Revista CESCO de Derecho de Consumo
http://revista.uclm.es/index.php/cesco

Nº 56/2025

ISSN 2254-2582

https://doi.org/10.18239/RCDC_2025.56.3735

EL *PHISHING* COMO RIESGO DE SEGURIDAD EN EL ECOSISTEMA DIGITAL DE PAGOS: ABORDAJE PRÁCTICO A LA LUZ DE LA JURISPRUDENCIA ESPAÑOLA Y DE LA STJUE DE 1 DE AGOSTO DE 2025*

Mª Nieves Pacheco Jiménez**
Profesora Titular de Derecho Civil
Universidad de Castilla-La Mancha

Resumen: Este trabajo tiene como premisa la STJUE (Sala Cuarta) de 1 de agosto de 2025, en el Asunto C-665/2023, que estima que la persona usuaria de una tarjeta no tiene derecho a la devolución de una operación no autorizada si se demora en notificarla al proveedor de servicios de pago deliberadamente o por negligencia grave; siendo lo más llamativo de este litigio que no había transcurrido el plazo legal máximo de trece meses para informar sobre operaciones no autorizadas. Esta sentencia evidencia la existencia de brechas de seguridad en el ecosistema digital de pagos, poniendo en jaque operaciones y transacciones, lo que redunda indefectiblemente en la e-confianza de las personas usuarias. De ahí que, partiendo de una consideración inicial del ecosistema digital, donde encuentran su encaje el comercio electrónico y las nuevas modalidades de pago, se plantea la necesidad de reforzar los conceptos de confianza y seguridad, puestos en entredicho con amenazas de ingeniería social como es el *phishing*; del que se realiza un abordaje práctico a la luz de la reciente jurisprudencia española y de la meritada sentencia del TJUE.

* Este trabajo es parte del Proyecto de I+D+i "Protección de consumidores y riesgo de exclusión social: seguimiento y avances" (f. PID2021-128913NB-I00), financiado por MICIU/AEI y "FEDER Una manera de hacer Europa", dirigido por Ángel Carrasco Perera y Encarna Cordero Lobato; del Proyecto de Investigación "El reto de la sostenibilidad en la cadena de suministros y la defensa del consumidor final" (ref. SBPLY/23/180225/000242), cofinanciado por el Fondo Europeo de Desarrollo Regional, en el marco del Programa Operativo de Castilla-La Mancha 2021- 2027, dirigido por Ángel Carrasco Perera y Ana Carretero García; de las Ayudas para la realización de proyectos de investigación aplicada, en el marco del Plan Propio de investigación, cofinanciadas en un 85% por el Fondo Europeo de Desarrollo Regional (FEDER), para el Proyecto de Investigación "Modelos jurídicos eficientes de consumo sostenible" (ref. 2022-GRIN-34487), dirigido por Ángel Carrasco Perera y Ana I. Mendoza Losana.
** ORCID ID: https://orcid.org/0000-0002-9062-2342
Miembro del Centro de Investigación en Economía Digital (CIEDI) de la Universidad Autónoma de Madrid.

Palabras clave: Ecosistema digital, medios de pago, *phishing*, responsabilidad, seguridad, confianza, diligencia.

Title: Phishing as a security risk in the digital payments ecosystem: A practical approach in light os Spanish case law and the CJEU judgment on 1st August 2025

Abstract: This study takes as its point of departure the judgment delivered by the Court of Justice of the European Union (Fourth Chamber) on 1st August 2025 in Case C-665/2023. In that decision, the Court held that a payment card user is not entitled to the reimbursement of an unauthorised transaction where the user fails to notify the payment service provider without undue delay, whether such delay is deliberate or the result of gross negligence. Notably, the case is distinguished by the fact that the statutory maximum period of thirteen months for reporting unauthorised transactions had not yet expired. The judgment reveals the existence of security gaps within the digital payments ecosystem, placing operations and transactions at risk and, in turn, eroding users' confidence in electronic environments. Accordingly, and following an initial conceptual examination of the digital ecosystem —within which electronic commerce and new payment methods are framed— this work argues for the need to reinforce the concepts of trust and security, which are called into question by social engineering threats such as phishing. A practical analysis of this phenomenon is therefore undertaken in light of the recent Spanish case law and the aforementioned judgment of the CJEU.

Key words: Digital ecosystem, payment instruments, phishing, liability, security, trust, due diligence.

1. CONSIDERACIONES INICIALES

Este trabajo parte de la STJUE (Sala Cuarta) de 1 de agosto de 2025, en el Asunto C-665/2023, que estima que la persona usuaria de una tarjeta no tiene derecho a la devolución de una operación no autorizada si se demora en notificarla al proveedor de servicios de pago deliberadamente o por negligencia grave; siendo lo más

llamativo de este litigio que no había transcurrido el plazo legal máximo de trece meses para informar sobre operaciones no autorizadas.

La referida sentencia responde a una cuestión planteada por el Tribunal de Casación de Francia, a raíz del caso de un cliente con una cuenta de depósito en oro que sufrió retiradas de efectivo diarias que él negó haber realizado. Lo cierto es que aquel notificó dichas operaciones a la entidad proveedora casi dos meses después de la primera operación sospechosa, pero el TJUE precisa que la obligación de notificación "lo antes posible" y "sin demora injustificada" tiene carácter autónomo y se distingue de la obligación de notificación en el antedicho plazo de trece meses desde la fecha del adeudo de una operación de pago no autorizada. Y ello en aras de garantizar la finalidad preventiva de la Directiva de Servicios de Pago (en el caso enjuiciado de aplicación la de 2007), evitando que la simple observancia del plazo de trece meses desvirtúe la seguridad jurídica y el equilibrio entre usuarios y proveedores.

Esta sentencia plantea varias cuestiones conexas relevantes que merecen un estudio autónomo, como son los medios de pago en constante evolución y su regulación, los riesgos de seguridad derivados de la utilización de dichos medios -máxime en el ecosistema digital-, y el concreto fraude del *phishing* en operaciones no autorizadas.

2. COMERCIO ELECTRÓNICO Y MEDIOS DE PAGO

2.1. Un nuevo ecosistema necesitado de una adecuada regulación

La denominada revolución digital, entendida como el cambio radical producido por la informática y la tecnología de la comunicación creando nuevas modalidades de conocimiento, transmisión de información o negocio, ha irrumpido con fuerza en el comercio y los servicios de pago, suponiendo un cambio de paradigma con respecto a las mecánicas típicas. La digitalización de la economía ha modificado la manera en que las personas consumidoras acceden a bienes y servicios, acelerando la expansión del comercio electrónico y modificando la naturaleza de los medios de pago.

La importancia del comercio electrónico, que alude a "las transacciones comerciales electrónicas (compraventa de bienes y prestación de servicios), así como las actividades y negociaciones previas y ulteriores a las mismas"[1], se ve reflejada en varios datos estadísticos, como son los de la Comisión Nacional de los Mercados y la Competencia (en lo sucesivo CNMC), que revelan que el comercio electrónico superó en España los 25 mil millones de euros en el cuarto cuatrimestre de 2024, un 12,8%

[1] DOMÍNGUEZ LUELMO, A., "Contratación Electrónica con consumidores", en MATA Y MARTÍN, R.M. (Dir.); JAVATO MARTÍN, A. Mª (Coord.) *et al*, *Los medios electrónicos de pago: problemas jurídicos,* Comares, Granada, 2007, p. 71. En sentido similar, *vid*. ILLESCAS ORTIZ, R., *Derecho de la Contratación Electrónica*, 2ª edición, Aranzadi, Cizur Menor, 2009, pp. 33-37.
En este tipo de comercio se diferencian varias relaciones contractuales teniendo en cuenta los sujetos implicados. Así, nos encontramos con las relaciones B2B "*Business to Business*", que son las realizadas entre dos empresas o empresarios, B2C "*Bussiness to consumer*", que son las realizadas entre una empresa y un consumidor, y P2P "*Peer to peer*", que son transferencias en las que las partes actúan simultáneamente como clientes y servidores en una red de ordenadores conectados entre sí.

más que el año anterior, conformando los sectores de actividad con mayores ingresos las agencias de viajes y operadores turísticos (7,9% de la facturación total), las prendas de vestir (6,6%), los servicios auxiliares a la intervención financiera (5,7%) y el transporte aéreo (5%)[2]. Asimismo, y según un estudio de PwC[3], entre 2020 y 2025 las transacciones electrónicas crecerán un 82%, pasando de un billón a 1,8 billones de operaciones. Y entre 2025 y 2030, este crecimiento será del 61%, llegando a superar los tres billones de transacciones mundiales. Es más, señala que "la forma en la que se mueve el dinero en nuestra sociedad va a experimentar la mayor transformación en décadas; y el nuevo ecosistema de los medios de pago resultante vendrá dado por la respuesta que den los bancos, las empresas de tecnología, los reguladores, los gobiernos y los consumidores a este desafío".

Pues bien, este escenario, de naturaleza cambiante, donde el comercio electrónico se ha consolidado como una modalidad predominante de consumo, potenciada por la conectividad global, los dispositivos móviles y las plataformas digitales, está inserto en un complejo ecosistema tecnológico y legal, que supone nuevos desafíos para el Derecho, dificultado por la concurrencia tecnológica y la diversidad de agentes implicados, especialmente en lo concerniente a la óptima seguridad de las personas usuarias.

2.2. Los medios de pago en la era digital

Los medios de pago engloban numerosas transacciones (v. gr., ingreso y retirada de efectivo en cuentas de pago, ejecución de adeudos domiciliados; operaciones mediante tarjeta de pago o dispositivo similar; transferencias; envío de dinero; operaciones a través de dispositivos de telecomunicación, digitales o informáticos; etc.), en las que intervienen varios sujetos: ordenante, proveedor de servicios de pago y beneficiario. Debe reseñarse que el cambio de paradigma respecto a las mecánicas típicas de contratación repercute también en los servicios de pago, que posibilitan la perfección de esas transacciones online, con alternativas variadas a las ofrecidas por la Banca tradicional.

