utilizando únicamente los datos de pago impresos en el propio instrumento, siempre que no se haya producido fraude o negligencia grave por su parte en el cumplimiento de sus obligaciones de custodia del instrumento de pago y las credenciales de seguridad y haya notificado dicha circunstancia sin demora."*

En definitiva, a la vista del contrato de cuenta corriente suscrito entre ambas partes, quedará justificada la responsabilidad de la entidad bancaria, salvo que se estime probado que ha existido negligencia grave por parte del Sr. López García, cuestión que será analizada en el epígrafe siguiente.

5.3. Sobre la carga de la prueba: ¿existe negligencia grave por parte del Sr. López García?

Anteriormente, se ha señalado que la responsabilidad que se imputa a la entidad bancaria deriva de un mal funcionamiento en sus medidas de seguridad, la cuales son empleadas para acceder al sistema de banca *online* del usuario y autorizar así cargos de forma fraudulenta. Dicha responsabilidad lo es, en definitiva, en tanto que la entidad es prestadora de servicios de pago a través del modelo de banca virtual puesta a disposición de sus clientes.

En lo que respecta a la carga de la prueba, el artículo 217 LEC, Párrafo 7º, establece que *"para la aplicación de lo dispuesto en los apartados anteriores de este artículo el Tribunal deberá tener presente la disponibilidad y facilidad probatoria que corresponde a cada una de las partes del litigio".* Por tanto, cuando se trata de prestaciones contractuales o no contractuales, del tenor del art. 1101 y 1902 CC con relación al artículo 217.2 LEC, se desprenderá que corresponde al perjudicado demandante la carga de la prueba de la culpa del causante del daño demandado. No obstante, esto no es así cuando "una disposición legal expresa" -art. 217.6 LEC- imponga a la **entidad financiera demandada la carga de probar que hizo cuanto le era exigible para prevenir el daño**; o cuando tal inversión de la carga de la prueba venga reclamada por los principios de "disponibilidad y facilidad probatoria" a los que se refiere el meritado artículo 217.7 LEC.

La referida "disposición expresa", aparece recogida, tanto en el **ámbito de consumo** (*Texto Refundido de la Ley para la Defensa de los Consumidores y Usuarios -RDL 1/2007, de 16 de noviembre*-), como en la **regulación de los servicios de pago** (RD *Ley 19/2018, de 23 de noviembre, de Servicios de Pago y otras medidas urgentes en materia financiera).*

Estos fundamentos son reiteradamente recogidos en Sentencias de las Audiencias Provinciales, como la SAP de Alicante (Sección 8ª) núm. 107/2018, de 12 marzo, la cual señala en un supuesto similar al que es objeto de análisis, que: "[…] La lógica de la norma de acceso a la fuente de la prueba y facilidad probatoria en lo que hace a la implementación de medidas de seguridad en la prestación de un servicio que se da por las entidades de crédito a sus clientes a través de una oficina virtual que se desenvuelve en redes bien de internet, bien de comunicaciones móviles, se presenta como criterio más que de razonable atención al caso en el que la propia seguridad y debida reserva de la red se contrapone al acceso por parte de un tercero distinto al titular de la misma que asume poner en la red pública un conjunto de comunicaciones para permitir operaciones bancarias que requiere de soluciones tecnológicas muy avanzadas que minimicen las amenazas contra la autenticidad, integridad y la confidencialidad de los datos que circulan a través de la red".

"(…) no es cierto que la carga de la prueba sobre la implementación de medidas de seguridad adecuadas, suficientes, eficientes y actuales al nivel de riesgo modalidades de ataques informáticos en la red bancaria de banca *online* lo sea a cargo del usuario del sistema, pues el marco de responsabilidad establecido para el caso de operaciones de pagos hechos por proveedores de servicios no autorizadas o ejecutadas incorrectamente, es el de la cuasi-objetividad tal cual se desprende de la regulación específica sobre la materia".

Llegados a este punto, resulta conveniente determinar el **grado de negligencia** que es necesario que concurra en el usuario para que pueda exonerarse a la entidad bancaria de la responsabilidad. En este sentido, la SAP Madrid (Sección 20ª) núm. 249/2022, de 1 de julio, señala que "las entidades bancarias, como prestadoras del servicio, tienen la obligación de acreditar que el usuario del instrumento de pago ha actuado de manera negligente y que para que pueda atribuirse al usuario la responsabilidad en operaciones bancarias mediante estos sistemas de pago, dicho comportamiento negligente ha de ser de entidad suficientemente grave y que implique algo más que la mera negligencia, lo que supone haber adoptado una conducta caracterizada por un grado significativo de falta de diligencia, poniéndose como ejemplo de ello, 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. 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".

Por su parte, la SAP de Pontevedra (Sección 3ª) 623/2022, de 1 de diciembre, determina que "como parámetro del actuar negligente también cabrá acudir al art. 1104 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"; siendo de nuevo posteriormente reproducido este fundamento por la SAP de Pontevedra (Sección 3ª) núm. 177/2023, de 23 de marzo.

