

CAPÍTULO 7

DERECHOS Y OBLIGACIONES DE LAS PARTES DEL CONTRATO DE SERVICIOS DE PAGO

I. LAS NORMAS SOBRE AUTORIZACIÓN Y EJECUCIÓN DE OPERACIONES DE PAGO COMO DERECHOS Y OBLIGACIONES CONTRACTUALES DE LAS PARTES

El título III del RDLSP se dedica a los «derechos y obligaciones en relación con la prestación y utilización de servicios de pago» pero, a decir verdad, lo que se regula en los artículos insertos en él son fundamentalmente obligaciones del PSP, con algunas excepciones que tienen al usuario como sujeto. Aquellas son, a su vez, derechos del usuario, en la medida en que, si los PSPs no cumplen sus obligaciones cuando tengan carácter imperativo o porque las partes las han incorporado voluntariamente en el contrato, generaran la correspondiente responsabilidad. Responsabilidad contractual prevista expresamente en la ley especial. El régimen contenido en los arts. 45 y 46 RDLSP, así como en la sección 3.^a del capítulo III constituye la positivización de algunos de los efectos jurídico-privados del incumplimiento de este régimen común de autorización y ejecución de las operaciones de pago, junto con algunas otras disposiciones previstas en otros preceptos de este título.

La mayoría de obligaciones recogidas en el título III, cuyos antecedentes más lejanos los encontramos en la Recomendación 88/590/CEE

relativa a los sistemas de pago y en particular a las relaciones entre titulares y emisores de tarjetas, y en la Ley Modelo de la UNCITRAL sobre transferencias internacionales de crédito del año 1992, podrían ser calificadas como operativas, porque se refieren precisamente a cómo deben prestarse los servicios de pago, a los requisitos que tiene que cumplir el proceso de pago: gastos, autorización, tratamiento de la orden, plazo de ejecución, etc. Junto a estas, se contienen también obligaciones en materia de protección de datos, de seguridad y de procedimientos de resolución alternativa de litigios. El hecho de que estos aspectos se contengan en el mismo título, a pesar de que podría parecer que no encajan del todo con el resto de disposiciones del mismo, no es baladí. Se trata también de derechos del usuario: el derecho a la protección de sus datos de carácter personal en la prestación de estos servicios, el derecho a la seguridad en la gestión de sus fondos, instrumentos y en el proceso de pago y el derecho a acudir a procedimientos alternativos de resolución de litigios con su proveedor. Esta estructura, que deriva de la propia norma europea desde la Primera Directiva de servicios de pago y, aunque más simplificada, incluso desde la Directiva de transferencias transfronterizas de 1997, es expresión de la *ratio legis* de este régimen especial: la tutela del usuario, no tanto en el sentido de protegerle de un perjuicio potencial —aunque algo de eso hay— sino en el de reequilibrar su posición en la relación contractual. Ello se pretende conseguir garantizando un conocimiento suficiente de los términos de la contratación (transparencia) para permitir la comparabilidad de servicios (a la vez que se fomenta la competencia) y la elección de los que mejor satisfagan sus necesidades, asegurando unos mínimos estándares de prestación en este título III RDLSP que, por un lado, aseguren que la dinámica del propio mercado no favorezca solo los intereses de los proveedores y, por el otro, armonicen las prácticas a nivel europeo en aras del mercado único. La Segunda Directiva de servicios de pago tiene diversas finalidades, pero de algún modo, se ha procurado conectarlas todas y el resultado es positivo, aunque mejorable. Y si el mercado aún no está preparado para una armonización completa— mediante Reglamento, como se espera en el futuro próximo—, es tarea del legislador nacional llegar hasta donde no ha llegado la norma europea, por las limitaciones inherentes a su propia naturaleza.

Lo contenido en el título III RDLSP es una suerte de *lex artis* para los proveedores de servicios de pago, concretada con gran detalle. Con carácter general, el contrato de servicios de pago implica el nacimiento una obligación de resultado¹ para el proveedor, si bien el régimen concreto de prestación regulado en el RDLSP impone una serie de obligaciones que podríamos denominar intermedias, que son de medios. Como se verá en el capítulo dedicado a la responsabilidad,

¹ SANTORO, V., «Considerazioni conclusive» en BANI, STASIO y SICARRONE ALIBRANDI (eds.), *The transposition... op. cit.*, pp. 217-224 (p. 220).

no basta con ingresar, transferir o retirar los fondos en cuestión, esto es, alcanzar el resultado pretendido por una operación de pago, sino que hay que hacerlo siguiendo unas reglas concretas, que aunque no limitan los procesos técnicos que deben seguirse², marcan la pauta sobre el cómo ha de lograrse dicho resultado. Una operación de pago solo se ejecuta correctamente si se cumplen todas esas obligaciones intermedias exigidas al PSP.