A pesar de que la Directiva europea 2007/64/CE, de 13 de noviembre, sobre servicios de pago en el mercado interior (en adelante DSP1)[4], y su correspondiente transposición al ordenamiento jurídico español por medio de la Ley 16/2009, de 13 de noviembre, de Servicios de Pago[5], reglamentaban de manera novedosa este entorno, la realidad práctica de las citadas operaciones fue generando la necesidad de una regulación revisada y actualizada, conforme a los incesantes avances tecnológicos. Ello se materializó en la Directiva (UE) 2015/2366, del Parlamento Europeo y del Consejo, de 25 de noviembre, sobre servicios de pago en el mercado

[2] *Vid*. https://www.cnmc.es/prensa/datos-comercio-electronico-4T-20250703 (consultado el 06/10/2025).
[3] Disponible en https://www.pwc.es/es/financiero/pwc-future-of-payments.pdf (consultado el 06/10/2025).
[4] BOE núm. 319, de 5 de diciembre de 2007.
[5] BOE núm. 275, de 14 de noviembre de 2009. Actualmente derogada.

interior (en lo sucesivo DSP2)[6], poniendo la misma de manifiesto insuficiencias de la DSP1. Así: "*ha demostrado ser en algunos casos, en su ámbito de aplicación y, en particular, en los elementos excluidos del mismo, como determinadas actividades conexas a los pagos, demasiado ambigua o general, o simplemente obsoleta, vista la evolución del mercado*"; "*ello ha generado inseguridad jurídica, posibles riesgos de seguridad en la cadena de pago y desprotección de los consumidores en determinados terrenos*". Asimismo, "*se ha constatado la dificultad que tienen los proveedores de servicios de pago para lanzar servicios de pago digitales, innovadores, seguros y de fácil uso, de modo que los consumidores y los minoristas puedan disfrutar de métodos de pago eficaces, cómodos y seguros a escala de la Unión*" (*ex* Considerando 4).

En línea con este progreso regulatorio, en los últimos años se ha producido la revisión de la DSP2; por lo que la Comisión Europea ha planteado dos propuestas para mejorar su ámbito de aplicación, publicadas en junio de 2023, a saber: una nueva Directiva (DSP3) y un nuevo Reglamento sobre los servicios de pago en la Unión Europea. Concretamente, el borrador de la nueva Directiva[7], a la luz de las lagunas y carencias que va demostrando la evolución tecnológica, actualiza y aclara las disposiciones sobre las entidades de pago e integra en estas a las entidades de dinero electrónico (abarcando emisión, mantenimiento de cuentas de pago que almacenan unidades de dinero electrónico y la transferencia de esas unidades), abriendo nuevas posibilidades de negocio para los pagos y para nuevas industrias (v. gr., acceso de los proveedores de servicios de pago no bancarios a los sistemas de pago y a las cuentas bancarias). Igualmente, refuerza la protección de las personas usuarias y la confianza en los servicios de pago incluyendo nuevas obligaciones de transparencia y de medidas para informar sobre riesgos de fraude.

En lo que concierne al ordenamiento jurídico español, la transposición de la DPS2 se materializa a través del Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en adelante RDLSP)[8]. Se articula sobre la base de un esquema muy similar al de la DSP2, lo que facilita la sistematicidad en la interpretación del conjunto normativo. Señala el RD-Ley que, "(…) *se hace preciso avanzar en la adaptación de la regulación de los nuevos cambios tecnológicos que permiten a los usuarios disponer de forma más fiable de nuevos servicios de pago y nuevos agentes que van implantándose de forma cada vez más intensa*". De ahí que los principales objetivos sean "*facilitar y mejorar la seguridad en el uso de sistemas de pago a través de Internet, reforzar el nivel de protección al usuario contra fraudes y abusos potenciales* (…), *así como promover la innovación en los servicios de pago a través del móvil y de Internet*"; teniendo

[6] BOE núm. 337, de 23 de diciembre de 2015.

[7] *Vid*. https://eur-lex.europa.eu/resource.html?uri=cellar:e09b163c-1687-11ee-806b-01aa75ed71a1.0007.02/DOC_1&format=PDF

[8] BOE núm. 284, de 24 de noviembre de 2018. Derogando expresamente en su disposición derogatoria única la Ley 16/2009, de 13 de noviembre, de Servicios de Pago.

en cuenta la necesidad de proteger a las personas consumidoras y usuarias, sin que se ponga freno a los adelantos tecnológicos.

3. LA IMPRESCINDIBLE SEGURIDAD Y SUS RIESGOS

3.1. El ecosistema digital

Las operaciones de pago efectuadas en ecosistema digital pueden exponer a las personas usuarias a determinados riesgos de seguridad, lo que, evidentemente, redunda en la confianza -entendida como expectativa de fiabilidad y protección jurídica- de estas a la hora de adquirir un determinado producto o servicio por vía del comercio electrónico. Ambos conceptos, confianza y seguridad, conectan los planos económico, tecnológico y jurídico, y resultan determinantes para la estabilidad del mercado digital. De hecho, la Agenda España Digital 2026[9] sitúa la ciberseguridad y la confianza en el uso de tecnologías digitales como ejes del crecimiento económico y de la cohesión social.

En el escenario de los medios de pago, la DSP2, en su Considerando 95, observa que "*todos los servicios de pago ofrecidos electrónicamente deben prestarse con la adecuada protección, gracias a la adopción de tecnologías que permitan garantizar una autenticación segura del usuario y minimizar el riesgo de fraude* (…)" y que un "*crecimiento sólido de los pagos por móviles y por internet debe ir acompañado de una mejora generalizada de las medidas de seguridad*". Y ello porque los riesgos de seguridad en este ámbito han ido aumentando en los últimos años, atendiendo a la mayor complejidad técnica, al continuo incremento del volumen de dichos pagos a nivel mundial y a los nuevos modelos de servicios de pago, como apunta el Considerando 7 DSP2. Así las cosas, resulta primordial para el adecuado funcionamiento del mercado de los referidos servicios disponer de medios de pago fiables y seguros. Ello redundará indefectiblemente en una adecuada protección frente a los riesgos a los que se exponen las personas usuarias[10]. De ahí que "*todos los servicios de pago ofrecidos electrónicamente deben prestarse con la adecuada protección, gracias a la adopción de tecnologías que permitan garantizar una autenticación segura del usuario y minimizar el riesgo de fraude* (…)"; y que "*un crecimiento sólido de los pagos por móviles y por internet debe ir acompañado de una mejora generalizada de las medidas de seguridad*", como estipula el Considerando 95 DSP2.

El riesgo de seguridad en el ecosistema digital es multidimensional. Desde el punto de vista técnico, incluye amenazas como el *phishing*, el *malware* financiero o la suplantación de identidad. Por eso cobra especial importancia la preservación de la seguridad en las credenciales personalizadas con el objeto de garantizar la protección de los fondos de la persona usuaria de servicios de pago y reducir los riesgos de

[9] *Vid*. https://espanadigital.gob.es/espana-digital (consultado el 09/10/2025).

[10] PACHECO JIMÉNEZ, Mª N., "Nuevas alternativas de pago online: proveedores de servicios de pago externo en un mercado más tecnológico y seguro", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm, 49, enero-abril 2019, p. 40.

fraude y acceso no autorizado a las distintas cuentas de pago (*ex* Considerando 69 DSP2). Este especial cuidado enlaza con la protección de datos personales, fundamental para sostener la confianza digital.

3.2. Reglamentación de medidas de seguridad

3.2.1. Normas técnicas de regulación

En este contexto descrito, y para mejorar la protección de usuarios y usuarias mediante el establecimiento de medidas de seguridad en los pagos electrónicos, la DSP2 facultó a la Comisión para la adopción de normas técnicas de regulación (RTS[11]), teniendo como base al documento de Directrices[12] (aplicadas a la prestación de servicios de pago ofrecidos a través de Internet por los proveedores de servicios de pago) presentado en diciembre de 2014 por la Autoridad Bancaria Europea (ABE)[13]. Posteriormente, en 2017, la Comisión introdujo algunas modificaciones sustantivas al borrador de RTS remitido por la EBA con la finalidad de reflejar mejor el mandado de la DSP2 y aportar mayor claridad y seguridad jurídica a todos los agentes interesados. Esas normas técnicas establecen que la autenticación reforzada[14] del/de la cliente será la base obligatoria para acceder a las cuentas de

[11] RTS, por sus siglas en inglés: *Regulatory Technical Standards.*

[12] *Vid.* https://www.eba.europa.eu/sites/default/files/documents/10180/1004450/44d07cf8-1721-4407-94a6-3a8c256149fa/EBA-GL-2014-12_ES_rev1%20GL%20on%20Internet%20Payments.pdf
Artículo 6: "*Las presentes Directrices constituyen unas expectativas mínimas, sin perjuicio de la responsabilidad de los PSP de tener que efectuar un seguimiento y evaluación de los riesgos asociados a sus operaciones de pago, desarrollar sus propias políticas de seguridad específicas y aplicar medidas de seguridad, contingencia, gestión de incidentes y continuidad de negocio adecuadas y proporcionales a los riesgos inherentes a los servicios de pago prestados".*
Artículo 7: "El propósito de las presentes Directrices es definir los requisitos mínimos comunes para los servicios de pago por internet enumerados a continuación, independientemente del dispositivo de acceso utilizado:
- [tarjetas] la realización de operaciones de pago con tarjeta, incluidas las tarjetas virtuales, a través de internet, así como el registro de los datos relativos a la tarjeta de pago para su empleo en «soluciones tipo monedero»;
- [transferencias] la realización de transferencias a través de internet;
- [mandato electrónico] la emisión y modificación de mandatos electrónicos relativos a adeudos domiciliados;
- [dinero electrónico] transferencias de saldos entre dos cuentas de dinero electrónico a través de internet".
Esas Directrices recogían políticas de seguridad periódicas, evaluación de riesgos, control y notificación de incidentes, control y mitigación de riesgos, procesos de trazabilidad, autenticación reforzada de clientes, seguimiento de las operaciones, protección de datos de pago sensibles, asistencia y orientación de clientes.