Respecto al marco legal, el RD-LSP prevé en su artículo 44, apartado primero, que *"cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá al proveedor de servicios de pago 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".* En otras palabras, si el usuario niega haber realizado operación alguna, como ocurre en el caso del Sr. López García, la carga probatoria sobre la autenticación, recaerá directamente sobre el proveedor. Asimismo, según indica el apartado segundo del citado precepto, es al proveedor de servicios de pago a quien le corresponde probar que el usuario de los mismos cometió fraude o

negligencia grave.

Ahora bien, la concurrencia de **negligencia grave** del usuario es uno de los aspectos que más incertidumbre ha venido generando en los últimos tiempos. En atención a la Directiva 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre, la negligencia es aquella que deriva de una conducta caracterizada por un **grado significativo de falta de diligencia**, lo que implica que la misma no surge como consecuencia del engaño al que ha sido inducido por parte del delincuente, sino por iniciativa propia del usuario en cuestión. En este sentido, algunos autores apuntan que no basta con cualquier omisión de las obligaciones que le son impuestas, sino que es necesaria una actitud descuidada o de inobservancia de las normas más esenciales en evitación del fraude y protección de su propio patrimonio[16]

Según lo dispuesto en el art. 1104 CC, *"la culpa o negligencia del deudor consiste en la omisión de aquella diligencia que exija la naturaleza de la obligación y corresponda a las circunstancias de las personas, del tiempo y del lugar. […]"*. Por tanto, teniendo en cuenta que en supuestos de *phishing* nos encontramos ante manipulaciones informáticas llevadas a cabo por delincuentes profesionales, siendo difíciles de detectar y evitar por un usuario medio, como es el Sr. López García, la entidad de crédito solo quedará exonerada de responsabilidad cuando la misma consiga demostrar que efectivamente el usuario ha utilizado el servicio sin una **mínima diligencia**, dando lugar así a una negligencia grave por parte del mismo.

No resulta aceptable trasladar al usuario una responsabilidad que no le corresponde dada su sensibilidad, criterio que ha sido mantenido por numerosas Audiencias. A modo de ejemplo, cabe señalar que la AP de Madrid considera, "no es un sistema fácil sino complejo, que no es detectable por el particular usuario, aun teniendo instalados antivirus porque el tema más de uso de estos es de sistemas, para lo que se requiere algo más que tener cuidado y tener instalado tanto en el ordenador como en el móvil un antivirus" (SAP de Madrid, Sección 21ª, núm. 372/2017, de 31 de octubre); y, a su vez, la SAP de Navarra (Sección 3ª) núm. 223/2023, de 9 marzo, destaca la elevada complejidad técnica que presente este tipo de conductas delictivas.

En esta línea, la SAP de Madrid (Sección 10ª) 24/2023, de 13 de enero, concluye que "[…] no podemos calificar la posible negligencia de la demandante en la conservación de sus

[16] MATARREDONDA CHORNET, L. y PEÑALOSA TORNÉ, C.: "Ciberdelincuencia. La responsabilidad civil bancaria", *Diario La Ley*, núm. 10431, Sección Tribuna, 2024, p. 3.

claves como “graves” 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”.

Asimismo, la SAP de Oviedo (Sección 5ª) núm. 404/2024, de 17 de septiembre, indicar que “el caso como el de autos, en el que los actores niegan haber realizado, ni autorizado las operaciones realizadas, salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante, la responsabilidad será del proveedor del servicio de pago, lo que comporta que pesa sobre él la carga de probar que la orden de pago no se vio afectada por "un fallo técnico u otra deficiencia del servicio prestado por dicho proveedor", o bien, probar que el cliente ha 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” .

En definitiva, cabe concluir que la **carga de la prueba** sobre la implementación de medidas de seguridad adecuadas, suficientes, eficientes y actuales le corresponde en todo caso al proveedor de servicios de pago. De este modo, la entidad BBVA es quien debe probar la negligencia grave del Sr. López en lo que a la custodia y uso de sus claves de seguridad en el sistema de servicios de pago *online* de su tarjeta de crédito se refiere. Solo así quedaría suficientemente acreditado que las operaciones en cuestión sí que fueron auténticas y, consiguientemente, que no estuvieron afectadas por un fallo técnico o cualquier otra deficiencia del sistema.

5.4. Sobre la posibilidad de recuperar la cantidad sustraída.

Tras haber sido víctima de una estafa, la realidad es que el usuario lo único que desea es recuperar su dinero, es decir, la cantidad total que ha sido objeto de sustracción.

En los últimos años, los Tribunales han venido reconociendo la responsabilidad de las entidades bancarias en la gran mayoría de supuestos, justificando así el derecho a reclamar como consecuencia de una mala praxis del banco, que le corresponde al consumidor. En esta misma línea se pronuncian todas las sentencias citadas hasta el momento, pues resulta bastante inusual encontrar un Fallo de una Sentencia en el que la entidad bancaria no sea

condenada a la devolución de la cantidad objeto de sustracción, a excepción de los casos en los que es evidente la actuación fraudulenta del perjudicado.

