UN NUEVO RÉGIMEN DE ACCESO A LAS CUENTAS DE PAGO: LA PSD2

Carlos Conesa, Sergio Gorjón y Gregorio Rubio (*)

(*) Carlos Conesa y Sergio Gorjón pertenecen a la Dirección General Adjunta de Innovación Financiera e Infraestructuras de Mercado; y Gregorio Rubio pertenece a la Dirección General de Operaciones, Mercados y Sistemas de Pago, del Banco de España.

Resumen

La industria financiera se enfrenta a un factor de competencia adicional al creciente proceso de digitalización: la aparición de una nueva tipología de proveedores de servicios de pago que actúan como agregadores de información o como iniciadores de las operaciones de pago. Estas entidades emergentes, legitimadas por la Segunda Directiva de Servicios de Pago del Parlamento Europeo y del Consejo, tienen ahora la posibilidad de establecer una relación directa con los clientes de las entidades de crédito, tanto realizando transacciones en su nombre, sin tener que constituirse en administradores de las cuentas de pago, como accediendo a información de indudable valor comercial. El nuevo panorama anticipa un previsible cambio del *statu quo* y de los modelos de negocio actuales de la banca, potenciando el desarrollo de nuevas propuestas de valor que beneficien tanto a sus clientes como al conjunto de la sociedad. Este artículo presenta las principales novedades que introduce la directiva europea, apunta algunos aspectos todavía pendientes de resolver y avanza el posible impacto que puede suponer la norma para los diversos tipos de proveedores de servicios.

1 Introducción

Desde hace años, la banca se enfrenta al desafío de encontrar la fórmula que le permita mejorar su rentabilidad en un contexto marcado tanto por el crecimiento de las exigencias regulatorias como por una presencia sostenida de bajos tipos de interés. A lo anterior se ha unido, recientemente, el reto de la digitalización como factor potencialmente disruptor, dadas la aparición y la consolidación de nuevos competidores procedentes de otras industrias.

Si bien las iniciativas de carácter innovador son constatables en la práctica totalidad de los servicios bancarios, es en el negocio de los pagos minoristas donde con mayor intensidad se hace notar la huella del colectivo emergente, denominado de forma genérica «empresas *FinTech*» (vease gráfico 1).

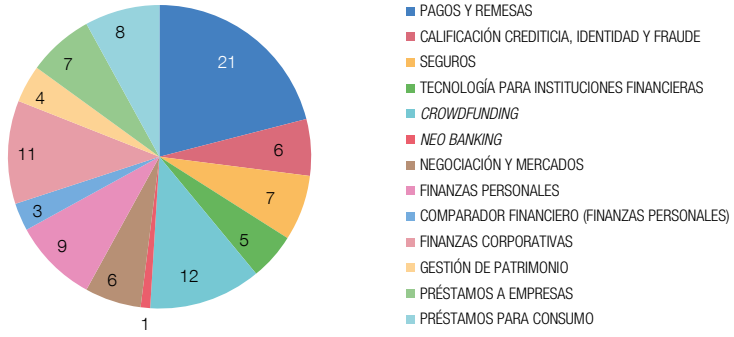
Ante la importancia de esta área de negocio para las entidades financieras[1], el sector ha reaccionado tratando de acelerar su proceso de cambio digital, en un intento por salvaguardar su protagonismo en los servicios de pago. Así, por ejemplo, se han registrado numerosas actuaciones, como la potenciación de los canales móviles, el fomento de nuevas formas de iniciación de las operaciones (tarjetas sin contacto, códigos QR) o la reducción de los plazos de ejecución actuales *(v. g.,* los pagos inmediatos). En paralelo, las entidades tradicionales están reforzando la colaboración con otros actores, toda vez que ven en dicha cooperación oportunidades para la mejora de la eficiencia y la explotación de otras líneas de negocio que permitan obtener fuentes de ingresos alternativas[2].

---

1 Las comisiones han ido ganando un gran protagonismo en las cuentas de resultados de los bancos, ante la contracción del margen de intereses, y en especial las asociadas a los servicios transaccionales y de pagos. Así, por ejemplo, Ernst & Young estima que las cuantías percibidas por las tarifas de los servicios de pago que prestan las entidades financieras globales, sin incluir el margen por intereses, suponen entre el 40 % y el 50 % de sus ingresos totales. Solo en España, las comisiones correspondientes al ejercicio 2016 (que incluyen otras actividades, como las relacionadas con los fondos de inversión, los planes de previsión social y seguros y la operativa con valores) reportaron 8.839 millones de euros a las ocho entidades de crédito cotizadas Esta cifra supuso un incremento del 1,2 % frente al ejercicio precedente y representa el 32,6 % de su facturación recurrente (margen de intereses más comisiones).

2 Estas fuentes se basan en gran medida, aunque no de forma exclusiva, en el aprovechamiento de los datos personales para la personalización de los servicios, el *marketing* y la publicidad.

EMPRESAS *FINTECH* POR CATEGORÍA DE SERVICIOS FINANCIEROS (%) GRÁFICO 1



FUENTE: Finnovista.

En esta coyuntura, se ha llevado a cabo una revisión exhaustiva de la principal norma reguladora de los servicios de pago en Europa, un proceso que introduce nuevos retos para sus actores y está contribuyendo a normalizar la estructura del mercado. La Segunda Directiva de Servicios de Pago o PSD2 *[Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, sobre servicios de pago en el mercado interior*[3]] es una norma ambiciosa y compleja que aspira a profundizar en la consecución de un mercado de servicios de pago integrado, competitivo, innovador y eficiente en la UE, sin por ello menoscabar la protección de los usuarios. De ahí la importancia que la norma atribuye a los aspectos relativos a la seguridad de los servicios de pago y, en especial, a regularizar la actividad de unos nuevos actores a los que los clientes de la banca podrán autorizar a acceder a las cuentas de pago que mantengan en una entidad financiera diferente.

Este artículo presenta las principales novedades que introducen la directiva europea y la normativa de segundo nivel que la ha desarrollado, apunta algunos aspectos todavía pendientes de resolver y avanza el posible impacto que puede suponer la norma para los diversos tipos de proveedores de servicios. Tras esta introducción, el segundo apartado hace un análisis detallado de la PSD2, centrándose primero en los aspectos relacionados con la seguridad, describiendo después los nuevos servicios de agregación de información e iniciación de pagos y analizando los diferentes canales de comunicación entre gestores de cuenta y entidades que prestan estos nuevos servicios; el apartado finaliza describiendo los detalles sobre la interacción entre los diversos tipos de proveedores y los principales problemas pendientes de resolver. El tercer apartado recoge algunos de los posibles efectos de la PSD2 y avanza el posible impacto de la norma sobre los diversos tipos de proveedores. El artículo termina con un apartado dedicado a las principales conclusiones.

2 La PSD2: el marco regulatorio como elemento dinamizador

En Europa, el regulador no ha querido permanecer como mero observador de los profundos cambios que están teniendo lugar en el área de los servicios de pago. Estos se han erigido en parte fundamental de un amplio abanico de actuaciones previstas con el objetivo último de conseguir una economía europea más robusta e integrada y que satisfaga las nuevas expectativas de los usuarios. Entre estas iniciativas, cabe destacar la propuesta de la Comisión Europea relativa a *Una Estrategia para el Mercado Único Digital de Europa*

3 http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

(2015)[4] y, más recientemente, el *Plan de acción de servicios financieros destinados a los consumidores: mejores productos y una oferta más variada* (2017)[5].

Sin embargo, en el área de los pagos el principal esfuerzo se ha centrado en la revisión de la Primera Directiva de Servicios de Pago o PSD1 (Directiva 2007/64), la norma reguladora básica de estos servicios durante años, que dio paso a la adopción de la PSD2 en 2015. La nueva directiva presenta dos grandes novedades: a) una mayor atención a los riesgos asociados a las nuevas estrategias nacidas de la transformación digital, y b) la incorporación de nuevos servicios de pago al perímetro regulatorio[6].

2.1 LA PSD2 Y LAS MEDIDAS DE SEGURIDAD PARA OPERACIONES DE PAGO ELECTRÓNICAS

En lo relativo a la seguridad en las operaciones de pago, la PSD2 se centra especialmente en las transacciones de carácter remoto, ya sea a través de Internet o por medio de dispositivos móviles. Este énfasis es una consecuencia directa del notable incremento que dichas transacciones han experimentado en los últimos años, impulsadas por el auge del comercio electrónico (véase cuadro 1).