[13] La ABE o EBA (por sus siglas en inglés *European Banking Authority*) "es una autoridad independiente de la UE que trabaja para garantizar un nivel efectivo y coherente de regulación y supervisión prudencial en todo el sector bancario europeo. Sus objetivos generales son mantener la estabilidad financiera en la Unión Europea (UE) y velar por la integridad, la eficiencia y el correcto funcionamiento del sector bancario". (*Vid*. https://www.eba.europa.eu/languages/home_es -consultado el 23/10/2025-)

[14] "Procedimiento basado en el uso de dos o más de los siguientes elementos, clasificados como conocimiento, posesión e inherencia: i) algo que solo conoce el usuario, por ejemplo, una contraseña, código o número de identificación personal fijos; ii) algo que solo posee el usuario, por ejemplo, token, tarjeta inteligente, teléfono móvil; iii) algo que caracteriza al propio usuario, por ejemplo, una

pago y para ejecutar pagos en línea. Además, para los pagos en línea, la seguridad se reforzará mediante la vinculación de la transacción a un código de un solo uso ("*one-time password*") asociado tanto al importe de la operación como al beneficiario del pago, lo que dificulta la interceptación fraudulenta de datos[15].

3.2.2. Reglamento Delegado (UE) 2018/389

Finalmente, todos estos avances terminaron plasmándose en el Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017[16]. De las medidas de seguridad contenidas en él se derivan dos objetivos clave de la DSP2, esto es: otorgar más protección a la persona consumidora mejorando el nivel de seguridad de los pagos y transacciones electrónicas; y aumentar la competencia e igualdad de condiciones en un mercado en constante evolución[17]. Así, el Reglamento fija los requisitos detallados, a través de normas técnicas de regulación, que los proveedores de servicios de pago han de cumplir cuando accedan a la cuenta de pago de una persona usuaria, cuando inicien una operación o de pago cuando realicen acciones a través de canales remotos susceptibles de fraude o abusos. Entre esos requisitos se refuerza el de la autenticación reforzada[18] (ya prevista por la EBA en su momento), cuando un/a usuario/a accede a su cuenta de pago en línea, inicia una operación de pago en línea o actúa a través de un canal remoto con riesgo de fraude.

Asimismo, constituye estándares de comunicación abiertos comunes y seguros[19] entre los proveedores de servicios de pago y los terceros proveedores para facilitar

---

característica biométrica, como su huella dactilar. Además, los elementos seleccionados deben ser independientes entre sí; es decir, la violación de uno no debe comprometer la seguridad de los otros. Al menos uno de los elementos no debe ser reutilizable ni reproducible (salvo para la inherencia) y su sustracción, de manera subrepticia, a través de internet no debe resultar posible. El procedimiento de autenticación fuerte se debe diseñar de tal forma que proteja la confidencialidad de los datos de autenticación" (*ex* art. 12 Directrices EBA).

[15] *Vid*. https://ec.europa.eu/commission/presscorner/detail/en/memo_17_4961 (consultado el 23/10/2025).

[16] DOUE de 13/03/2018. *Vid*. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R0389&from=ES

[17] *Vid.* http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm

[18] Arts. 4-9 del Reglamento: Se indican las medidas de seguridad para la aplicación de la autenticación reforzada de clientes, a saber: código de autenticación, vinculación dinámica, requisitos de los elementos categorizados como conocimiento, requisitos de los elementos categorizados como posesión, requisitos aplicables a los dispositivos y programas informáticos vinculados a los elementos categorizados como inherencia, e independencia de los elementos. Por su parte, los arts. 10 a 21 regulan las exenciones de la autenticación reforzada de clientes, concretamente: información de cuentas de pago, pagos sin contacto en el punto de venta, terminales no atendidas para tarifas de transporte o pagos de aparcamiento, beneficiarios de confianza, operaciones frecuentes, transferencias de créditos entre cuentas mantenidas por la misma persona física o jurídica, operaciones de escasa cuantía, procesos y protocolos de pago corporativo seguro, operación remota de pago con nivel bajo de riesgo. Realiza, además, una referencia al cálculo de los índices de fraude de las operaciones. Finaliza con el cese de exenciones basadas en el análisis del riesgo de la operación y con una mención a la supervisión realizada por los propios proveedores de servicios de pago.

[19] En los arts. 28-36 del Reglamento se instituyen las medidas y requisitos para lograr unos estándares de comunicación abiertos, comunes y seguros, englobando para ello requerimientos de identificación y trazabilidad, obligaciones generales para las interfaces de acceso, opciones de las interfaces de acceso,

el acceso a cuentas de pago con consentimiento del/de la usuario/a. En tanto en cuanto la DSP2 pretende impulsar la competencia y la innovación en el sector financiero a través de la actividad de terceras partes (*Third Party Providers*)[20], la regulación al respecto dada por el Reglamento resulta fundamental. En este sentido, la calidad de los servicios de iniciación de pagos[21] y de información sobre cuentas[22] dependerá del óptimo funcionamiento de las interfaces empleadas, promoviendo esa comunicación abierta común y segura (*ex* Considerando 22).

3.2.3. Reglamento (UE) 2016/679 (RGPD)

En estrecha conexión con estas medidas, en tanto en cuanto se trata de preservar la seguridad de cierta información expuesta en los pagos digitales evitando posibles fraudes, se encuentra el 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 (RGPD)[23]. Así, actúa como norma transversal de protección y seguridad jurídica**,** garantizando que todo tratamiento de datos realizado por bancos, proveedores de servicios de pago y *fintechs* respete los principios de licitud, lealtad, minimización de la exposición, seguridad y transparencia. Y ello porque la pérdida o uso indebido de tales datos no solo genera perjuicios patrimoniales, sino también una erosión profunda de la confianza pública en el sistema.

Básicamente, los artículos de aplicación en el escenario de los pagos digitales serían: Arts. 5 y 6, en lo atinente al tratamiento de datos en sintonía con los principios anteriormente señalados, con especial mención al consentimiento de la persona interesada. Arts. 12-22, referentes a los derechos digitales fundamentales de las personas usuarias de servicios de pago (acceso, rectificación, supresión, limitación, oposición). Art. 25, sobre medidas técnicas y organizativas adoptadas por los responsables del tratamiento para garantizar que los datos tratados son los estrictamente necesarios para cada uno de los fines específicos. Art. 32, relativo a la seguridad del tratamiento, indicando la seudonimización y el cifrado de datos personales; la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento; la rapidez en la disponibilidad y acceso a los datos en caso de incidente físico o técnico; un proceso de verificación, evaluación y valoración periódico de la eficacia de las medidas.

---

obligaciones relativas a las interfaces específicas, medidas de contingencia para las interfaces específicas, certificados, seguridad de las sesiones de comunicación y el intercambio de datos.

[20] Para desarrollo pormenorizado, *vid*. PACHECO JIMÉNEZ, Mª N., *op. cit*., pp. 32 y ss.

[21] La DSP2 los define como aquellos que posibilitan *"iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago"* (*ex* art. 4.15).

[22] La DSP2 los define como aquellos servicios *"en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago"* (*ex* art. 4.16).

[23] DOUE de 04/05/2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016R0679

De lo expuesto se colige la sinergia entre el RGPD y la DSP2, de manera que se reduce la asimetría de información entre proveedores de servicios de pago y las personas usuarias, disminuye el riesgo de fraude o uso indebido de datos y se favorece la competencia basada en la confianza.

3.2.4. Digital Service Act

El Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales (*Digital Service Act* -DSA-)[24], forma parte del paquete legislativo sobre servicios y mercados digitales, junto con la *Digital Markets Act* (DMA). Mientras que esta regula la competencia y el poder de mercado de las grandes plataformas, la DSA se centra en la seguridad, la transparencia y la responsabilidad en el entorno digital, actualizando el marco jurídico sobre comercio electrónico. Ha de reseñarse que esta no es una norma específica sobre medios de pago, aunque sí tiene implicaciones importantes en materia de seguridad digital y confianza, que afectan de manera indirecta a los servicios de pago electrónicos, así como a las plataformas que los ofrecen o intermedian. Para ello se fomenta la confianza y transparencia en las plataformas a través de la trazabilidad de los comerciantes que operan en ellas; se procura la información clara sobre las condiciones de los servicios y mecanismos de pago; y se aplican sistemas de verificación de identidad digital de los oferentes. En definitiva, puede decirse que la DSA actúa a modo de complemento ya que crea un marco de confianza digital más amplio para las transacciones electrónicas basándose en los principios de trazabilidad, transparencia y mitigación del riesgo.

4. *PHISHING* COMO RIESGO DE SEGURIDAD

4.1. Conceptualización

El recorrido hecho hasta ahora permite evidenciar la relevancia de la seguridad en el entorno de los medios de pago electrónicos, omnipresentes en el ecosistema digital. Pero esa seguridad se puede ver profundamente comprometida cuando hablamos de *phishing*[25], como tipo particular de ingeniería social.

Una de las modalidades más peligrosas del *phishing* es el *pharming*. Esta técnica consiste en modificar el sistema de resolución de nombres de dominio (DNS "Domain Name System" o Sistema de Nombres de Dominio), que se encarga de convertir una dirección tecleada en el navegador a una dirección IP numérica, para conducir a la víctima a una página web falsa, en apariencia idéntica a la web de confianza, pero

[24] DOUE de 27/10/22. Disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32022R2065

[25] RIBÓN define en sentido amplio el *phishing* como la "pesca de datos", que tiene como objetivo provocar un daño patrimonial a un tercero, sin su consentimiento, mediante la utilización fraudulenta de sus claves (RIBÓN SEISDEDOS, E., *Fraudes bancarios y defensa del afectado. Nuevas tendencias defraudatorias. Especial referencia al phishing bancario*, Editorial Tirant lo Blanch, Valencia, 2024, p. 31).
Desde el punto de vista penal, se trata de un delito de estafa cibernética con manipulación informática (*ex* art. 248.2 del Código Penal).

que en realidad ha sido creada por el atacante para obtener los datos privados de la persona usuaria[26].

