FACULTAD DE DERECHO

¿ESTAMOS PROTEGIDOS CONTRA EL FRAUDE *ONLINE*? LA DIRECTIVA (UE) 2015/2366 SOBRE SERVICIOS DE PAGO EN EL MERCADO INTERIOR Y LOS PAGOS ELECTRÓNICOS

Autora: Raquel María Cuesta Gómez

5º E-3 A

Derecho mercantil

Tutor: Bruno Walter Martín Baumeister

Madrid

Abril, 2022

RESUMEN

Los pagos electrónicos son una realidad que ha llegado en los últimos años para quedarse. Con esto en mente, el legislador europeo sentó las bases para crear un mercado uniforme e impulsó el uso de tecnologías digitales a través de la Directiva 2007/64/CE. Años más tarde, surgió la Directiva (UE) 2015/2366, con el objetivo de incrementar la seguridad de los pagos en el Espacio Económico Europeo, así como para fomentar la innovación y favorecer la adaptación de los servicios bancarios a las nuevas tecnologías. El objetivo de este trabajo es analizar el impacto que la Directiva (UE) 2015/2366 tiene sobre la seguridad de los pagos electrónicos, poniendo el foco de atención en el régimen de responsabilidad en caso de pagos no autorizados o que no cuenten con un sistema de autenticación reforzada de clientes (SCA).

Palabras clave: PSD2, servicio de pago, pago electrónico, autorización, autenticación reforzada de clientes, fraude *online*.

ABSTRACT

Electronic payments are a reality that has come to stay in recent years. With this in mind, the European legislator laid the foundations for creating a uniform market and boosted the use of digital technologies through Directive 2007/64/EC. Years later, Directive (EU) 2015/2366 has emerged, with the aim of increasing the security of payments in the European Economic Area, as well as to promote innovation and encourage the adaptation of banking services to new technologies. The aim of this paper is to analyze the impact that Directive (EU) 2015/2366 has on the security of electronic payments, with emphasis on the liability regime in case of unauthorized payments or payments without a strong customer authentication requirement (SCA).

Key words: PSD2, payment service, electronic payment, authorization, strong customer authentication, online fraud.

Tabla de contenidos

LISTADO DE ABREVIATURAS

ABE:	Asociación Bancaria Europea.
AISP:	Proveedor de Servicios de Información sobre Cuentas (*Account Information Service Provider*).
API:	Interfaz de Programación de Aplicaciones (*Application Programming Interfaces*).
BBVA:	Banco Bilbao Vizcaya Argentaria, S.A.
BCE:	Banco Central Europeo.
CE:	Comisión Europea.
Cfr.:	Indica que la idea expresada se ha extraído de la obra que se cita pero no se recoge en sus exactos términos.
CP:	Código Penal.
EEE:	Espacio Económico Europeo.
EM:	Estado Miembro.
Estudio:	Estudio sobre el Impacto de la Directiva 2007/64/CE *(Study on the Impact of the Directive 2007/64/CE).*
Ibidem:	Indica que el trabajo que se cita es el mismo que el citado en la nota inmediatamente anterior, coincidiendo autor, título y edición.
INE:	Instituto Nacional de Estadística.
Informe:	Informe Final del Proyecto de Normas Técnicas de Regulación sobre Autenticación Reforzada de Clientes y comunicación común y segura bajo el artículo 98 de la Directiva 2015/2366 *(Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)).*

OJ:	Ordenamiento Jurídico.
Op. cit.:	Hace referencia a cualquier tipo de obra citada con anterioridad (mismo autor, mismo título y misma edición) pero no de forma inmediata, puesto que hay otras referencias intercaladas.
P. ej.:	Por ejemplo.
PISP:	Proveedor de Servicios de Iniciación de Pagos (*Payment Initiation Service Provide*r).
Propuesta:	Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2013/36/UE y 2009//110/CE, y se deroga la Directiva 2007/64/CE /* COM/2013/0547 final - 2013/0264 (COD).
PSD:	Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior.
PSD2:	Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior.
PSP:	Proveedor de Servicios de Pago.
PwC:	*PriceWaterhouseCoopers.*
RAE:	Real Academia Española.
SAP:	Sentencia de la Audiencia Provincial.
SCA:	Autenticación Reforzada de Clientes (*Strong Customer Authentication*).
SEPA:	Zona Única de Pagos en Euros (*Single Euro Payments Area*).
STS:	Sentencia del Tribunal Supremo.
TPV:	Terminal Punto de Venta.

UE:	Unión Europea.
Vid.:	Indica dónde se puede ampliar la información. También sirve para hacer remisiones internas dentro del propio trabajo.

INTRODUCCIÓN

En los últimos años, la CE ha realizado varios esfuerzos para eliminar las fronteras internas dentro de la UE, con el objetivo de permitir la libre circulación de los bienes, personas, servicios y capitales[1]. Como medio para lograr este objetivo, entre otras medidas, ha promulgado la PSD2[2], que ofrece una revisión de la PSD[3]. Ambas directivas tratan de crear un marco común que asegure a los consumidores que cualquier pago realizado dentro del EEE será fácil, eficiente y seguro[4]. No obstante, la PSD2 va más allá y pone el foco de atención en seguir avanzando en un mercado interior más integrado, establecer normas exhaustivas relativas a los servicios de pago, la apertura de los mercados de pago a nuevos actores y lograr la base jurídica necesaria para la SEPA[5].

Este trabajo estudia los principales efectos de la PSD2 sobre la seguridad en los pagos electrónicos, con el objetivo de examinar si las nuevas medidas introducidas permiten una disminución real de los casos de fraude *online*, así como el impacto que estas medidas han tenido en España, específicamente a nivel de legislación, jurisprudencia y sobre nuestro sistema bancario y empresas.

El desarrollo de las tecnologías de la comunicación y la llegada de la SARS-CoV-2 han provocado un impulso del comercio electrónico. Según datos del INE, las ventas del comercio electrónico minorista aumentaron un 71,2% entre junio de 2019 y junio de 2020. No obstante, hubo un ligero descenso del 2% respecto de mayo de 2019 debido a la vuelta a la normalidad[6]. Este aumento de los pagos electrónicos ha dejado a los consumidores de estos servicios en una posición muy vulnerable, en especial a los titulares de tarjetas

---

[1] *Cfr*. Considerando 1 PSD.
[2] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE («DOUE» núm. 337, de 23 de diciembre de 2015).
[3] Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE («DOUE» núm. 319, de 5 de diciembre de 2007).
[4] *Cfr*. OFICINA DE PUBLICACIONES DE LA UNIÓN EUROPEA, "Servicios de Pago en la UE", *EUR-Lex*, 2 de julio de 2010 (disponible en https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=celex:32007L0064; última consulta 1/04/2022).
[5] *Cfr*. OFICINA DE PUBLICACIONES DE LA UNIÓN EUROPEA, "Normas revisadas sobre servicios de pago en la Unión Europea", *EUR-Lex*, 28 de junio de 2016 (disponible en https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=celex:32015L2366; última consulta 1/04/2022).
[6] *Cfr*. CIFRAS INE, "El salto del comercio electrónico", *Boletín informativo del Instituto Nacional de Estadística*, junio de 2020 (disponible en https://www.ine.es/ss/Satellite?L=es_ES&c=INECifrasINE_C&cid=1259952923622&p=1254735116567&pagename=ProductosYServicios%2FINECifrasINE_C%2FPYSDetalleCifrasINE; última consulta 13/03/2022).

de pago, que continúan siendo el objetivo de muchos delincuentes[7]. Es por ello por lo que un estudio sobre el aumento de la seguridad en los pagos electrónicos es un tema que está a la orden del día y que, además, cuenta con una importancia capital para poder entender los fallos y puntos fuertes del sistema.

La metodología seguida por el presente trabajo consiste en realizar un análisis detallado de la PSD2 para entender el sistema creado por esta norma y los nuevos requisitos que incorpora para, finalmente, analizar el impacto que ha tenido en España.

Para ello, vamos a estudiar, en primer lugar, los antecedentes de la PSD2 y cuáles fueron las deficiencias del sistema que hicieron necesario su nacimiento, así como las principales características de la PSD, la norma que precedió a la PSD2.

A continuación, vamos a realizar un análisis de las novedades introducidas por la PSD2 a nivel de seguridad de los servicios de pago, centrándonos en las nuevas medidas de protección de los consumidores.

Finalmente, estudiaremos qué efectos ha tenido esta regulación sobre nuestro OJ, sobre nuestro sistema bancario y sobre las empresas españolas, así como el papel que está teniendo nuestra jurisprudencia a la hora fomentar la incorporación de estas nuevas medidas.

[7] *Cfr*. OCU, "Fraudes online: te roban y ni te enteras", *Noticias OCU*, 25 de mayo de 2021 (disponible en https://www.ocu.org/dinero/tarjetas/noticias/fraudes-tarjetas-online; última consulta 14/03/2022).

CAPÍTULO I. CONTEXTO DE LA PSD2 Y PRINCIPALES CARACTERÍSTICAS

1. EVOLUCIÓN DEL MERCADO DE PAGOS ELECTRÓNICOS DESDE LA PSD

La PSD, publicada en 2007, supuso el primer intento de regulación de los servicios de pago. Esta surgió con el principal objetivo de facilitar el nacimiento de un mercado único de servicios de pago, ya que la fragmentación y falta de armonización del marco jurídico de los servicios de pago en la UE impedía este objetivo[8]. Como consecuencia, el Parlamento Europeo y el Consejo de la UE elaboraron, en la PSD, un marco común para los servicios de pago que sustituyó la normativa nacional de cada país del EEE[9].

Así, la PSD trató de lograr una armonización de los sistemas de pago de la UE, facilitando un mercado único de bienes y servicios y apoyando una mayor competencia en los servicios de pago[10].

A pesar de que la PSD no logró crear un marco común para los servicios de pago, su papel fue fundamental, ya que sentó la bases para la futura labor de mejora de la competencia y facilitó que las nuevas tecnologías superaran rápidamente la legislación y las prácticas de mercado existentes[11]. Así, desde su entrada en vigor, el mercado de pagos minoristas ha experimentado importantes innovaciones técnicas. Además, el volumen de los pagos electrónicos ha incrementado incesantemente[12].

Según un artículo publicado por el banco Santander[13], "siete de cada diez usuarios creen que los pagos digitales se impondrán al dinero en efectivo; planeando la mitad de ellos recurrir menos a este último".

---

[8] *Cfr.* MERCADO-KIERKEGAARD, S., "Harmonising the regulatory regime for cross-border payment services", *Computer Law & Security Report*, vol, 23, n. 2, 2007, pp. 177-178.
[9] *Cfr.* OFICINA DE PUBLICACIONES DE LA UNIÓN EUROPEA, "Servicios de Pago en la UE…", *op. cit.*
[10] *Cfr.* DONNELLY, M., "Payments in the digital market: Evaluating the contribution of Payment Services Directive II", *Computer Law & Security Review*, vol. 32, n. 6, 2016, p. 836.
[11] *Cfr.* Considerandos 3 y 4 PSD2.
[12] *Cfr.* INE, "Equipamiento y uso de TIC en los hogares. Año 2021", *INEbase*, 15 de noviembre de 2021 (disponible en https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735576692; última consulta 13/03/2022).
[13] SANTANDER, "Pagos digitales: ¿qué son y cuáles son los más usados?", *Sala de Comunicación Santander*, 30 de agosto de 2021 (disponible en https://www.santander.com/es/stories/pagos-digitales-que-son-y-cuales-son-los-mas-usados; última consulta 4/03/2021).

En 2013, la CE organizó una revisión independiente de la eficacia de la PSD en el denominado Estudio sobre el Impacto de la Directiva 2007/64/CE[14][15]. El Estudio trataba temas como las tasas y cargos por servicios de pago y la fragmentación del mercado.

A la luz de este Estudio y de los rápidos cambios tecnológicos, la CE desarrolló la PSD2, que determina de forma expresa en su artículo 114, la derogación de la PSD.

Durante el proceso de aprobación de la PSD2, la CE era consciente de que la nueva coyuntura del mercado de pagos electrónicos hacía necesario el aumento de la seguridad de los pagos electrónicos[16]. Así, la CE convirtió este objetivo en una de las principales metas de la PSD2[17].

De este modo, la PSD2 introduce importantes cambios en el marco regulador de los servicios de pago, como la ampliación del ámbito de cobertura, la aclaración del alcance de los derechos de los consumidores y las obligaciones de los proveedores y la introducción de requisitos de seguridad y autenticación reforzada[18].

Facilitar estos pagos electrónicos es esencial para el desarrollo del comercio *online*, ya que la preocupación de los consumidores en torno a la seguridad de los pagos electrónicos se considera una de las principales barreras para el crecimiento de este[19]. Por esta razón, el establecimiento de un marco jurídico sólido y eficaz para los pagos electrónicos es un factor de apoyo esencial para la realización de la estrategia para el Mercado Único Digital de la CE[20].

