PSD2: Escenario actual tras su implantación y retos jurídicos del "*open banking*"

Paula De Biase
Counsel de Pérez-Llorca
DEPARTAMENTO DE CORPORATE
RESPONSABLE DE LA PRÁCTICA DE SERVICIOS FINANCIEROS

Álvaro Basco Domínguez
Abogado de Pérez-Llorca
DEPARTAMENTO DE CORPORATE

Índice/

Resumen: A diferencia de la mayoría de las directivas regulatorio-financieras publicadas desde la crisis de 2008 – que han tenido en líneas generales un carácter más restrictivo sobre la operativa bancaria bajo un enfoque de supervisión y/o transparencia frente a clientes – 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 ("**PSD2**"), introduce un reto distinto. Se incrementan las medidas de seguridad ante fraudes digitales a la vez que se promueve la apertura del espacio financiero a más jugadores (*open banking*), regulando las obligaciónes y condiciones bajo las cuales las entidades financieras deben compartir ciertos datos de cliente, siempre que estén expresamente autorizados por estos, con terceros proveedores que pueden, a su vez, desarrollar otros servicios de pago con base en dicha información. Todo ello, conlleva no solo un reto de adaptación tecnológica o en cuestiones de cumplimiento normativo o *compliance*, sino también un reto estratégico y operativo para muchas entidades.

El presente trabajo destaca resumidamente las principales novedades derivadas de la PSD2 y el nuevo escenario tras su trasposición, tratando en particular algunos de los principales retos relacionados con el *open banking*, y la aplicación de la autenticación reforzada en operaciones de pago.

Abstract: Unlike most of the financial regulatory directives issued since the 2008 financial crisis – which have generally been more restrictive as regards banking operations, focusing on supervision and/or transparency for clients – Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market and amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (the "**PSD2**") introduces a different challenge. Security measures against digital fraud have been increased, while promoting the opening of the financial market to more players (open banking), regulating the obligation and conditions under which financial institutions must share certain customer data, provided that customers have expressly authorised this, with third party providers who may, in turn, develop other payment services based on such information. All of this entails challenges for many entities, both in terms of adapting technology and compliance issues, and in terms of strategy and operations.

This article summarises the main developments arising from the PSD2 and the new scenario following its transposition, and in particular addresses some of the main challenges related to open banking and the application of strong customer authentication in payment transactions.

Palabras clave: Segunda Directiva de servicios de pago (PSD2), autenticación reforzada, terceros proveedores, agregación financiera, servicios de iniciación de pagos, *open banking*.

Keywords: Second Payment Services Directive (PSD2), strong customer authentication, third party providers, financial aggregation, payment initiation services, open banking.

PSD2: Escenario actual tras su implantación y retos jurídicos del "*open banking*"

I. Introducción

La **PSD2** fue transpuesta en España con cierto retraso mediante el Real Decreto-ley 19/2018 de servicios de pago y otras medidas urgentes en materia financiera ("**RDL de Servicios de Pago**") y su desarrollo reglamentario fue aprobado por el Real Decreto 736/2019 de régimen jurídico de los servicios de pago y las entidades de pago.

A pesar de que la PSD2 y sus normas técnicas de desarrollo – en particular 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 ("**RTS SCA & CSC**") – ya entraron en vigor, en la práctica todavía quedan cuestiones por depurar desde un punto de vista técnico y/o aclaraciones legales para que la PSD2 despliegue todo su poder disruptivo en el mercado. En particular, se hace necesaria tanto una implementación técnica plena de los nuevos estándares de comunicación segura a través de interfaces de programación de aplicaciones ("**APIs**") y aclaraciones sobre la viabilidad de ciertos modelos de negocio, como la puesta en marcha de la autenticación reforzada para el comercio electrónico, que tiene como fecha límite para desplegar sus efectos el 31 de diciembre de 2020.

La trasposición tardía, así como la complejidad técnica derivada de los expedientes de adaptación a la PSD2 y/o de aprobación de nuevos servicios de pago ha ralentizado la concesión de autorizaciones regulatorias, y hasta la fecha, hay muy pocos proveedores registrados ante el Banco de España para la prestación de los nuevos servicios de pago[1] regulados bajo la PSD2. No obstante, es importante reconocer que en ciertas materias que la PSD2 permitía una opción nacional sobre su implementación, en líneas generales, España ha adoptado el camino que otorga más flexibilidad al sector de los servicios de pago. En este sentido, es destacable la incorporación de una nueva excepción a la obtención de una autorización como entidad de pago, exigiéndose solamente un registro simplificado para la prestación de servicios de pago, distintos a información sobre cuentas ("**AIS**[2]"), e iniciación de pagos ("**PIS**[3]"), que limiten sus operaciones a 3 millones de euros mensuales (como media de los últimos 12 meses)[4]. Para ciertos modelos de negocio en los que su calificación como un servicio de pago esté clara, este régimen podría otorgar más flexibilidad y efectividad para nuevas *Fintechs* y *start-ups* del sector que el proyecto de *sandbox* regulatorio[5], el cual se encuentra pendiente de aprobación por las Cortes.