Lo más habitual es la suplantación de la identidad de una entidad bancaria por parte del delincuente con la finalidad de adquirir información confidencial sobre contraseñas de cuenta bancarias, tarjetas de crédito, o cualquier otra información relevante que permita entrar en las cuentas de usuarios y usuarias en Internet. De hecho, la Oficina de Seguridad del Internauta (OSI)[27] viene detectando campañas de *phishing* contra varias entidades bancarias con el objetivo de engañar a sus clientes para que estos hagan clic en un enlace que redirige a una web maliciosa que suplanta la identidad de la entidad, capturando así sus claves y datos. Sin embargo, el *phishing* no se agota en los Bancos, ya que también lo sufren pasarelas de pago online (v. gr., PayPal, Mastercard, Visa), páginas de compraventa y subastas (v. gr., Amazon, eBay); y servicios de almacenamiento en la nube (v. gr., Google Drive, Dropbox).

Más allá del *pharming*, encontramos más modalidades. A saber: A) *Scamming* o práctica mediante la cual se capta a personas, generalmente por medio del correo electrónico, induciendo a entregar dinero, datos personales u otros bienes de valor presentando una información falsa, como puede ser anuncios en webs de trabajo, chats[28] o incluso *romance scams* (la víctima establece una relación de confianza emocional con el estafador, que inventa una emergencia para pedir dinero). B) *Carding* o fraude basado en el robo y falsificación de tarjetas bancarias a través de un *software* o, incluso, robando los datos en momentos de despiste del propietario legítimo, para utilizarlas de forma ilegítima, realizando compras de importes muy reducidos[29]. C) *Vishing* o estafa utilizada por los ciberdelincuentes para engañar a las personas usuarias a través de llamadas de teléfono fraudulentas, suplantando la identidad de empresas u organizaciones, y obtener así información personal, guiarles para que descarguen e instalen programas maliciosos, así como intentar que realicen algún pago bajo algún pretexto[30]. D) *Smishing*, como fraude similar, pero, en vez de contactar a través de una llamada telefónica, los ciberdelincuentes contactan a través de un SMS en el que generalmente se invita a llamar a un número de teléfono o a pulsar en un enlace de una web falsa y fraudulenta con el objetivo de obtener información personal (usuario y contraseña, correos, número de teléfono) o bancaria (claves), para robar dinero[31]. E) SIM *swapping,* que consiste en duplicar la tarjeta

[26] VALLS PRIETO, J., *Derecho de las nuevas tecnologías, el mercado digital en la Unión Europea*, Editorial Reus, Madrid, 2019, p. 528. Asimismo, *vid*. http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/

[27] *Vid*. https://www.osi.es/es (consultado el 27/10/2025)

[28] RIBÓN SEISDEDOS, E., *op*, *cit.*, p. 40.
Vid. también https://www.zurich.ch/en/services/knowledge/cybersecurity/scam-scammer-scamming (consultado el 27/10/2025).

[29] *Vid.* https://www.ciberseguridad.eus/ciberglosario/carding# (consultado el 27/10/2025).

[30] *Vid.* https://www.incibe.es/ciudadania/tematicas/ingenieria-social-fraudes-online/vishing (consultado el 27/10/2025)

[31] *Vid.* https://www.incibe.es/aprendeciberseguridad/smishing (consultado el 27/10/2025)

SIM del teléfono móvil, obteniendo todo tipo de información sobre su titular para poder suplantarle y despojarle de su cuenta bancaria[32].

Por último, y no menos importante, es la repercusión de la Inteligencia Artificial (IA) en este concreto ámbito. El objeto de la IA es la simulación de la inteligencia humana a través de algoritmos[33], a partir de una información incorporada por su programador, persona usuaria o adquirida por la máquina de fuentes digitales o a través de estímulos del mundo real, percibidos por la máquina mediante sensores[34]. En la medida en que la IA procesa ingentes cantidades de datos, extrae patrones y conocimientos útiles, de manera que los sistemas de aprendizaje automático pueden realizar análisis complejos, identificar tendencias ocultas y proporcionar información con gran precisión, puede ser utilizada para perpetrar ataques de *phishing* escribiendo *mails* fraudulentos mucho más creíbles[35]. Se trata del denominado *spear phishing* (ciberataque muy personalizado) con el que los atacantes, aprovechando los algoritmos de aprendizaje automático, pueden examinar grandes cantidades de datos para elaborar mensajes personalizados. Además, con las técnicas de generación de lenguaje natural, se pueden generar contenidos más persuasivos imitando la comunicación humana. Por último, se pueden imitar patrones de comunicación legítimos, lo que dificultaría que las medidas de seguridad tradicionales detectasen el contenido malicioso[36].

---

[32] *Vid.* https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-sim-swapping.html (consultado el 17/10/2025).
Un caso actual al respecto es el resuelto por la Sala de lo Civil del Tribunal Supremo de 9 de abril de 2025 (JUR 2025, 84706), que rechaza el recurso de Ibercaja contra un cliente que había sido víctima de un ataque de *SIM swapping*, realizándose quince transferencias desde sus cuentas bancarias, diez mediante Bizum y cinco a través de Ibercaja Directo. El Tribunal Supremo falla que Ibercaja Banco S.A. debe reintegrar a un cliente 56.474,63 euros sustraídos, al considerar que la entidad incumplió su deber de adoptar medidas de seguridad adecuadas para detectar operaciones claramente anómalas. Concretamente indica: "que las buenas prácticas bancarias exigen la activación de sistemas automáticos capaces de identificar conductas sospechosas y bloquear o verificar operaciones de alto riesgo".

[33] En palabras más técnicas: un algoritmo es una estructura de control finita, abstracta y compuesta para cumplir un propósito, resolver un problema, hacer predicciones o guiar la ejecución de una tarea, siendo capaz de aprender con experiencia de entrenamiento. Consta de tres partes: una entrada o *input* (datos sobre los que se aplican las instrucciones); procesamiento (con lo recibido en el *input,* el algoritmo elabora una serie de cálculos lógicos para resolver el problema); salida (*output*) o resultado obtenido. *Vid*. PALMA ORTIGOSA, A., "El ciclo de vida de los sistemas de Inteligencia Artificial. Aproximación técnica de las fases presentes durante el diseño y despliegue de los sistemas algorítmicos", en COTINO HUESO, L. (Dir.) *et al*, *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Thomson Reuters Aranzadi, Cizur Menor, 2022, p. 32.

[34] GUTIÉRREZ GARCÍA, E., *Inteligencia artificial y Derechos Fundamentales: Hacia una convivencia en la era digital,* Colex, A Coruña, 2024, p. 23.

[35] *Vid*. https://www.iproup.com/innovacion/40707-inteligencia-artificial-como-es-utilizada-para-ataques-phishing y https://computerhoy.com/tecnologia/estafadores-inteligencia-artificial-emails-phishing-estafas-1183326 (consultado el 28/10/2025)

[36] *Vid*. https://www.metacompliance.com/es/blog/phishing-and-ransomware/how-ai-enables-sophisticated-phishing-attacks (consultado el 28/10/2025)

4.2. Operación no autorizada

Aunque el *phishing* no es en sí mismo un pago o transferencia no autorizada**,** sino la operación de obtención de información fraudulenta, puede ocurrir que, a consecuencia de ese *phishing*, se utilicen datos robados para ejecutar un pago sin autorización; pero también que la víctima proporcione voluntariamente sus datos, aunque bajo engaño. En definitiva, el *phishing* puede ocasionar una operación no autorizada, pero no todas las operaciones no autorizadas proceden de *phishing* (también pueden derivar de robo de tarjetas, *malware*, acceso físico a cuentas, etc.).

Se abordará a continuación el supuesto de transacción fraudulenta *online* sin consentimiento por parte de la persona titular de la cuenta. De ahí que deban clarificarse brevemente ciertos términos, esto es, qué es una orden de pago y cuándo se entiende no autorizada. Para ello, se acudirá a la regulación dispensada por el RD-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera[37] (en lo sucesivo RDLSP).

Una orden de pago aparece definida en el artículo 3, apartado 28, RDLSP como "*toda instrucción cursada por un ordenante o beneficiario[38] a su proveedor de servicios de pago[39], por la que se solicita la ejecución de una operación de pago*"; siendo operación de pago "*una acción iniciada por el ordenante[40] o por cuenta de éste, o por el beneficiario, consistente en ingresar, transferir o retirar fondos, con independencia de cualesquiera obligaciones subyacentes entre el ordenante y beneficiario*" (*ex* art. 3, apartado 26).

Por su parte, el art. 36.1 RDLSP distingue entre operaciones autorizadas y no autorizadas como prosigue: "*Las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado consentimiento para su ejecución. A falta de tal consentimiento, la operación de pago se considerará no autorizada. El consentimiento para la ejecución de una operación de pago podrá darse también por conducto del beneficiario o del proveedor de servicios de iniciación de pagos*". Continúa estableciendo que "*el ordenante y su proveedor de servicios de pago acordarán la forma en que se dará el consentimiento, así como el procedimiento de notificación del mismo*". Evidentemente, el consentimiento es el elemento nuclear de la operación de pago, lo que distingue entre si es autorizada o no. Ese consentimiento "*podrá otorgarse con anterioridad a la ejecución de la operación o, si así se hubiese convenido, con posterioridad a la misma, conforme al procedimiento y límites*

[37] BOE núm. 284, de 24 de noviembre de 2018.