Ahora bien, no existe una regla generalizada y por ello es necesario analizar caso por caso. El hecho de haber sido víctima de *phishing*, no necesariamente conlleva que la entidad bancaria sea condenada a devolver el dinero al usuario. Por ello, es preciso tomar en consideración las características concretas de cada supuesto, probando a su vez todos los extremos necesarios para acreditar la existencia de esta responsabilidad contractual.

Respecto al supuesto práctico que viene siendo objeto de análisis, no cabe duda de que el Sr. López García ha sido víctima de un tipo de fraude conocido como *PHISHING* O ESTAFA INFORMÁTICA, el cual se encuentra regulado en el art. 249 CP. En este sentido, la SAP de Oviedo (Sección 4ª), núm. 142/2024, de 21 de marzo, señala en su Fundamento de Derecho Segundo que, "se está, pues, ante un tipo de estafa informática cometida mediante la captación de datos bancarios, induciendo a error a la víctima tras hacerse pasar por la propia entidad bancaria, a la que suplantan a través de correos electrónicos (técnica conocida como *"phishing"*) o bien a través de SMS fraudulentos como en este caso (*"smishing"*), con el objetivo final de que los clientes proporcionen sus datos de carácter personal y claves bancarias para acceder así a sus cuentas de forma fraudulenta. La excusa frecuentemente utilizada, como sucedió en este caso, es la de informar sobre un acceso no autorizado a las cuentas *online*, de tal modo que los clientes alertados ante esa circunstancia, intentan comunicar con el Banco cuando en realidad lo que hacen es facilitar sus datos bancarios al defraudador".

El acceso a la cuenta corriente titularidad del Sr. López García y a las mencionadas operaciones bancarias se produjo sin hacer frente a unas mínimas y exigibles medidas de seguridad por parte de la entidad. El hecho de no haber recibido mensaje alguno a fin de confirmar dichas operaciones, parece indicar que efectivamente no se llevó a cabo ningún sistema de autenticación de doble factor por parte de la entidad bancaria BBVA.

De la contestación a la reclamación extrajudicial, no ha quedado suficientemente acreditado que la entidad BBVA haya llevado a cabo un proceso de verificación, automático y deliberado, para comprobar la naturaleza de las operaciones realizadas, a todas luces sospechosas ya que jamás antes se había realizado por el Sr. López García unas transacciones por un importe tan elevado. Precisamente, esto podría haber llevado al banco a actuar de

forma diligente y retener dicha cantidad hasta verificar que efectivamente se trataban de operaciones queridas y realizadas por el propio titular de la cuenta.

Por contra, la entidad simplemente obvió la existencia de una anomalía sin precedentes entre los movimientos del Sr. López García, sin poner en funcionamiento medida de seguridad alguna, hasta que el propio afectado lo puso en su conocimiento. A mayor abundamiento, teniendo en cuenta la cuantía de las operaciones realizadas, BBVA no puso a disposición del cliente las medidas reforzadas necesarias que unas operaciones de esta entidad requieren.

Por todo ello, resulta evidente que, en el supuesto que nos ocupa, no existe ningún tipo de actuación fraudulenta o negligente por parte del Sr. López García, debiendo por tanto la entidad BBVA asumir la responsabilidad.

5.5. Sobre la acción de responsabilidad frente al BBVA por las operaciones no autorizadas: procedimiento, órgano competente, cuantía y plazo para su ejercicio.

Tras la negativa de la entidad bancaria a la reclamación extrajudicial efectuada por parte del Sr. López García, el mismo se vería obligado a acudir a la vía judicial. De este modo, cabría interponer una **DEMANDA DE JUICIO VERBAL, en ejercicio de acción de responsabilidad contractual y reclamación de cantidad,** frente a la entidad "Banco Bilbao Vizcaya Argentaria, S.A.", en su legal representación, con CIF A-48265169 y domicilio social en Plaza de San Nicolás, núm. 4, 48005, Bilbao, pudiendo ser notificada en su oficina sita en Avenida Palencia, núm. 3, 47010, Valladolid.

En este sentido, de acuerdo con lo dispuesto en los arts. 45, 51.1 y 52 de la LEC, cabe señalar que resulta competente para conocer de dicha demanda el **Juzgado de Primera Instancia de Valladolid**, que por turno corresponda, por ser el domicilio del demandado o a aquel en el que tenga establecimiento abierto al público o representante autorizado para actuar en nombre de la entidad. Respecto al tipo procedimiento a seguir, corresponde dar a la presente demanda la tramitación prevista para el juicio verbal en el Título III de la LEC, arts. 437 y ss., puesto que el importe objeto de reclamación no excede de 15.000 euros (art. 250.2 LEC).

Respecto a la cuantía del procedimiento, se cifra en TRES MIL TRESCIENTOS SESENTA Y CUATRO EUROS CON CINCUENTA Y SEIS CÉNTIMOS (3.364,56€), conforme a lo dispuesto en los arts. 251.1ª y 253.1 LEC.