1 Información sobre cuentas e iniciación de pagos.

2 Desde su definición en inglés "*Account Information Services*".

3 Desde su definición en inglés "*Payment Initiation Services*".

4 Se trataba de una excepción de elección nacional desde PSD1 que España solo ha optado por utilizarla al trasponer la PSD2.

5 Se trata del proyecto de ley de trasformación digital del sistema financiero que incluye la creación de un *sandbox* o espacio controlado de pruebas. Esta iniciativa responde a la necesidad de impulsar la innovación como elemento esencial para un desarrollo económico sostenible y equitativo. Una vez entre en vigor, se prevé que el *sandbox* permitirá llevar a cabo proyectos tecnológicos de innovación en el sistema financiero en fase de prueba con clientes reales pero por un tiempo limitado antes de la obtención de la licencia regulatoria pertinente, cuyo periodo de tramitación podría reducirse como consecuencia de la información compartida con los reguladores en fase *sandbox*.

Antes de centrarnos en algunos retos derivados de los nuevos modelos de *open banking* y la implementación de la autenticación reforzada, para contextualizar la problemática, pasaremos a resumir las principales novedades derivadas de la implementación de la PSD2 en nuestro ordenamiento.

II. Principales novedades de RDL de Servicios de Pago

Las principales novedades derivadas de la trasposición de la PSD2 en nuestro ordenamiento pueden subdividirse en cuatro grandes bloques:

- La primera gran novedad es la regulación de dos nuevos servicios de pago (los AIS y PIS), y, en particular, el régimen aplicable a la autorización de dichos proveedores, así como las obligaciones derivadas de la relación entre estos últimos y los proveedores gestores de cuentas.

- En un segundo bloque, podemos incluir ciertas modificaciones relevantes del régimen de excepciones a la aplicación de la normativa de servicios de pago y, en particular pero no exclusivamente, a la excepción de red limitada. Asimismo, se introduce una nueva excepción al régimen completo de autorización (exigiendo un registro más sencillo) para la prestación de ciertos servicios de pago[6] que no sobrepasen el umbral de 3 millones de euros al mes.

- El tercer bloque está relacionado con obligaciones contractuales o de responsabilidad frente a los usuarios, incluyendo en particular (i) equiparación de la microempresa a consumidor, (ii) regulación de ventas vinculadas, (iii) prohibición de recargo por utilización de un determinado instrumento de pago, y (iv) cambios en los límites de responsabilidad del ordenante en caso de operaciones de pago no autorizadas.

- Por último, destacamos todos los cambios relacionados con la seguridad en las comunicaciones entre usuarios, proveedores y sus bancos, incluyendo tanto las obligaciones de autenticación reforzada de operaciones, como los nuevos estándares de comunicación entre terceros proveedores y entidades gestoras de cuentas.

III. Autenticación reforzada

El RDL de Servicios de Pago define en su artículo 3, "autenticación" como el "procedimiento que permita al proveedor de servicios de pago comprobar la identidad de 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" y "autenticación reforzada de cliente" conocida por sus siglas

6 Se excluye de dicha posibilidad la prestación de información sobre cuentas e iniciación de pagos.

en inglés como SAC, como "la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), 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 identificación".

Con la implementación de la PSD2, los proveedores de servicios de pago son obligados a utilizar dicha autenticación reforzada de doble factor cuando el ordenante (i) acceda a su cuenta de pago en línea; (ii) inicie una operación de pago electrónico y/o (iii) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.

Esto implica que los distintos proveedores de servicios de pago tienen que implementar nuevas soluciones tecnológicas cumplidoras de los parámetros de autenticación reforzada y a la vez, migrar sus distintos clientes (ya sean personas físicas o comercios) hacia el uso de dichas nuevas soluciones. Además, en aras de permitir una experiencia de usuario de un solo clic (extremamente deseable por muchos comercios online), es necesario que dichas soluciones puedan permitir la gestión de la aplicación de las distintas excepciones a la autenticación reforzada previstas en el RTS SCA & CSC, siempre que esto sea posible. Entre dichas excepciones se encuentran, por ejemplo, operaciones de baja cuantía, las realizadas con beneficiarios de confianza incluidos en una lista previamente por el ordenante, operaciones frecuentes con un mismo proveedor y transferencias de créditos entre cuentas mantenidas por la misma persona.