[38] "*La persona física o jurídica que sea el destinatario previsto de los fondos que hayan sido objeto de una operación de pago*" (*ex* art. 3, apartado 6 RDLSP).

[39] "*Las entidades y organismos contemplados en los apartados 1 y 2 del artículo 5, y las personas físicas o jurídicas que se acojan a las exenciones previstas en los artículos 14 y 15*" (*ex* art. 3, apartado 31 RDLSP).

[40] "*La persona física o jurídica titular de una cuenta de pago que autoriza una orden de pago a partir de dicha cuenta o, en el caso de que no exista una cuenta de pago, la persona física o jurídica que dicta una orden de pago*" (*ex* art. 3, apartado 29 RDLSP).

acordados entre el ordenante y su proveedor de servicios de pago". También es importante destacar el punto tres del citado artículo, y es que "*el ordenante podrá retirar el consentimiento en cualquier momento, pero no después de la irrevocabilidad a que se refiere el artículo 52* RDLSP[41]*; cuando el consentimiento se hubiese dado para una serie de operaciones de pago, su retirada implicará que toda futura operación de pago que estuviese cubierta por dicho consentimiento se considerará no autorizada*".

Atendiendo a estos aspectos, el *phishing* descrito en epígrafes anteriores provocaría una operación no autorizada en la medida en que no hay aprobación ni consentimiento por parte del/de la cliente, que no ejecuta la orden de pago; siendo el ciberdelincuente quien la ejecuta valiéndose del engaño.

4.3. Responsabilidad

Lo expuesto hasta ahora nos lleva al escenario donde se ha ejecutado una operación de pago derivada de *phishing*. La cuestión más problemática estriba en dirimir si esa responsabilidad debería recaer en el/la cliente, por facilitar datos personales o/y financieros a los ciberdelincuentes; o si, por el contrario, la responsabilidad recae sobre el proveedor de servicios de pago, por no revisar la operación fraudulenta.

Pues bien, se parte de la base de que la responsabilidad de ambas partes se impone en el contrato suscrito entre estas, denominado contrato marco, esto es, "*un contrato de servicio de pago que rige la ejecución futura de operaciones de pago individuales y sucesivas, y que puede estipular la obligación de abrir una cuenta de pago y las correspondientes condiciones para ello*" (*ex* art. 3, apartado 9 RDLSP). Generalmente, el proveedor de servicios de pago tendrá un apartado exclusivo concerniente a seguridad, indicando la utilización de métodos de seguridad, así como la obligación por parte del/de la cliente de proteger sus claves, debiendo avisar

[41] Art. 52: Irrevocabilidad de una orden de pago:
"1. *El usuario de servicios de pago no podrá revocar una orden de pago después de ser recibida por el proveedor de servicios de pago del ordenante, salvo que se especifique otra cosa en el presente artículo.*
2. Cuando la operación de pago sea iniciada por un proveedor de servicios de iniciación de pagos, o por el beneficiario o a través de él, el ordenante no revocará la orden de pago una vez haya dado al proveedor de servicios de iniciación de pagos su consentimiento para iniciar la operación de pago o una vez haya dado su consentimiento para que se ejecute la operación de pago al beneficiario.
3. No obstante, en los casos de adeudo domiciliado y sin perjuicio de los derechos de devolución fijados en este real decreto-ley, el ordenante podrá revocar una orden de pago a más tardar al final del día hábil anterior al día convenido para el adeudo de los fondos en la cuenta del ordenante.
4. En el caso en que el momento de recepción se corresponda con una fecha previamente acordada entre el usuario de servicios de pago que inicia la orden y su proveedor de servicios de pago, aquél podrá revocar la orden de pago a más tardar al final del día hábil anterior al día convenido.
5. Una vez transcurridos los plazos establecidos en los apartados 1 a 4 anteriores, la orden de pago podrá revocarse únicamente si así se ha convenido entre el usuario de servicios de pago y los correspondientes proveedores de tales servicios de pago. En los casos indicados en los apartados 2 y 3 anteriores será necesario, además, el consentimiento del beneficiario. De haberse convenido así en el contrato marco, el proveedor de servicios de pago correspondiente podrá cobrar gastos por la revocación".

rápidamente al antedicho proveedor en caso de sospechar que un tercero tiene acceso a aquellas.

El contenido de este contrato marco, en lo que atañe a responsabilidad, obedece a la regulación del RDLSP, concretamente a su artículo 45, que preceptúa: "(…) *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*". Para que la acción de reintegración del dinero efectivamente sustraído fructifique deben concurrir los siguientes requisitos: a) la falta de autorización de la operación de pago por parte de la víctima; b) la presencia de un daño, materializado en la cantidad sustraída; c) la relación de causalidad entre la conducta y el daño generado. Así las cosas, el proveedor de servicios de pago incurrirá en una responsabilidad cuasi objetiva, siempre que no quiebre la relación de causalidad por existencia de diligencia cualificada (consistente en la obligación del proveedor de proporcionar a su cliente mecanismos de seguridad acordes para garantizar la seguridad y privacidad de las credenciales) o por culpa de la víctima por negligencia grave o fraude[42].

Todo esto sin perjuicio de lo establecido en el artículo 43, que obliga al ordenante a comunicar al proveedor de servicios de pago inmediatamente que la operación que se ha llevado a cabo no ha sido autorizada por este, esto es: "*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* (…), *y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo*".

El artículo 45 realiza una salvedad a la responsabilidad derivada de operaciones no autorizadas, que no es otra que: "*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*". Esta exención de responsabilidad conecta con el artículo 46 RDLSP, relativo a la responsabilidad del ordenante en caso de operaciones de pago no autorizadas. En este sentido "*el ordenante podrá quedar obligado a soportar, hasta un máximo de 50 euros, las pérdidas derivadas de operaciones de pago no autorizadas resultantes a la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero, salvo que: a) al ordenante no le resultara posible detectar la pérdida, la sustracción o la apropiación indebida de un instrumento de pago antes de un pago, salvo cuando el propio ordenante haya actuado fraudulentamente, o b) 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*". Asimismo "*el ordenante soportará*

[42] CALVO SAN JOSÉ, Mª J., *op. cit*., p. 1800.

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, una o varias de las obligaciones que establece el artículo 41"[43]. Particularmente, este artículo se refiere a la obligación de utilizar el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del mismo, debiendo proteger sus credenciales de seguridad personalizadas; y a la obligación de notificación sin demora al proveedor de servicios de pago, en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada. Pues bien, es esta concreta situación de demora en la notificación la que supone la base del litigio que resuelve la STJUE (Sala Cuarta) de 1 de agosto de 2025, en el Asunto C-665/2023, que abordaré líneas más abajo, que estima que el usuario de una tarjeta no tiene derecho a la devolución de una operación no autorizada si se demora en notificarla al proveedor de servicios de pago deliberadamente o por negligencia grave.

Por su parte, el art. 42 RDLSP contempla las obligaciones del proveedor de servicios en relación con los instrumentos de pago, y son: a) se cerciorará de que las credenciales de seguridad personalizadas del instrumento de pago únicamente sean accesibles para la persona usuaria facultada para utilizar dicho instrumento; b) se abstendrá de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso de que deba sustituirse un instrumento de pago ya entregado al/a la usuario/a de servicios de pago; c) garantizará que en todo momento estén disponibles medios adecuados y gratuitos que permitan a la persona usuaria de servicios de pago efectuar una notificación (para la situación de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, *ex* art. 41) o solicitar un desbloqueo; d) ofrecerá al/a la usuario/a de servicios de pago la posibilidad de efectuar una notificación gratuitamente y sin cobrar (para la situación anteriormente señalada); e) impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación (para los casos de extravío, sustracción o apropiación indebida del instrumento o de su utilización no autorizada).

Teniendo en cuenta la regulación descrita, se aplica una responsabilidad cuasi objetiva de los proveedores de servicios de pago, pudiendo exonerarse siempre que la persona operante actúe de forma fraudulenta o se produzca por su culpa o dolo[44]. No obstante, en la práctica, la distribución de la responsabilidad es más compleja de determinar, en la medida en que puede plantearse la duda de si el/la cliente ha actuado con la debida diligencia[45] a la hora de salvaguardar sus contraseñas, habida

[43] El proveedor de servicios de pago quedaría exonerado de responsabilidad al romperse la relación de causalidad por culpa de la víctima (*vid*. CALVO SAN JOSÉ, Mª J., "La responsabilidad civil de los bancos en los delitos de estafa por *phishing*", *Actualidad jurídica iberoamericana*, núm. 18, 2023, p. 1797).

[44] CALVO SAN JOSÉ, Mª J., *op. cit*., p. 1796.

[45] En la práctica se ha demostrado que cuando la persona usuaria denuncia haber sido víctima de *phishing*, la estrategia habitual de las entidades bancarias pasa por imputar negligencia a la propia víctima, culpándola de haberse dejado engañar y haber facilitado a los ciberdelincuentes contraseñas y claves que han propiciado las operaciones no autorizadas. Autoras como CALVO SAN JOSÉ consideran que esta es una vía de disuasión a la hora de exigir responsabilidad a la entidad bancaria; a la vez que recuerda que

cuenta de las exponenciales habilidades de los ciberdelincuentes, que pueden, por ejemplo, inducir a error con páginas clonadas o valerse de la Inteligencia Artificial para crear un *phishing* personalizado. Y, por otro lado, también resulta complicado dirimir si el proveedor de servicios de pago ha empleado realmente todos los métodos de seguridad posibles para que el fraude no se ejecute.