Pero no debe desconocerse que no toda la prestación de servicios de pago implica la ejecución de operaciones de pago. Es en este punto donde la presencia del resto de capítulos del título III, aparte del dedicado propiamente a la ejecución, debe llamar especialmente la atención, así como la rúbrica del propio Título. Quiere decirse que para aquellos servicios que no consistan en la ejecución de órdenes de pago el régimen jurídico especial es menos detallado. Sería el caso, por ejemplo, de los servicios de emisión de instrumentos de pago o de adquisición de operaciones de pago, cuando se configuren de modo tal que no es el mismo proveedor quien ejecuta las operaciones y, muy en particular, del servicio de información sobre cuentas. Como se ha visto en sede de transparencia, el servicio de iniciación de pagos se asimila a la ejecución de una operación de pago singular y como tal, también a este servicio se refieren las obligaciones sobre ejecución, en la medida en que sean aplicables. Más allá de algún artículo dedicado en exclusiva a este servicio, a los instrumentos de pago o a los adeudos domiciliados, todas las demás previsiones deben entenderse aplicables a todos los contratos de servicios de pago, es decir, a estos contratos como categoría, pues no se distingue entre unos u otros contratos individualizados³. Ello no obsta a la innegable constatación de que el régimen legal está diseñado fundamentalmente, desde la perspectiva del usuario que actúa como ordenante y su proveedor y, en particular, pensando, sobre todo —aunque no exclusivamente—, en el contrato de cuenta de pago.

Para finalizar esta introducción, resta exponer el ámbito de aplicación y el alcance de las reglas contenidas en este título III RDLSP. Tienen carácter imperativo en todo caso cuando el usuario sea un consumidor o microempresa. Mayor novedad presenta el hecho de que cuando no estemos ante un consumidor, solo algunas disposiciones tienen carácter dispositivo y el resto serán igualmente imperativas. De modo que puede distinguirse ya un amplio núcleo de obligaciones estructurales en la prestación de servicios de pago que en ningún caso

² Para eso hay otras normas que interactúan con el RDLSP, como el Reglamento SEPA, el Reglamento de pagos transfronterizos en euros o el Reglamento de tasas de intercambio.

³ Sobre la no distinción se lamentaba al hilo de la LSP LÓPEZ JIMÉNEZ, J. M., *Comentarios...*, *op. cit.*, p. 565. También se refiere a ella, PEÑAS MOYANO, M. J., *Régimen Jurídico...*, *op. cit.*, pp. 76-77, poniendo en valor que la LSP supuso «abandonar la perspectiva individualizada y de régimen escaso a favor de una disciplina unitaria que fuera aplicable a los aspectos fundamentales de su utilización».

pueden ser eludidas, y otro conjunto de obligaciones configuradas como de especial protección que, por tanto, son disponibles cuando el usuario no merezca dicho tratamiento tuitivo, lo que se destacará debidamente en los apartados siguientes.

Por último, incluso cuando el usuario sea consumidor o microempresa, la ley permite la posibilidad de que las partes pacten un régimen aligerado para los instrumentos de pago de escasa cuantía, cuestión ya tratada a la que nos remitimos para evitar reiteraciones.

Así pues, lo expuesto en los apartados siguientes puede leerse en clave de derechos del usuario de servicios de pago, cuando se exponga el análisis sobre las obligaciones impuestas al proveedor. Y viceversa: las obligaciones del usuario de servicios de pago son reflejo del derecho del proveedor a no resultar responsable en determinadas situaciones⁴. Es decir, el cumplimiento o incumplimiento por parte del usuario de sus obligaciones delimitan el ámbito de responsabilidad del PSP.

II. OBLIGACIONES DEL PROVEEDOR DE SERVICIOS DE PAGO (Y DERECHOS DEL USUARIO)

1. Gastos aplicables

Por si hubiera quedado alguna duda de que lo que se prevé en cuanto a gastos en el Título dedicado a la transparencia, el título III comienza con un capítulo dedicado a disposiciones comunes, cuyo único precepto con contenido sustantivo es el art. 35 RDLSP, titulado «gastos aplicables», donde se configura una obligación para el proveedor de servicios de pago, que, a su vez, supone el reconocimiento del correspondiente derecho para el usuario.

Salvo las excepciones a las que se ha hecho referencia, que deben acordarse en el contrato y tener un importe adecuado y acorde al coste efectivamente soportado, se prohíbe al PSP cobrar al usuario «por el cumplimiento de sus obligaciones de información o por las medidas correctivas o preventivas contempladas en este título». Llama la atención, como sucede también en la Directiva, que este precepto se refiera no solo a excepciones contempladas en el título en el que se inserta sino también a las del anterior. Sin perjuicio de que convendría respetar la sistemática de las normas, nunca está de más un recordatorio de qué no es susceptible de generar beneficio económico para el proveedor.