Para poder aplicar dichas excepciones, los proveedores de servicios de pago están obligados a realizar un análisis de los riesgos de fraude que ello pueda entrañar y, para ello, es fundamental que los sistemas tecnológicos utilizados permitan la trasmisión de distintos datos asociados a la transacción. Así, es fundamental que los sistemas e infraestructuras de pagos en los cuales se apoyan los emisores a través de las marcas licenciatarias (Visa, MasterCard, Amex, etc.) permitan que la información que se trasmite con cada transacción sea lo más completa posible de forma que permita dicho análisis de riesgo por los proveedores de pago y así puedan gestionar y autorizar el mayor número de excepciones posible a la aplicación de la autenticación reforzada.

El RTS SCA & CSC entró en vigor el 14 de septiembre de 2019 y estaba previsto que tanto la autenticación reforzada como los nuevos estándares de comunicación seguros por APIs resultasen de aplicación desde esa fecha. No obstante, conocedora de los desafíos asociados a estos cambios normativos y su impacto en comercio electrónico[7] manifestados por el sector, la Autoridad Bancaria Europea ("**EBA**") otorgó cierta flexibilidad a las autoridades nacionales (en el caso español, el Banco de España) para coordinar con los proveedores de servicios de pago bajo su supervisión, un tiempo adicional limitado para adaptarse a los procedimientos de la autenticación reforzada, pero únicamente en lo que se refiere a las

7 Se debe tener en cuenta que la experiencia de usuario actual de utilización del número de tarjeta, validez y CCV más código OTP enviado el móvil no sería suficiente para cumplir la autenticación reforzada, pues la información de número de tarjeta, validez y CCV no puede ser considerada como un elemento que solo conoce el ordenante.

operaciones de comercio electrónico (la normativa de autenticación para acceder a cuentas online, por ejemplo, entró en vigor el 14 de septiembre).

En su Opinión de fecha 16 de octubre de 2019, la EBA aclaró que dicho "tiempo adicional limitado" no podría exceder del 31 de diciembre de 2020. Como consecuencia de ello, los proveedores de servicios de pago afectados han presentado ante el Banco de España el pasado mes de diciembre de 2019 sus planes de migración para el cumplimiento de la autenticación reforzada antes del 31 de diciembre de 2020. Mientras algunos proveedores utilizan soluciones propias, otros se apoyan en soluciones de terceros.

A fecha de cierre de este artículo, asociaciones del sector de pagos reclaman a la EBA una nueva extensión de la fecha de migración, teniendo en cuenta la ralentización del calendario de migración como consecuencia de la COVID-19, en particular, en relación con los sectores de servicios y comercios más afectados (como restauración u hotelería). Todavía no está decidido si la EBA flexibilizará la fecha del 31 de diciembre de 2020. Los reguladores nacionales reciben información trimestral actualizada sobre el calendario que han trazado los proveedores de pago en su plan de migración y podrán remitir a la EBA información precisa sobre posibles retrasos e impacto real declarado por las entidades. Lo que sí está claro es que el impacto de la implementación de la autenticación reforzada en el comercio electrónico será seguramente mayor de lo que se esperaba cuando se aprobó dicha "prórroga/flexibilidad supervisora", teniendo en cuenta el incremento del canal de venta online como consecuencia de la pandemia.

IV. *Open banking* y nuevos proveedores de pago

Tal y como se indicó anteriormente, una de las principales novedades de la PSD2 es la regulación de los servicios de AIS[8] y de PIS[9], y la obligación de que los proveedores de pago gestores de cuenta (normalmente entidades de crédito) den acceso a la información relacionada con las cuentas de sus clientes a dichos proveedores, siempre que los clientes lo autoricen expresamente a través de un sistema de comunicación segura regulada a estos efectos. Los proveedores de dichos nuevos servicios (AIS y PIS) son conocidos como TPPs (del inglés, *Third Party Providers*) y se regula por la PSD2 únicamente su acceso a información relacionada con cuentas de pago y la iniciación de operaciones de pago (es decir, no se regula el acceso a información financiera en general como seguros, fondos, etc. – no de pago – o incluso el acceso a información no financiera relacionada).