4.4. Análisis de jurisprudencia española

Llegados aquí, y para evidenciar la realidad en nuestros tribunales de litigios sobre *phishing*, he considerado oportuno seleccionar algunas sentencias de los últimos cuatro años con pronunciamientos relativos a la responsabilidad por *phishing* bancario que pretenden dar respuesta a las cuestiones previamente planteadas. Así:

- SAP Madrid 28 febrero 2022[46]: Versa sobre un litigio contra el Banco Bilbao Vizcaya Argentaria S.A. al permitir una transferencia de la cuenta de la actora a un Banco de Tailandia sin su preceptiva autorización. Si bien lo cierto es que lo solicitó una administrativa de la actora siguiendo un procedimiento inusual y BBVA no llevó a cabo ninguna medida de diligencia para detectar un posible fraude. Se trata de una modalidad de estafa conocida como "fraude del CEO" (mezcla de técnicas de ingeniería social y *phishing*), consistente en que un empleado de la empresa a quien se pide hacer transferencias o el acceso a datos de cuentas, recibe un correo (puede ser también por WhatsApp o cualquier otra vía de comunicación) supuestamente (se utilizan direcciones de correo con un nombre similar al real donde se enlaza a un *malware*) de su jefe (CEO, presidente/a o director/a) pidiéndole que le ayude a ejecutar una operación financiera confidencial y urgente. Así las cosas, se ordenaron dos transferencias en las fechas de 18.1.2018 y 22.1. 2018 y por los importes de 303.234,44 € y 379.043,05 €, siendo que la primera transferencia, a diferencia de la segunda, sí que fue efectivamente realizada, teniendo como cuenta de destino la del Banco DBS BANK HONG KONG LIMITED, por persona que no estaba autorizada para dar orden alguna en nombre de la actora. Pero la cuestión es que la entidad bancaria demandada no detectó que se estaba cometiendo un fraude ya que la persona que ordenada no era apoderada ni estaba autorizada y, además, nunca hasta la fecha la actora había realizado ningún pago a China. La SAP estima mala praxis en la actuación de BBVA al ejecutar una orden de transferencia procedente de una persona que no figuraba en la lista de apoderados de la actora recogida por la entidad bancaria: "Resulta evidente que en el caso hubo un incumplimiento contractual del Banco al ejecutar una orden de pago sin comprobar su legitimidad, es decir, que provenía efectivamente del titular (o autorizado) de la cuenta, al no disponer de un sistema adecuado de seguridad que previniera tal tipo de órdenes fraudulentas ni adoptar medidas concretas y específicas en el caso cuando toma conocimiento de una situación operativa anormal que debió, cuando menos de forma puntual y

la entidad bancaria tiene la obligación de promover un sistema telemático seguro acorde con los riesgos de ciberseguridad existentes. (*Vid*. CALVO SAN JOSÉ, Mª J., *op. cit*., p. 1802).

[46] JUR 2022, 114095.

excepcional, a verificar cualquiera orden que se diera en relación a las cuentas de la demandante".

- SAP Alicante 23 junio 2023[47]: Resuelve la demanda contra Banco Santander S.A. por falta de actuación diligente al recibir las clientas demandantes un SMS falso indicando que su cuenta bancaria había resultado bloqueada y que debían pinchar en el enlace facilitado para desbloquearla; al hacerlo, se les condujo a un portal igual al del Banco Santander, donde se pidió y dio la clave de acceso a la Banca online. Los estafadores, con ese acceso, realizan una primera transferencia por importe de 4900€ el 23 de diciembre, tras la recepción del falso SMS; y una segunda transferencia al día siguiente por un importe de 500€. Ese mismo día, se recibe un SMS del Banco Santander informando de la realización de transferencias por Banca a distancia, facilitando un número de teléfono por si no se hubieran autorizado. Las perjudicadas llaman inmediatamente a dicho teléfono advirtiendo de las transferencias no autorizadas y comparecen la misma mañana del día 24 de diciembre en la sucursal del Banco Santander y ante la Guardia Civil. Pero no fue hasta el día 28 de diciembre cuando se inició el *recall* vía SEPA, impidiendo que dentro de las 24 horas desde la transferencia ordenada se produjese la anulación por el propio Banco Santander. En definitiva, la Sala concluye que "la inicial negligencia de las usuarias hubiera podido ser fácilmente subsanada mediante una actuación diligente de la sucursal".

- SAP Cáceres 3 septiembre 2024[48]: Resuelve un litigio sobre reclamación de indemnización con la entidad bancaria UNICAJA BANCO, S.A. por movimientos no autorizados de la cuenta de la parte actora, al haber sido objeto de *phishing*. El 11 de junio de 2022, el demandante recibió un SMS de UNICAJA informándole de que su cuenta había sido bloqueada y debía someterse a un proceso de verificación a través de un enlace web que le enviaban. Tras acceder al enlace, recibió un nuevo mensaje con una clave de seguridad que introdujo. Al día siguiente pudo comprobar que se habían realizado movimientos no autorizados, concretamente varias transferencias: dos, en la cuenta de la que es titular junto con su esposa, por valor de 4.998 euros; y otras dos con cargo a la cuenta de otra persona, en la que el matrimonio está autorizado, por valor de 4900 euros. Al darse cuenta de ello la demandante se personó en la sucursal bancaria para informar de lo ocurrido y pedir el bloqueo de las cuentas, trasladándose posteriormente a las dependencias de la Guardia Civil de su localidad para interponer la correspondiente denuncia. La entidad financiera demandada se opuso a la pretensión de los actores asumiendo que los mismos habían sido víctimas de una estafa, negando, por ende, cualquier tipo de responsabilidad, y sosteniendo que existe negligencia por la parte actora al facilitar las claves que permitían el acceso de los delincuentes para ordenar las transferencias, de tal modo que sin ella no puede consumarse el fraude. Sin embargo, el tribunal no aprecia la existencia de negligencia grave ni incumplimiento por parte de los demandantes, pudiendo tratarse de un supuesto de estafa, a través de *phishing,* o

[47] JUR 2023, 398694.
[48] JUR 2024, 420659.

algunas de sus variantes conocidas como *smishing* o *vishing.* Es más, "en la medida en que personas ajenas al Banco, vulnerando su sistema de seguridad, fueron los que mandaron el supuesto enlace para desbloquear la cuenta, origen de la estafa, entiende el juzgador de instancia que hubo un fallo por el proveedor del servicio de pago". Concluye que "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 todas 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".

- STS, Sala Primera de lo Civil, de 9 de abril de 2025[49]: El procedimiento deriva de la realización de hasta quince transferencias bancarias no autorizadas a través de la aplicación del banco IBERCAJA Banco S.A., llegando a robar al cliente hasta 83.000 euros. El Banco se exculpó argumentando que las transferencias habían sido autorizadas puesto que habían cumplido con el doble factor de autenticación, alegando que no era trabajo del Banco saber si esas transferencias habían sido autenticadas por el usuario o por un tercero. El Tribunal indica que es obligación del usuario de los servicios adoptar todas las medidas razonables para proteger sus credenciales de seguridad personalizadas y de comunicar una operación de pago no autorizada o ejecutada incorrectamente sin demora injustificada al Banco, para que este la rectifique y reintegre de inmediato. Y, además, reafirma que la responsabilidad del proveedor de servicios de pago en caso de operaciones no autorizadas es cuasi objetivo, en el sentido de que, primero, una vez se notifique la existencia de una operación no autorizada o ejecutada incorrectamente, el proveedor debe responder, salvo que acredite la existencia de fraude; y, segundo, que, cuando el usuario niegue haber utilizado la operación o alegue que esta se ejecutó incorrectamente, corresponde al Banco acreditar que la operación fue "autenticada, registrada con exactitud y contabilizada". Sin embargo, dicho registro de la operación no resulta suficiente para demostrar que fue autorizada ni que el usuario ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave. Y, aunque la entidad acredite que la operación fue autenticada, registrada con exactitud y contabilizada, no puede eximirse de responsabilidad, pues debe probar que la operación no resultó afectada por un fallo técnico u otra deficiencia del servicio prestado. Por lo que, en el caso objeto del litigio, y a la luz de los hechos probados, se trata de una conducta diligente del usuario de los servicios, que informó de forma inmediata y reiterada al personal de la entidad, cumpliendo su obligación de notificación expresada en la normativa; mientras que el servicio prestado por el Banco se calificaría de defectuoso, por un lado, por no tomar en

[49] JUR 2025, 84706

consideración la información recibida, y, por otro, por omitir la adopción de medidas para detectar maniobras fraudulentas.

- SJI núm. 3 Málaga núm. 350/2025[50]: En este litigio se condena al BBVA a devolver 8.400€ a una clienta víctima de *phishing* bancario en octubre de 2021 por considerarse no autorizada la operación, una vez que se quedaron acreditadas la autenticación reforzada ni la diligencia debida en materia de seguridad. El caso se desarrolló como prosigue: la clienta de la entidad bancaria comenzó a recibir mensajes SMS en el mismo hilo que la referida entidad utiliza para comunicarse con sus clientes; y en ellos se le informaba de "actividad inusual" y del "bloqueo temporal" de su tarjeta, acompañados de un enlace HTTPS que aparentaba ser de la entidad. La clienta, confiando en su autenticidad, accedió al enlace y facilitó sus credenciales, lo que provocó el bloque inmediato de su dispositivo. Desde otro terminal comprobó que se había abierto sesión en su cuenta desde un nuevo dispositivo denominado "Angélica", que se había ampliado el límite de su tarjeta hasta 9.000€ y que se había efectuado una operación de 8.400€ a favor del comercio *wirexapp.com*. La clienta denunció los hechos ante la Guardia Civil y formuló reclamación ante BBVA. Pues bien, la entidad, en un principio devolvió la cantidad sustraída, pero posteriormente la retiró alegando que la operación había sido autorizada mediante clave OTP enviada por SMS al teléfono de la actora. Y aquí estriba la controversia del caso: si la operación fue efectivamente autorizada o no. La entidad argumentó que la transacción se validó mediante sistema 3D Secure, combinando contraseña, dispositivo y firma biométrica. Pero el Juzgado consideró que no se acreditó la autenticación reforzada, ni se probó la validación mediante CVV1 o CVV2; añadiendo que tampoco se justificó que el acceso desde un nuevo dispositivo fuera detectado o bloqueado. El Juzgado falla afirmando que clientes y clientas no tienen el deber de ser expertos/a en ciberseguridad, mientras que el Banco sí tiene el deber de protegerlos. Así, las entidades financieras gestionan sistemas complejos y disponen de los recursos técnicos necesarios para detectar patrones anómalos; por lo que, cuando no activan los mecanismos de verificación que la normativa impone, incumplen su obligación de diligencia profesional. En el caso enjuiciado se produjo una coexistencia de mensajes legítimos y falsos, no se alertó del incremento repentino del límite de crédito ni del acceso desde un nuevo dispositivo. De ahí que sea fundamental que las entidades adopten medidas tecnológicas adecuadas para prevenir esos riesgos ya que, de lo contrario, estarán incumpliendo sus deberes de supervisión.