⁴ En palabras de TAPIA HERMIDA «los dos momentos sucesivos de las operaciones de pago que resultan relevantes a los efectos de imputar derechos, obligaciones y responsabilidades a las partes implicadas son los de su autorización y de su ejecución» (TAPIA HERMIDA, A. J., «La regulación de los servicios...», *op. cit.*, [versión digital]).

Esta obligación contenida en el art. 35.1 RDLSP es disponible cuando el usuario no sea consumidor o microempresa.

Es también en este artículo, en su apartado 2, donde se establece como norma vinculante la aplicación de la regla de gastos compartidos (*share – SHA*), lo que debe ponerse en relación con la prohibición para el PSP de detraer concepto alguno del importe de la operación, a la que luego se hará referencia. El apartado 3 prohíbe a los beneficiarios cobrar gastos al ordenante por la utilización de un instrumento de pago determinado, aunque sí se les permite ofrecer una reducción u otra ventaja (por ejemplo, obsequios o mejores promociones para futuras compras) que incentive la utilización de alguno en concreto (art. 35.4 RDLSP).

Al respecto, la Sentencia del TJUE de 2 de diciembre de 2021, *Vodafone Kabel Deutschland*, C-484/20, ECLI:EU:C:2021:975, sentó el criterio de que la prohibición establecida en el art. 62.4 DSP2 se aplica a todas las operaciones iniciadas a partir de la entrada en vigor de la directiva el 13 de enero de 2018, con independencia de que el contrato subyacente se suscribiese conforme a la Primera Directiva de servicios de pago y de que, hasta dicho momento, se cobrasen gastos por la utilización de los citados instrumentos de pago⁵. Este precepto de la norma europea es el que prohíbe a los beneficiarios exigir el pago de gastos por la utilización de instrumentos de pago SEPA o sometidos al Reglamento de tasas de intercambio. En virtud de la opción concedida por el art. 64.5 DSP2, el legislador español decidió ampliar esta prohibición a cualquier instrumento de pago. Tal criterio jurisprudencial es plenamente aplicable también en el caso español, pues así lo dispone expresamente la propia disp. trans. 5.^a, cuando se refiere con carácter general a los contratos en vigor⁶. Nótese que, en su redacción original, la Ley de servicios de pago de 2009 sí permitía a los beneficiarios el cobro de gastos adicionales por la utilización de un instrumento de pago específico, estableciéndose la nulidad de toda cláusula del contrato marco de servicios de pago que impidiese a los beneficiarios hacer uso de tal facultad (art. 24.3 LSP); pero este régimen fue modificado en diciembre de 2018 para el periodo de *vacatio legis* de los títulos II y III del RDLSP, estableciéndose la prohibición de gastos adicionales que, después, entraría en vigor como el régimen definitivo establecido en la nueva norma de servicios de pago⁷.

⁵ FD 24-30.

⁶ Disposición transitoria quinta RDLSP: «Contratos en vigor. Los contratos que los proveedores de servicios de pago que operen en España tengan suscritos con su clientela, a la fecha de entrada en vigor de este real decreto-ley, para la regulación de las condiciones en las que ha de tener lugar la prestación de los servicios de pago a los que se refiere este real decreto-ley, seguirán siendo válidos una vez entre en vigor la misma, sin perjuicio de la aplicación, a partir de dicho momento, de las disposiciones de carácter imperativo que resulten más favorables para los consumidores y microempresas».

⁷ El art. 24.3 LSP fue modificado por la disp. fin. 2.^a de la Ley 11/2018, de 28 de diciembre, por la que se modifica el Código de Comercio, el texto refundido de la Ley de Sociedades de

2. La obligación de autenticación reforzada y la autorización de la orden de pago

Desde que comenzara la progresiva electrificación de los pagos, su seguridad ha sido la principal preocupación; concretamente, cómo evitar el fraude ha ocupado una posición preminente entre las prioridades de todos los actores del mercado, incluyendo proveedores, usuarios y, por supuesto, legisladores⁸. Pero la expansión del comercio electrónico, la aparición de nuevos tipos de servicios en relación a la cadena de pago y la popularización de los servicios de pago en línea, incluso a través de dispositivos móviles, hicieron escalar exponencialmente el riesgo de fraude planteando a su vez grandes desafíos desde el punto de vista normativo⁹. Y de aquí surgieron las dos grandes medidas introducidas por la Segunda Directiva de servicios de pago¹⁰: la primera, la inclusión en su ámbito de aplicación de los servicios de información sobre cuentas y de iniciación de pagos; la segunda, que aquí nos ocupa, es la necesidad de autenticación reforzada de clientes, aplicable fundamentalmente —aunque no solo— a las operaciones de pago remotas¹¹ que se consideran generalmente sujetas a mayores riesgos¹².