Por otra parte, en lo que al plazo para ejercitar la correspondiente acción se refiere, el art. 43.1 del RD-LSP, señala que *"el usuario de servicios de pago obtendrá la rectificación por parte del proveedor de servicios de pago de una operación de pago no autorizada o ejecutada incorrectamente únicamente si el usuario de servicios de pago se lo comunica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 60, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo."*

Sin embargo, en palabras de RIBÓN SEISDEDOS[17], ello no debe llevarnos a la confusión de la falta de acción transcurrido dicho término, cuando lo que se pretenda es la exigencia de responsabilidad contractual derivada de estas operaciones no autorizadas. En este sentido, según el art. 45.3 del citado decreto, *"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.*

Así, determinada la naturaleza civil de la acción ejercitada en la presente demanda, es menester señalar que existe una concurrencia de responsabilidades en el presente procedimiento, como se reconoció en la ya reiterada SAP de Alicante, de 12 de marzo de 2018: "Barclays si infringió sus obligaciones, tanto contractuales de implementación del sistema de las medidas de seguridad exigibles para un uso seguro por su cliente, como extracontractuales, al no haber actuado con diligencia tras la denuncia del fraude informático padecido en la cuenta de la cliente al acceder al sistema *online* terceros no autorizados para operar con aquella".

Consecuencia de esta concurrencia de responsabilidad contractual y extracontractual, cabe concluir que el plazo para el ejercicio de la acción personal se correspondería con el previsto en el apartado segundo del artículo 1.964 del CC. De este modo, el Sr. López García dispondría de un **plazo de cinco años**, a contar desde que pudo exigirle a su entidad bancaria el cumplimiento de la obligación, por lo que en este caso no cabe entender que la acción haya prescrito.

[17] RIBÓN SEISDEDOS, E.: *Fraudes bancarios y defensa del afectado*…, op. cit., p.296.

5.6. Sobre la prejudicialidad penal y la falta de litisconsorcio pasivo.

Por su parte, la entidad financiera podría argumentar que la denuncia da lugar a la existencia de un posible procedimiento penal pudiendo considerar, erróneamente, que existe una causa de *prejudicialidad penal*, conforme al art.40 LEC. Sin embargo, tal premisa no puede mantenerse ya que, en este supuesto, se está ejercitando una demanda de responsabilidad frente a la entidad bancaria con quién el Sr. López García contrató el servicio de banca *online*.

A este respecto, GONZÁLEZ SÁNCHEZ[18] señala que la suspensión del proceso civil está íntimamente relacionada con la importancia que precisamente esos hechos de apariencia delictiva tienen respecto de la decisión que debe adoptarse en el proceso civil. Esto es, debe tratase de una **influencia decisiva** de tal modo que la resolución del proceso penal sea fundamental a la hora de otorgar o denegar la tutela solicitada en vía civil, lo que concuerda con lo dispuesto en el apartado segundo del art. 10 LOPJ: *"No obstante, la existencia de una cuestión prejudicial penal de la que no pueda prescindirse para la debida decisión o que condicione directamente el contenido de ésta determinará la suspensión del procedimiento mientras aquélla no sea resuelta por los órganos penales a quienes corresponda, salvo las excepciones que la ley establezca"*.

En cuanto a la jurisprudencia emanada del Tribunal Supremo viene siendo un tanto restrictiva, considerando así que, para que pueda operar la prejudicialidad penal como causa de suspensión: "la sentencia a dictar haya de fundarse exclusivamente en el supuesto de la existencia del delito, lo que -como ya se ha dicho- no se produce en el presente caso, pues la decisión que se adopte en el procedimiento penal no afecta a las pretensiones instadas en el suplico del escrito de demanda iniciador del juicio civil de que se trata, debiendo añadirse que ese criterio contenido en el citado art. 363 de la Ley de Enjuiciamiento Civil viene corroborado en el art. 10 de la Ley Orgánica del Poder Judicial que al establecer que a los solos efectos prejudiciales, cada orden jurisdiccional podrá conocer de asuntos que no le estén atribuidos privativamente, creando un sistema de integración al respecto, únicamente exceptúa la existencia de cuestión prejudicial penal de la que no pueda prescindirse para la debida decisión o que condicione directamente el contenido de ésta, lo que no acontece en el caso planteado en el que - repetimos- las peticiones de ineficacia contractual instadas en la demanda del juicio civil tiene aspectos de solución independientes de lo que pudiera merecer el procedimiento penal también planteado" (STS 947/1989, de 15 de diciembre); argumento que a su vez comparte la STS 209/2013, de 4 de abril.

[18] GONZÁLEZ SÁNCHEZ, J. L.: *Las cuestiones prejudiciales penales en el proceso civil,* La Ley, Madrid, 2002, p.43.