Poco después de la publicación de la PSD2, el número de licencias para constituir empresas *PayTech,* entendidas como cualquier compañía que desarrolle soluciones que

---

[14] LONDON ECONOMICS AND *IFF*, "Study on the impact of Directive 2007/64/EC on Payment Services in the Internal Market and on the Application of Regulation (EC) No. 924/2009 on Cross-Border Payments in the Community, Final Report", *London Economics*, febrero de 2013 (disponible en https://ec.europa.eu/info/sites/default/files/study-impact-psd-24072013_en.pdf; última consulta 12/02/2022).

[15] Traducción realizada por la autora.

[16] *Cfr.* Considerando 7 PSD2.

[17] *Cfr.* LOESCH, S., "Payments Services Directive", *A Guide to Financial Regulation for Fintech Entrepreneurs*, Wiley, New York, 2018, pp. 229-231.

[18] *Cfr.* BRENER, A., "Payment Service Directive II and Its Implications" en Lynn, T., Mooney, J. G., Rosati, P., Cummins, M. (ed.), *Disrupting Finance. FinTech and Strategy in the 21st Century*, Palgrave McMillan, Dublin, 2019, pp. 104-109.

[19] *Cfr.* Considerando 7 PSD2.

[20] *Cfr.* COMISIÓN EUROPEA, "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Una Estrategia para el Mercado Único Digital de Europa", *EUR-Lex*, 6 de mayo de 2015 (disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192; última consulta 10/02/2022).

mejoren las características de los medios de pago apoyándose en la tecnología[21], concedidas en la UE aumentó vertiginosamente. En sólo 24 meses, este número se multiplicó por cuatro, pasando de 350 entidades en 2017 a 1475 en 2019. La licencia de Entidad de Pago era la más popular entre las entidades *PayTech* no bancarias, seguida de la de Entidad de Dinero Electrónico[22].

Cabe mencionar que muchas de estas licencias han sido solicitadas por entidades bancarias tradicionales con el objetivo de no quedarse obsoletas en la prestación de servicios de pago[23]. Y es que el número de pagos en línea no ha hecho más que crecer, haciendo que muchos individuos hayan visto una oportunidad de negocio en este sector[24].

Según datos de la consultora *PwC*, se estima que las operaciones electrónicas crezcan un 82% entre 2020 y 2025[25]. Además, Víctor Cruzado afirma que, en 2025, los pagos electrónicos instantáneos representarán el 25% de las operaciones mundiales[26].

2. PRINCIPALES DIFICULTADES DE LA PSD QUE PRECIPITARON SU DEROGACIÓN

El objetivo principal de la PSD era crear un marco jurídico uniforme para los servicios de pago en todo el EEE y proporcionar los fundamentos legislativos para la SEPA[27]. Estas medidas se consideraban esenciales para la creación de un mercado único de servicios de

---

[21] *Cfr.* ASOCIACIÓN ESPAÑOLA FINTECH E INSURTECH, "Libro Blanco de PayTech: La Evolución del sector PayTech y los nuevos retos regulatorios", *Asociación Fintech*, 2020 (disponible en https://www.asociacionfintech.es/wp-content/uploads/2020/12/AEFI_Libro-Blanco-PayTech-2020_Diciembre-2020-1.pdf; última consulta 10/02/2015).

[22] *Cfr.* POLASIK, M., HUTERSKA, A., IFTIKHAR, R., MIKULA, S., "The impact of Payment Services Directive 2 on the PayTech sector development in Europe", *Journal of Economic Behavior and Organization*, vol. 170, 2020, p. 389.

[23] *Ibídem*, p. 386.

[24] *Cfr.* INE, "Equipamiento y uso de TIC en los hogares…", *op. cit.*

[25] *Cfr.* PWC ESPAÑA, "Los pagos electrónicos casi se triplicarán en 2030 hasta superar los 3 billones de operaciones en el mundo", *PwC España – Entorno digital* (disponible en https://www.pwc.es/es/sala-prensa/notas-prensa/2021/pagos-electronicos-triplicar-2030.html#:~:text=Las%20estimaciones%20incluidas%20en%20el,transacciones%20en%20todo%20el%20mundo; última consulta 09/02/2022).

[26] *Cfr.* CRUZADO, V., "Los pagos electrónicos instantáneos supondrán el 25% de las transacciones mundiales en 2025", *Expansión*, 16 de octubre de 2021 (disponible en https://www.expansion.com/empresas/banca/2021/10/16/6169641b468aeb985c8b468e.html; última consulta 09/02/2022).

[27] *Cfr.* Considerandos 4 y 5 PSD.

pago, que a su vez formaba parte de la infraestructura necesaria para el perfeccionamiento del mercado interior[28].

2.1. Libro Verde: Hacia un mercado europeo integrado de pagos mediante tarjeta, pagos por Internet o pagos móviles

Como se expuso *supra*, tras la aprobación de la PSD, la CE comenzó a tomar medidas para abordar la limitación de su enfoque. El Libro Verde de la CE[29], que precedió a la PSD2, dio gran importancia a la necesidad de impulsar el comercio electrónico. Según este, el comercio electrónico representa una parte importante del mercado de pagos minoristas en euros. Este mercado es uno de los mayores mercados del mundo, por lo que lograr una mayor integración podría traer beneficios económicos considerables[30].

Para el Libro Verde, este mercado contaba con tres problemas fundamentales que impedían su crecimiento: (a) la diversidad de métodos de pago de unos EEMM a otros, (b) el coste de los pagos, y (c) la seguridad de estos. Estas dificultades provocaban una fragmentación del mercado de pagos electrónicos, con un reducido número de sistemas de pagos electrónicos nacionales bien implantados[31].

Una plena integración de los pagos electrónicos permitiría la creación de un mercado único digital en la UE. Este, a su vez, permitiría que los consumidores pudieran utilizar una única cuenta bancaria para todas sus operaciones de pago, que las empresas y administraciones públicas pudieran simplificar y racionalizar sus procedimientos de pago y centralizar todas las operaciones realizadas en la UE, que los comerciantes pudieran obtener soluciones de pago electrónico baratas, seguras y eficientes, que los PSP redujeran sus costes aprovechando economías de escala y que los proveedores de tecnología pudieran basar su labor de desarrollo en instrumentos paneuropeos[32].

Con el objetivo de impulsar la integración de los pagos con tarjeta, los pagos electrónicos y los pagos móviles, el Libro Verde propuso cinco posibles vías: (a) acceso

---

[28] *Cfr.* Considerando 1 PSD.
[29] COMISIÓN EUROPEA, "Libro Verde: Hacia un mercado europeo integrado de pagos mediante tarjeta, pagos por Internet o pagos móviles", *EUR-Lex*, 2012 (disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52011DC0941&from=es; última consulta 02/02/2022).
[30] *Cfr. Ibidem*, p. 3.
[31] *Cfr. Ibidem*, p. 5.
[32] *Cfr. Ibidem*, p. 7.

transfronterizo al mercado, (b) transparencia y eficacia de costes en la tarificación de los servicios de pago, (c) normalización, (d) interoperabilidad entre proveedores de servicios, y (e) seguridad de los pagos[33].

Respecto de la última vía, puso el foco de atención en la prevención del fraude. Según el Libro Verde, la incorporación de tarjetas que funcionan con firma o tarjetas que cuentan con *chip* y PIN, permitió una reducción de la utilización fraudulenta de tarjetas en operaciones de pago físicas. No obstante, las actividades fraudulentas seguían creciendo en las operaciones de pago a distancia, específicamente aquellas realizadas por Internet[34].

2.2. Estudio sobre el Impacto de la Directiva 2007/64/CE

Por su parte, el Estudio elaborado por London Economics and *iff*[35] concluyó que, aunque la PSD había logrado algunos de sus objetivos generales, entre ellos contribuir sustancialmente a un mercado único de servicios de pago, no podía observarse ningún impacto positivo sustancial respecto a la entrada en el mercado de nuevos proveedores, las innovaciones técnicas y la eficacia de la prestación de servicios de pago. El Estudio también detectó dificultades en cuanto al alcance y la cobertura de la PSD, especialmente en el contexto del crecimiento del comercio electrónico, el desarrollo de diferentes tipos de servicios de pago y la atribución de responsabilidad por pagos no autorizados. Además, consideró que, aunque la PSD adoptara un modelo de armonización total, el margen de maniobra de los EEMM para introducir excepciones, así como el carácter abstracto de varios principios y la falta de claridad del lenguaje utilizado, podría dar lugar a la heterogeneidad de los enfoques en los EEMM. Todo esto provocaría la imposibilidad de la adopción de un marco normativo armonizado[36].

Como corolario, el Estudio enumeró los problemas más importantes sobre los que tendría que trabajar la CE para lograr corregir las deficiencias de la PSD[37].

Según este, la PSD otorgaba a los EEMM un amplio abanico de posibilidades, lo que tuvo un impacto negativo en el proceso de integración del mercado de pagos electrónicos.

---

[33] *Cfr. Ibidem,* pp. 8-23.
[34] *Cfr. Ibidem,* pp. 21-22.
[35] *Cfr.* LONDON ECONOMICS AND *IFF, op. cit.*, pp. 268-275.
[36] *Cfr.* KEMP, R., "Mobile payments: Current and emerging regulatory and contracting issues", *Computer Law & Security Review*, vol. 29, n. 2, 2013, pp. 175-179.
[37] *Cfr.* LONDON ECONOMICS AND *IFF, op. cit.* pp. 274-275.

Además, esta situación provocó que el propio Estudio tuviera dificultades para comprobar la eficacia y diferencias de la normativa adoptada por cada EM.

El Estudio también mencionaba que la PSD incorporaba riesgos de *compliance* para los proveedores, al no ser clara a la hora de diferenciar entre servicios de pago tradicionales y servicios de pago basados en dinero electrónico.

Por otro lado, la PSD no se pronunciaba sobre determinados servicios de pago, en especial sobre los servicios de iniciación de pagos. El Estudio consideró estos servicios de vital importancia ya que permiten estimular la innovación en el campo de los servicios de pago.

Además, muchas actividades quedaban exentas, lo que provocaba un tratamiento desigual entre los diferentes PSP. A pesar de que algunas de las exenciones eran proporcionadas, otras provocaban una desigualdad injusta entre proveedores.

La PSD, además, establecía reglas mitigantes para pagos de bajo valor, eximiendo a estos total o parcialmente de determinadas normas incorporadas en la PSD. No obstante, el diseño de los instrumentos de pago de bajo no favorecía ni a proveedores ni a usuarios, lo que provocaba que su uso fuera muy limitado.

Finalmente, las diferencias de trato entre las *two-leg* y las *one-leg transactions*[38] provocaba que los usuarios de estas operaciones no supieran a qué protección acogerse.

2.3. Propuesta de directiva del Parlamento Europeo y del Consejo sobre servicios de pago en el mercado interior

Tras revisar el marco europeo y la PSD, y tras consultar el Libro Verde[39], la CE llegó a la conclusión de que era necesaria una reforma de la normativa relativa a los pagos electrónicos.

---

[38] El término *one-leg-transaction* es una expresión que surgió a raíz de la PSD para referirse a aquellas operaciones en las que el ordenante o el beneficiario del servicio de pago se encuentra fuera de la Unión Europea. Uno de los problemas más señalados por las organizaciones de consumidores tras la aprobación de la PSD fue la falta de protección de este tipo de operaciones, ya que la PSD sólo protegía aquellas operaciones en las que el ordenante y el beneficiario del servicio de pago se encontraban situados en la Unión Europea (*two-leg-transactions*). Muchos críticos señalaron que el tipo de consumidor más propenso a utilizar *one-leg-transactions* eran los inmigrantes que utilizan las remesas de pago para enviar dinero a casa y que esta categoría era especialmente vulnerable.

[39] *Cfr.* COMISIÓN EUROPEA, "Libro Verde…", *op. cit.*

Una vez más, la Propuesta de la CE[40] puso el foco de atención en el mayor desarrollo del mercado europeo de pagos electrónicos. Según esta, los grandes avances alcanzados en la integración de los mercados de pago minoristas europeos se debían principalmente al trabajo conjunto de la PSD, el Reglamento (CE) n.º 924/2009[41] y a la Segunda Directiva sobre dinero electrónico[42]. No obstante, el dinamismo del mercado de pagos minoristas provocaba el constante surgimiento de nuevos segmentos de mercado, por lo que la fragmentación por las fronteras nacionales seguía siendo un problema latente[43].

Específicamente comentó los cambiantes hábitos de pago de los consumidores, así como el número cada vez mayor de pagos con tarjeta de crédito y débito, el auge del comercio electrónico y la creciente popularidad de los teléfonos inteligentes. Según esta, todos estos cambios allanaron el camino para la aparición de nuevos medios de pago[44]. Como consecuencia, era importante aumentar la seguridad de los pagos, lo que permitiría a los usuarios beneficiarse del mercado interior, especialmente del comercio electrónico[45].

Este cambio de enfoque político se refleja en la PSD2, que afirma que para garantizar la protección de los usuarios y el desarrollo de un entorno adecuado para el comercio electrónico, es necesaria la seguridad[46].