Capital aprobado por el Real Decreto Legislativo 1/2010, de 2 de julio, y la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, en materia de información no financiera y diversidad. Todo apunta a que, dado que finalmente la nueva norma de pagos se adoptó como Real Decreto-Ley, el Gobierno olvidó incluir un apartado en la disp. fin. 13.^a que estableciese la entrada en vigor inmediata del art. 35 RDLSP. Nótese que cuando se aprueba el RDLSP en noviembre de 2018, España llevaba ya 10 meses de retraso en la transposición de la Segunda Directiva de servicios de pago que debería haberse producido, a más tardar, el 13 de enero de 2018 (*vid.* art. 115.1 DSP2). Además, el art. 35.2 RDLSP tiene la particularidad de que los sujetos destinatarios no son los proveedores, sino los propios beneficiarios y que, en realidad, está regulado un aspecto que no forma parte estricta de la relación de servicios de pago.

⁸ *vid.* COMISIÓN EUROPEA, Comunicación «Una nueva baza para Europa: las tarjetas de pago electrónicas», COM (86)754 final, 1987 y Recomendación 87/598/CEE. Sobre la creciente preocupación por la seguridad en el periodo inmediatamente anterior a la publicación de la Segunda Directiva de servicios de pago, véase también PACHECO JIMÉNEZ, M^a. N., «Evolución de los servicios de pago: hacia el mercado único digital», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 39, 2015 (versión digital); sobre la importancia de la ciberseguridad en los pagos electrónicos, su conexión con la confianza de los consumidores y la construcción del mercado único *vid.* LEAL CORONADO, M., «La revolución de los medios de pago en el contexto de los nuevos modelos de contratación», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 45, 2018 (versión digital).

⁹ Considerando 4 DSP2.

¹⁰ Además de las que aquí se citan, que son las que presentan mayor relevancia desde el punto de vista de la relación contractual entre el usuario y el PSPs, se incluyeron también obligaciones generales de seguridad y de notificación de incidentes, *vid.* arts. 95, 96 DSP2 y 66 y 67 RDLSP.

¹¹ Art. 3.27 RDLSP: «Operación remota de pago: operación de pago iniciada a través de internet o de un dispositivo que pueda utilizarse para la comunicación a distancia».

¹² MEZZACAPO, S., «PSD2, online and mobile payments: what transparency for the future of payments?» en BANI, STASIO y SICARRONE ALIBRANDI (eds.), *The transposition of PSD2 and open banking*, Bergamo University Press-Sestante edizioni, Bérgamo, 2021, pp. 69-108.

Por autenticación se entienden dos procedimientos de seguridad diferentes. Por un lado, aquel mediante el cual el PSP comprueba la identidad del usuario, por el otro, el que permite verificar la validez de la utilización de un instrumento de pago concreto. Por lo general, esta autenticación se realiza mediante la utilización de credenciales de seguridad personalizadas, que no son sino elementos únicos y personalizados proporcionados al titular por su proveedor para permitirle llevar a cabo la autenticidad¹³. Así, la contraseña de entrada y la clave de firma al servicio en línea del proveedor, el PIN y el código de valor de verificación (CVV) de las tarjetas, las tarjetas de coordenadas, etc., son clásicos ejemplos de credenciales de seguridad personalizadas. La autenticación reforzada de clientes (abreviada como SCA por sus siglas en inglés —*strong customer authentication*—) no es ni más ni menos que lo que su propio nombre indica: el mismo proceso, pero con mayor seguridad porque se utilizan no uno sino varios elementos para asegurar la verificación, al menos, dos. Aunque la definición legal de autenticación reforzada de clientes contenida en el art. 3.5 RDLSP evidencia que no necesariamente esos elementos tienen que ser credenciales de seguridad personalizadas. Lo que se requiere es que puedan categorizarse como elementos que solo el usuario conozca —de conocimiento—, que solo él posea —de posesión— o que solo él sea —de inherencia—, y que aquellos utilizados en cada momento sean independientes entre sí, es decir, «que la vulneración de uno no compromete la fiabilidad de los demás»¹⁴ y que pertenezcan a categorías diferentes¹⁵. La utilización de, al menos, dos factores debe generar un «código de autenticación» de un solo uso. Por ejemplo, un usuario puede utilizar su clave y un número recibido por SMS para acceder a su cuenta de pago en línea es este caso, los elementos personalizados son su clave y su número de teléfono, a través del cual recibe el mensaje con ese código de autenticación. Otros modelos de autenticación reforzada pueden no suponer que el usuario reciba dicho código, por ejemplo, cuando se utilizan aplicaciones de confirmación electrónica de operaciones¹⁶.