Asimismo, la AP de Barcelona (Sección 14ª) en su Sentencia núm. 151/2013 de 7 marzo, ha señalado que "En cuanto dicha causa de desestimación de la demanda debe rechazarse, pues la actora ante el hecho de disposiciones por terceros en su cuenta *online* con Caixa de Catalunya lo denuncia ante los Mossos d'Esquadra, y, se instruyen unas Diligencias Previas, cuyo resultado de las mismas se ignora; lo cual no impide que ejercite aquí demanda de responsabilidad contractual frente a la entidad crediticia con quién contrató dicho servicio de banca *online*"; mientras que la AP de Pontevedra (Sección 3ª) recoge en su ya mencionada Sentencia núm. 177/2023, de 23 de marzo, que "(…) al margen de la cuestión penal de la estafa objeto allí de instrucción y cuya tramitación actual se obvia justificar en autos casi un año después, lo que resulta es que la discusión objeto aquí de conocimiento y decisión, es distinta, concretándose en la responsabilidad de la entidad bancaria en razón del complimiento, adecuado y diligente, de las obligaciones que se le imponen en la gestión de los servicios de pago que presta y, en todo caso, si medió o no negligencia/grave por parte de su cliente en la custodia de sus credenciales. Es perceptible que el análisis del vínculo negocial y obligaciones exigibles derivadas del mismo y de la posible negligencia grave por parte de la aquí actora antes referidos, determinante de la responsabilidad reclamada y objeto de litis, no se ve mediatizado, sujeto ni interferido por la instrucción de la causa penal esgrimida porque en ella el bien jurídico protegido alcanza y trasciende a la protección del patrimonio de las víctimas, abarcando la necesidad de proteger también la seguridad del tráfico financiero y mercantil que facilitan las nuevas tecnologías lo que dista bastante de la responsabilidad y actuaciones que vienen a sostener esta pretensión".

Dicho esto, en este caso no resulta necesario esperar a la conclusión de la causa penal, porque lo que se está debatiendo en ella es la responsabilidad criminal de los autores directos. En este procedimiento, al margen del resultado del procedimiento penal, lo que se valora es la responsabilidad civil de la entidad bancaria.

Por otro lado, tampoco cabría que la entidad alegue falta de litisconsorcio pasivo necesario en el presente sobreseimiento, dado que el objeto de la presente demanda se circunscribe entorno a las obligaciones que mantiene la entidad demandada con el cliente por el incumplimiento de obligaciones relativas al sistema de banca *online*, donde las únicas partes legitimadas son entidad financiera y consumidor. Este razonamiento se expuso en la SAP de Castellón (Sección 3ª), núm. 39/2014, de 4 de febrero.

5.7. Sobre los intereses que resultan de aplicación.

En todo caso la cuantía objeto de restitución por parte de la entidad bancaria a causa de las disposiciones fraudulentas, deberá verse incrementada en los correspondientes **intereses legales**, por aplicación de lo dispuesto en los arts. 1101 y 1108 del Código Civil y, en su caso, los imperativos del art. 576 LEC desde que fuere dictada en primera instancia la resolución judicial.

Sobre este particular se pronuncia la SAP de Baleares (Sección 5ª) 132/2023, de 17 de febrero, señalando que "la cantidad a cuyo abono se condena a la parte demandada devengará, conforme a los artículos 1100, 1101 y 1108 del Código Civil, el interés legal desde la fecha de los cargos en cuenta hasta hoy, así como el interés que determina el artículo 576 de la Ley de Enjuiciamiento Civil desde la fecha de la presente resolución hasta que la misma haya sido totalmente ejecutada".

Asimismo, la SAP de Madrid (Sección 10ª), núm. 328/2020, de 21 de julio, rechaza la petición de la entidad de la supresión de la imposición de intereses al indicar que "(…) tampoco cabe excluir los intereses desde la intimación extrajudicial, al no poder sostenerse con rigor que la oposición de la entidad bancaria ha sido razonable, entre otras razones, ya que ha rehusado dar cumplimiento a la obligación prevista legalmente, como se deduce de la misiva enviada el día 3/9/2018", donde se afirma, dado que se han realizado (los cargos) "con lectura del Chip EMU y tecleo de PIN", e incluso los términos vertidos en el escrito de interposición del recurso van mucho más allá de lo aducido en el escrito de contestación a la demanda. (…)".

Por tanto, deberá tenerse en cuenta el interés legal del dinero desde la fecha en que se produjeron las operaciones no autorizadas, el 20 de noviembre de 2024, pues es en ese momento en el que se produce el perjuicio para Don José Antonio López García. Subsidiariamente, se deberán tener en cuenta los intereses devengados desde que se reclamó el importe a la entidad BBVA y esta incumplió su obligación legal de restituir dicho importe (25 de noviembre de 2024).

5.8. Sobre la condena en costas.

Conforme a lo dispuesto en el art. 394 de la LEC, en los procesos declarativos se impondrán las costas a la parte que haya visto rechazada todas sus pretensiones, salvo que el Tribunal aprecie, y así lo razone, que el caso presentaba serias dudas de hechos o de derecho. Consta a su vez realizado **requerimiento fehaciente y justificado de pago** por parte del Sr. López García, con carácter previo a la presentación de la demanda, por lo que ha de apreciarse en todo caso la mala fe de la entidad bancaria, según lo establecido en el art. 395 LEC.

A este respecto, RIBÓN SEISDEDOS[19] señala en su obra que la claridad de la normativa sobre la responsabilidad del proveedor de servicios de pago en supuestos de operaciones no autorizadas por el titular junto con el carácter cuasi-objetivo de su responsabilidad, no permite la invocación de la existencia de dudas para pretender una exoneración de costas en caso de que exista una reclamación previa del afectado.