Profundizando en las recomendaciones del BCE *(Recommendations for the security of internet payments*[7]) y las directrices de la Autoridad Bancaria Europea (EBA, por sus siglas en inglés) *(Directrices sobre la seguridad de los pagos por Internet*[8]), la PSD2 ha hecho de la seguridad en los pagos electrónicos uno de sus ejes vertebradores. La norma prescribe la aplicación obligatoria de medidas y procedimientos de seguridad específicos en las operaciones de pago electrónicas, y en especial en las que tienen lugar a distancia.

Estas medidas y procedimientos se articulan en torno al concepto de «autenticación reforzada del cliente»[9], cuyas principales características se resumen en el cuadro 2.

El concepto de autenticación reforzada del cliente, sin embargo, no pudo definirse en detalle en la propia directiva, tanto por su complejidad técnica como por la granularidad que hubiera sido necesario incorporar en la norma y por la gran diversidad de los casos sujetos a su aplicación. En consecuencia, la PSD2 se limitó a especificar una serie de principios generales, y estableció que la EBA, en estrecha colaboración con el BCE, sería la encargada de desarrollar el marco jurídico detallado que debía regir la seguridad de los pagos electrónicos.

Con este objetivo, la EBA comenzó a trabajar en la redacción de unas normas técnicas de regulación centradas en la cobertura de los aspectos relevantes en materia de autenticación reforzada de los clientes y comunicación abierta, común y segura *(RTS on Strong Customer Authentication and Common and Secure Communication,* que en adelante denominaremos RTS, por sus siglas en inglés).

---

4 http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0192&from=ES.

5 http://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0013.02/DOC_1&format=PDF y su anejo http://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0013.02/DOC_2&format=PDF.

6 Junto con ello, la PSD2 introduce otras medidas de ajuste fino relacionadas, principalmente, con su ámbito de aplicación y con el régimen prudencial de los proveedores de servicios de pago que regula específicamente (las entidades de pago).

7 http://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf?3b8c24c7dc9fa5f57204d212c66f2dc7.

8 https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_ES+Guidelines+on+Internet+Payments.pdf/44d07cf8-1721-4407-94a6-3a8c256149fa.

9 Más conocido en el ámbito de los servicios de pago como *Strong Customer Authentication* o SCA, por sus siglas en inglés.

EVOLUCIÓN DEL COMERCIO ELECTRÓNICO EN EL MUNDO (a) CUADRO 1

Miles de millones de dólares

	2011	2012	2013	2014	2015	2016
Norteamérica	327,77	373,03	419,53	469,49	523,09	580,24
Asia-Pacífico	237,86	315,91	388,75	501,68	606,54	707,60
Europa Occidental	218,27	255,59	291,47	326,13	358,31	387,94
Europa del Este y Central	30,89	40,17	48,56	57,96	64,35	68,88
América Latina	28,33	37,66	45,98	55,95	63,03	69,60
Oriente Medio y África	14,41	20,61	27,00	33,75	39,56	45,49
TOTAL MUNDIAL	**856,97**	**1.042,98**	**1.221,29**	**1.444,97**	**1.654,88**	**1.859,75**

FUENTE: eMarketer (2013).

a Incluye las compras efectuadas por cualquier canal digital (PC, móvil y tabletas) de viajes, descargas digitales o entradas de espectáculos. Se excluye la cifra correspondiente al juego en línea. Los datos agregados pueden no coincidir con la suma de las partidas individuales por el efecto redondeo.

Las RTS recogen los principales elementos de la autenticación reforzada, tratando de mantener la neutralidad desde un punto de vista tecnológico y respetando los diversos modelos de negocio. Incluyen también ciertas excepciones en función del riesgo de la operación, su importe y el canal por el que se realiza, como refleja el cuadro 2. Las RTS establecen, asimismo, el régimen jurídico aplicable al acceso a las cuentas de pago, un elemento crucial a la hora de fijar la forma en que los diversos proveedores de servicios de pago interactuarán entre ellos, que se explica con más detalle en la siguiente sección.

Tras un tortuoso proceso, las RTS han dado lugar al *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*[10], que se publicó el 13 de marzo de 2018.

No obstante, en este artículo se han mantenido las referencias a las RTS, por dos motivos. Por un lado, en atención a la práctica del mercado, que preferentemente sigue refiriéndose a este reglamento delegado como *RTS on Strong Customer Authentication and Common and Secure Communication.* Por otro lado, al hecho de que el reglamento solo será de aplicación a partir del 14 de septiembre de 2019. En cualquier caso, las referencias a las RTS deben entenderse realizadas al Reglamento Delegado (UE) 2018/389.

10 – Este reglamento delegado de la Comisión puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.SPA&toc=OJ:L:2018:069:TOC.
– Con carácter previo, la EBA había publicado su propuesta el día 23.2.2017: https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf.
– La Comisión Europea anunció el 24.5.2017, mediante un escrito dirigido a la EBA, su intención de introducir ciertos cambios en determinados artículos de las RTS propuestas por la EBA. Estos cambios pueden consultarse en: http://www.eba.europa.eu/documents/10180/1806975/%28EBA-2017-E-1315%29%20Letter+from+O+Guersent%2C%20FISMA+re+Commission+intention+to+amend+the+draft+RTS+on+SCA+and+CSC+-Ares%282017%292639906.pdf/efbf06e1-b0e9-4481-88e5-b70daa663cb9.
– Este escrito motivó que la EBA emitiera una *Opinión,* el 29.6.2017, en la que expresaba su posición respecto de los cambios anunciados por la Comisión Europea: https://www.eba.europa.eu/documents/10180/1894900/EBA+Opinion+on+the+amended+text+of+the+RTS+on+SCA+and+CSC+%28EBA-Op-2017-09%29.pdf/df60c6ac-a284-4772-b1d5-66c7073d28af.

PRINCIPALES CARACTERÍSTICAS REGULATORIAS DE LA AUTENTICACIÓN REFORZADA DE CLIENTES EN LA PSD2 CUADRO 2

La autenticación reforzada del cliente en la PSD2

Consiste en: autenticación basada en el uso de dos o más elementos de seguridad independientes.		Elementos de seguridad:	— Conocimiento (algo que solo conoce el usuario). — Posesión (algo que solo posee el usuario). — Inherencia (algo que es el usuario).
		Independientes:	— La vulneración de uno no compromete la fiabilidad de los demás. — No exigencia de dispositivos diferentes.
		Credenciales de seguridad personalizadas:	Elementos de seguridad facilitados por el proveedor de servicios de pago (PSP) o vinculados por él al cliente.
Obligatoria cuando:	— Acceso cuenta pago *online.* — Operación de pago electrónico. — Acción remota que entrañe riesgo. — Presencia de un TPP.	Elemento de seguridad dinámico si:	— Operación de pago electrónico remota. — Presencia de un PISP.
Posibilidad de exenciones en función de:	— Nivel de riesgo (TRA). — Importe. — Canal.		
Acompañado de:	Mecanismos de monitorización de transacciones.		

FUENTE: Banco de España.

2.2 LOS NUEVOS SERVICIOS DE PAGO EN LA PSD2: INICIACIÓN DE PAGOS (PIS) Y AGREGACIÓN DE INFORMACIÓN (AIS)

Tradicionalmente, las entidades de crédito han sido las principales oferentes de servicios de pago, que facilitaban sobre las cuentas a la vista que mantenían sus depositantes. La PSD1 reguló detalladamente los servicios de pago y estableció una reserva de actividad, que limitaba tales servicios a entidades autorizadas y sujetas a supervisión, entidades que pasaron a denominarse, de forma genérica, «proveedores de servicios de pago» (PSP).

De forma simplificada, este término incluía fundamentalmente las entidades de crédito y las entidades de pago[11]. La novedad principal de la PSD1 fue, precisamente, la creación de esta última clase de proveedores, con un régimen de supervisión proporcional a los riesgos correspondientes a su actividad, limitada a intermediar pagos, a diferencia del amplio conjunto de servicios que caracteriza la operativa de las entidades de crédito.