Es importante destacar que ambos servicios ya venían siendo prestados antes de la implementación de PSD2. Sin embargo, no había un marco de comunicación estandarizada segura a estos efectos entre los proveedores, ni tampoco una obligación legal expresa por parte de los proveedores gestores de cuenta de compartir dicha información[10] con los TPPs.

8 Definido como el "servicio en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago".

9 Definido como el "servicio que permite iniciar una orden de pago, a petición del usuario de servicios de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago".

10 A estos efectos, se utilizaba una técnica conocida como screen-scrapping a través de la cual el TTP podría extraer datos de una aplicación o sistema con objeto de volcarlos en otro para posteriormente trabajar con ellos, sin una identificación separada ("el TTP entra como si estuviera accediendo el propio usuario").

Muchos modelos de negocios colaborativos (que representan lo que se denomina en el mercado como *open banking*) se basan en la posibilidad de utilizar la información financiera de clientes para prestar servicios de valor añadido al mismo, ya sea de forma directa (por ejemplo, agregando la información financiera en formatos que permitan controlar mejor sus ingresos y gastos, y/o proponiendo servicios más acordes con su perfil personal) o de forma indirecta (por ejemplo, permitiendo que un tercero analice su crédito/solvencia con base en dicha información disponible en línea y ahorrando el tiempo y coste derivado de suministrar información al respecto por otras vías). En este contexto, los modelos de agregación financiera utilizados normalmente no se limitan únicamente a información sobre cuentas de pago, lo que nos lleva a un primer reto de integración, al tener que aplicar la PSD2 en un contexto de negocio mucho más amplio y, en muchos casos, todavía no regulado más allá de las limitaciones derivadas de la normativa general de protección a consumidores y usuarios y la de protección de datos.

Otra vertiente del *open banking* radica en la posibilidad de que TPPs puedan iniciar operaciones de pago desde cuentas de otros proveedores. Se trata de permitir que un comercio, por ejemplo, al integrar un proveedor de iniciación de pagos, pueda ofrecer a sus clientes la posibilidad de pagar con transferencias bancarias[11] desde distintos bancos sin tener que dirigirse a la página web de banca online de su banco. Dicha comunicación con la entidad gestora de la cuenta es realizada por el TPP que, a su vez, se comunica con el comercio indicando que la transacción ha sido efectuada.

En este contexto, uno de los puntos que están en discusión a nivel europeo son aspectos de identificación del cliente (*Know Your Customer* – KYC) en dichas operaciones y quién debe ser considerado cliente. Por ejemplo, en las operaciones de iniciación de pago, se plantea si sería el usuario que solicita la orden o el comercio/plataforma *Business to Business* (B2B) con quien el proveedor de servicios de iniciación de pagos suscribe un contrato para integrar su solución de iniciación de pagos. En este sentido, es importante destacar los trabajos que están actualmente en marcha con el fin de promover criterios armonizados entre las distintas autoridades nacionales competentes. En particular, la consulta que se ha lanzado desde la EBA el pasado 5 de febrero de 2020[12], sobre la revisión de las directrices de factores de riesgo de blanqueo de capitales y financiación del terrorismo.

Otras materias que han estado en discusión y van siendo objeto de aclaraciones por las autoridades competentes (en particular, a través de la herramienta de preguntas y respuestas de la EBA y/o directrices y opiniones emitidas por la misma) son las relativas al contenido concreto de la información que debe ser proporcionada a través de las APIs. En este sentido, uno de los puntos debatidos ha sido, por ejemplo, si era obligatorio informar del nombre del titular de la cuenta –cuestión que fue objeto de aclaración por la EBA[13] en el sentido de que sería obligatorio siempre que el nombre del titular sea una información visible por la interfaz online que tiene acceso el usuario–.

11 Operativa de gran utilidad para el pago de importes altos que podrían no ser cubiertos por límites de las tarjetas.

12 https://eba.europa.eu/eba-consults-revised-guidelines-money-laundering-and-terrorist-financing-risk-factors

13 Q&A actualizado a fecha 20 de diciembre de 2020 https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4081

V. Conclusiones

La implementación de la PSD2 en España ha traído consigo un gran reto a nivel tecnológico y estratégico para el sector. El nuevo escenario de *open banking* es una realidad imparable no solo a nivel europeo, sino que también está en discusión o viene siendo implementada en muchos otros países. La mayoría de las nuevas reglas de juego de este nuevo escenario colaborativo ya están en vigor. No obstante, todavía queda camino por recorrer para una total implementación y normalización de los nuevos estándares de comunicación segura utilizados, así como para la implementación de las medidas de autenticación reforzada en comercio electrónico.