Por otro lado, ocurre que no se ha visto respetado el **plazo de un mes** del que dispone la entidad financiera a la hora de dar respuesta a las reclamaciones recibidas, según prevé el artículo 21.3 del TRLGDCU.

Por todo ello, resulta evidente la mala fe de la entidad bancaria, así como la propia buena fe del Sr. López García, toda vez que intentó una solución extrajudicial por la vía interna de la entidad financiera evitando así el iniciar un procedimiento judicial, con los costes que ello conlleva.

En definitiva, procedería la imposición de las costas a la entidad bancaria como parte demandada que es en el presente procedimiento, por apreciarse **mala fe** en su actuación. Habiéndose desentendido y negando toda responsabilidad que pueda tener, amparándose en unas alegaciones carentes de fundamento y, por tanto, obligando al Sr. López García a asistir a la vía judicial para ver resarcidos sus derechos.

[19] RIBÓN SEISDEDOS, E.: *Fraudes bancarios y defensa del afectado*…, op. cit., p.306.

6. CONCLUSIONES.

En el presente Trabajo Fin de Máster se ha llevado a cabo un análisis integral del fenómeno denominado *phishing*, haciendo especial referencia a la responsabilidad contractual que deben asumir las entidades bancarias en el supuesto de que se originen operaciones no autorizadas por los usuarios de los servicios de pago. Sobre la base de todo ello, han sido extraídas las siguientes conclusiones:

I. Don José Antonio López García ha sido víctima de un tipo de fraude denominado *phishing* dado que, mediante el envío de un correo electrónico en el que el *phisher* **suplantaba la identidad de la entidad** BBVA, consiguió inducirle a error y acceder a la información confidencial de su cuenta corriente, lo que le permitió llevar a cabo una serie de operaciones fraudulentas.

II. Una de las principales exigencias derivadas del Real Decreto-Ley 19/2018, de 23 de noviembre, de Servicios de Pago y otras medidas urgentes en materia financiera, se basa en la obligación que tienen las entidades bancarias de implementar **sistemas de seguridad** adecuados, que les permita detectar transferencias y disposiciones no autorizadas por el usuario, reforzando así la seguridad de las transacciones digitales. Prueba de ello, es el sistema de **autenticación de doble factor**, el cual permite verificar la identidad del titular de la cuenta, en un primer momento, a través de la contraseña de acceso a la banca online y, posteriormente, por medio de un código único temporal que es enviado en ese instante al dispositivo personal del usuario, a fin de autenticar la operación en cuestión.

III. En relación con las obligaciones del usuario de los servicios de pago (art. 41 RD-LSP), el mismo deberá **comunicarlo a su entidad financiera** tan pronto como haya tenido conocimiento de la utilización no autorizada de su instrumento de pago, dejando constancia fehaciente de dicha notificación, al igual que hizo el Sr. López García. En todo caso, el instrumento de pago debe ser utilizado de acuerdo con las condiciones que regulan su emisión y utilización, estando así el usuario obligado a adoptar *"todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas"*, por lo que la diligencia esperada se corresponde con la de un **consumidor medio**. Sin embargo, según la reiterada jurisprudencia del Tribunal Supremo, esto no implica la existencia de un **deber de autoprotección** respecto del

Sr. López García, puesto que el engaño producido podría ser calificado como idóneo en atención al contexto en el que se produce, siendo así la causa de la percepción errónea de la realidad por parte del mismo.

IV. La normativa vigente prevé un sistema de **responsabilidad de riesgo** a cargo de la entidad bancaria, como proveedora de los servicios de pago, que solo cede en caso de actuación fraudulenta o de incumplimiento, deliberado o por negligencia grave, por parte del usuario de la banca electrónica (artículo 46 RD-LSP). En este sentido, se trata de una responsabilidad de **naturaleza cuasi-objetiva**, derivada de la exigencia a la entidad titular del servicio *online* de adoptar medidas de seguridad necesarias y renovables ante los distintos modos de fraude informático. Por tanto, salvo que se acredite la existencia de la referida **negligencia grave**, la entidad BBVA deberá responder del reintegro de los importes obtenidos de forma fraudulenta de la cuenta del Sr. López García.

V. Respecto a la **carga de la prueba** sobre la implementación de medidas de seguridad adecuadas y suficientes, se le atribuye en todo caso al **proveedor de servicios de pago** (art. 44 RD-LSP). Por ello, es a la entidad BBVA a quien le corresponde demostrar que las operaciones en cuestión sí que fueron auténticas, no estando así afectadas por un fallo técnico o cualquier otra deficiencia del sistema y, consiguientemente, que existió una negligencia grave por parte del Sr. López García, en lo que a la custodia y uso de claves de seguridad en el sistema de servicios de pago *online* de su tarjeta de crédito se refiere.