---

[40] *Cfr.* COMISIÓN EUROPEA, "Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2013/36/UE y 2009//110/CE, y se deroga la Directiva 2007/64/CE /* COM/2013/0547 final - 2013/0264 (COD)", *EUR-Lex*, 2013, p. 9 (disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013PC0547&from=GA; última consulta 10/02/2022).

[41] Reglamento (CE) n.º 924/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativo a los pagos transfronterizos en la Comunidad y por el que se deroga el Reglamento (CE) nº 2560/2001 («DOUE» núm. 266, de 9 de octubre de 2009).

[42] Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE («DOUE» núm. 267, de 10 de octubre de 2009).

[43] *Cfr.* COMISIÓN EUROPEA, "Propuesta de DIRECTIVA…", pp. 2-4.

[44] *Cfr. Ibidem*, p. 2.

[45] *Cfr. Ibidem*, pp. 13-30.

[46] *Cfr.* Considerando 95 PSD2.

3. NOVEDADES INCORPORADAS POR LA PSD2 PARA SUPERAR LAS DIFICULTADES DE LA PSD

Debido a que la PSD no logró el nivel de armonización deseado, la posibilidad de que los EEMM establezcan excepciones se ha reducido en la PSD2[47]. Así, aunque la supervisión de los servicios de pago es una cuestión encargada a las autoridades competentes de cada EM, estas se ven limitadas en su forma de actuar. En muchos casos, la PSD2 exige que la ABE elabore directrices y proyectos de normas técnicas[48][49]. Estos deben elaborarse en estrecha colaboración con el BCE, tras consultar a todas las partes interesadas. En cuanto a la aplicabilidad de estas medidas, se exige a las autoridades competentes y a las entidades financieras que hagan todo lo posible para cumplir las directrices. En el plazo de dos meses a partir de la publicación de las directrices, la autoridad competente de cada EM debe informar a la ABE sobre si cumple o tiene la intención de cumplir las directrices y, en caso contrario, también debe informar a la ABE, exponiendo sus motivos[50].

Además, la PSD2 ha regulado aquellas actividades que quedan exentas con umbrales claros e inequívocos, inspirándose en criterios objetivos y verificables.

Por otro lado, la PSD2 refuerza los derechos de los consumidores. Así, la PSD2 reduce la responsabilidad por pagos no autorizados de 150 a 50 euros, otorga un derecho incondicional de reembolso durante un período de ocho semanas y elimina los recargos cuando el consumidor utilice una tarjeta de crédito o de débito[51].

En línea con este objetivo de reforzar los derechos de los consumidores, la PSD2 modifica el régimen de responsabilidad de los PSP, incorporando el término de SCA y aumentando la responsabilidad del proveedor en detrimento de la del ordenante[52]. El objetivo de estas

---

[47] *Cfr.* Artículos 86.1 PSD y 107.1 PSD2.
[48] P. ej., Considerando 35 PSD2.
[49] Además, en la PSD2 se refuerza la función de la ABE para desarrollar un registro central de las instituciones de pago autorizadas y para contribuir a la resolución de litigios entre autoridades nacionales.
[50] *Cfr.* Artículo 16. 3 del Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo de 24 de noviembre de 2010 por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión («DOUE» núm. 331, de 15 de diciembre de 2010, páginas 12 a 47).
[51] *Cfr*. OFICINA DE PUBLICACIONES DE LA UNIÓN EUROPEA, "Normas revisadas sobre servicios…", *op. cit.*
[52] Según el artículo 4.8 PSD2, un ordenante es "la persona física o jurídica titular de una cuenta de pago que autoriza una orden de pago a partir de dicha cuenta, o, en caso de que no exista una cuenta de pago, la persona física o jurídica que dicta una orden de pago".

nuevas medidas es reducir el riesgo de fraude para así aumentar la seguridad de los pagos electrónicos.

El legislador europeo considera que los servicios de pago son esenciales para mantener determinadas actividades económicas y sociales de gran importancia[53]. Además, "el desarrollo continuado de un mercado único integrado de pagos electrónicos seguros es esencial para apoyar el crecimiento de la economía de la Unión y para garantizar que los consumidores, los comerciantes y las empresas en general disfruten de posibilidades de elección y condiciones de transparencia en los servicios de pago de modo que puedan aprovechar plenamente las ventajas del mercado interior[54]".

Los servicios de pago han evitado en gran medida la regulación de la UE hasta hace poco. No obstante, dicha regulación es necesaria ya que, siempre que se redacte y aplique correctamente, puede ser una herramienta eficaz para crear incentivos que aumenten la innovación, el desarrollo económico y la competencia[55].

Por otro lado, la PSD2 busca abrir el mercado de pagos a empresas que ofrezcan servicios de pago basados en el acceso a cuentas de pago[56]. Así, introduce dos figuras novedosas: los *proveedores de servicios de iniciación de pagos* y los *proveedores de servicios de información sobre cuentas*. Según el artículo 4.18 PSD2, un PISP es aquel "proveedor de servicios de pago que ejerce a título profesional las actividades a que se refiere el anexo I, punto 7". Entre estas actividades, cabe destacar la posibilidad de iniciar una orden a petición de un usuario de servicio de pago respecto de una cuenta de pago alojada en un proveedor distinto de servicios de pago[57]. Por su parte, el artículo 4.19 PSD2 determina que un AISP es aquel que "ejerce a título profesional las actividades a que se refiere el anexo I, punto 8. Así, estos permiten, entre otras cosas, que los usuarios de servicios de pago dispongan de una visión general de su situación financiera para que puedan gestionar mejor sus finanzas personales [58].

---

[53] *Cfr.* Considerando 7 PSD2.
[54] *Cfr.* Considerando 5 PSD2.
[55] *Cfr.* ROMĀNOVA, I., GRIMA, S., SPITERI, J., & KUDINSKA, M., "The Payment Services Directive 2 and competitiveness: The perspective of European FinTech Companies", *European Research Studies Journal*, vol, 21, n. 2, 2018, p. 20.
[56] *Cfr.* OFICINA DE PUBLICACIONES DE LA UNIÓN EUROPEA, "Normas revisadas sobre servicios…", *op. cit.*
[57] *Cfr. Ibidem.*
[58] *Cfr. Ibidem.*

Cabe mencionar que la PSD2 ha tratado de superar los errores cometidos a la hora de regular los instrumentos de pago de bajo valor, tema en el que profundizaremos más adelante[59].

Finalmente, con la PSD2, las *one-leg-transactions* quedan protegidas por las disposiciones relativas a los requisitos de información y transparencia (Título III) y a los derechos y obligaciones de las partes (Título IV), aunque sólo respecto a las partes de la operación de pago que tienen lugar en la UE, lo que pone solución a las deficiencias de la PSD2.

[59] *Vid.* Reglas especiales para los pagos de bajo valor, p. 35.

CAPÍTULO II. REDUCCIÓN DE LA RESPONSABILIDAD DEL ORDENANTE POR LAS OPERACIONES NO AUTORIZADAS

A pesar de que la PSD2 introduce numerosas novedades, este trabajo se centra en aquellas medidas tendentes a aumentar la seguridad de los pagos electrónicos, específicamente en la reducción de la responsabilidad del ordenante en los casos en los que no se haya dado el requisito de la autorización.

Desde un principio, la PSD2, deja muy clara su posición respecto a la necesidad de servicios de pago fiables y seguros para lograr el buen funcionamiento de un mercado de servicios de pago y, ulteriormente, para lograr el mantenimiento de actividades económicas y sociales de gran importancia. La PSD2 también señala que es consciente de que los riesgos de seguridad en los pagos electrónicos han ido aumentando en los últimos años debido a un gran número de variables[60].

Con la llegada de la PSD2, se ha reducido aún más la responsabilidad del ordenante por las operaciones no autorizadas, por ejemplo, al exigir pruebas justificativas para demostrar el fraude o la negligencia grave del ordenante[61], al aplicar las mismas normas cuando las operaciones no autorizadas se inician a través de un servicio de iniciación de pagos[62], y al imposibilitar la responsabilidad del ordenante en caso de que no se haya aplicado una SCA[63].

Este enfoque más estricto en materia de seguridad que exige, en general, el uso de tecnologías capaces de garantizar la autenticación segura del usuario, busca contribuir a la reducción del riesgo de fraude en todos los medios de pago, especialmente en los pagos electrónicos, así como a la protección de la confidencialidad de los datos financieros del usuario (incluidos los datos personales)[64].

[60] *Cfr.* Considerando 7 PSD2.
[61] *Cfr.* Artículo 72.1 PSD2.
[62] *Cfr.* Artículo 73.2 PSD2.
[63] *Cfr.* Artículo 74.2 PSD2.
[64] *Cfr.* Considerando 69 PSD2.

1. OPERACIONES DE PAGO NO AUTORIZADAS: PRINCIPALES CARACTERÍSTICAS Y DIFICULTADES

1.1. Definición de operaciones de pago no autorizadas

El concepto de *operaciones de pago no autorizadas* no se ha modificado sustancialmente en la PSD2. Se considera que una operación de pago está autorizada cuando el ordenante haya dado su consentimiento. Esta suele darse antes de la ejecución de la operación de pago, aunque existe la posibilidad de una ratificación o aprobación *a posteriori*[65].

El consentimiento debe darse en la forma y mediante el procedimiento acordado por las partes[66], por ejemplo, facilitando un nombre de usuario y una contraseña, comunicando los datos de la tarjeta de crédito o escaneando un código QR y un PIN.

En general, es bastante fácil distinguir entre operaciones de pago autorizadas y no autorizadas. Sin embargo, en algunas situaciones resulta más difícil hacer dicha distinción.

El artículo 73 PSD2 establece la obligación de los EEMM de velar por que el PSP devuelva el importe de una operación de pago no autorizada inmediatamente y, a más tardar, al final del día hábil siguiente a aquel en el que se haya observado o notificado la operación, salvo en un caso en el que profundizaremos más adelante. Así, el PSP deberá restituir la cuenta de pago al estado en el que se encontraba antes de haberse realizado la operación no autorizada y velará por que la fecha de valor del abono no sea posterior a la fecha de adeudo del importe. El objetivo de estas previsiones es evitar que los ordenantes no responsables sufran algún daño financiero derivado de las operaciones no autorizadas.

Por lo tanto, cuando un ordenante advierta que se han realizado una o varias operaciones de pago no autorizadas y quiera obtener una rectificación, tendrá que notificarlo al PSP[67].

Lamentablemente, la PSD2 no modifica la redacción de la PSD, que exige que dicha notificación se realice sin demora injustificada y, en todo caso, dentro de un plazo máximo de trece meses desde la fecha del adeudo. Si bien está claro que una vez transcurridos trece meses desde la fecha de adeudo ya no es posible la rectificación, no está claro si el ordenante puede obtener la rectificación si notificó la operación no

[65] *Cfr.* Artículo 64. 1 PSD2.
[66] *Cfr. Ibidem.*
[67] *Cfr.* Artículo 71.1 PSD2.

autorizada en el plazo de trece meses, pero con una demora injustificada tras tener conocimiento de la operación no autorizada.

Los PSP sólo pueden eludir esta obligación de reembolsar al ordenante inmediatamente (y a más tardar el día hábil siguiente) cuando el PSP tenga motivos razonables para sospechar que puede haberse cometido un fraude y los comunique a la autoridad nacional pertinente por escrito[68]. Esta última premisa ha sido añadida por la PSD2 con el objetivo de evitar que los PSP concluyan con demasiada facilidad la presencia de motivos objetivos de sospecha de fraude para poder aplazar una devolución. En caso de sospecha de fraude por parte del ordenante, el PSP puede llevar a cabo[69] una investigación en un plazo razonable antes de reembolsar al pagador (lo que, por supuesto, no tendrá que hacer cuando se demuestre realmente el fraude del pagador).

Además, es importante destacar que esta obligación de reembolsar al pagador se impone al PSP. Por lo tanto, los PSP no pueden limitarse a remitir al titular de la tarjeta a la compañía de tarjetas de crédito para que le devuelvan el importe cargado.

Por último, el abono en la cuenta del pagador no impide que el pagador sea responsable, total o parcialmente, de las operaciones de pago no autorizadas en un momento posterior, es decir, una vez que se haya decidido que el pagador puede ser responsable de las operaciones no autorizadas.

Finalmente, cabe mencionar que la PSD2 no sólo regula la responsabilidad de las operaciones de pago a las que el ordenante ha dado su consentimiento directamente, sino también la de las operaciones de pago que se inician a través de un PISP[70].

Los servicios de iniciación de pagos ofrecen a los usuarios dos ventajas principalmente: (a) la posibilidad de comprar en línea, incluso si no tienen una tarjeta de crédito; (b) la seguridad de que se ha iniciado una transferencia para incentivar al beneficiario a liberar los bienes o prestar el servicio sin demora indebida[71].