En la doctrina evidenciada en estas sentencias relativas a entidades bancarias se colige una responsabilidad cuasi objetiva de los proveedores de servicios de pago según el artículo 45 RD-ley 19/2018, que traslada a la entidad el riesgo operativo de su actividad tecnológica, garantizando que la operación sea correctamente autenticada, ejecutada y registrada. La persona usuaria, en cambio, queda protegida

[50] Al tiempo de la conclusión de este artículo no se dispone de referencia en base de datos pública ni de suscripción.

frente a la opacidad y complejidad de los sistemas digitales bancarios, a no ser que se demuestre que actuó con dolo o negligencia grave, lo que exoneraría a la referida entidad. Asimismo, los artículos 44 y 46 RD-ley 19/2018 son de aplicación en varios de los supuestos señalados en las sentencias. El artículo 44 contempla la situación en la que el/la usuario/a niega haber autorizado una operación de pago ya ejecutada o aquella otra en la que alega que la operación se ejecutó de manera incorrecta, correspondiendo al proveedor de servicios de pago demostrar que la operación de pago en cuestión fue autenticada, registrada con exactitud y contabilizada, y que no se vio alterada por algún fallo técnico u otra deficiencia del servicio; y, por tanto, debiendo probar que la persona usuaria del servicio de pago cometió fraude o negligencia grave. El artículo 46 regula la responsabilidad de la persona ordenante cuando las pérdidas derivadas de operaciones no autorizadas sean resultado de una actuación fraudulenta o del incumplimiento, deliberado o por negligencia grave, de las obligaciones establecidas en el artículo 41, relativas a la protección de credenciales y a la notificación, sin demora indebida (y en un plazo máximo de trece meses, de conformidad con el artículo 43 RD-ley 19/2018[51]), al proveedor de servicios de pago del extravío, sustracción, apropiación indebida o utilización no autorizada del instrumento de pago.

Pues bien, me centraré justo en esta situación de demora injustificada por parte de la persona ordenante a la hora de comunicar una operación no autorizada o ejecutada incorrectamente porque supone el conflicto que se encausa en el Asunto C-665/2023, resuelto por la STJUE (Sala Cuarta) de 1 de agosto de 2025[52].

4.5. Análisis de la STJUE (Sala Cuarta) de 1 de agosto de 2025, Asunto C-665/2023, IL c. Veracash SAS

El asunto tiene origen en un litigio entre IL y la entidad *Veracash SAS*, relativo a varias operaciones de retirada de efectivo no autorizadas efectuadas con una tarjeta de pago que IL alega no haber recibido.

IL tiene una cuenta de depósito de oro en *Veracash*. El 24 de marzo de 2017 esta entidad envía al domicilio de IL una nueva tarjeta de retirada de efectivo y de pago. Entre el 30 de marzo y el 17 de mayo de 2017 se efectuaron retiradas de efectivo diarias de esa cuenta. IL alega no haber recibido dicha tarjeta de pago, ni mucho menos autorizado esas retiradas, presentando una demanda ante el Tribunal de Primera Instancia de Évry (Francia) pidiendo la condena de *Veracash* al reembolso de las cantidades correspondientes a esas retiradas de efectivo y al pago de una indemnización por daños y perjuicios.

En primera instancia se desestima parcialmente la demanda, por lo que IL interpone recurso de apelación ante el Tribunal de Apelación de París, que lo desestima mediante sentencia de 3 de enero de 2022. Y lo fundamenta, al igual que el Tribunal

[51] Transcripción del artículo 71 DSP2.
[52] (ECLI: EU:C:2025:640)

de Primera Instancia, en el hecho de que el actor no había notificado a *Veracash* las retiradas "sin demoras indebidas" y "de inmediato", sino el 23 de mayo de 2017; esto es, cerca de dos meses después de la primera retirada reclamada.

IL eleva recurso de casación invocando que, en consideración al artículo L. 133-24 del Código Monetario y Financiero francés (reflejo del art. 58 DSP1 y del actual art. 71 DSP2), el usuario de una tarjeta bancaria dispone, para realizar la notificación por operación no autorizada, de un plazo de treces meses desde la fecha del adeudo reclamado. Sin embargo, *Veracash* alega que dicho artículo acoge un doble plazo, siendo el de trece meses un plazo límite. Añadiendo que, en su opinión, la lógica de esta disposición lo que exige es que el usuario notifique de inmediato a su proveedor se servicios de pago.

El Tribunal de Casación decide suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

1) ¿Deben interpretarse los artículos 56, 58, 60 y 61 de la DSP1 en el sentido de que el ordenante se ve privado del derecho a la devolución del importe de una operación no autorizada cuando ha tardado en notificar a su proveedor de servicios de pago la operación de pago no autorizada, aunque lo haya hecho en los trece meses siguientes a la fecha del adeudo?
2) En caso de respuesta afirmativa a la primera cuestión prejudicial, ¿la privación del derecho del ordenante a la devolución está supeditada a que la tardanza en la notificación sea deliberada o por negligencia grave por su parte?
3) En caso de respuesta afirmativa a la primera cuestión prejudicial, ¿se priva al ordenante del derecho a la devolución de todas las operaciones no autorizadas o solo de aquellas que podrían haberse evitado si la notificación no se hubiera efectuado con tardanza?

Las respuestas a las tres cuestiones prejudiciales, que pretenden aclarar el alcance de la obligación de comunicación "sin tardanza injustificada" en materia de operaciones de pago no autorizadas, reforzando la diligencia exigible al usuario y delimitando la responsabilidad de las entidades financieras, se concatenan como prosigue.

En cuanto a la primera cuestión, la Sala recuerda que el art. 58 DSP1 dispone que la persona usuaria de servicios de pago está obligada a notificar "sin tardanza justificada" a su proveedor de servicios de pago que ha llegado a su conocimiento una operación de pago no autorizada; y "a más tardar" a los trece meses desde la fecha del adeudo. Por consiguiente, el derecho a obtener la rectificación de una operación no autorizada estaría supeditada al cumplimiento previo de un doble requisito temporal. Es reseñable que no todas las versiones lingüísticas del meritado art. 58 DSP1 utilizan la conjunción "y" para unir esos dos requisitos temporales. Pero sí que todas las versiones señalan como obligación del/de la usuario/a de servicios de pago la de notificar "sin tardanza injustificada" a su proveedor de una operación

no autorizada desde el momento en que tiene conocimiento de dicha operación. Sin embargo, el plazo de trece meses comenzaría a computar desde la fecha del adeudo. En definitiva, se trataría de dos requisitos temporales diferentes: uno de naturaleza subjetiva, en tanto en cuanto implica que el/la usuario/a actúe lo antes posible ante las circunstancias en las que se encuentra; y otro de carácter objetivo, que empieza a contar a partir de la fecha del adeudo de la operación que dio lugar a la reclamación.

Por tanto, y según la Sala, la redacción literal del art. 58 DSP1 indica que, en principio, para obtener la rectificación de una operación, la persona usuaria de servicios de pago está obligada "tanto a notificar sin tardanza injustificada a su proveedor de servicios de pago que ha llegado a su conocimiento una operación de pago no autorizada, como a efectuar dicha notificación a más tardar a los trece meses desde la fecha del adeudo". Esa interpretación literal se ve corroborada por el Considerando 31 de la propia DSP1, que entiende que esa notificación "lo antes posible" tiene como finalidad reducir los riesgos y las consecuencias de las operaciones de pago no autorizadas. Además de que en el sistema de régimen de responsabilidad regulado por la DSP1 la obligación de notificación es condición para que dicho régimen pueda aplicarse a favor de la persona usuaria. Asimismo, y en cuanto al plazo de trece meses, aludiendo a la jurisprudencia del Tribunal de Justicia, la Sala entiende que ese lapso de tiempo tiene por objeto garantizar la seguridad jurídica tanto de las personas usuarias de servicios de pago como de los proveedores de estos servicios. Concluyendo, el art. 58 DSP1 "debe interpretarse en el sentido de que el usuario de servicios de pago, en principio, se verá privado del derecho a obtener la rectificación de una operación si no notificó sin tardanza injustificada a su proveedor se servicios de pago que llegó a su conocimiento una operación de pago no autorizada, aun cuando se lo hubiera notificado en los trece meses siguientes a la fecha del adeudo". En consecuencia, el plazo de trece meses no neutralizaría la obligación de notificar sin tardanza.

Mediante su segunda cuestión prejudicial, el órgano jurisdiccional remitente pretende averiguar si los artículos 58, 60.1 y 61.2 de la DSP1, en relación con el artículo 56, apartado 1, letra b), deben interpretarse en el sentido de que, en el supuesto de una operación de pago no autorizada a raíz de la utilización de un instrumento de pago extraviado, robado o sustraído, o de la utilización no autorizada de dicho instrumento, si la persona ordenante notificó esa operación a su proveedor de servicios de pago en los trece meses siguientes a la fecha del adeudo, aquella se vería privada de su derecho a obtener la rectificación efectiva de la referida operación por haber tardado en notificarla a su proveedor de servicios de pago deliberadamente o por negligencia grave. Debe recordarse aquí la respuesta a la primera cuestión prejudicial sobre la existencia de un doble requisito temporal *ex* art. 58 DSP1.