VI. En cuanto al **grado de negligencia** que es necesario que concurra en el usuario para que pueda exonerarse a la entidad bancaria de la responsabilidad, es uno de los aspectos que más incertidumbre ha venido generando en los últimos tiempos. Según el criterio mantenido por las Audiencias, "ha de ser de entidad suficientemente grave y que implique algo más que la mera negligencia, lo que supone haber adoptado una conducta caracterizada por un grado **significativo** de falta de diligencia", como podría ser el hecho de guardar las credenciales relativas a la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros. Asimismo, derivada del art. 1104 CC, se exige la diligencia asociada a la naturaleza de la obligación y a las circunstancias personales, de tiempo y lugar. Por todo ello, cabe concluir que la falta de diligencia no surge como

consecuencia del engaño al que ha sido inducido el usuario por parte del delincuente, sino por **iniciativa propia** del mismo.

VII. Atendiendo a las circunstancias del supuesto fáctico planteado, el Sr. López García estaría legitimado para interponer una **demanda de juicio verbal,** puesto que el importe objeto de reclamación no excede de 15.000 euros (art. 250.2 LEC), en ejercicio de **acción de responsabilidad contractual y reclamación de cantidad**, frente a la entidad BBVA, con expresa imposición en costas dada la concurrencia de mala fe. En este caso, resulta competente para conocer de la misma el **Juzgado de Primera Instancia de Valladolid**, que por turno corresponda, por ser el domicilio del demandado o a aquel en el que tenga establecimiento abierto al público o representante autorizado para actuar en nombre de la entidad. Por último, no cabe entender que la acción haya prescrito, dado que el Sr. López García dispondría de un plazo de cinco años, a contar desde que pudo exigirle a su entidad bancaria el cumplimiento de la obligación (art. 1.964.2 CC).

VIII. La cuantía del procedimiento se cifra en TRES MIL TRESCIENTOS SESENTA Y CUATRO EUROS CON CINCUENTA Y SEIS CÉNTIMOS (3.364,56€), debiendo ser incrementada con el **interés legal del dinero** desde la fecha en que se produjeron las operaciones no autorizadas (20 de noviembre de 2024), pues es en ese momento en el que se produce el perjuicio para el Sr. López García; o subsidiariamente, desde que el mismo reclamó extrajudicialmente el importe a la entidad BBVA y esta incumplió su obligación legal de restituirlo (25 de noviembre de 2024).

IX. En este procedimiento, al margen del resultado del procedimiento penal, lo que se valora es la responsabilidad civil de la entidad BBVA, por lo que no cabría alegar por parte de la misma la existencia de una causa de **prejudicialidad penal** como causa de suspensión, por el hecho de que el Sr. López García haya interpuesto una denuncia con carácter previo. Del mismo modo, tampoco tendría cabida la **falta de litisconsorcio pasivo**, dado que el objeto de la demanda se circunscribe entorno a las obligaciones que mantiene la entidad demandada con el cliente por el incumplimiento de obligaciones relativas al sistema de banca *online*.

7. BIBLIOGRAFÍA.

CALVO SAN JOSÉ, M. J.: "La responsabilidad civil de los bancos en los delitos de estafa por "*phishing*", *Actualidad Jurídica Iberoamericana*, núm. 18, 2023, pp. 1788-1809.

CONSEJO DE CONSUMIDORES Y USUARIOS, *Banca on line y protección de los consumidores*, Madrid, 2001.

FERNÁNDEZ CABRERA, M.: "La tutela penal del comercio electrónico" en: MADRID PARRA, Agustín (director) y BLANCO SÁNCHEZ, María Jesús (coordinadora) *Derecho Mercantil y Tecnología*, Aranzadi, Navarra, 2018, capítulo 21, pp. 607-630.

GÓMEZ-LINACERO CORRALIZA, A.: "Responsabilidad civil de los bancos frente a la estafa informática: preguntas y respuesta en clave práctica", *Diario La Ley*, núm. 10590, Sección Tribuna, 2024.

GONZÁLEZ SÁNCHEZ, J. L.: *Las cuestiones prejudiciales penales en el proceso civil,* La Ley, Madrid, 2002.

HERAS HERNÁNDEZ, Mª M.: "El modelo de responsabilidad civil de las entidades financieras en función de su profesionalidad", *Cuadernos de Derecho y Comercio,* núm. 27, Madrid, 1998.

LUNA ZACATE, F.: "Phishing: la amenaza constante", Seguritecnia, núm. 468, 2019, pp. 74-76.

MATARREDONDA CHORNET, L. y PEÑALOSA TORNÉ, C.: "Ciberdelincuencia. La responsabilidad civil bancaria", *Diario La Ley*, núm. 10431, Sección Tribuna, 2024.

MARTÍNEZ DE SALAZAR BASCUÑANA, L.: "Protección de particulares frente a malas prácticas bancarias", *Estudios de Derecho Judicial*, núm. 55, CGPJ, Madrid, 2005.

PACHECO JIMÉNEZ, M. N.: "*Phishing* e imputación de responsabilidad en el ámbito bancario", *Centro de Estudios de Consumo*, Toledo, 2017.

PIQURES CASTELLOTE, F.: "Conocimientos básicos en Internet y utilización para actividades ilícitas" en *Delitos contra y a través de las nuevas tecnologías ¿Cómo reducir su impunidad?*, Madrid, 2006.