Este tipo de servicios de pago no entraba en el ámbito de aplicación de la PSD y, por tanto, no estaba regulado en el pasado. Esto implicaba, entre otras cosas, que no quedaba claro sobre quién recaía la responsabilidad por operaciones no autorizadas. Finalmente,

[68] *Cfr*. Artículo 73.1 PSD2.
[69] *Cfr*. Considerando 71 PSD2.
[70] *Cfr.* Artículo 64.2 PSD2.
[71] *Cfr.* Considerando 27 PSD2.

es interesante mencionar que los ordenantes tienen derecho a utilizar los servicios de iniciación de pagos (incluso si no existe una relación contractual entre el PISP y el PSP gestor de cuentas[72]), a menos que su cuenta de pago no sea accesible en línea[73].

Es bastante común que sea imposible recuperar los fondos de una persona que ha iniciado una operación de pago no autorizada. Es por ello por lo que es muy importante determinar quién debe responder: el usuario de los servicios de pago o el PSP.

Cabe mencionar que la PSD2 innova al determinar que, si la operación de pago se inicia a través de un PISP, será PSP gestor de cuenta el que deba reembolsar la cantidad inmediatamente y "a más tardar al final del día hábil siguiente[74]" (salvo en un caso que estudiaremos más adelante). Si finalmente es el PSP el responsable de la operación no autorizada, este deberá resarcir de inmediato al PSP gestor de cuenta, a petición de este.

1.2. Operaciones anteriores a la notificación

En la práctica, casi todos los debates versan sobre operaciones que han tenido lugar antes de la notificación de pérdida, robo o apropiación indebida del instrumento de pago (y, por tanto, han tenido lugar antes del bloqueo del instrumento de pago). El principio básico no ha cambiado en la PSD2. El ordenante es responsable, pero su responsabilidad está limitada si no ha actuado de forma fraudulenta, ni ha violado sus obligaciones *ex* artículo 69 PSD2 con negligencia grave[75]. El único cambio en el régimen básico de responsabilidad se refiere al alcance de la responsabilidad del pagador, que se reduce de 150 euros a 50 euros. Esta disminución de la responsabilidad se justifica por la necesidad de garantizar un alto nivel de protección de los consumidores. Sin embargo, dado que la responsabilidad del pagador sigue siendo ilimitada en caso de negligencia grave, los riesgos financieros para los consumidores apenas se reducen.

Dado que el pagador es responsable sin limitación alguna cuando actúa con negligencia grave en relación con las obligaciones impuestas por el artículo 69 de la PSD2, es importante centrarse brevemente en estas obligaciones.

---

[72] *Cfr.* Artículo 66.5 PSD2.
[73] *Cfr.* Artículo 66. 1 PSD2.
[74] *Cfr.* Artículo 73.2 PSD2.
[75] *Cfr.* Artículo 74.1 PSD2.

En primer lugar, el ordenante debe utilizar el instrumento de pago de acuerdo con las condiciones que rigen la emisión y el uso de un instrumento de pago, que, sin embargo, deben ser objetivas, no discriminatorias y proporcionadas[76]. El requisito de que las condiciones contractuales que determinan las obligaciones del pagador sean objetivas, no discriminatorias y proporcionadas es nuevo y reconoce explícitamente que los PSP no son completamente libres de determinar las obligaciones del pagador en las condiciones contractuales[77].

En segundo lugar, el usuario de servicios de pago debe notificar al PSP, o a la entidad especificada por éste, sin demora indebida cuando tenga conocimiento de la pérdida, el robo o la apropiación indebida del instrumento de pago[78]. En los casos en que no sea posible determinar el momento en que el usuario de los servicios de pago tuvo conocimiento de la pérdida, el robo o la apropiación indebida del instrumento de pago, debe tomarse en consideración el momento en que el ordenante debería haber tenido objetivamente conocimiento de la pérdida, el robo o la apropiación indebida .

Dado que sólo la violación de estas obligaciones con intención o negligencia grave da lugar a una responsabilidad ilimitada, la cuestión sigue siendo qué constituye una negligencia grave. El concepto de negligencia grave aún no está definido en los artículos de la PSD2. Sin embargo, el considerando 72 PSD2 proporciona una orientación adicional. Al igual que el artículo 33 PSD, dicho considerando estima que a la hora de evaluar la posible negligencia de un usuario, se deben tener en cuenta todas las circunstancias y que la presunta negligencia debe evaluarse atendiendo a las normas del país.

La novedad es que el artículo 72 PDS2 determina explícitamente que el mero incumplimiento de un deber de diligencia no constituye negligencia grave. La negligencia grave se refiere a algo más que una mera negligencia, es decir, a una conducta que presenta un grado significativo de descuido. Esta descripción de la negligencia grave coincide con la jurisprudencia de varios EEMM de la UE (por ejemplo, coincide con la jurisprudencia de Bélgica[79]). Otra novedad es que el considerando 72 PSD2 ofrece un

[76] *Cfr.* Artículo 69.1.a PSD2.
[77] *Cfr.* DONNELLY, M., "Payments in the digital market: Evaluating the contribution of Payment Services Directive II", *Computer Law & Security Review*, vol. 32, n. 6, 2016, p. 833.
[78] *Cfr.* Artículo 69.1.b PSD2.
[79] *Cfr.* MERCADO-KIERKEGAARD, S., *op. cit.*, pp. 177-187.

ejemplo de negligencia grave: "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[80]".

Por último, es importante destacar que, al igual que en la PSD, la PSD2 determina que el ordenante sólo puede ser considerado responsable, sin limitación alguna, de aquellas operaciones de pago no autorizadas que hayan sido posibles debido a la negligencia grave del ordenante. Si no existe un vínculo causal entre la negligencia grave del pagador y las operaciones no autorizadas, la responsabilidad por esas operaciones no autorizadas queda limitada a 50 euros.

Es importante destacar que el artículo 74.1 PSD2 se refiere a dos situaciones en las que el ordenante no puede ser considerado responsable de las operaciones de pago no autorizadas (ni siquiera si ha actuado con negligencia grave):

a) Cuando la pérdida, el robo o la apropiación indebida del instrumento de pago no era detectable para el ordenante antes de un pago.
b) Cuando la pérdida fue causada por actos o falta de acción de un empleado, agente o sucursal de un PSP o de una entidad a la que se subcontrataron sus actividades.

1.3. Operaciones posteriores a la notificación

En lo que respecta a las operaciones de pago no autorizadas que hayan tenido lugar después de la notificación de pérdida, robo o apropiación indebida del instrumento de pago, la PSD2 no contiene muchos cambios. El PSP sigue siendo responsable de todas las operaciones que hayan tenido lugar, una vez notificada la pérdida, el robo o la apropiación indebida del instrumento de pago (excepto cuando el propio ordenante haya actuado de forma fraudulenta)[81]. Además, el PSP debe asegurarse de que el ordenante pueda notificar la pérdida, el robo o la apropiación indebida en cualquier momento del día[82]. Si no existe tal posibilidad, el ordenante no puede ser considerado responsable de

[80] Como apuntar el PIN en una nota que se guarda junto con el instrumento de pago, por ejemplo. Otro ejemplo podría ser el caso en el que el pagador dejara el instrumento de pago en un lugar fácilmente accesible para terceros o el pagador introdujera un PIN o una contraseña a sabiendas de que una tercera persona le estaba espiando. Sin embargo, el mero hecho de que otra persona haya podido averiguar la contraseña o el PIN (por ejemplo, espiando el PIN), no es suficiente para constituir una negligencia extrema, dado que la negligencia grave requiere algo más que una simple negligencia.
[81] *Cfr.* Artículo 74. 3 PSD2.
[82] *Cfr.* Artículo 70.1.c PSD2.

ninguna operación no autorizada excepto cuando haya actuado de forma fraudulenta[83]. La única innovación de la PSD2 se refiere al hecho de que el ordenante debe poder notificar gratuitamente la pérdida, el robo o la apropiación indebida y cobrar, si acaso, únicamente los costes de sustitución directamente imputables al instrumento de pago[84].

2. INCORPORACIÓN DEL CONCEPTO DE AUTENTICACIÓN REFORZADA DE CLIENTES EN LA PSD2

Como hemos expuesto *supra*, una de las principales novedades de la PSD2 es la reducción de la responsabilidad del ordenante de 150 a 50 euros en caso de operaciones no autorizadas. No obstante, el último párrafo del artículo 74.1 PSD2 puntualiza que, en caso de que el ordenante no haya actuado de forma fraudulenta o con negligencia grave, los EEMM podrán reducir esta responsabilidad atendiendo a la naturaleza de las credenciales de seguridad personalizadas por el instrumento de pago y las circunstancias específicas de la pérdida, robo o apropiación indebida de dicho instrumento.

Además, si el PSP no exige una SCA, el ordenante sólo soportará las consecuencias económicas en caso de haber actuado de forma fraudulenta[85].

El concepto de SCA aparece por primera vez en la PSD2. Por su parte, la PSD sólo hacía referencia al concepto de autenticación al establecer que, cuando un usuario negara haber autorizado una operación de pago o afirmara que se había ejecutado de manera incorrecta, el PSP debía demostrar que la operación había sido autenticada, registrada con exactitud y contabilizada[86]. Además, el artículo 4.19 PSD definía el concepto de autenticación como un procedimiento que permite al PSP comprobar la utilización de un instrumento de pago específico.

[83] *Cfr.* Artículo 74. 3 PSD2.
[84] *Cfr.* Artículo 70.1.d PSD2.
[85] *Cfr.* Artículo 74.2 PSD2.
[86] *Cfr.* Artículo 59.1 PSD.

2.1. Definición del concepto de autenticación en la PSD2 y diferencias con el concepto de autenticación reforzada de clientes

La PSD2 define el concepto de *autenticación* como "el procedimiento que permita al proveedor de servicios de pago comprobar la identidad del usuario de un servicio de pago o la validez de la utilización de determinado instrumento de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario[87]". A su vez, la propia PSD2 define el concepto de *credenciales de seguridad personalizadas* como aquellos "elementos personalizados que el proveedor de servicios de pago proporciona al usuario de servicios de pago a efectos de autenticación[88]".

Cabe mencionar que la PSD2 realiza una diferencia entre los conceptos de *autenticación* y *autenticación reforzada de clientes*, definiendo la segunda idea como "la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario[89]), posesión (algo que solo posee el usuario[90]) e inherencia (algo que es el usuario[91]), que son independientes —es decir, que la vulneración de uno no compromete la fiabilidad de los demás—, y concebida de manera que se proteja la confidencialidad de los datos de autenticación[92]".

2.2. Requisitos para que una autenticación adquiera el carácter de reforzada

Como señalamos *supra*, la PSD2 exige que la ABE elabore directrices y proyectos de normas técnicas en determinadas situaciones[93]. Así, en su artículo 98.1.a, establece la posibilidad de que la ABE desarrolle, "en estrecha cooperación con el BCE y tras consultar a todas las partes interesadas pertinentes, incluidas las del mercado de servicios de pago", un proyecto de normas técnicas de regulación sobre los requisitos de la SCA. No obstante, dicho proyecto se encuentra en desarrollo, por lo que actualmente sólo contamos con el Informe Final del Proyecto de Normas Técnicas de Regulación sobre

[87] Artículo 4.29 PSD2.
[88] Artículo 4.31 PSD2.
[89] Como un PIN o una contraseña.
[90] Como una tarjeta de pago o un *token.*
[91] Como una huella dactilar, el escaneo del iris o el reconocimiento de facial.
[92] Artículo 4.30 PSD2.
[93] *Vid.* Novedades incorporadas por la PSD2 para superar las dificultades de la PSD, p. 19.

Autenticación Reforzada de Clientes y comunicación común y segura bajo el artículo 98 de la Directiva (UE) 2015/2366[94][95].

Dicho Informe determina los requisitos para que una autenticación adquiera el carácter de "reforzada" en su Capítulo 2, referido a las medidas de seguridad para la aplicación de la SCA[96].

Según este, la autenticación basada en dos o más elementos clasificados como conocimiento, posesión e inherencia, dará lugar a la generación de un código de autenticación, que será aceptado una sola vez por el PSP cuando el ordenante lo utilice. En relación con este código, el artículo 4 del Informe establece que los PSP deberán adoptar medidas de seguridad que garanticen que:

a) Ninguna información pueda derivarse de la divulgación del código de autenticación.
b) No sea posible generar un nuevo código de autenticación basado en el conocimiento de cualquier otro código de autenticación generado previamente.
c) El código de autenticación no pueda ser falsificado.
d) Ninguno de los elementos categorizados como conocimiento, posesión e inherencia puedan ser identificados como incorrectos.
e) El número de intentos de autenticación fallidos que bloqueen de forma temporal o permanente las acciones a que se refiere el artículo 97.1, letras a), b) y c) PSD2 nunca sea superior a cinco.
f) Las comunicaciones estén protegidas de tal forma que no puedan capturarse datos relativo a la autenticación.
g) El tiempo máximo sin actividad después de que el pagador haya sido autenticado no sea superior a cinco minutos.

Además, el artículo 5 del Informe determina que los PSP deben adoptar medidas de seguridad que permitan al ordenante conocer el importe de la operación de pago y el beneficiario, y que el código de autenticación generado y aceptado sea específico para el

---

[94] EBA, "Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)", *European Banking Authority*, 2017 (disponible en https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf?retry=1; última consulta 10/02/2022).
[95] Traducción realizada por la autora.
[96] *Cfr. Ibidem,* pp. 20-22.

importe de la operación de pago. Es decir, cualquier cambio en el importe o en el beneficiario debe dar lugar a la invalidación del código de autenticación generado.