Sin embargo, los servicios prestados por ciertas entidades especializadas sobre las cuentas de los clientes en otras entidades quedaron fuera del ámbito de la PSD1 y, por tanto, pasaron a prestarse en la UE sin una regulación específica. Los principales servicios de este tipo son el de iniciación del pago en una cuenta de otra entidad (o PIS, por sus siglas en inglés, *payment initiation service)* y el ofrecimiento de información consolidada sobre saldos y operaciones de varias cuentas de pago en diversas entidades (denominado habitualmente AIS, por sus siglas en inglés, *account information service).* La característica fundamental de estos servicios es que la entidad prestadora no requiere administrar una cuenta de pago, sino que tiene el consentimiento del cliente para operar u obtener infor-

11 También forman parte del conjunto de proveedores de servicios de pago las entidades de dinero electrónico, junto con las instituciones de giro postal y las autoridades públicas y monetarias en determinadas circunstancias. No obstante, dado que la cuota de mercado de estas instituciones y organismos es muy reducida, y puesto que la regulación de las entidades de dinero electrónico en su condición de proveedores de servicios de pago se remite a la de las entidades de pago, en este artículo, por simplicidad, el término «entidades de pago» hace referencia a todos estos proveedores de servicios de pago, y en particular a las entidades de dinero electrónico cuando actúan como tales proveedores.

mación de cuentas que este tiene en otras entidades. Las empresas que se han especializado en este tipo de servicios son «terceras empresas» en la tradicional relación bilateral entre el PSP y su cliente, por lo que se les suele denominar «proveedores terceros» o TPP, por sus siglas en inglés *(third party providers).*

Inicialmente, y en tanto las RTS que desarrollan la PSD2 no entren en vigor, el principal método utilizado por estos TPP para acceder a las cuentas de pago de sus clientes en otras entidades consistía en el uso de las credenciales de seguridad personalizadas de los clientes. Así, los TPP solicitaban a los titulares sus credenciales y accedían a las cuentas de sus clientes del mismo modo y con los mismos permisos que el propio titular[12], utilizando técnicas habitualmente conocidas como *screen scraping.* Desde un punto de vista técnico, el *screen scraping* es un método de programación que, mediante ingeniería inversa, permite extraer de una representación de datos mostrados en una pantalla (a través de una página web o de un archivo pdf, por ejemplo) los propios datos que conforman la representación para volcarlos en otra aplicación. En el ámbito bancario, esta técnica posibilita que cualquier entidad, con acceso a una cuenta de pago *online* de un cliente, pueda extraer los datos representados en la cuenta y operar con ellos.

Esta operativa tenía implicaciones en términos de seguridad y de eficiencia, ya que, sin identificarse, los TPP (no vinculados con la entidad gestora de la cuenta) podían acceder a la información de los clientes utilizando un canal pensado para estos últimos. Por tanto, los TPP «suplantaban al cliente» y tenían acceso potencial a más información de la estrictamente necesaria para prestar los servicios demandados por dichos clientes. Esta situación resultaba posible ya que, como regla general, las entidades gestoras de cuenta habilitan un único mecanismo de acceso a todas las cuentas, productos y posiciones de sus clientes[13]. Por tanto, por esta vía, los TPP podían tener una visión completa sobre la posición global del cliente, sin que este fuera necesariamente consciente de ello y con independencia del alcance del permiso concedido.

Sin embargo, estos servicios de iniciación de pagos o de agregación de información pueden ofrecer soluciones de utilidad a comerciantes y consumidores (como una visión consolidada de sus saldos y operaciones) o canales de pago alternativos para la operativa de comercio *online* sin necesidad de utilizar instrumentos de pago específicos, como las tarjetas de pago. Asimismo, y como parte de la amplia tendencia hacia la «banca abierta» (habitualmente denominada *open banking)*[14], se puede considerar que el cliente de un PSP debe poder disponer de su propia información y cederla a terceros si así lo desea. En consecuencia, la PSD2 responde al objetivo del regulador de permitir el desarrollo y la consolidación de estos servicios de iniciación y agregación (PIS y AIS), en un contexto

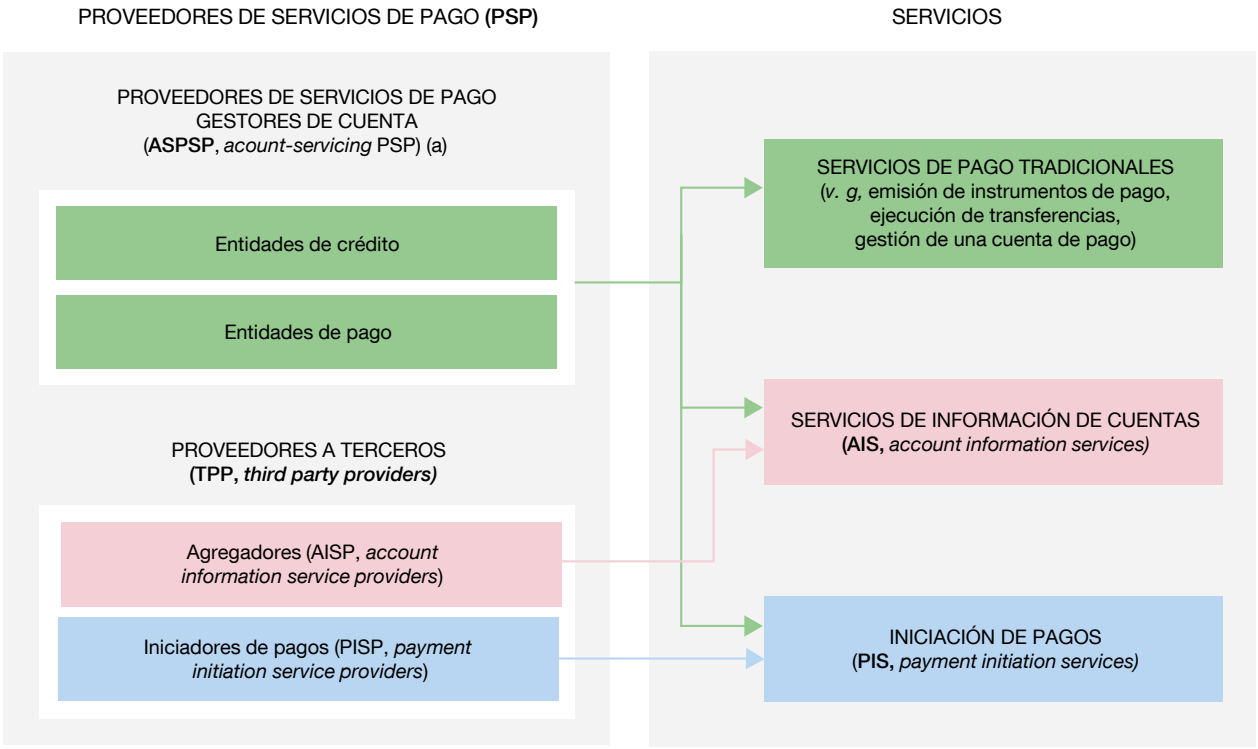
12 Ha sido, y es, objeto de profundo debate si esta práctica tiene cabida dentro de la Directiva 2007/64/CE o PSD1, toda vez que la compartición de las credenciales de seguridad personalizadas puede entenderse como un incumplimiento de las obligaciones que la directiva impone al usuario del servicio de pago. No obstante, como la directiva no prohíbe expresamente tal compartición, su prohibición en el contexto de los nuevos servicios de pago ha sido rebatida por algunos tribunales, al entender tal prohibición como una restricción a la libre competencia.

13 Esto se realiza así por razones tales como la maximización de la experiencia de usuario de los clientes, la política comercial, la reducción de costes, la facilidad de mantenimiento, la actualización de las aplicaciones, etc.

14 El concepto de banca abierta puede definirse [véase Brodsky y Oaks (2017)] como un modelo colaborativo en el que los datos bancarios se comparten entre dos o más actores sin relación entre sí, para proveer nuevos servicios al mercado. Aunque no es estrictamente necesario, normalmente se asume que el intercambio de datos entre entidades tiene lugar a través de Interfaces para la Programación de Aplicaciones (API, por sus siglas en inglés), que consisten en interfaces de comunicación estandarizadas que posibilitan el intercambio de información entre aplicaciones informáticas. En el apartado siguiente se profundiza en este concepto.

ENTIDADES Y SERVICIOS DE PAGO

ESQUEMA 1



FUENTES: European Payments Council y Banco de España.

a Para simplificar el cuadro, solo se incluyen las principales categorías de ASPSP (entidades de crédito y entidades de pago); existen, no obstante, otras entidades menos significativas que pueden actuar como ASPSP, como, por ejemplo, las entidades de dinero electrónico o las instituciones de giro postal.

que proporcione a los consumidores una protección adecuada tanto de sus pagos como de la información asociada a sus cuentas.