RIBÓN SEISDEDOS, E.: *Fraudes bancarios y defensa del afectado. Nuevas tendencias defraudatorias. Especial referencia al phishing bancario*, Tirant lo Blanch, Valencia, 2024.

RODRÍGUEZ ALMIRÓN, F.: "El delito de estafa informática. ¿Es posible determinar la responsabilidad civil de la entidad financiera en base al artículo 120.3 del Código Penal como consecuencia del «*phishing*»?", *Revista de Derecho Penal y Criminología*, núm. 30, 2023, pp. 273-304.

USERA, L.: "Desfalcos por *phishing*", *Revista Dialnet*, núm. 46, 2007, pp. 24-26.

VELASCO NÚÑEZ, E.: *Fraude digital y contra medios de pago. Defraudaciones mediante phishing, bizum; criptoactivos, tokens y otros medios de pago*, La Ley, Madrid, 2024.

WEBGRAFÍA.

Análisis jurisprudencial de estafas por phishing. IBERLEY. <https://www.iberley.es/temas/analisis-jurisprudencial-estafas-phishing-67281> [Fecha de consulta: 10/11/2024].

BANCO BILBAO VIZCAYA AREGENTARIA, S.A.: *PSD2: la autenticación reforzada.* <https://www.bbva.es/general/seguridad/herramientas/doble-autenticacion.html> [Fecha de consulta: 23/11/2024].

BANCO DE ESPAÑA: *¿Qué es el phishing y cómo evitarlo? ¡No piques!* <https://clientebancario.bde.es/pcb/es/blog/que-es-el-phishing-y-como-evitarlo.html> [Fecha de consulta: 15/12/2024].

INSTITUTO NACIONAL DE CIBERSEGURIDAD: *Autenticación de dos factores* (2FA). <https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras/autenticacion-de-dos-factores> [Fecha de consulta: 01/11/2024].

Phishing bancario. ¿Puedo reclamar al Banco? DPG LEGAL, S.L.<https://www.dpglegal.es/es/noticia/phising-puedo-reclamar-al-banco/> [Fecha de consulta: 25/11/2024].

8. REFERENCIAS JURISPRUDENCIALES.

- Sentencia de la Audiencia Nacional

  SAN, Sala de lo Penal, Sección 3ª, núm. 7/2020, de 25 de marzo.

- Sentencias del Tribunal Supremo:

  STS, Sala de lo Civil, Sección 1ª, núm. 947/1989, de 15 de diciembre.

  STS, Sala de lo Penal, Sección 2ª, núm. 162/2012, de 15 de marzo.

  STS, Sala de lo Civil, Sección 1ª, núm. 209/2013, de 4 de abril.

  STS, Sala de lo Penal, Sección 2ª, núm. 854/2014, de 2 de diciembre.

  STS, Sala de lo Civil, Sección 1, núm. 311/2016, de 12 de mayo.

  STS, Sala de lo Civil, Sección 1ª, núm. 470/2019, de 17 de septiembre.

  STS, Sala de lo Penal, Sección 1ª, núm. 49/2020, de 12 de febrero.

- Sentencias de Audiencias Provinciales:

  SAP de Barcelona, Sección 14ª, núm. 151/2013, de 7 de marzo.

  SAP de Castellón, Sección 3ª, núm. 39/2014, de 4 de febrero.

  SAP de Madrid, Sección 21ª, núm. 372/2017, de 31 de octubre.

  SAP de Alicante, Sección 8ª, núm. 107/2018, de 12 marzo.

  SAP de Madrid, Sección 10ª, núm. 328/2020, de 21 de julio.

  SAP de Madrid, Sección 20ª, núm. 184/2022, de 20 de mayo.

  SAP de Madrid, Sección 20ª, núm. 249/2022, de 1 de julio.

SAP de Pontevedra, Sección 3ª, núm. 623/2022, de 1 de diciembre.

SAP de Madrid, Sección 10ª, núm. 24/2023, de 13 de enero.

SAP de Baleares, Sección 5ª, núm. 132/2023, de 17 de febrero.

SAP de Navarra, Sección 3ª, núm. 223/2023, de 9 de marzo.

SAP de Pontevedra, Sección 3ª, núm. 177/2023, de 23 de marzo.

SAP de Valladolid, Sección 1ª, núm. 405/2023, de 23 de octubre.

SAP de Oviedo, Sección 4ª, núm. 142/2024, de 21 de marzo.

SAP de Oviedo, Sección 5ª, núm. 404/2024, de 17 de septiembre.

9. LEGISLACIÓN.

- Real Decreto, de 24 de julio de 1889, por el que se publica el Código Civil.
- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de Consumidores y Usuarios y otras leyes complementarias
- Directiva (UE) 2015/2366 del Parlamento y del Consejo, de 25 de noviembre, sobre Servicios de Pago en el Mercado Interior.
- Real Decreto-Ley 19/2018, de 23 de noviembre, de Servicios de Pago y otras medidas urgentes en materia financiera.