Todas estas medidas deben garantizar la confidencialidad, autenticidad e integridad del montante de la operación, del beneficiario de esta y de la información que se muestra al pagador en las fases de autenticación.

Por su parte, el artículo 6 del Informe obliga a los PSP a adoptar medidas que mitiguen el riesgo de que los elementos de la SCA sean descubiertos o revelados a partes no autorizadas y a los ordenantes a evitar la divulgación de estos elementos.

Como mencionamos *supra*, el artículo 4.30 PSD2 determina que los elementos categorizados como conocimiento, posesión e inherencia sean independientes. Así, el Informe puntualiza, en su artículo 9, que los PSP garanticen que el uso de los elementos de SCA esté sujeto a medidas que aseguren que el incumplimiento de uno de los elementos no comprometa la fiabilidad de los demás.

Como consecuencia, cuando un usuario realice una compra por Internet, se le podrán exigir dos de los siguientes tres tipos de requisitos: (a) una contraseña o PIN[97], (b) un mensaje que se recibirá en el móvil del usuario, y/o (c) la huella dactilar o reconocimiento facial[98].

Así, por ejemplo, las operaciones realizadas con tarjeta de crédito en Internet que requieren que el titular de la tarjeta introduzca el número de tarjeta, fecha de caducidad y código de verificación, así como un código de autenticación generado por la introducción de estos datos y que el usuario suele recibir a través de un mensaje en el móvil, implican una SCA. Por el contrario, una operación que no requiere dicho código de autenticación, no implica una SCA.

En caso de que el PSP no cumpla estos requisitos y, por lo tanto, no aplique una SCA, el ordenante sólo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta[99].

---

[97] Según la definición de la RAE, un PIN es una contraseña alfanumérica utilizada en algunos aparatos o dispositivos electrónicos.
[98] *Cfr.* IBERLEY, "Entrada en vigor de las nuevas formas de pago por internet", *Iberley Noticias*, 2019 (disponible en https://www.iberley.es/noticias/entrada-vigor-nuevas-formas-pago-internet-29778; última consulta 15/03/2022).
[99] *Cfr.* Artículo 74.2 PSD2.

2.3. Exenciones a la autenticación reforzada de clientes

El mismo artículo 98.1.b PSD2, también encarga a la ABE especificar las exenciones de la aplicación del artículo 97, apartados 1, 2 y 3, referidos a la aplicación de la SCA por los PSP, la iniciación de operaciones de pago electrónico y la seguridad de las operaciones realizadas por PSP.

Siguiendo estas líneas, la ABE ha propuesto varias exenciones al requisito de SCA en el mismo Informe. Según la ABE, se trata de exenciones restringidas con umbrales claros e inequívocos basados en criterios objetivos y verificables, ya que la autenticación segura del cliente debe seguir siendo el principio básico[100].

La primera exención se encuentra en el artículo 10 del Informe y se refiere la información de la cuenta de pago. Según este, los PSP están exentos de aplicar una SCA cuando el usuario de los servicios de pago se limita a acceder al saldo de una o más cuentas de pago o a las operaciones de pago ejecutadas en los últimos 90 días a través de una o más cuentas designadas, siempre y cuando no se revelen datos de pago confidenciales.

La segunda exención está relacionada con los pagos sin contacto en los puntos de venta (en los que el pagador y el beneficiario están presentes de forma simultánea). Según el artículo 11 del Informe, este tipo de pagos no necesita una SCA si el importe individual de la operación es inferior a 50 euros y el importe acumulado o el número de operaciones de pago electrónico iniciadas con anterioridad no exceda, respectivamente, de 150 euros o de 5 operaciones de pago individuales consecutivas.

El artículo 12 del informe deja exentas aquellas operaciones que se realizan a través de un terminal de pago no atendido (p. ej. Parquímetro) con el objetivo de pagar una tasa de transporte o de aparcamiento.

Por su parte, el artículo 13 deja exentas aquellas operaciones de pago iniciadas por el ordenante en las que el beneficiario esté incluido en una lista de beneficiarios de confianza previamente creada o confirmada por el ordenante a través de su PSP de confianza, así como una serie de operaciones de pago con el mismo importe y el mismo beneficiario iniciadas por el ordenante, siempre que la SCA se haya utilizado cuando se inició el primer pago de esa serie.

---

[100] *Cfr.* EBA, *op. cit.* pp. 9, 23-28.

El artículo 14 exime de una SCA aquellas transferencias en las que el ordenante y el beneficiario sean la misma persona y ambos sean titulares de cuentas de pago en el mismo PSP gestor de cuentas.

También quedan exentas las operaciones de pago electrónico a distancia iniciadas por el ordenante, siempre que el importe de la operación no exceda de 30 euros y que el importe acumulado o el número de operaciones de pago electrónico a distancia anteriores iniciadas por el ordenante desde la última aplicación de la SCA no exceda, respectivamente, de 100 euros o de 5 operaciones de pago electrónico a distancia individuales consecutivas, según el artículo 15 del informe.

Por último, el artículo 16 exime a las operaciones de pago electrónico a distancia identificadas por el PSP como de bajo nivel de riesgo según sus mecanismos de supervisión de operaciones[101], siempre que se cumplan varios requisitos estrictos y detallados, que deben garantizar que existe realmente un bajo nivel de riesgo. Estos requisitos implican, entre otros:

a) Que el importe de la operación de pago electrónico no supere el "valor umbral de exención" correspondiente al índice de fraude del PSP.
b) Que el importe de la operación no supere los 500 euros.
c) Que los mecanismos de supervisión de operaciones del PSP le permitan realizar un análisis de riesgo en tiempo real de la operación de pago electrónico.
d) Que no se haya identificado ningún patrón de gasto o comportamiento anormal del ordenante.
e) Que no se haya identificado ninguna información inusual sobre el acceso al vicio/software del ordenante.
f) Que no se haya identificado ninguna infección de malware en ninguna sesión del procedimiento de autentificación.
g) Que no se haya identificado ningún escenario de fraude conocido en la prestación de servicios de pago.

[101] El artículo 2 del mismo Informe obliga a los PSP a contar con mecanismos de supervisión de operaciones con el objetivo de que puedan detectar operaciones de pago no autorizadas o fraudulentas. Estos mecanismos deben basarse en el análisis de las operaciones de pago teniendo en cuenta los elementos propios de un usuario de servicios de pago y el uso normal por parte de este de credenciales de seguridad personalizadas. Además, deberán tener en cuenta aquellos elementos de autenticación que hayan sido comprometidos o robados, el montante de cada operación de pago, escenarios de fraude conocidos en la prestación de servicios de pago y signos de infección de *malware.*

h) Que la ubicación del pagador no sea anormal.
i) Que la ubicación del beneficiario no se identifique como de alto riesgo.
j) Que la tasa de fraude global del PSP no supere un determinado porcentaje determinado en las normas técnicas reglamentarias propuestas.

3. DETERMINACIÓN DE SUJETO SOBRE EL QUE RECAE LA CARGA DE LA PRUEBA

El artículo 72 PSD2 trata de la carga de la prueba y repite en gran medida las normas incorporadas en el artículo 59 PSD. Así, la PSD2 determina que si un usuario de servicios de pago niega haber autorizado una operación o considera que se ha realizado de forma incorrecta, los EEMM deberán exigir que sea el proveedor el que deba demostrar que sí hubo autenticación, registro y contabilización. Además, el proveedor deberá demostrar que no hubo fallo técnico en la operación o deficiencia del servicio[102].

Esta afirmación que deja claro que una mera presunción de negligencia grave no puede, en ningún caso, ser suficiente para responsabilizar al pagador de forma automática. En otras palabras, el mero hecho de que otra persona haya tenido la oportunidad de utilizar el instrumento de pago y haya podido averiguar las credenciales de seguridad personalizadas del pagador, no probará, en ningún caso, una negligencia grave. Siempre serán necesarias otras pruebas de apoyo para responsabilizar al pagador sin ninguna limitación.

El artículo 72 PSD2 determina en este contexto que, cuando el instrumento de pago no está presente en el punto de venta, como en el caso de los pagos electrónicos, es conveniente que el PSP esté obligado a aportar pruebas de la supuesta negligencia, ya que los medios del ordenante para hacerlo son muy limitados en estos casos. Las condiciones contractuales cuyo efecto sea aumentar la carga de la prueba sobre el consumidor o reducir la carga de la prueba sobre el emisor deben considerarse nulas y sin efecto.

[102] *Cfr.* Artículo 72.1 PSD2.

4. REGLAS ESPECIALES PARA LOS PAGOS DE BAJO VALOR

El artículo 63 PSD2 determina que ciertas normas que establecen la responsabilidad por las operaciones de pago no autorizadas pueden ser objeto de excepción por contrato para los instrumentos de pago de bajo valor y el dinero electrónico (al menos si se cumplen ciertas condiciones). Es de esperar que los PSP utilicen a menudo estas exclusiones en sus contratos de duración estándar.

Los instrumentos de pago de bajo valor son instrumentos que no permiten operaciones de pago individuales que superen los 30 euros y que tienen un límite de gasto de 150 euros o almacenan fondos que no superan los 150 euros en ningún momento[103]. Si los instrumentos de pago de bajo valor no permiten su bloqueo o la prevención de su uso posterior, el PSP no debe garantizar que se disponga de medios adecuados que permitan al titular del instrumento notificar el robo, la pérdida o la propiedad indebida del mismo. Además, el PSP no puede ser considerado responsable de las operaciones que se realicen después de la notificación de la pérdida o el robo del instrumento. Si el instrumento de pago se utiliza de forma anónima o el PSP no está en condiciones, por otras razones intrínsecas al instrumento de pago, de demostrar que una operación ha sido autorizada, el PSP no estará obligado a demostrar que las operaciones han sido autorizadas. Tampoco podrá ser considerado responsable de las operaciones no autorizadas. Los artículos 73 y 74 PSD2, que asignan la responsabilidad de las operaciones de pago no autorizadas, no se aplican al dinero electrónico cuando el PSP del ordenante no tiene la capacidad de congelar la cuenta de pago en la que está almacenado el dinero electrónico o bloquear el instrumento de pago.

[103] *Cfr.* Artículo 63.1 PSD2.

CAPÍTULO III. EFECTOS DE LA PSD2 EN ESPAÑA

1. TRANSPOSICIÓN DE LA PSD2 AL ORDENAMIENTO JURÍDICO ESPAÑOL

1.1. Normas que transpusieron la PSD y la PSD2

La ya derogada Ley 16/2009, de 13 de noviembre, de servicios de pago fue la que introdujo principalmente la PSD en el OJ nacional[104][105]. Esta trató, entre otras cosas, de "establecer normas comunes, como mejor sistema para ofrecer seguridad jurídica, tanto en el ámbito nacional como en el transfronterizo, toda vez que son uniformes las condiciones y los requisitos de información aplicables a los servicios de pago, así como establecer un sistema común de derechos y obligaciones para proveedores y para usuarios en relación con la prestación y utilización de los servicios de pago[106]", con el principal objetivo de lograr una mayor eficiencia de los mercados. Para ello, estableció un régimen de responsabilidad para PSP en caso de que se realizara una operación de pago no autorizada.

La transposición de la PSD2 se ha realizado a través del Real Decreto-Ley 19/2018[107], del Real Decreto 736/2019[108] y de la Orden ECE/1263/2019[109][110]. La transposición de la

---

[104] *Cfr.* UNIÓN EUROPEA, "Medidas nacionales de transposición comunicadas por los Estados miembros relativas a la Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007 , sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE (Texto pertinente a efectos del EEE)", *EUR-Lex* (disponible en https://eur-lex.europa.eu/legal-content/ES/NIM/?uri=CELEX:32007L0064; última consulta 03/04/2022).

[105] La transposición de la PSD también se realizó a través de la Corrección de errores de la Ley 16/2009, de 13 de noviembre, de servicios de pago, el Real Decreto 712/2010, de 28 de mayo, de régimen jurídico de los servicios de pago y de las entidades de pago y la Orden EHA/1608/2010, de 14 de junio, sobre transparencia de las condiciones y requisitos de información aplicables a los servicios de pago.

[106] *Cfr.* Exposición de motivos de la Ley 16/2009, de 13 de noviembre, de servicios de pago («BOE» núm. 275, de 14/11/2009).

[107] Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera («BOE» núm. 284, de 24/11/2018).

[108] Real Decreto 736/2019, de 20 de diciembre, de régimen jurídico de los servicios de pago y de las entidades de pago y por el que se modifican el Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico, y el Real Decreto 84/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito («BOE» núm. 308, de 24/12/2019).

[109] Orden ECE/1263/2019, de 26 de diciembre, sobre transparencia de las condiciones y requisitos de información aplicables a los servicios de pago y por la que se modifica la Orden ECO/734/2004, de 11 de marzo, sobre los departamentos y servicios de atención al cliente y el defensor del cliente de las entidades financieras, y la Orden EHA/2899/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios («BOE» núm. 313, de 30/12/2019).