Adicionalmente, la PSD2 confiere a cualquier titular de una cuenta de pago accesible *online,* el derecho a poder iniciar una orden de pago a través de un PSP distinto a aquel en el que está abierta dicha cuenta. Del mismo modo, la directiva reconoce el derecho de cualquier titular de una o de varias cuentas de pago accesibles *online* a acceder a la información contenida en tales cuentas a través de un proveedor de servicios de pago distinto a aquel o aquellos en los que aquellas estén abiertas. En otras palabras, los servicios de AIS y PIS se incluyen dentro del perímetro regulatorio, con las debidas salvaguardas, para proporcionar a los consumidores una protección adecuada.

Por otro lado, la PSD2 admite la posibilidad de que haya PSP que solo presten servicios de PIS o AIS, sin gestionar directamente cuentas de pago. Por ello, el tipo de entidades reconocidas como PSP se amplía, resultando un panorama bastante complejo, que se resume, sintéticamente, en el esquema 1. Los PSP quedan divididos en dos grupos básicos: los que gestionan cuentas de pago de sus clientes (denominados habitualmente «ASPSP», por sus siglas en inglés, *Account-servicing Payment Service Provider)* y los TPP, que prestan servicios de AIS o PIS sin gestionar cuentas de clientes[15]. Dentro del primer

15 No debe olvidarse, sin embargo, que algunos servicios de pago, como el envío de dinero, por ejemplo, no requieren de la existencia de cuentas de pago.

REQUISITOS PRUDENCIALES DE LA PSD2 CUADRO 3

Comparación entre los requisitos aplicables a los proveedores de servicios de pago que solo prestan servicios de Iniciación de pagos de agregación, de información sobre cuentas de pago y los aplicables a las entidades de pago que prestan servicios de pago como gestores de cuentas de pago.

Criterio	ASPSP	PISP	AISP
Servicios de pago	Todos	Iniciación de pagos	Información sobre cuentas de pago y operaciones de pago designadas
Posesión de fondos de clientes	Sí	No	No
Capital mínimo (euros)	125.000	50.000	No
Recursos propios	Sí	No	No
Seguro de responsabilidad civil profesional	No	Sí	Sí
Autorización	Sí	Sí	No
Registro	Sí	Sí	Sí
Pasaporte	Sí	Sí	Sí
Requisitos organizativos	Todos	Todos	Solo de seguridad y continuidad
Aplicación PSD2	Sí	Sí	Limitada: supervisión más requisitos de información y seguridad
Posibilidad de exenciones	Sí, en función del valor medio de operaciones de pago, con pérdida del pasaporte	No	Sí, con carácter imperativo y sin pérdida de pasaporte

FUENTE: Banco de España.

grupo se encuadran, fundamentalmente, las entidades de crédito y las entidades de pago; en el segundo grupo se suele diferenciar entre proveedores de servicios de iniciación (PISP) y agregadores de información (AISP). No obstante, es importante destacar que los ASPSP pueden prestar todo tipo de servicios de pago, incluyendo PIS y AIS, y que un TPP podría prestar tanto servicios de iniciación de pagos como de agregación de información, siempre que cumpliera con los correspondientes requisitos regulatorios que se detallan en el cuadro 3.

La PSD2 establece los requisitos prudenciales que se exigen a entidades que actúan exclusivamente como proveedoras de servicios de PIS o AIS[16]. En razón de la limitada actividad que llevan a cabo estas entidades (y de sus riesgos inherentes), dichos requisitos son menos exigentes que los requeridos a las entidades que gestionan cuentas de pago. El cuadro 3 ofrece un resumen de los principales requisitos aplicables a las diferentes categorías[17].

La PSD2 establece también las normas básicas necesarias para regular el intercambio de información entre los ASPSP y las entidades que provean servicios de AIS y PIS, que aparecen resumidas en el cuadro 4. Un elemento fundamental que determina la interacción entre ambos grupos de proveedores es la posible ausencia de una relación contractual entre ellos, ya que la PSD2 no exige que haya un acuerdo específico entre el proveedor gestor de cuenta y la entidad que provea servicios de iniciación o de agregación. Además, esta última tendrá derecho a utilizar los procedimientos de autenticación que los ASPSP hayan facilitado a sus propios clientes. Adicionalmente, la directiva no permite la

16 Estos requisitos se refieren a los proveedores de servicios de pago que no están sujetos a otros requisitos prudenciales en virtud de su naturaleza, es decir, a los exigidos a las entidades de pago que actúan como ASPSP.

17 Para los ASPSP se ha tomado el caso de las entidades de pago, ya que las entidades de crédito, atendiendo al amplio rango de servicios que prestan, están sujetas a requerimientos más exigentes.

MARCO OPERATIVO APLICABLE A LOS PISP Y AISP

CUADRO 4

Criterio	PISP	AISP
Servicio vinculado a la existencia de cuentas online	Sí	Sí
Relación contractual con ASPSP	No	No
Obligación de identificarse ante ASPSP	Sí	Sí
Posibilidad de utilizar credenciales y procedimientos de autenticación facilitados por ASPSP	Sí	Sí
Obligación de utilizar SCA	Sí	Sí
Con elemento dinámico	Sí	No
Obligación de utilizar CSC	Sí	Sí
Salvaguarda de información y credenciales de seguridad	Sí	Sí
Existencia de un contrato marco con el ordenante	No	Sí
Posibilidad de denegación de acceso por el ASPSP	Solo si hay razones objetivas y documentadas	Solo si hay razones objetivas y documentadas
Discriminación de órdenes por el ASPSP	No	No

FUENTE: Banco de España.

discriminación injustificada de las órdenes cursadas por el usuario a través de un PISP o un AISP, y en particular en lo relativo a los plazos, la prioridad y los gastos aplicables.

El resultado de todo lo anterior es que los ASPSP deben facilitar la operativa del cliente a través de los PISP y AISP (que, en la práctica, actúan como competidores directos de los primeros), aun cuando no puedan obtener ninguna contraprestación específica por ello[18]. Este enfoque tiene implicaciones muy amplias, puesto que, en ausencia de una relación contractual entre ASPSP y AISP o PISP, es en la propia norma y en sus desarrollos (RTS) donde se ha de fijar la forma en la que estos dos grupos de entidades, con intereses contrapuestos en muchos casos, han de intercambiar de forma segura información sensible para el cliente de ambas. En los siguientes apartados se analiza con mayor detalle cómo la norma aborda este punto particular.

2.3 LA INTERACCIÓN ENTRE PROVEEDORES DE SERVICIOS DE PAGO EN LA PSD2: ACCESO DIRECTO *VERSUS* INTERFAZ DEDICADA (API)

La situación descrita en los apartados anteriores evidencia la importancia creciente de los aspectos relativos a la seguridad dentro la regulación en materia de acceso a las cuentas de pago. Por esta razón, la PSD2 impone la utilización de estándares de comunicación abiertos, comunes y seguros (o CSC, por sus siglas en inglés) en la identificación de entidades, la autenticación de clientes y la notificación de información, así como en la implementación de las medidas de seguridad que deben regir las relaciones entre los diversos proveedores de servicios de pago participantes en la operación. De esta manera, se trata de asegurar la integridad de los fondos, la confidencialidad de la información y la salvaguarda de las credenciales de seguridad personalizadas de los usuarios.

Sin embargo, la directiva no prescribe el uso de un estándar de comunicación determinado. En su lugar, otorga un mandato a la EBA para que, en estrecha colaboración con el BCE, especifique los requisitos que deberían satisfacer dichos estándares, de forma que estén alineados con el espíritu de la directiva. La PSD2 se limita a precisar que los están-

18 Los ASPSP deben aplicar a los TPP las mismas condiciones que aplicarían a sus clientes si estos estuvieran realizando la operación directamente y no a través de una entidad interpuesta. Por ello, los ASPSP no pueden cargar a los TPP comisiones adicionales y están obligados a prestar los servicios de forma gratuita en caso de que la consulta de información o la iniciación del pago de manera directa fuesen gratuitas para el cliente, como es habitual en la mayoría de los casos.

dares han de garantizar, al menos, la interoperabilidad de las diferentes soluciones tecnológicas de comunicación y han de permitir la utilización de todos los tipos de dispositivos que, con carácter habitual, se utilicen en el mercado para efectuar servicios de pago.