ZUNZUNEGUI ha llamado la atención sobre la incorrecta transposición de esta definición dado que, además de lo dicho, la autenticación reforzada debe ser «concebida de manera que se proteja la confidencialidad de los datos de autenticación» (art. 4.30 DSP2), pero en el RDLSP lo que se exige es que se proteja «la confidencialidad de los datos de

¹³ Art. 3 RDLSP, apartados 4 y 10.

¹⁴ En este sentido, el art. 9 RTS SCA-SCS, exige que los proveedores se aseguren de que el uso de los elementos de autenticación reforzada «esté sujeto a medidas que garanticen que, en términos de tecnología, algoritmos y parámetros, el quebrantamiento de uno de los elementos no compromete la fiabilidad de los demás».

¹⁵ AUTORIDAD BANCARIA EUROPEA, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, EBA-Op-2018-04, 2018, p. 7.

¹⁶ Un ejemplo sería la ya eliminada aplicación CaixaBank Sign.

identificación», y acertadamente señala este autor que, como acaba de exponerse, no son lo mismo los datos de autenticación que los datos de identificación¹⁷. No obstante, en la práctica, una implementación segura de los procesos de autenticación debería proteger ambos tipos de datos, porque a lo que se refiere ese último inciso es precisamente al diseño e implementación de los procesos utilizados para llevar a cabo la autenticación reforzada, esto es, a la ciberseguridad de los canales utilizados por los PSP tanto para comunicarse con sus clientes (por ejemplo, el acceso a la web o la aplicación móvil), como para transmitir la autorización de las operaciones.

La aplicación de la autenticación reforzada de clientes es una de las obligaciones nucleares de todo proveedor de servicios de pago. Se establece en el art. 68 RDLSP, en sede de seguridad; aunque, a mi juicio, tendría quizás más sentido incorporarla en sede de consentimiento. Es cierto, sin embargo, que la estructura de la Segunda Directiva de servicios de pago, idéntica en el RDLSP, no aborda el otorgamiento del consentimiento de una manera individualizada sino circunscrito a la autorización de operaciones de pago que, a su vez, se entiende como una fase previa o inicial de la ejecución. El hecho de que la autenticación sea una obligación aplicable en más operaciones que solo en la de pago *stricto sensu* realmente hubiera hecho extraña su ubicación en sede de «autorización de las operaciones de pago», pero la importancia de esta obligación que podría calificarse de transversal aconsejaría sistematizarla de manera independiente, incardinada en el propio consentimiento del usuario, cuyas normas deberían positivizarse de manera ordenada, no solo en relación a la operación de pago como tal sino, de manera más general, a la prestación del servicio de que se trate¹⁸.

La autenticación reforzada ha de llevarse a cabo conforme a las normas técnicas del Reglamento Delegado de autenticación reforzada. Con carácter general se establece en esta norma de nivel 2 que los supuestos en que deberá ser aplicada son el acceso a la cuenta de pago en línea, las operaciones de pago electrónico y cuando el usuario «realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos». La indeterminación señalada en último lugar traslada al proveedor la obligación de evaluar y decidir sobre de qué tipo de acciones entrañan un riesgo de fraude «u otros abusos» y es esta una de las razones por las que el nivel de seguridad ofrecido al usuario puede ser un elemento diferenciador de los competidores. En sentido estricto, el nivel de seguridad será más o menos homogéneo en

¹⁷ ZUNZUNEGUI, F., «Luces y sombras...», *op. cit.*, (versión digital).

¹⁸ El capítulo II del título III del RDLSP (idénticamente con la diferente numeración de la Segunda Directiva de servicios de pago) se titula «autorización de operaciones de pago», pero en él se regulan cuestiones dispares que no tienen que ver estrictamente con la autorización, *vid.* arts. 39 a 41, 48 y 49 RDLSP. Esta es también la razón por la que ha decidido abordarse en este trabajo con una sistemática diferente a la prevista en el Derecho positivo.

los casos obligatorios, pero en aquellos donde hay cierta discrecionalidad o respecto de las excepciones legales (art. 68.6 RDLSP en relación a los arts. 10 a 18 RTS SCA-SCS) que el PSP puede decidir no aplicar y utilizar también en esos supuestos la autenticación reforzada, ofrecen margen para diseñar el servicio de un modo u otro.

En relación a las operaciones de pago, se aplicará la autenticación reforzada a aquellas iniciadas por el ordenante —una transferencia— o a las iniciadas por este a través del beneficiario —por ejemplo, los pagos con tarjeta—, pero no será de aplicación a las operaciones iniciadas por el beneficiario —como los adeudos domiciliados—¹⁹.