[110] *Cfr.* UNIÓN EUROPEA, "Medidas nacionales de transposición comunicadas por los Estados miembros relativas a la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE

normativa europea a nuestro OJ permite (a) mejorar la protección de los usuarios e inversores del mercado de servicios de pago, (b) incrementar la eficacia de su marco normativo[111], (c) adaptar la regulación a los nuevos cambios tecnológicos, y (d) permitir la oferta de servicios innovadores[112].

Cabe mencionar que el mayor trabajo de transposición se ha hecho a través del Real Decreto-Ley 19/2018, una norma que emana del poder ejecutivo y no del poder legislativo. Es decir, nos encontramos ante una norma que no se ha tramitado en las Cortes Generales debido a su extraordinaria y urgente necesidad[113]. La razón por la que la PSD2 se ha tramitado principalmente a través de un Real Decreto-Ley puede deberse a que la tramitación de la PSD2 se realizó después del 13 de enero de 2018, fecha límite para su transposición[114].

1.2. Principales diferencias entre la PSD2 y el Real Decreto-Ley 19/2018 en materia de responsabilidad

Antes de mencionar las principales diferencias entre una y otra norma, cabe mencionar que el artículo 107 PSD2 establece una armonización total, lo que implica que los EEMM no pueden, en general, mantener o introducir normas en su legislación nacional que ofrezcan una protección adicional a los PSP. Por el contrario, estos pueden reducir aún más la responsabilidad del ordenante que no haya actuado de forma fraudulenta o haya incumplido sus obligaciones intencionadamente[115][116].

Esto, unido a la extraordinaria y urgente necesidad, y salvo en dos excepciones[117], ha provocado que la transposición de la PSD2 haya sido prácticamente literal, no

(Texto pertinente a efectos del EEE)", *EUR-Lex* (disponible en https://eur-lex.europa.eu/legal-content/ES/NIM/?uri=celex:32015L2366; última consulta 03/04/2022).

[111] *Cfr*. CEF CIVIL MERCANTIL, "Real Decreto-Ley de servicios de pago y otras medidas urgentes en materia financiera", *Centro de Estudios Financieros*, 16 de noviembre de 2018 (disponible en https://www.civil-mercantil.com/19-2018-servicio-de-pago.html; última consulta 15/03/2022).

[112] *Cfr*. FUNDACIÓN BBVA MICROFIANZAS, "Servicios de pago y medidas urgentes en materia financiera", *Revista de actualidad jurídica para la inclusión y el desarrollo social*, n. 17, 2018 (disponible en https://www.fundacionmicrofinanzasbbva.org/revistaprogreso/servicios-pago-medidas-urgentes-materia-financiera/; última consulta 15/03/2022).

[113] Artículo 86 de la Constitución Española («BOE» núm. 311, de 29/12/1978).

[114] Artículo 115 PSD2.

[115] Teniendo en cuenta, en particular, la naturaleza de las credenciales de seguridad personalizadas y las circunstancias específicas en las que el instrumento de pago se haya perdido, haya sido robado o se haya sustraído.

[116] Artículo 74.1 PSD2.

[117] Los contratos marco y el *ius variandi.*

adaptándose su contenido a la normativa nacional. Como consecuencia, algunas disposiciones del Real Decreto-Ley 19/2018 resultan contradictorias con respecto de otras normas del OJ español[118].

Respecto al tema que nos atañe: el aumento de la seguridad y la reducción de la responsabilidad del ordenante por los pagos no autorizados, el Real Decreto-Ley 19/2018 ha incorporado el concepto de SCA, "en la forma, con el contenido y con las excepciones previstas en la correspondiente norma técnica aprobada por la Comisión Europea[119], cuando el ordenante acceda a su cuenta de pago en línea, inicie una operación de pago electrónico o realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos[120121]".

Además, el Real Decreto-Ley 19/2018 ha variado el significado de *autenticación reforzada de clientes* cambiando una sola palabra pero que provoca ciertos problemas interpretativos[122].

Si acudimos al artículo 4.30 PDS2 y al artículo 3.5 del Real Decreto-Ley 19/2018, podemos comprobar que la norma estatal sólo varía un concepto de la definición original: cambia la palabra autenticación por identificación. Como señala Fernando Zunzunegui, "se trata de una transposición incorrecta que crea inseguridad jurídica pues los «datos de autentificación» no coinciden con los «datos de identificación. El artículo 98 PSD2 diferencia entre «identificación» y «autenticación». La autenticación utiliza medios de identificación electrónica. Comprende un proceso de identificación y comunicación con los usuarios. En dicho proceso, los PSP deben garantizar la identificación segura en las comunicaciones entre el dispositivo del ordenante y los dispositivos de aceptación del beneficiario. En suma los «datos de autenticación» comprenden los «datos de

---

[118] *Cfr.* ZUNZUNEGUI, F., "Luces y Sombras de la Transposición de la Directiva de Servicios de Pagos (PSD2)", *Revista de Derecho Bancario y Bursátil*, n. 159, 2020, p. 92.

[119] Como consecuencia, la CE aprobó el Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros («DOUE» núm. 69, de 13 de marzo de 2018, páginas 23 a 43).

[120] Artículo 68.1 Real Decreto-ley 19/2018.

[121] Como podemos comprobar, la redacción es prácticamente idéntica a la que nos brinda el artículo 97.1 PSD2, lo que es una muestra más de la transposición casi literal de la PSD2 al Ordenamiento interno.

[122] *Cfr.* ZUNZUNEGUI, F., *op. cit.*, pp. 104-105.

identificación», pero también otros como las credenciales de seguridad personalizadas que se transmiten al usuario"[123].

El deber de los PSP de aplicar la SCA se ha recogido, en el artículo 68 del Real Decreto-Ley 19/2018.

2. JURISPRUDENCIA SOBRE LA RESPONSABILIDAD DEL PROVEEDOR DE SERVICIOS DE PAGO

La jurisprudencia sobre la responsabilidad del PSP en España es bastante escasa, sobre todo en relación con el nuevo Real Decreto-Ley 19/2018, ya que la mayor parte de los casos se produjeron durante la vigencia de la antigua Ley 16/2009. Sin embargo, los tribunales tienden a inspirarse en esta nueva regulación para decidir el fallo de su sentencia.

2.1. STS 332/2020, de 12 de febrero

La STS 332/2020[124] trata la posible responsabilidad de la entidad bancaria CaixaBank por no haber activado unos mecanismos suficientes que evitaran fisuras en su sistema de seguridad.

Según los antecedentes de hecho, el acusado, aprovechando su posición de arrendatario y su amistad con la parte demandante, consiguió hacerse con las llaves de su casa. Una vez hubo accedido a la vivienda, se hizo con las claves y contraseñas de la tarjeta de crédito y del *router* de la demandante. Gracias a esta información, pudo realizar dos transferencias bancarias, una de 598 euros y otra de 2.300 euros, los días 7 y 10 de julio, respectivamente.

Cabe mencionar que el acusado simuló el reintegro de dichas cantidades mediante transferencia bancaria. No obstante, el sobre que debía incluir el dinero se encontraba vacío y el sistema de seguridad de la entidad no detectó este defecto hasta 24 horas después del supuesto ingreso.

[123] *Ibidem*, p. 8.
[124] Sentencia del Tribunal Supremo núm. 332/2020, de 12 de febrero.

En este caso concreto, vamos a centrarnos en la responsabilidad de la entidad bancaria, sin entrar a conocer si el acusado fue finalmente condenado por un delito de estafa o no.

El recurso interpuesto por CaixaBank se basa en su discrepancia por haber sido condenada como responsable civil subsidiaria *ex* artículo 120.3 CP.

La sentencia afirma que la actividad bancaria mediante la operativa *online* presenta algunos riesgos relativos a la posible suplantación de identidad de quien contrata con la entidad. Es por ello por lo que la entidad bancaria debe ofrecer y poner en práctica un sistema seguro, "de manera que las consecuencias negativas de los fallos en el mismo no deberán ser trasladados al cliente[125]".

Durante el transcurso de los hechos, se encontraba en vigor la Ley 16/2009, de 13 de noviembre que, como ya sabemos, incorporó la PSD al OJ Español. Con el objetivo de promover un entorno que propicie el ágil desarrollo de las operaciones de pago, esta ley introdujo un capítulo sobre los riesgos operativos y de seguridad de los PSP.

Así, la Ley 16/2009 introdujo un régimen de responsabilidad del PSP en los casos de operaciones no autorizadas que obliga al PSP a devolver de forma inmediata el importe de una operación no autorizada.

Como ya mencionamos *supra*, la PSD2 sustituyó a la PSD y fue transpuesta parcialmente por el Real Decreto-ley 19/2018. La PSD2 establece normas exhaustivas para los servicios de pago, con el objetivo de lograr un marco armonizado para la prestación de servicios de pago en el EEE y un mayor nivel de protección de los consumidores de estos servicios[126].

Analizando ambas directivas, así como la tendencia de la legislación en los pagos electrónicos, la sentencia considera que CaixaBank contaba con un deber objetivo de cuidado como PSP y, por lo tanto, la considera responsable por los daños causados.

[125] STS 332/2020, de 12 de febrero, Fundamento Jurídico Tercero.
[126] *Cfr.* OFICINA DE PUBLICACIONES DE LA UNIÓN EUROPEA, "Normas revisadas sobre servicios…", *op. cit.*

2.2. SAP de Madrid 293/2019, de 2 de julio

En esta sentencia[127], la AP de Madrid analiza la posible responsabilidad de la entidad bancaria BBVA por los perjuicios causado a la demandante.

Los antecedentes de hecho de la SAP de Madrid 293/019 afirman que la parte demandante era titular de una cuenta bancaria en el BBVA.

Entre el 23 y 30 de noviembre de 2016, se produjeron varios movimientos anómalos en esta cuenta, produciendo un perjuicio de 28.894,21 euros a la demandante.

La parte demandante considera que el BBVA tuvo una actitud negligente a la hora de evitar que se produjera un fraude en el uso por terceros de su tarjeta de crédito, asociada a la cuenta de la que se sustrajo el dinero.

La actuación del demandado es más compleja que la simple utilización de una tarjeta de crédito. Éste realizó varias extracciones en cajeros por encima del límite de 600 euros diarios. Además, realizó diversos traspasos de dinero y varias compras utilizando la misma tarjeta de crédito.

Para la resolución de este caso, la sentencia alude a los artículos 27, 28, 29, 30, 31 y 32 de la Ley 16/2009, que es la que estaba en vigor durante el transcurso de los hechos. No obstante, también menciona los artículos 41 a 46 del Real Decreto-ley 19/2018 como inspiración para resolver el caso.

Tras un análisis de toda esta normativa, la AP de Madrid concluye que no hubo demora indebida por parte de la demandante a la hora de notificar la sustracción de la tarjeta de crédito al BBVA. De hecho, la demandante procedió al bloqueo de la tarjeta en cuanto fue consciente de la actividad irregular. Además, denunció los hechos al día siguiente. Además, queda probado que las operaciones no fueron autorizadas y que la demandante ni actuó de forma fraudulenta ni con negligencia grave.

Por todo ello, la AP de Madrid considera que la entidad bancaria debe asumir el perjuicio económico causado a la parte demandante.

[127] Sentencia de la Audiencia Provincial de Madrid núm. 293/2019, de 2 de julio.

3. EFECTOS DE LA TRANSPOSICIÓN DE LA PSD2 SOBRE LAS EMPRESAS Y ENTIDADES BANCARIAS NACIONALES

3.1. Proceso de adaptación de las entidades bancarias a la PSD2

3.1.1. Principales retos de las entidades bancarias tradicionales ante la entrada en vigor de la PSD2: la amenaza de nuevos competidores

La entrada en vigor de la PSD2 constituye una amenaza para los operadores tradicionales de pagos, ya que provoca una erosión del volumen de operaciones, ingresos y fidelidad de los clientes. Esto se debe a que la PSD2 permite el nacimiento de nuevos PSP muy competitivos. Además, la PSD2 facilita que numerosas *FinTech* compitan con las empresas de servicios financieros tradicionales en la oferta de servicios de financiación.

El número de empresas *PayTech* no bancarias en la UE ha ido creciendo en los últimos años. Un gran aumento se produjo en 2018, año en el que la mayoría de los países del EEE llevaron a cabo la transposición de la PSD2[128].

A finales de 2019, casi el 75% de todas las licencias se concedieron a entidades que se habían establecido antes de la adopción de esta normativa a nivel de la UE. Por lo tanto, solo alrededor de una cuarta parte de todas las nuevas licencias de *PayTech* estaban asociadas a nuevas incorporaciones y pueden relacionarse directamente con el estímulo del espíritu empresarial por parte de la PSD2. Curiosamente, la gran mayoría de estas nuevas empresas *PayTech* se fundaron en el período anterior a las transposiciones nacionales de la PSD2. Esto puede sugerir una anticipación por parte de numerosos inversores del sector de las tecnologías de pago a los cambios normativos. Después de las transposiciones nacionales de la PSD2, el impulso para establecer nuevas entidades *PayTech* se ralentizó[129].