Por el contrario, la PSD2 sí aborda expresamente uno de los aspectos más controvertidos del principal método empleado hasta ahora para acceder a las cuentas de pago por parte de un tercero: la «suplantación del cliente» por parte de un TPP, utilizando las credenciales de seguridad personalizadas del cliente y accediendo a la cuenta del mismo modo y con los mismos permisos que el propio titular, sin identificarse como un tercero. Para mitigar los riesgos asociados a esta práctica, la PSD2 impone a los PISP y a los AISP la obligación de identificarse ante el ASPSP cada vez que accedan a las cuentas de pago de un cliente. Sin embargo, evita prescribir un modelo de acceso determinado. Conforme a lo especificado en las RTS, esta identificación habrá de realizarse mediante el uso de certificados cualificados de sello electrónico o certificados cualificados de autenticación de sitio web[19]. Los certificados garantizan, respectivamente, el origen y la autenticidad de los datos asociados a una persona jurídica y autentifican el sitio web vinculado a ella.

Sin embargo, la directiva no trata expresamente la técnica de *screen scraping,* cuyo tratamiento, por tanto, ha quedado enmarcado exclusivamente en las RTS sobre los estándares de comunicación.

Atendiendo a estas circunstancias, las RTS no imponen una forma determinada de acceso, sino que permiten tanto el denominado «acceso directo» como el establecimiento de «interfaces dedicadas»:

- El *acceso directo* consiste en la utilización por parte del TPP del canal de comunicación establecido por el ASPSP para sus clientes (normalmente, una aplicación de banca *online),* que es el canal habitual en el que los PISP y AISP han basado sus modelos de negocio y que han venido utilizando hasta ahora para acceder a la información sobre las cuentas de pago de sus clientes, utilizando técnicas de *screen scraping. A priori,* este es el acceso preferido por la mayoría de TPP que ya estaban prestando este servicio antes de la implantación de la PSD2. Respecto al uso que se hacía de este canal antes de la PSD2, un cambio sustancial es la obligación que tienen ahora los TPP de identificarse como tales a la hora de acceder a la información de los clientes.

- El acceso mediante una *interfaz dedicada* implica el desarrollo, por parte del ASPSP, de un canal de comunicación específico para TPP, distinto del canal de banca *online* utilizado por los clientes de la entidad. Aunque las RTS no lo expliciten, se asume generalmente que la implementación práctica de esta opción tendrá lugar a través de las denominadas «interfaces de programación de aplicaciones» (API, por sus siglas en inglés), pues es esta la técnica actualmente seguida por la industria para la interconexión y el desarrollo de aplicaciones[20].

---

19 Ambos certificados están definidos en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, artículo 3, apartados 30 y 39, respectivamente: (http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=ES).

20 Las API constituyen un medio técnico que permite conectar dos aplicaciones de *software* entre sí para acceder a sus funcionalidades mediante el intercambio de mensajes o datos en formato estándar.

COMPARATIVA ENTRE EL RÉGIMEN DE ACCESO A CUENTAS DE PAGO DE LA PSD2 Y LA INICIATIVA *OPEN BANKING* DEL REINO UNIDO

CUADRO 5

PSD2	*Open Banking* del Reino Unido
Es, sobre todo, un **marco regulatorio.**	Es, sobre todo, una **filosofía de negocio.**
Es la herramienta elegida por las **autoridades europeas** para la integración de los pagos minoristas en la UE.	Es la vía elegida por las **autoridades británicas** para poner fin al *statu quo* de la banca minorista en el Reino Unido.
Su **finalidad principal** es la armonización de los servicios de pago en la UE, la seguridad en la cadena de pagos y la protección de los consumidores.	Su **finalidad principal** es aumentar la competencia en la industria bancaria, mejorar la eficiencia y estimular la innovación.
Para conseguirlo, establece las **medidas de seguridad** que deben rodear la provisión de **servicios de pago,** incluye en el perímetro regulado todos los servicios de pago y determina los requisitos prudenciales y operativos que deben satisfacer los **proveedores de servicios de pago.**	Para conseguirlo, abre primero (marzo de 2017) el acceso a cierta **información estandarizada** (productos bancarios y datos de referencia) y, posteriormente (enero de 2018), el acceso a las **cuentas corrientes** personales y de pequeñas y medianas empresas por terceros autorizados.
Ello debe conducir a una mayor competencia en condiciones equivalentes a lo largo de la UE y, así, a **servicios y métodos de pago** innovadores, eficaces, cómodos y seguros.	Lo primero permite trazar el mapa **de productos y servicios bancarios** al por menor (incluidos los de pago) en el Reino Unido; lo segundo permite: i) la **personalización** de tales productos y servicios, ya sea por sus oferentes primeros o por entidades terceras debidamente reguladas, y ii) la prestación de servicios de iniciación e información.
En su concepción holística de los servicios de pago, regula el **acceso a las cuentas de pago por terceros autorizados,** ya sea para iniciar pagos o para obtener información agregada.	El **acceso** a las cuentas corrientes por terceros se produce a través de interfaces de programación de aplicaciones **(API)**, basadas en un **estándar abierto** que rige la compartición **segura** de los datos.
No establece ninguna forma específica de **acceso** a las cuentas de pago, sino las **condiciones** en que debe producirse aquel; los proveedores de servicios de pago gestores de cuentas son quienes determinan el acceso por terceros a las cuentas de pago.	El **estándar** ha sido desarrollado por la Open Banking Implementation Company. Esta compañía se estableció en 2016; su gobernanza, composición y financiación fueron determinadas por las autoridades británicas; participan en ella los **nueve** mayores **bancos y compañías hipotecarias** del Reino Unido, para los que es obligatoria la aplicación del estándar.
Las **condiciones de acceso** se precisan en una RTS desarrollada por la EBA con la intervención de la Comisión Europea. **Todos los proveedores de servicios de pago gestores de cuenta** deben proveer un medio de acceso a las cuentas de pago que satisfaga dichas condiciones, pero no se especifica ningún estándar. No obstante, las autoridades europeas han mostrado su preferencia por el acceso a través de API y confían en que la industria en su conjunto diseñe los **estándares** en consonancia.	El **diseño** sigue las recomendaciones del denominado *Open Banking Working Group,* así como los mandatos de la PSD2 aplicables.

FUENTE: Banco de España.

Esta falta de concreción es, precisamente, uno de los aspectos diferenciales más significativos entre la apertura de cuentas de pago promovida por la PSD2 y el concepto general de banca abierta u *open banking,* estrechamente vinculado a la apertura de cuentas mediante la estructuración de datos y el uso de API estandarizadas. Uno de los ejemplos más destacados de *open banking* es la iniciativa británica de banca abierta. El cuadro 5 ofrece un breve resumen de las principales diferencias y similitudes entre esta iniciativa y la PSD2. Aunque las diferencias son fruto, sobre todo, de los distintos objetivos que inspiran ambos marcos operativos, las similitudes son tales que permitirían incluir también la PSD2 dentro del amplio concepto de banca abierta.

En todo caso, y cualquiera que sea la opción finalmente elegida por el ASPSP para transmitir la información, esta deberá permitir la comunicación segura entre el ASPSP y el TPP y, como se ha recalcado, la identificación de las terceras partes ante el ASPSP. También deberá hacer posible el uso de los procedimientos de autenticación que hubiera implemen-

tado el ASPSP. Adicionalmente, dado que el mecanismo de acceso ha de fundamentarse en estándares de comunicación abiertos, comunes y seguros, las interfaces deberán seguir estándares de comunicación emitidos por organismos de estandarización europeos o internacionales y sus especificaciones técnicas habrán de documentarse y ponerse gratuitamente a disposición de los AISP y de los PISP, al menos con seis meses[21] de antelación a la fecha de su implementación. Durante un plazo equivalente, los PISP y los AISP dispondrán de mecanismos suficientes para poder validar sus aplicaciones y programas.

2.4 EVOLUCIÓN DE LAS DISCUSIONES SOBRE LAS RTS Y RETOS PENDIENTES

La EBA se ha enfrentado a numerosas dificultades a la hora de concretar el régimen jurídico del acceso a las cuentas de pago por parte de los PISP o los AISP; ha resultado complejo conciliar los múltiples y, en ocasiones, contradictorios objetivos perseguidos por la PSD2.

Desde un punto de vista técnico, se podía optar por elaborar unas RTS muy detalladas que inequívocamente reforzaran la seguridad de los estándares (con el peligro de vincular las RTS a una tecnología concreta) o, por el contrario, formular una serie de principios generales que pudieran perdurar y no perjudicasen la innovación (con el riesgo de no reforzar suficientemente la seguridad). Desde la óptica de la homogeneización, se tuvo que optar entre una regulación precisa, que asegurara un adecuado grado de armonización a escala europea, y la introducción de normas más flexibles, que permitieran el desarrollo de diferentes soluciones de pago en la UE.