Ahora bien, no hay que perder de vista que esta obligación sí es de las que supone un coste elevado para los proveedores que probablemente en algún momento será repercutido en el precio de los servicios que ofrece. Por ello, y en aras de la proporcionalidad, se establecen importantes excepciones a esta obligación²⁰ supeditadas al registro trimestral de las operaciones²¹ y, algunas de ellas, también a que el PSP disponga de mecanismos de supervisión de las operaciones que le permitan detectar actividad sospechosa a través del análisis de las operaciones de pago de sus usuarios y el uso de sus credenciales de se-

¹⁹ AUTORIDAD BANCARIA EUROPEA, *Final Report Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)*, EBA/RTS/2017/02, 2017, p. 7.

²⁰ «Las medidas de seguridad han de ser compatibles con el nivel de riesgo que entraña el servicio de pago [...] Para permitir el desarrollo de medios de pago accesibles y de fácil uso para pagos de bajo riesgo (por ejemplo, los pagos de escasa cuantía y los pagos sin contacto en el punto de venta, basados o no en un teléfono móvil), en las normas técnicas de regulación se deberían especificar exenciones de la aplicación de los requisitos de seguridad» (considerando 96 DSP2). *vid.* ALVARADO HERRERA, L., «Autenticación reforzada de cliente y responsabilidad en la segunda directiva de servicios de pago», *Revista de Derecho del Sistema Financiero*, núm. 5, 2023, pp. 87 y ss.

²¹ «Con el fin de hacer uso de las exenciones establecidas en los artículos 10 a 18, los proveedores de servicios de pago registrarán y supervisarán los siguientes datos para cada tipo de operaciones de pago, desglosando las operaciones remotas y no remotas de pago y con una frecuencia al menos trimestral:

el valor total de las operaciones de pago no autorizadas o fraudulentas de conformidad con lo dispuesto en el artículo 64, apartado 2, de la Directiva (UE) 2015/2366, el valor total de todas las operaciones de pago y el índice de fraude resultante, incluido un desglose de las operaciones de pago iniciadas por medio de una autenticación reforzada de clientes y las iniciadas al amparo de cada una de las exenciones;

el valor medio de las operaciones, incluido un desglose de las operaciones de pago iniciadas por medio de una autenticación reforzada de clientes y las iniciadas al amparo de cada una de las exenciones;

el número de operaciones de pago en que se ha aplicado cada una de las exenciones y su porcentaje con respecto al número total de operaciones de pago.

2. Los proveedores de servicios de pago pondrán los resultados de la supervisión realizada de conformidad con el apartado 1 a disposición de las autoridades competentes y de la ABE, a petición de estas y previa notificación a la autoridad o autoridades competentes pertinentes» (art. 21 RTS SCA-SCS).

guridad²². Es decir, el proveedor está legalmente obligado a monitorear o supervisar el comportamiento de pago de sus usuarios para ser capaz de prevenir y revertir casos de fraude y de operaciones no autorizadas. Hay, además, otra razón por la que esta cuestión resulta especialmente relevante y es que no aplicar la autenticación reforzada cuando sea obligatorio traslada al proveedor todo el riesgo de la operación, liberando de responsabilidad al usuario en caso de operación no autorizada, como se verá en su momento.

Siempre y cuando el PSP monitoree el comportamiento de pago de sus clientes, no estará obligado a utilizar la autenticación reforzada cuando el usuario solo pretenda acceder a determinada información de una o varias cuentas de pago en línea, concretamente, al saldo disponible o a los movimientos de los últimos 90 días, salvo que sea el primer acceso o hayan transcurrido más de 90 días desde el último. Tampoco se requiere para los pagos sin contacto en el punto de venta si, cumulativamente el importe de la operación es como máximo de 50 €, el importe acumulado de las operaciones iniciadas sin contacto desde la última aplicación de la autenticación reforzada no exceda de 150 € y no se han hecho más de cinco operaciones iniciadas sin contacto desde la última vez que se aplicó este tipo de autenticación. Asimismo, será potestativa cuando se trate traspasos, o de pagos en una terminal no atendida con el fin de abonar una tarifa de transporte o de aparcamiento²³.

Se exceptúan también de la obligación de aplicar la autenticación reforzada, esta vez sin condiciones aparte del registro de la operación, aquellas realizadas a beneficiarios de confianza y las operaciones frecuentes —o recurrentes— posteriores a la primera de la serie (la creación de una serie de operaciones frecuentes con carácter permanente, su modificación y la primera ejecución sí deben autenticarse reforzadamente). Igualmente, las operaciones remotas de escasa cuantía, es decir, inferior a 30 €, siempre que el importe acumulado de las operaciones remotas de pago electrónico previas desde la última aplicación de la autenticación reforzada no exceda de 100 € o, alternatively, el número de operaciones previas no exceda de cinco consecutivas. Finalmente, también puede evitarse la aplicación de la autenticación

²² De acuerdo con el art. 2 RTS SCA-SCS, dichos mecanismos deben tener en cuenta «factores basados en el riesgo», al menos: listas de elementos de autenticación comprometidos o sustraídos; el importe de cada operación de pago; supuestos de fraude conocidos en la prestación de servicios de pago; señales de infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación; en caso de que el dispositivo o el programa informático de acceso sea facilitado por el proveedor de servicios de pago, un registro de la utilización del dispositivo o el programa informático de acceso facilitado al usuario de los servicios de pago y de su uso anormal.