Como ya comentamos *supra*[130], la PSD2 exige que estos nuevos competidores cumplan con las mismas normas que los PSP tradicionales cuando se hayan iniciado operaciones no autorizadas.

---

[128] *Vid.* UNIÓN EUROPEA, "Medidas nacionales de transposición …", *op. cit.*
[129] *Cfr.* POLASIK, M., HUTERSKA, A., IFTIKHAR, R. Y MIKULA, S., *op. cit.*, pp. 385-401.
[130] *Vid.* Operaciones de pago no autorizadas: principales características y dificultades, p. 25.

3.1.2. Oportunidades clave para las entidades bancarias tradicionales

La PSD2 es parte de una tendencia mundial en la regulación bancaria que se centra en la seguridad, la innovación y la competencia en el mercado[131]. La mayoría de los ejecutivos bancarios están atentos a la amenaza que la PSD2 puede suponer. No obstante, también exploran oportunidades de negocio innovadoras y potencialmente lucrativas. De hecho, numerosos bancos han afirmado estar trabajando en varios escenarios para poder aprovechar las oportunidades de negocio que ofrece la PSD2[132].

Además, es importante que estos analicen la posibilidad de aliarse con socios tecnológicos que puedan ayudarles a flexibilizar y dinamizar la arquitectura de sus tecnologías, así como a escalar rápidamente en este sector. En el marco de la seguridad de los pagos, es importante mencionar que una tecnología flexible es esencial para actualizar las herramientas de prevención del fraude y cumplir con los continuos cambios normativos[133].

Cabe mencionar que, a pesar de que los bancos tradicionales cuentan con una ventaja capital: una larga trayectoria que les ha permitido ganarse la confianza de los clientes, si estos no mejoran el implementan novedosos controles y herramientas que permitan detectar y evitar riesgos de fraude, podrían perder su papel protagonista como principales PSP.

Por ello, muchos bancos ya están tratando de liderar el mercado de pagos electrónicos incorporando las nuevas normas introducidas por la PSD2. De hecho, muchos ejecutivos afirman que el cumplimiento de la PSD2 es una parte esencial en la transformación digital que están desarrollando[134].

Es decir, aunque la PSD2 plantea importantes retos para las entidades bancarias, también brinda importantes oportunidades de negocio siempre y cuando sean capaces de adaptar sus estructuras y tecnologías a las exigencias de seguridad introducidas por la PSD2.

---

[131] *Cfr*. BOTTA, A. *ET AL.*, "PSD2: Taking advantage of open-banking disruption", *Global Banking Practice*, 2018, p. 1 (disponible en https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption#; última consulta 03/04/2022).
[132] *Ibidem*, pp. 1-2.
[133] *Ibidem*, pp. 2-3.
[134] *Ibidem*, p. 7.

3.1.3. Interfaces de Programación de Aplicaciones: Bizum

Gracias a la legislación europea sobre los servicios de pago, se hizo posible el nacimiento de APIs[135] como *Bizum*.

Bizum es un PSP español que surgió como fruto de la iniciativa de la banca española. Como hemos estudiado *supra*, la llegada de la PSD2 supuso la aparición de potenciales amenazas y oportunidades para las entidades bancarias tradicionales. Así, *Bizum* es un claro ejemplo del intento de los bancos españoles de adaptarse a las nuevas condiciones del mercado con el objetivo de no perder competitividad.

Actualmente son 28 los bancos que respaldan esta iniciativa[136]. *Bizum* ofrece un método de pago instantáneo de cuenta a cuenta[137], por lo que gracias a ella los particulares pueden tanto enviar dinero como realizar compras *online* a través de su teléfono móvil.

Como podemos comprobar, *Bizum* cae bajo el ámbito de aplicación de la PSD2 sobre servicios de pago y, por ello, se ve obligada a cumplir con los requisitos de SCA. Así, *Bizum* obliga a sus clientes a utilizar al menos dos de los tres tipo de factores de autenticación exigidos por la PSD2 y por el Informe de la ABE[138][139]: un teléfono móvil, una contraseña o código PIN y una huella dactilar o reconocimiento facial.

El objetivo es reducir el fraude, protegiendo al máximo tanto el envío de dinero como las compras *online* de sus clientes. Para ello, además, *Bizum* no sólo está obligado a cumplir con los requisitos de SCA, sino también a comunicar periódicamente los datos de fraude, con el objetivo de que la autoridad competente pueda llevar a cabo un seguimiento[140].

---

[135] *Cfr.* BBVA, "Todo lo que hay que saber de la PSD2", *Regulación Financiera*, 17 de octubre de 2019 (disponible en https://www.bbva.com/es/lo-saber-la-psd2/#:~:text=PSD2%20es%20una%20regulaci%C3%B3n%20europea,bancarios%20a%20las%20nuevas%20tecnolog%C3%ADas; última consulta 15/03/2022).

[136] Según la página oficial de *Bizum*, los bancos que colaboran con este proveedor de pagos son: CaixaBank, Santander, BBVA, Sabadell, Unicaja Banco, Kutxabank, Caja Rural, iberCaja, Grupo Cooperativo Cajamar, Abanca, Bankinter, Laboral Kutxa, EVO, BancaMarch, Eurocaja Rural, Caja de Ingenieros, Banca Pueyo, Banco Mediolanum, Cajalmentralejo, Arquia Banca, Banco Caminos, Caixa Guissona, Caixa Ontinyent, Cajasur, Deutsche Bank, Imagin, ING, Liberbank, Openbank, Orange Bank y Targo Bank.

[137] *Cfr.* BIZUM, "Elige "Pagar con Bizum" en tus compras online", *Bizum Web*, 2020 (disponible en https://bizum.es/pagar-compra-online/; última consulta 13/02/2022).

[138] *Vid.* Requisitos para que una autenticación adquiera el carácter de reforzada, p. 29.

[139] *Cfr.* BIZUM, "Bizum nació cumpliendo la PSD2, la normativa europea de seguridad de pago en eCommerce", *Bizum Blog*, 21 de diciembre de 2020 (disponible en https://bizum.es/blog/normativa-psd2-seguridad-pago-ecommerce/; última consulta 13/02/2022).

[140] *Cfr.* BANCO DE ESPAÑA, "Guía del Proceso de Comunicación de Datos de Fraude bajo la PSD2", *Banco de España Eurosistema*, 2020 (disponible en https://sedeelectronica.bde.es/f/websede/INF/SPA/descargar/Guia_del_proceso_de_Comunicacion_de_Datos_de_Fraude_bajo_la_PSD2.pdf; última consulta 16/03/2022).

3.2. Incorporación de medidas seguridad por parte de las empresas españolas

En los últimos años, el uso de teléfonos móviles para realizar compras por Internet ha adquirido una importancia capital. La razón de esta importancia es que el comercio móvil permite que los *smartphones* se conviertan en el punto en el que se encuentran la oferta y demanda de determinados productos[141]. En Reino Unido[142], por ejemplo, se realizaron ventas por valor de 6.600 millones de libras esterlinas en el verano de 2012. Sobre este total, un 0,64% fueron ventas a través del teléfono móvil, lo que ascendería a unos 42 millones de libras esterlinas. Si comparamos estos datos con las cifras obtenidas en el año anterior, podemos comprobar que las compras a través del teléfono móvil crecieron en un 300%.

Como podemos comprobar, los pagos electrónicos ascienden vertiginosamente. De hecho, un artículo de la Universidad de California en Davis afirmó que los pagos electrónicos crecerían en casi mil millones de dólares en cuestión de cuatro años[143][144].

No obstante, no parece que todas las empresas estén concienciadas con la importancia incorporar medidas que aseguren la seguridad en los pagos electrónicos. Según un estudio realizado en 2020[145], sólo el 54% de las empresas españolas utilizan un sistema de gestión del fraude *online*, un 12% más que en 2019. Por otro lado, según el mismo estudio, sólo un 60% de las empresas encuestadas conocen los cambios normativos introducidos por la PSD2, relativos al proceso de SCA.

Además, este estudio revela que el 65% de los usuarios siguen acudiendo a la conexión directa con el banco adquiriente como medio de pago. No obstante, ha habido un incremento del 18% en el uso de PSP.

---

[141] *Cfr*. KEMP, R., "Mobile payments: Current and emerging regulatory and contracting issues", *Computer Law & Security Review*, vol. 29, n. 2, 2013, p. 175.
[142] *Ibidem*, p. 176.
[143] Según este artículo, las ventas *business-to-consumer* en el entorno *online* ascendieron a 1.471 millones de dólares en 2014. Además, el mismo artículo estimó unas ventas en el mismo entorno de 2.356 millones de dólares para 2018.
[144] *Cfr*. TRAUTMAN, L. J., "E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from Paypal", *UC Davis Business Law Journal*, vol. 16, 2016, p. 265.
[145] *Cfr*. ADIGITAL, CONFIANZAONLINE, ECOMMERCENEWS, "Estudio de Medios de Pago y Fraude Online", *Creative Commons*, 2020 (disponible en https://www.adigital.org/doc/202010_estudio-de-medios-de-pago-y-fraude-online-2020.pdf; última consulta 13/02/2022).

CONCLUSIONES

Tras realizar un análisis de los principales efectos de la PSD2 sobre la seguridad de los pagos electrónicos, podemos concluir que la PSD2 está cumpliendo los objetivos marcados por el Parlamento Europeo y el Consejo de la UE. Las nuevas medidas adoptadas, así como la reducción de la ambigüedad y de las posibilidades de los EEMM, ha permitido corregir las principales deficiencias de la PSD, logrando una reducción de los casos de fraude en los pagos electrónicos. Y es que, en 2019, un año más tarde de la fecha límite para transponer la PSD2, se registró el segundo porcentaje de fraude más bajo en pagos con tarjeta desde 2007, año en el que entró en vigor la PSD[146]. El 80% de dichas operaciones fraudulentas se llevaron a cabo principalmente a través de Internet o dispositivos móviles[147].

La adopción de medidas más estrictas, como el aumento de la responsabilidad del PSP, han fomentado la creación e implantación de innovadores mecanismos tendentes a evitar fisuras en los sistemas de seguridad de estas entidades. De hecho, en 2020, el 42% de las empresas disponían de un equipo dedicado a gestionar pagos y el fraude[148].

En este sentido, la jurisprudencia española ha fomentado la introducción de sistemas para evitar el fraude, haciendo responsable al PSP ante la falta de una actuación negligente o fraudulenta del ordenante, especialmente en aquellos casos en los que dicho proveedor no contaba con un mecanismo adecuado para evitar el fraude. Con este objetivo en mente, los tribunales españoles utilizaron la PSD2 para inspirar su decisión, a pesar de tratarse de casos que habían tenido lugar antes del nacimiento de dicha norma. Esta actuación por parte de los órganos de justicia españoles demuestra su alineación con los objetivos de la CE de luchar por un mercado de pagos electrónicos más seguro.

Por otro lado, cabe destacar que la PSD2 ha ido más allá y ha abierto un gran abanico de oportunidades tanto para las entidades bancarias tradicionales como para otro tipo de entidades, permitiéndoles ofrecer nuevos tipos de servicios más tecnológicos y eficientes. Así, han nacido numerosas iniciativas, como las *superapps* o las APIs, y nuevas figuras y competidores. El aumento de la competitividad en el mercado también concurre en el

---

[146] *Cfr.* BCE, "Un informe del BCE señala que el fraude en los pagos con tarjeta se redujo en 2019", *Dirección General de Comunicación*, 2021 (disponible en https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/ComunicadosBCE/NotasInformativasBCE/21/presbce2021_140.pdf; última consulta 4/03/2022).
[147] *Ibidem*.
[148] *Cfr.* ADIGITAL, CONFIANZAONLINE, ECOMMERCENEWS, *op. cit.*, p. 35.

objetivo de la CE de aumentar las posibilidades de elección de los consumidores, comerciantes y empresas.

Gracias al aumento de la seguridad en el mercado de pagos electrónicos, así como a las innovaciones tecnológicas introducidas, se estima que las operaciones electrónicas crezcan un 82% entre 2020 y 2025[149][150].

No obstante, es importante seguir avanzando en el desarrollo de una legislación que garantice la seguridad de los pagos electrónicos. A pesar de que el número de empresas que utilizan sistemas de gestión del fraude *online* ha aumentado en un 12% en los últimos años, sólo el 54% de las empresas utilizaban un sistema de gestión del fraude *online* en 2020. Además, en ese mismo año, el 40% de las empresas aún no conocían los cambios normativos en el proceso de SCA y, de entre las que sí conocían dichos cambios normativos, sólo el 37% contaba con una estrategia para minimizar el impacto de la regulación de la PSD2 sobre su negocio.