Los principales problemas, sin embargo, han surgido por los diferentes enfoques de los distintos tipos de proveedores, resultantes de sus intereses antagónicos. Teniendo en cuenta la competencia directa entre los agentes implicados, las RTS se han elaborado buscando la mejor manera de conciliar los intereses legítimos de los PISP y los AISP, de un lado, y de los ASPSP, de otro. Todo ello en un contexto en el que la regulación no permite modular contractualmente las relaciones entre ellos para establecer unas medidas de seguridad apropiadas para los riesgos introducidos ni para acordar una adecuada contraprestación por el acceso a una infraestructura muy costosa. Esta última peculiaridad supuso, además, que los PISP y los AISP recelasen abiertamente de todo mecanismo de acceso a las cuentas de pago distinto del acceso directo facilitado por el ASPSP a sus clientes, ya que entendían que no existían incentivos para que los ASPSP ofrecieran soluciones realmente eficaces y operativamente fiables a través de API creadas al efecto.

Para solventar los recelos mencionados anteriormente, las RTS dispusieron explícitamente que las interfaces dedicadas tendrían que ofrecer, en todo momento, niveles de disponibilidad y de rendimiento no inferiores a los correspondientes a los accesos directos (interfaces de la banca *online),* al tiempo que se introducía la obligación de monitorizar dichos niveles y poner las estadísticas resultantes a disposición de la autoridad nacional competente. Asimismo, las interfaces dedicadas debían contar con mecanismos de contingencia equivalentes a los de los accesos directos, en previsión de que las interfaces dedicadas pudieran no operar con iguales niveles de disponibilidad y de rendimiento que las interfaces de banca *online.*

Sin embargo, los PISP y los AISP expresaron en diferentes foros la posible insuficiencia de estas medidas de contingencia. En su opinión, dichas propuestas se limitaban a implantar mecanismos que restaurasen, sin dilaciones, la disponibilidad de la interfaz dedicada, pero no garantizaban su buen funcionamiento en todo momento y, por ello, podían llegar

21 En la propuesta inicial de la EBA, este plazo era de tres meses, plazo que en la solución final de la Comisión Europea se mantiene solo para las modificaciones posteriores de las interfaces.

a poner en peligro la continuidad de la actividad de PISP y AISP. Este punto de vista fue compartido por el regulador europeo, el cual, a raíz de esta circunstancia, optó por incluir en las RTS medidas que incentivaran la implementación por parte de los ASPSP de interfaces dedicadas realmente eficientes.

En consecuencia, entre las medidas de contingencia[22], la Comisión Europea promovió la inclusión del denominado *fall back mechanism,* por el cual se permite a los PSP y AISP poder hacer uso del acceso directo mediante las interfaces ofrecidas directamente por el ASPSP a sus clientes a través de la banca *online,* en caso de que la interfaz dedicada no funcione correctamente. El inconveniente de esta propuesta es que su mera existencia supone un potente desincentivo para el desarrollo de interfaces dedicadas, pues implica que los ASPSP no solo tendrán que implementar las correspondientes interfaces específicas, sino que, además, deberán acomodar las interfaces de banca *online* a las disposiciones establecidas en las RTS en previsión de que hubieran de ser utilizadas por los PISP o los AISP, en aplicación del *fall back mechanism.*

Para evitar estos efectos colaterales, la Comisión Europea ha contemplado la posibilidad de que las autoridades nacionales competentes puedan eximir a los ASPSP, previa consulta a la EBA, de la obligación de adaptar las interfaces de banca *online* (acceso directo) a las normas establecidas en las RTS, siempre que se cumplan determinados requisitos. Entre estos destaca la exigencia de que las interfaces dedicadas sean diseñadas y probadas a satisfacción de los PISP y AISP, así como que se utilicen durante al menos tres meses para verificar que cualquier incidente se resuelve sin retrasos indebidos.

La solución de la Comisión Europea busca equilibrar los intereses y las obligaciones de ambas partes, pero presenta algunos retos importantes en términos de su implementación práctica. Por un lado, las RTS carecen del nivel de concreción que sería deseable en cuestiones tales como los indicadores clave de rendimiento, los niveles de servicio objetivo o los requisitos que han de satisfacer las interfaces dedicadas para poder ser eximidos de la implementación del *fall back mechanism.* La falta de precisión se ve agravada por el hecho de que la evaluación del rendimiento y el cumplimiento de los niveles de servicio se realizan por las partes en conflicto (ASPSP, PISP y AISP), a cuya satisfacción deben poder validarse las interfaces dedicadas.

La EBA está trabajando en unas directrices sobre las condiciones que deben cumplirse para que pueda ser otorgada la exención de la obligación de adaptar las interfaces de banca *online* a las normas establecidas en las RTS, con el objetivo de mitigar la falta de concreción comentada y, a la vez, facilitar la necesaria consulta previa por parte de las autoridades nacionales competentes para poder eximir a los ASPSP de implementar el *fall back mechanism.* A estos efectos, el 13 de junio de 2018 la EBA publicó el correspondiente documento de consulta, invitando a todas las partes interesadas a remitir cuantos comentarios consideraran oportunos[23].

---

22 De conformidad con las RTS, las medidas de contingencia habrán de activarse cuando el funcionamiento de las interfaces específicas no se ajuste a los requisitos establecidos en las RTS o cuando dichas interfaces no sean capaces de atender cinco peticiones de acceso consecutivas en menos de 30 segundos. A efectos de evaluar el funcionamiento de las interfaces específicas, los ASPSP deben definir indicadores clave de rendimiento totalmente transparentes, así como niveles de servicio objetivos, que no han de ser menos exigentes que los establecidos para las interfaces de banca *online.* Las interfaces, los indicadores y los objetivos deberán ser monitorizados por las autoridades y sometidos a pruebas de resistencia *(stress test)* por los propios ASPSP.

23 Este documento de consulta está accesible en: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-the-conditions-to-be-met-to-benefit-from-an-exemption-from-contingency-measures-under-article-33-6-of-regulation-eu-2018/389-rts-on-sca-csc-.

Sin embargo, estas directrices no serán suficientes para mitigar un segundo factor de incertidumbre derivado de la falta de especificación de los estándares de comunicación abiertos, comunes y seguros que satisfarían los preceptos establecidos en las propias RTS. Esta circunstancia deja sin referencias válidas a los ASPSP a la hora de diseñar las interfaces dedicadas, lo que podría dificultar el despliegue de soluciones efectivas y coherentes con las RTS, en un entorno de tiempo y recursos escasos.

Por si ello fuera poco, la falta de concreción de las RTS relacionada con el acceso de los PISP y los AISP a las cuentas de pago a través de las interfaces de banca *online* (acceso directo) es otro obstáculo importante para la implementación de las RTS. En este ámbito, las RTS se limitan a recordar que estos proveedores deben tomar todas las medidas necesarias para atender las restricciones operativas que impone la PSD2, y en particular la prohibición de acceder, almacenar o procesar datos de clientes con una finalidad distinta al servicio por ellos contratado. No se ofrecen medidas concretas que aseguren su cumplimiento más allá de algunas disposiciones relativas al registro y notificación de operaciones. Una consecuencia previsible será que, en la medida en que el *screen scraping* siga siendo un método de acceso habitual, el cumplimiento de los requisitos de la PSD2 por los PISP y los AISP quedará confiado a un ejercicio de propia autolimitación por parte de estos.

Consciente de estos problemas, la Comisión Europea ha promovido la creación de un grupo de análisis con representantes de todas las partes relevantes. Su objetivo es establecer las funcionalidades básicas que han de satisfacer las API que pretendan validar su adecuación a las RTS. Para ello, entre otras iniciativas, el grupo pretende realizar una revisión informal de las especificaciones técnicas de algunas API estandarizadas de ámbito paneuropeo. Esto permitirá disponer de un número razonable de estándares que, estando alineados con los requerimientos de las RTS y de la PSD2, puedan servir como referencia tanto para los ASPSP como para las respectivas autoridades nacionales.

La Comisión Europea confía en que este grupo de análisis sea capaz de completar de manera efectiva y consensuada las RTS, favoreciendo con ello una amplia implementación de interfaces dedicadas sustentadas en un número limitado de API estandarizadas. Se conseguiría así erradicar el uso del *screen scraping* y, además, se sentarían las bases para la generalización de un modelo de negocio basado verdaderamente en un entorno de *open banking,* si bien limitado a las cuentas de pago. Adicionalmente, se favorecería el cumplimento de otras disposiciones normativas, y en particular de la relativa a la protección de datos.