²³ Serían ejemplos, los pagos realizados en un parquímetro o en un peaje automatizado.

reforzada cuando el usuario sea una persona jurídica que utilice procesos y protocolos de pago corporativo seguro²⁴.

La última exclusión posible se basa, precisamente, en los datos recabados en la supervisión del comportamiento de pago de los clientes que deben permitir calcular los índices de fraude conforme al art. 19 RTS SCA-SCS, en cuyo caso, se permite al PSP no aplicar la autenticación reforzada a aquellas operaciones cuyo nivel de riesgo se haya calificado como bajo, conforme a las condiciones de los arts. 18 y 20 RTS SCA-SCS²⁵.

En la práctica, la implementación de la autenticación reforzada de clientes ha sido una de las cuestiones más complejas derivadas de la revisión del marco jurídico europeo de los servicios de pago. Tanto es así que la aplicación del reglamento delegado se retrasó más de un año para permitir a los proveedores la puesta a punto de sus procesos²⁶ y, aún a día de hoy, es una de las materias sobre las que más preguntas se presentan a la Autoridad Bancaria Europea a través de su servicio «*Single Rulebook Q&A*»²⁷. Solo va abordarse aquí una de todas las cuestiones abiertas que plantea esta medida de seguridad, que es la relativa a las aplicaciones móviles de *wallet* o tokenización de instrumentos de pago, que se trae a

²⁴ «Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes para personas jurídicas que inicien operaciones de pago electrónico mediante el uso de procesos o protocolos de pago que solo estén disponibles para los ordenantes que no sean consumidores, cuando las autoridades competentes estén convencidas de que dichos procesos o protocolos garantizan unos niveles de seguridad al menos equivalentes a los previstos por la Directiva (UE) 2015/2366» (art. 17 RTS SCA-SCS).

²⁵ De acuerdo con el art. 18 RTS SCA-SCS para que el nivel de riesgo de una operación de pago se considere bajo el índice de fraude para ese tipo de operaciones (calculado con arreglo al art. 19) debe ser equivalente o inferior al índice de fraude de referencia especificado del anexo del Reglamento para los «pagos remotos electrónicos con tarjeta» y las «transferencias de créditos remotos electrónicas»; el importe de la operación no puede superar el valor umbral de exención por tipo de operación (de acuerdo con dicho anexo) y es preciso que el proveedor no hayan detectado, como consecuencia de la realización de un análisis del riesgo en tiempo real, gastos o pautas de comportamiento anormales en el ordenante, información inusual sobre el dispositivo o programa informático de acceso del ordenante, infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación, supuestos conocidos de fraude en la prestación de servicios de pago, una ubicación anormal del ordenante o una ubicación de alto riesgo del beneficiario. Por su parte, el art. 20 RTS SCA-SCS determina que las exenciones basadas en el análisis del riesgo de la operación deberán cesar cuando los índices de fraude calculados por los proveedores superen los índices de referencia.

²⁶ AUTORIDAD BANCARIA EUROPEA, *Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions*, EBA-Op-2019-11, 2019. Incluso la elaboración del Reglamento Delegado fue tortuosa, sucediéndose varias comunicaciones públicas entre la ABE y la Comisión Europea con opiniones dispares (vid. SANTAMARÍA, J., «La segunda Directiva de Servicios de Pago y sus impactos en el mercado» en *Nota Técnica*, núm 31, Instituto de Estudios Financieros, 2018, p. 5).

²⁷ Desde 2018, cuando se puso en marcha este servicio, se habían presentado 167 preguntas sobre autenticación reforzada y estándares seguros de comunicación. Algunas de las preguntas y respuestas anteriores en materia de servicios de pago se recogen en COMISIÓN EUROPEA, *Your questions on PSD, Payment Services Directive 2007/64/EC Questions and answers*, 2011.

colación por su relevancia práctica, dada la creciente adopción de esta solución de pago, y por su conexión con la propuesta de evaluar la conveniencia de extender la aplicación del régimen de servicios de pago a algunos proveedores de servicios tecnológicos.