Finalmente, cabe destacar que, a pesar de las cifras esperanzadoras obtenidas en 2019, el aumento de las operaciones a distancia está provocando un correlativo aumento del fraude *online*. La Memoria Anual sobre la Vigilancia de Sistemas de Pago de 2014 afirma que el repunte en las tasas de fraude con tarjeta tuvo su origen en el aumento de las operaciones remotas que, entre 2013 y 2014, aumentaron en un 0,03%[151]. Es por ello por lo que cada vez es más importante la aplicación efectiva de normas técnicas de regulación para la SCA, así como las demás medidas para evitar el fraude *online*.

La PSD2 ha demostrado un gran potencial para lograr el objetivo final de la CE: armonizar el marco jurídico de los pagos electrónicos para, finalmente, lograr un mercado interior más integrado. Además, el enfoque llevado a cabo por la CE, poniendo el foco de atención en el aumento de la seguridad de los pagos electrónicos ha sido acertado, logrando un aumento de las operaciones *online* tanto a nivel nacional como internacional.

---

[149] *Cfr.* PWC ESPAÑA, *op. cit.*

[150] Por otro lado, también cabe destacar el efecto de la SARS-CoV-2 en el crecimiento del volumen de los pagos electrónicos. Y es que, con la llegada del confinamiento, las ventas *online* aumentaron un 26%. Además, un estudio afirma que el 1% de los habitantes españoles realizaron su primera compra *online* durante este período.

[151] *Cfr.* BANCO DE ESPAÑA, "Memoria Anual sobre la Vigilancia de Sistemas de Pago", *Banco de España Eurosistema*, 2014, p. 33 (disponible en https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaAnualSistemasPago/15/MAV2015.pdf; última consulta 16/03/2022).

BIBLIOGRAFÍA

1. LEGISLACIÓN

Corrección de errores de la Ley 16/2009, de 13 de noviembre, de servicios de pago («BOE» núm. 99, de 24 de abril de 2010).

Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE («DOUE» núm. 267, de 10 de octubre de 2009).

Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE («DOUE» núm. 337, de 23 de diciembre de 2015).

Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE («DOUE» núm. 319, de 5 de diciembre de 2007).

Ley 16/2009, de 13 de noviembre, de servicios de pago («BOE» núm. 275, de 14 de noviembre de 2009).

Orden ECE/1263/2019, de 26 de diciembre, sobre transparencia de las condiciones y requisitos de información aplicables a los servicios de pago y por la que se modifica la Orden ECO/734/2004, de 11 de marzo, sobre los departamentos y servicios de atención al cliente y el defensor del cliente de las entidades financieras, y la Orden EHA/2899/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios («BOE» núm. 313, de 30 de diciembre de 2019).

Orden EHA/1608/2010, de 14 de junio, sobre transparencia de las condiciones y requisitos de información aplicables a los servicios de pago («BOE» núm. 148, de 18 de junio de 2010).

Real Decreto 712/2010, de 28 de mayo, de régimen jurídico de los servicios de pago y de las entidades de pago («BOE» núm. 131, de 29 de mayo de 2010).

Real Decreto 736/2019, de 20 de diciembre, de régimen jurídico de los servicios de pago y de las entidades de pago y por el que se modifican el Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico, y el Real Decreto 84/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito («BOE» núm. 308, de 24 de diciembre de 2019).

Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera («BOE» núm. 284, de 24 de noviembre de 2018).

Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo de 24 de noviembre de 2010 por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión («DOUE» núm. 331, de 15 de diciembre de 2010).

Reglamento (CE) n.º 924/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativo a los pagos transfronterizos en la Comunidad y por el que se deroga el Reglamento (CE) nº 2560/2001 («DOUE» núm. 266, de 9 de octubre de 2009).

Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros («DOUE» núm. 69, de 13 de marzo de 2018).

2. JURISPRUDENCIA

Sentencia de la Audiencia Provincial de Madrid núm. 293/2019, de 2 de julio.

Sentencia del Tribunal Supremo núm. 332/2020, de 12 de febrero.

3. CAPÍTULOS DE LIBROS

Brener, A., "Payment Service Directive II and Its Implications" en Lynn, T., Mooney, J. G., Rosati, P., Cummins, M. (ed.), *Disrupting Finance. FinTech and Strategy in the 21st Century*, Palgrave McMillan, Dublin, 2019, pp. 103-119.

Loesch, S., "Payments Services Directive", *A Guide to Financial Regulation for Fintech Entrepreneurs*, Wiley, New York, 2018, pp. 229-237.

4. ARTÍCULOS DE REVISTA

Donnelly, M., "Payments in the digital market: Evaluating the contribution of Payment Services Directive II", *Computer Law & Security Review*, vol. 32, n. 6, 2016, pp. 827–839.

Kemp, R., "Mobile payments: Current and emerging regulatory and contracting issues", *Computer Law & Security Review*, vol. 29, n. 2, 2013, pp. 175-179.

Mercado-Kierkegaard, S., "Harmonising the regulatory regime for cross-border payment services", *Computer Law & Security Report*, vol, 23, n. 2, 2007, pp. 177-187.

Polasik, M., Huterska, A., Iftikhar, R., Mikula, S., "The impact of Payment Services Directive 2 on the PayTech sector development in Europe", *Journal of Economic Behavior and Organization*, vol. 178, 2020, pp. 385-401.

Romānova, I., Grima, S., Spiteri, J., Kudinska, M., "The Payment Services Directive 2 and competitiveness: The perspective of European FinTech Companies*", European Research Studies Journal*, vol, 21, n. 2, 2018, pp. 3–22.

Trautman, L. J., "E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from Paypal", *UC Davis Business Law Journal*, vol. 16, 2016, pp. 261-307.

Zunzunegui, F., "Luces y Sombras de la Transposición de la Directiva de Servicios de Pagos (PSD2)", *Revista de Derecho Bancario y Bursátil*, n. 159, 2020, pp. 89-112.

5. RECURSOS DE INTERNET

Adigital, Confianzaonline, Ecommercenews, "Estudio de Medios de Pago y Fraude Online", *Creative Commons*, 2020 (disponible en https://www.adigital.org/doc/202010_estudio-de-medios-de-pago-y-fraude-online-2020.pdf; última consulta 13/02/2022).

Asociación Española Fintech e Insurtech, "Libro Blanco de PayTech: La Evolución del sector PayTech y los nuevos retos regulatorios", *Asociación Fintech*, 2020 (disponible en https://www.asociacionfintech.es/wp-content/uploads/2020/12/AEFI_Libro-Blanco-PayTech-2020_Diciembre-2020-1.pdf; última consulta 10/02/2015).

Banco de España, "Guía del Proceso de Comunicación de Datos de Fraude bajo la PSD2", *Banco de España Eurosistema*, 2020 (disponible en https://sedeelectronica.bde.es/f/websede/INF/SPA/descargar/Guia_del_proceso_de_Comunicacion_de_Datos_de_Fraude_bajo_la_PSD2.pdf; última consulta 16/03/2022).

Banco de España, "Memoria Anual sobre la Vigilancia de Sistemas de Pago", *Banco de España Eurosistema*, 2014 (disponible en https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaAnualSistemasPago/15/MAV2015.pdf; última consulta 16/03/2022).

BBVA, "Todo lo que hay que saber de la PSD2", *Regulación Financiera*, 17 de octubre de 2019 (disponible en https://www.bbva.com/es/lo-saber-la-psd2/#:~:text=PSD2%20es%20una%20regulaci%C3%B3n%20europea,bancarios%20a%20las%20nuevas%20tecnolog%C3%ADas; última consulta 15/03/2022).

BCE, "Un informe del BCE señala que el fraude en los pagos con tarjeta se redujo en 2019", *Dirección General de Comunicación*, 2021 (disponible en

https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/ComunicadosBCE/NotasInformativasBCE/21/presbce2021_140.pdf; última consulta 4/03/2022).

Bizum, "Bizum nació cumpliendo la PSD2, la normativa europea de seguridad de pago en eCommerce", *Bizum Blog*, 21 de diciembre de 2020 (disponible en https://bizum.es/blog/normativa-psd2-seguridad-pago-ecommerce/; última consulta 13/02/2022).

Bizum, "Elige "Pagar con Bizum" en tus compras online", *Bizum Web*, 2020 (disponible en https://bizum.es/pagar-compra-online/; última consulta 13/02/2022).

Botta, A., Digiacomo, N., Höll, R y Oakes, L., "PSD2: Taking advantage of open-banking disruption", *Global Banking Practice*, 2018, (disponible en https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption#; última consulta 03/04/2022).

CEF Civil Mercantil, "Real Decreto-Ley de servicios de pago y otras medidas urgentes en materia financiera", *Centro de Estudios Financieros*, 16 de noviembre de 2018 (disponible en https://www.civil-mercantil.com/19-2018-servicio-de-pago.html; última consulta 15/03/2022).

Cifras INE, "El salto del comercio electrónico", *Boletín informativo del Instituto Nacional de Estadística*, junio de 2020 (disponible en https://www.ine.es/ss/Satellite?L=es_ES&c=INECifrasINE_C&cid=1259952923622&p=1254735116567&pagename=ProductosYServicios%2FINECifrasINE_C%2FPYSDetalleCifrasINE; última consulta 13/03/2022).

Comisión Europea, "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Una Estrategia para el Mercado Único Digital de Europa", *EUR-Lex*, 2015 (disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192; última consulta 10/02/2022).

Comisión Europea, "Libro Verde: Hacia un mercado europeo integrado de pagos mediante tarjeta, pagos por Internet o pagos móviles", *EUR-Lex*, 2012 (Disponible en https://eur-lex.europa.eu/legal-

content/ES/TXT/PDF/?uri=CELEX:52011DC0941&from=es; última consulta 02/02/2022).

Comisión Europea, "Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2013/36/UE y 2009//110/CE, y se deroga la Directiva 2007/64/CE /* COM/2013/0547 final - 2013/0264 (COD)", *EUR-Lex*, 2013 (disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013PC0547&from=GA; última consulta 10/02/2022).

Cruzado, V., "Los pagos electrónicos instantáneos supondrán el 25% de las transacciones mundiales en 2025", *Expansión*, 16 de octubre de 2021 (disponible en https://www.expansion.com/empresas/banca/2021/10/16/6169641b468aeb985c8b468e.html; última consulta 09/02/2022).

EBA, "Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)", *European Banking Authority*, 2017 (disponible en https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf?retry=1; última consulta 10/02/2022).

Fundación BBVA Microfianzas, "Servicios de pago y medidas urgentes en materia financiera", *Revista de actualidad jurídica para la inclusión y el desarrollo social*, n. 17, 2018 (disponible en https://www.fundacionmicrofinanzasbbva.org/revistaprogreso/servicios-pago-medidas-urgentes-materia-financiera/; última consulta 15/03/2022).

Iberley, "Entrada en vigor de las nuevas formas de pago por internet", *Iberley Noticias*, 2019 (disponible en https://www.iberley.es/noticias/entrada-vigor-nuevas-formas-pago-internet-29778; última consulta 15/03/2022).

INE, "Equipamiento y uso de TIC en los hogares. Año 2021", *INEbase*, 15 de noviembre de 2021 (disponible en

https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735576692; última consulta 13/03/2022).

London Economics and *iff*, "Study on the impact of Directive 2007/64/EC on Payment Services in the Internal Market and on the Application of Regulation (EC) No. 924/2009 on Cross-Border Payments in the Community, Final Report", *London Economics*, 2013 (disponible en https://ec.europa.eu/info/sites/default/files/study-impact-psd-24072013_en.pdf; última consulta 12/02/2022).

OCU, "Fraudes online: te roban y ni te enteras", *Noticias OCU*, 25 de mayo de 2021 (disponible en https://www.ocu.org/dinero/tarjetas/noticias/fraudes-tarjetas-online; última consulta 14/03/2022).

Oficina de Publicaciones de la Unión Europea, "Normas revisadas sobre servicios de pago en la Unión Europea", *EUR-Lex*, 28 de junio de 2016 (disponible en https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=celex:32015L2366; última consulta 1/04/2022).

Oficina de Publicaciones de la Unión Europea, "Servicios de Pago en la UE", *EUR-Lex*, 2016 (disponible en https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=celex:32007L0064; última consulta 1/04/2022).

PwC España, "Los pagos electrónicos casi se triplicarán en 2030 hasta superar los 3 billones de operaciones en el mundo", PwC España – Entorno digital (disponible en https://www.pwc.es/es/sala-prensa/notas-prensa/2021/pagos-electronicos-triplicar-2030.html#:~:text=Las%20estimaciones%20incluidas%20en%20el,transacciones%20en%20todo%20el%20mundo; última consulta 09/02/2022).

Santander, "Pagos digitales: ¿qué son y cuáles son los más usados?", *Sala de Comunicación Santander*, 30 de agosto de 2021 (disponible en https://www.santander.com/es/stories/pagos-digitales-que-son-y-cuales-son-los-mas-usados; última consulta 4/03/2021).

Unión Europea, "Medidas nacionales de transposición comunicadas por los Estados miembros relativas a la Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE,

2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE (Texto pertinente a efectos del EEE)", *EUR-Lex* (disponible en https://eur-lex.europa.eu/legal-content/ES/NIM/?uri=CELEX:32007L0064; última consulta 03/04/2022).