Pues bien, el régimen de responsabilidad por operaciones de pago no autorizadas implica, según el art. 59 DSP1, un mecanismo de carga de la prueba favorable a la persona usuaria de servicios de pago ya que es el proveedor de esos servicios quien ha de probar que la operación de pago fue autenticada, registrada con exactitud y

contabilizada. En la práctica ese régimen de prueba se aplica desde el momento en que la notificación prevista en el art. 58 DSP1 se ha efectuado dentro del plazo estipulado, conllevando una obligación de devolución inmediata del importe de la operación, de conformidad con el art. 60.1 DSP1. Pero esta obligación de devolución inmediata resulta mitigada por ciertas excepciones, enunciadas en el art. 61 DSP1; entre ellas que las pérdidas sean fruto de la actuación fraudulenta o del incumplimiento, deliberado o por negligencia grave, de las obligaciones contempladas en el art. 56 DSP1 por parte de la persona ordenante. Concretamente, el apartado 1, letra b) de dicho artículo señala la obligación de informar al proveedor de servicios de pago (o a la entidad que este designe), sin demoras indebidas, en cuanto tenga conocimiento de ello, del extravío, el robo, la sustracción o la utilización no autorizada de su instrumento de pago. De darse este supuesto, se eximiría al proveedor de servicios de pago de su obligación de devolver el importe de las operaciones de pago no autorizadas.

Por consiguiente, de los arts. 58, 60.1, y 61.2 DSP1 considerados conjuntamente y en relación con el artículo 56, apartado 1, letra b), se desprende que, en el supuesto de una operación de pago no autorizada que sea consecuencia de la utilización de un instrumento de pago extraviado, robado o sustraído, o de la utilización no autorizada de tal instrumento, y habiendo la persona ordenante notificado de esas circunstancias a su proveedor de servicios de pago en los trece meses siguientes a la fecha del adeudo, dicho ordenante podría verse privado de su derecho a obtener la devolución de la referida operación si tardó en notificar la operación de pago no autorizada a su proveedor de servicios de pago, deliberadamente o por negligencia grave. Y ello porque se trataría de un incumplimiento manifiesto de la obligación de diligencia.

En cuanto a la tercera cuestión prejudicial sobre si se privaría a la persona ordenante del derecho a la devolución de todas las operaciones no autorizadas o únicamente de aquellas que podrían haberse evitado si la notificación no se hubiera efectuado con tardanza, concluye que ha de apreciarse por separado cada operación. Así, los artículos 58, 60.1 y 61.2 DSP1, en relación con el artículo 56, apartado 1, letra b), deben interpretarse de este modo: cuando, por un lado, existan operaciones de pago no autorizadas sucesivas a raíz de la utilización de un instrumento de pago extraviado, robado o sustraído, o de la utilización no autorizada de tal instrumento, y, por otro lado, la persona ordenante, a pesar de haber respetado el plazo de trece meses desde la fecha del adeudo, tardó, en parte, en notificarlas a su proveedor de servicios de pago, deliberadamente o por negligencia grave, en principio, aquella solo se verá privada del derecho a obtener la devolución de las pérdidas ocasionadas como consecuencia de las concretas operaciones que haya tardado en notificar a su proveedor de servicios deliberadamente o por negligencia grave.

5. CONSIDERACIONES FINALES

La STJUE (Sala Cuarta) de 1 de agosto de 2025, en el Asunto C-665/2023, que estima que la persona usuaria de una tarjeta no tiene derecho a la devolución de una operación no autorizada si se demora en notificarla al proveedor de servicios de pago

deliberadamente o por negligencia grave (incluso sin haber transcurrido el plazo legal máximo de trece meses para informar sobre operaciones no autorizadas), evidencia la existencia de brechas de seguridad en el ecosistema digital de pagos que ponen en jaque operaciones y transacciones.

Este ecosistema digital no deja de evolucionar, a la par que las complicaciones en materia de seguridad, lo que redunda en la confianza de las personas usuarias. Este estudio, partiendo de una consideración inicial del ecosistema digital, donde encuentran su encaje el comercio electrónico y las nuevas modalidades de pago, plantea la necesidad de reforzar los conceptos de confianza y seguridad, determinantes para la estabilidad del mercado digital.

El riesgo de seguridad en el ecosistema digital es multidimensional. Desde el punto de vista técnico, incluye amenazas como el *phishing*, el *malware* financiero o la suplantación de identidad. Para evitar las indeseables consecuencias que estas amenazas pueden conllevar, se implementan normas técnicas de regulación que pretenden evitar y, en su caso, mitigar las resultas de estas actividades maliciosas.

Concretamente, el *phishing,* como técnica de ingeniería social basada en la suplantación de identidad bajo una apariencia de entidad legítima y de confianza, manipula a las personas para que revelen información personal y financiera de carácter sensible. En el específico ámbito bancario, que es el elegido en esta investigación para ejemplificar este tipo de fraudes, tanto la normativa europea (a través de sus sucesivas Directivas de Servicios de Pago de 2007 y de 2015) como la nacional (con el RD-ley 19/2018), estipulan una serie de medidas para resolver la situación derivada de una operación de pago no autorizada, produciéndose la inversión de la carga de la prueba, en tanto en cuanto el proveedor de servicios de pago es el que se halla en mejores condiciones de probar que la operación ha sido autenticada, registrada con exactitud y contabilizada. Sin embargo, ello no obsta para que la entidad pueda eximirse de su responsabilidad, de carácter cuasi objetivo, cuando la persona usuaria no comunique esa operación no consentida sin demora injustificada en cuanto tenga conocimiento de la situación y, en todo caso, dentro de un plazo máximo de treces meses contados desde la fecha del adeudo. Pueden contemplarse aquí dos requisitos temporales, a cuya interpretación práctica ha contribuido la STJUE de 1 de agosto de 2025, analizada convenientemente en el epígrafe anterior.

Se trataría, pues, de dos requisitos temporales diferentes: uno de naturaleza subjetiva, que implica que el/la usuario/a actúe lo antes posible ante las circunstancias en las que se encuentra; y otro de carácter objetivo, que empieza a contar a partir de la fecha del adeudo de la operación que dio lugar a la reclamación. Por lo tanto, a pesar de que el plazo de treces meses se haya respetado, si existe tal demora injustificada en la comunicación de la operación no autorizada, el proveedor de servicios de pago quedará exento de su responsabilidad de devolución inmediata. De los pronunciamientos de la Sala al respecto puede deducirse un equilibrio de responsabilidades basado en que, por un lado, la persona usuaria debe reaccionar

diligentemente cuando recibe la información de una operación no autorizada, debiendo comunicar sin tardanza a su proveedor de servicios de pago; por otro, este proveedor solo puede negase a reembolsar si demuestra un perjuicio real por la demora (v. gr., reclamaciones tardías y pérdidas financieras imprevisibles). En definitiva, se mantiene la protección general (basada en una responsabilidad cuasi objetiva) frente a fraudes electrónicos que propician operaciones de pago no autorizadas, pero se refuerza la obligación de diligencia de la persona usuaria.

A la luz de lo expuesto, los tribunales están obligados a determinar convenientemente varios aspectos: ¿cuándo conoció realmente la persona usuaria esa operación?; ¿cuánto tiempo transcurrió hasta que avisó oportunamente a su proveedor de servicios de pago?; ¿ese tiempo fue razonable atendiendo a las circunstancias? Responder a estas cuestiones conlleva una tarea nada desdeñable de armonización de plazos para poder considerar la notificación tardía como causa legítima de oposición al reembolso. En este nuevo escenario los proveedores de servicios de pago tendrán que ofrecer una información más estricta a sus clientes sobre cómo detectar operaciones no autorizadas y cómo notificarlas y, por ende, sobre las consecuencias de una demora injustificada. Por su parte, las personas usuarias deberán ser más diligentes en la supervisión activa de sus cuentas para poder percatarse de operaciones de pago no autorizadas de carácter sospechoso, probando el momento exacto en que tuvieron conocimiento de ello y justificando adecuadamente su demora, en caso de haberla.

6. BIBLIOGRAFÍA

CALVO SAN JOSÉ, Mª J., "La responsabilidad civil de los bancos en los delitos de estafa por *phishing*", *Actualidad jurídica iberoamericana*, núm. 18, 2023.

DOMÍNGUEZ LUELMO, A., "Contratación Electrónica con consumidores", en MATA Y MARTÍN, R.M. (Dir.); JAVATO MARTÍN, A. Mª (Coord.) *et al*, *Los medios electrónicos de pago: problemas jurídicos,* Comares, Granada, 2007.

GUTIÉRREZ GARCÍA, E., *Inteligencia artificial y Derechos Fundamentales: Hacia una convivencia en la era digital,* Colex, A Coruña, 2024.

ILLESCAS ORTIZ, R., *Derecho de la Contratación Electrónica*, 2ª edición, Aranzadi, Cizur Menor, 2009, pp. 33-37.
PACHECO JIMÉNEZ, Mª N., "Nuevas alternativas de pago online: proveedores de servicios de pago externo en un mercado más tecnológico y seguro", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm, 49, enero-abril 2019.

PALMA ORTIGOSA, A., "El ciclo de vida de los sistemas de Inteligencia Artificial. Aproximación técnica de las fases presentes durante el diseño y despliegue de los sistemas algorítmicos", en COTINO HUESO, L. (Dir.) *et al*, *Derechos y garantías ante*

la inteligencia artificial y las decisiones automatizadas, Thomson Reuters Aranzadi, Cizur Menor, 2022.

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

VALLS PRIETO, J., *Derecho de las nuevas tecnologías, el mercado digital en la Unión Europea*, Editorial Reus, Madrid, 2019.