Sin embargo, la experiencia de los trabajos que sobre este particular se desarrollaron en el *Euro Retail Payments Board*[24] evidencia las dificultades para poder llegar a acuerdos en áreas tan relevantes como el tratamiento del consentimiento del titular de la cuenta de

---

24 El *Euro Retail Payments Board* (ERPB) fue creado en diciembre de 2013 por el BCE en sustitución del Consejo SEPA, con el objetivo de fomentar el desarrollo de un mercado de pagos al por menor en euros integrado, innovador y competitivo en la Unión Europea. A finales de 2016, el ERPB decidió crear un grupo de trabajo sobre servicios de iniciación de pagos, que presentó el correspondiente informe en noviembre de 2017. Este informe está disponible en:
https://www.ecb.europa.eu/paym/retpaym/shared/pdf/8th-ERPB-meeting/PIS_working_group_report.pdf?483e4d28242cd84322850a01e549d116.
En lo relativo a los aspectos técnicos de las API, los trabajos de este grupo están siendo continuados por el grupo de análisis promovido por la Comisión Europea.
Un segundo informe de dicho grupo, referido a otros requerimientos necesarios para la integración europea de los servicios de iniciación de pagos, puede consultarse aquí:
https://www.ecb.europa.eu/paym/retpaym/euro/html/index.en.html.

pago, el ámbito en el que debe producirse la autenticación del cliente, la información que el ASPSP ha de facilitar al PISP, la provisión combinada de servicios de iniciación de pagos y de agregación de información o la identificación de indicadores claves.

A fin de asegurar una pacífica implementación de las RTS, el grupo de análisis promovido por la Comisión Europea no solo deberá ser capaz de completar estos trabajos, sino que, además, habrá de alinear sus interpretaciones con las realizadas por las autoridades nacionales y la EBA, en el ámbito de sus respectivas competencias. La consecución de unos objetivos tan ambiciosos determinará el posible éxito de las RTS y, por tanto, de los aspectos básicos de la nueva regulación de los servicios de pago en Europa.

La falta de acuerdo en dicho grupo derivaría en una proliferación de soluciones divergentes que obstaculizaría enormemente tanto la implementación de las RTS como la armonización de los servicios de pago en la UE. Si, por el contrario, el grupo culminara con éxito sus esfuerzos, las RTS serían un instrumento eficaz para acomodar de manera razonable y suficiente los importantes sesgos y compromisos impuestos por la PSD2, y conseguir que la industria trabaje conjuntamente en asuntos que, además de ser fundamentales en su operativa diaria, resultan estratégicos para su futuro.

3 El posible impacto de la PSD2

Tras analizar en las secciones anteriores las principales tendencias en cuanto a la digitalización de los servicios de pago y la complejidad de la PSD2, procede ahora evaluar el posible impacto de estos cambios sobre la estructura y la configuración futura del mercado. Lógicamente, es imposible anticipar con precisión la escala de esta transformación, más aún cuando muchas de las novedades regulatorias carecen todavía del detalle necesario. No obstante, ya es posible identificar algunas tendencias de fondo sobre las que aventurar potenciales escenarios y sus previsibles implicaciones sobre los diferentes tipos de proveedores.

Uno de los rasgos característicos del nuevo entorno digital en los servicios de pago es la creciente disociación entre la administración de la cuenta de pago y el acceso a la información de las operaciones que se producen sobre ella. La apertura y la gestión de las cuentas de pago (en su mayoría, cuentas bancarias) son actividades sometidas a una regulación exigente, por tratarse de fondos del público que han de ser salvaguardados. Tradicionalmente, el ASPSP y el cliente titular de la cuenta han sido los únicos con visibilidad sobre ella, por lo que la prestación del servicio de pago exigía una relación comercial directa entre ambos. Sin embargo, la popularización de soluciones de pago *online,* basadas en el uso de tarjetas e integradas en los portales web de los comerciantes, contribuyó a diluir parcialmente ese vínculo, aun cuando la relación subyacente siguiera muy presente.

La aplicación de la PSD2 acentuará previsiblemente este proceso de disociación, al reconocer la posibilidad de establecer un intermediario (el PISP) que interactúe, en nombre del cliente, entre este y el proveedor de servicios de pago que administre su cuenta. Los agregadores de información, por su parte, también podrán acceder a las cuentas de pago de los clientes e interactuar directamente en su nombre con diversas entidades.

Como se apuntó en la sección precedente, la consecuencia de este régimen es que las entidades intermedias podrán establecer ahora una relación directa con los clientes, accediendo a información de indudable valor comercial, sin tener que soportar las cargas asociadas a la administración de las cuentas de pago, como el mantenimiento y la mejora de la infraestructura, el consumo de recursos propios, los costes de seguridad informática

y de cumplimiento regulatorio, etc. Esta asimetría busca fomentar la competencia dentro de la industria de pagos y, con ello, su eficiencia y modernización y debe ser objeto de especial atención a fin de evitar situaciones de injustificadas ventajas competitivas para las entidades intermedias.

Por otro lado, este sistema de apertura a terceros autorizados es, a su vez, el causante de un potencial conflicto entre el interés creciente por mejorar los niveles de protección de la información personal (algo que la PSD2 recoge en las disposiciones en materia de seguridad) y la aspiración de fomentar la innovación la y competencia en el espacio de los servicios de pago. Tanto los bancos como el resto de proveedores de servicios de pago están obligados a cumplir con las cada vez más exigentes normas sobre protección de datos[25] y con las exigencias que se derivan de la PSD2 y de su normativa de desarrollo. Por tanto, existe una clara necesidad de garantizar que la información de carácter personal suministrada por parte de un proveedor de servicios de pago administrador de cuenta a un PISP o a un AISP sea tratada de forma segura y que no infrinja la normativa sobre protección de datos.

En este contexto, en su papel de gestora de las cuentas, la banca aduce la presencia de serias dificultades para poder establecer las salvaguardas necesarias que permitan asegurar que los terceros tratan dicha información en los términos solicitados por los clientes. Esto responde, entre otras razones, a la ya comentada inexistencia de un marco contractual directo entre ambas partes que delimite con claridad sus compromisos. Si a esto se añade la responsabilidad del ASPSP derivada de la normativa sobre protección de datos, el sector queda expuesto a una situación bastante compleja, por lo que se impone un análisis detallado de sus implicaciones, una posible orientación y la cooperación de las distintas autoridades competentes.

Finalmente, el régimen informativo de carácter aperturista que preconiza la PSD2 es todavía bastante asimétrico. La directiva establece que la información sobre las cuentas de pago sea accesible a terceros, aunque limita su almacenamiento, consulta y empleo exclusivamente a la prestación del servicio de pago contemplado en la norma (es decir, en los términos en que este está regulado). No obstante, la normativa no impide que, con el explícito consentimiento del cliente y al margen del servicio de pago de que se trate, esta misma información pueda ser recopilada simultáneamente para otros fines.

Además, en la medida en que los proveedores terceros no gestionen, a su vez, cuentas de pago (como es el caso de los AISP), estos no tienen obligación alguna de compartir con los ASPSP o con cualquier otro tercero interesado los contenidos de sus respectivas bases de datos[26]. Esta falta de reciprocidad puede, a su vez, desembocar en una mayor concentración del «mercado de datos» por la presencia de economías de escala y efectos de red en dicho ámbito. En consecuencia, es previsible que las tensiones que genere esta situación obliguen a discutir en el futuro si se establecen reglas similares a las de la PSD2 en otras áreas ajenas a los servicios de pago. En tanto esto no se produzca, el escenario descrito podría originar desventajas competitivas para los ASPSP frente a otros proveedores.

Como ya se ha indicado, es difícil anticipar unas implicaciones nítidas de la PSD2, pero cabe hacer algunas reflexiones preliminares, teniendo en cuenta la heterogeneidad de los

25 La normativa básica es el Reglamento (UE) 2016/679, de protección general de datos.

26 Esto resulta particularmente relevante en el caso de grandes compañías tecnológicas que hayan optado por operar como AISP y que ya disponen de una amplia base de clientes e información comercial extensa sobre ellos a la que enriquecer sobre la base de estos nuevos *inputs*.

diversos tipos de proveedores, a los que hasta ahora nos hemos referido como grupos predominantemente homogéneos.

Centrándonos primero en los proveedores de servicios de pago gestores de cuenta (ASPSP), es evidente que las entidades bancarias tienen una posición hegemónica en este grupo, aunque parece que no todos los bancos están reaccionando de igual forma ante los cambios de la PSD2. Es previsible que algunos bancos tradicionales[27] (sobre todo, los de tamaño mediano y pequeño) no modifiquen su conducta competitiva y reaccionen de forma pasiva a la PSD2, implantando solo los cambios imprescindibles para cumplir con la normativa. Este tipo de entidades se limitaría a transmitir a terceros autorizados la información de las cuentas de pago que sus respectivos clientes hayan querido ceder a estos nuevos proveedores. Así las cosas, cabe pensar que estas entidades no desarrollarán un API propio para facilitar la transmisión de la información, sino que permitirá el reaprovechamiento del canal de banca electrónica que ofrecen a sus clientes.

Por el contrario, otras entidades bancarias (posiblemente, las de mayor tamaño o de reciente creación —bancos de Internet sin sucursales—) podrían percibir la PSD2 como una oportunidad. En consecuencia, aunque serán ASPSP frente a terceros, según les obliga la norma, podrían también contemplar la posibilidad de actuar como terceros autorizados para obtener información de cuentas o iniciar pagos en las cuentas de sus clientes (antiguos y nuevos) en otras entidades. Como ASPSP, es previsible que desarrollen interfaces dedicadas, basadas en API, para mejorar la seguridad y la eficiencia de la transmisión de información. Asimismo, es posible pensar que este tipo de entidades lleve a cabo un esfuerzo sustancial para mejorar la experiencia de pago *online,* adaptar sus interfaces de comunicación con los clientes y lograr mantener la vinculación con ellos.

En cuanto a los proveedores de servicios de iniciación o agregación (TPP), se percibe incluso una mayor heterogeneidad, dentro de la que cabría distinguir tres grandes categorías. Por un lado, se situarían las pequeñas compañías, dedicadas únicamente a proveer soluciones de iniciación de pagos o de información de cuentas. Es previsible que el mayor desafío y limitación de este tipo de entidades sea carecer inicialmente de una base de clientes, por lo que, posiblemente, podrían basar su modelo de negocio en prestar un servicio concreto o en proveer una innovación tecnológica específica que cubra necesidades puntuales en el mercado.

En segundo lugar, es posible que empresas tecnológicas de gran tamaño (en ocasiones, denominadas *bigtechs),* con una amplia base de clientes y un extenso catálogo de servicios no financieros, muestren interés en actuar como agregadores de información o iniciadores de pagos. La obtención de una licencia para prestar servicios de agregación supondría un coste reducido para este tipo de compañías y, a cambio, les ofrecería la posibilidad de combinar la amplísima información de que ya disponen sobre los gustos y preferencias de sus clientes con datos financieros sobre sus cuentas de pago. Esto último, combinado con el uso de técnicas analíticas avanzadas, podría contribuir a ampliar y a mejorar la gama de productos y servicios ofrecidos a sus clientes, incluyendo, además, la experiencia de pago en sus plataformas cuando opten por solicitar una licencia como PISP. En este caso, la prestación de servicios de pago podría ser un primer paso hacia una creciente involucración en el área de los servicios financieros.

27 Aquellos distintos a los bancos digitales, creados específicamente para operar a través de Internet (también denominados *challenger banks).*

Finalmente, hay que tener presente que las propias entidades bancarias, como ya se ha destacado, no tienen limitación alguna para actuar como proveedores de servicios de agregación o de iniciación de pagos. En principio, los bancos podrían prestar este tipo de servicios para tratar de retener y fidelizar a su clientela, pero también para ganar cuota de mercado, intentando captar clientes de otras entidades.

Las interacciones entre estos grupos de ASPSP y TPP serán necesariamente complejas, y es difícil anticipar el escenario final cuando todavía no existe claridad sobre algunos aspectos importantes de la PSD2. El resultado último dependerá de diversos factores, tales como la naturaleza de la estructura bancaria de cada país, el apetito innovador de sus bancos, la cantidad y el tamaño de las entidades que tengan interés en entrar en el mercado como terceros autorizados, el grado de fidelización de la clientela bancaria o, en su caso, la eventual respuesta regulatoria final.

En cualquier caso, lo más probable es que surja una situación en la que algunas entidades bancarias se adaptarán y serán capaces de prosperar en el nuevo entorno, mientras que otras encontrarán dificultades para poder seguir manteniendo una relación fluida con sus clientes. Por parte de los nuevos entrantes, las pequeñas *startups,* para hacer frente al reto de su escasa base de clientes, podrían establecer alianzas con las entidades bancarias. Sin embargo, las grandes plataformas tecnológicas constituyen la gran incógnita de esta ecuación. Si son capaces de aprovechar la coyuntura que se les presenta, estos actores emergentes estarán llamados a ser la principal amenaza competitiva para la banca tradicional, exhibiendo un serio potencial para transformar la realidad del sector financiero tal y como ha venido conociéndose hasta el momento.

4 Conclusiones

Hoy en día, el ritmo y la profundidad de la innovación financiera están estrechamente vinculados a la aplicación intensiva de las nuevas tecnologías, en lo que se refiere tanto al diseño y a la provisión de productos y servicios típicamente bancarios como al modo en que se organizan y ejecutan los procesos y procedimientos necesarios para su comercialización y soporte.

En esta coyuntura, ha sido precisamente la industria de los servicios de pago la que de manera más visible ha sido tributaria del grueso de estos cambios, sin dejar por ello de ser el ámbito que anticipa un mayor recorrido potencial en un futuro inmediato. El regulador, con la PSD2 como mayor exponente, no ha querido limitar, sino más bien lo contrario, las actuales presiones competitivas a que está sometido el sector, posibilitando un acceso amplio, por parte de terceras partes autorizadas, a las cuentas de pago que, principalmente, han estado gestionadas por los bancos.

De este modo, la explotación de la información sobre los clientes, que mantiene intacto su carácter estratégico, deja de ser una prerrogativa exclusiva de la banca para pasar a ser objeto de un manejo más universal —con las adecuadas garantías— en beneficio tanto de los propios clientes como del conjunto de la sociedad.

Se abre un escenario de incertidumbre para la banca tradicional, que deberá, como en múltiples ocasiones anteriores, hallar la fórmula que resulte más adecuada para mitigar los riesgos asociados a la nueva realidad y alcanzar el mejor aprovechamiento posible de las amplias oportunidades abiertas. Los mayores retos para la banca son la redefinición de los modelos de negocio y la cooperación con los nuevos agentes, junto con la potencial amenaza que pueden suponer las grandes empresas tecnológicas. Estos factores marcarán el paso de una evolución que, sin ningún lugar a dudas, dejará una profunda huella en los mercados de servicios financieros.

Glosario de términos

AIS: *Account Information Service*

AISP: *Account Information Service Provider*

API: *Application Programming Interface*

ASPSP: *Account-servicing Payment Service Provider*

B2C: *Business-to-Consumer*

CSC: *Common and Secure Communication*

ERPB: *Euro Retail Payments Board*

PIS: *Payment Initiation Service*

PISP: *Payment Initiation Service Provider*

PSD1: 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

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, 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

PSP: *Payment Service Provider*

RTS: *Regulatory Technical Standards*

SCA: *Strong Customer Authentication*

TPP: *Third-Party Provider*

TRA: *Transaction Risk Analysis*

BIBLIOGRAFÍA

AUTORIDAD CATALANA DE LA COMPETENCIA (2017). *Sistemas de Pago,* n.º 16/2017, Barcelona.

BBVA RESEARCH (2015). «PSD2, perspectiva del modelo de negocio: las API financieras fomentarán la innovación en el modelo de negocio», *Situación Economía Digital,* diciembre.

BRODSKY, L., y L. OAKES (2017). *Data sharing and open banking,* McKinsey & Company Financial Services, Londres & San Francisco.

CAPGEMINI (2018). *World FinTech Report.*

CARBÓ VALVERDE, S., y F. RODRÍGUEZ FERNÁNDEZ (2017). «Proyecciones de la digitalización financiera en España, 2017-2020», *Cuadernos de Información Económica,* septiembre.

COMISIÓN EUROPEA (2018). *Reglamento Delegado (UE) 2018/389, de 27 de noviembre de 2017, por el que se complementa la Directiva 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.*

KPMG (2017). *El nivel de madurez digital del sector financiero en España.*

PARLAMENTO EUROPEO Y CONSEJO (2015). *Directiva (UE) 2015/2366, 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.*

– (2016). *Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en relación con el tratamiento de datos personales y la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).*

SANTAMARÍA, J. (2018). *La Segunda Directiva de Servicios de Pago y sus impactos en el mercado,* Fundació Caixa d'Enginyers, Nota Técnica n.º 31, enero.