La ABE, en respuesta a diversas preguntas planteadas por los operadores, ha ido definiendo un criterio de interpretación de la normativa para el caso de utilización por el usuario de estas aplicaciones de tokenización de instrumentos de pago. En primer lugar, registrar una tarjeta o cualquier otro instrumento en estas aplicaciones supone crear una versión digitalizada del instrumento o, si se prefiere, un token del mismo, que es una acción realizada por un canal remoto que puede «entrañar un riesgo de fraude en el pago u otros abusos». Por tanto, es una operación sujeta a la obligación de aplicar autenticación reforzada que, además, permitirá al proveedor vincular al instrumento original y al usuario con el instrumento tokenizado²⁸. Lo mismo sucede cuando se emite un nuevo token asociado a un instrumento que sustituye otro previamente registrado²⁹. También el inicio de operaciones con la versión digitalizada de la tarjeta requiere la aplicación de la autenticación reforzada de clientes, salvo que sean aplicables algunas de las excepciones expuestas *supra*³⁰. Y pese a que el dispositivo en el que se encuentre el programa que almacena los instrumentos de pago digitalizados cuente con medidas de seguridad como controles biométricos, esos elementos o mecanismos de seguridad no pueden considerarse parte del proceso de autenticación reforzada porque no los controla el PSP³¹. Lo que sí se permite, de acuerdo con las reglas generales aplicables a la externalización, es que los PSPs subcontraten la gestión de los procesos de autenticación reforzada con los proveedores de servicios de *wallet*, o con cualquier otro tercero, pero ello no supondrá el traslado del riesgo a ese otro proveedor, y el PSP seguirá siendo responsable frente al usuario del cumplimiento de los requisitos exigidos por la legislación de servicios de pago³², lo que es por otra parte la solución aplicable respecto a los servicios bancarios y de inversión.

Que el usuario actúe a través de proveedores de servicios de pago terceros no exime de la obligación de aplicar la autenticación reforzada y, de hecho, el proveedor de servicios de pago gestor de cuenta está obligado a permitir a estos proveedores terceros utilizar los procedimientos de autenticación facilitados al usuario.

De lo expuesto en este apartado se desprende pues que las primeras obligaciones del PSP consistirán en proporcionar al usuario las

²⁸ Q&A 2020_5622 y Q&A 2021_6141.

²⁹ Q&A 2022_6464.

³⁰ Q&A 2020_5622.

³¹ Q&A 2021_6145.

³² Q&A 2018_4047.

correspondientes credenciales de seguridad personalizadas para que pueda operar de forma remota, y en tener disponibles los medios y procedimientos adecuados para proceder a su autenticación, sencilla o reforzada según los casos.

3. Iniciación de la operación de pago y acceso a la cuenta de pago en sentido amplio

Para que una operación de pago se ejecute, el primer paso necesario es que la orden de pago llegue al proveedor de servicios de pago. Aunque ni el RDLSP, ni la Segunda Directiva de servicios de pago definen qué hay que entender por iniciación de la operación de pago, de la función que la legislación reserva al PSIP debe concluirse que se trata de la transmisión de la orden de pago autorizada. El art. 36 RDLSP determina que una orden de pago se considera autorizada cuando el usuario haya consentido su ejecución y, acto seguido, especifica —cosa que no hacía la legislación anterior de forma explícita— que el consentimiento no solo puede darlo directamente el ordenante, sino que puede ser transmitido también «por conducto» del beneficiario³³ o del proveedor de servicios de iniciación de pagos. La operación podrá considerarse iniciada cuando dicha orden de pago sea recibida por el proveedor de servicios de pago —en su caso, gestor de cuenta—, instante que jurídicamente suele coincidir con la recepción «física» de la orden, pero que también puede ser pospuesto en el tiempo —independientemente de quién transmita la orden, puede ser una transferencia planificada, un adeudo domiciliado o una orden transmitida por un PSIP—, en cuyo caso no se considerará recibida hasta el momento acordado entre las partes o, si el día previsto es inhábil, el día hábil siguiente (art. 50 RDLSP)³⁴.

La siguiente obligación del PSP es aceptar la orden de pago si esta cumple con los términos pactados en el contrato y, en caso contrario, notificar al usuario el rechazo de la orden «lo antes posible» y a más tardar en plazo de un día hábil, su motivación y el procedimiento para rectificar los posibles errores de hecho de que adolezca la orden (art. 51 RDLSP).

³³ Esto incluye los casos en que la orden se transmite directamente por el propio beneficiario (adeudos domiciliados) y aquellas en las que la transmite el ordenante a través del beneficiario (generalmente, con instrumento de pago a través de TPV física o virtual).

³⁴ Art. 3.13 RDLSP: «Día hábil: día de apertura comercial, a los efectos necesarios para la ejecución de una operación de pago, de los proveedores de servicios de pago del ordenante o del beneficiario que intervienen en la ejecución de la operación de pago. En el caso de cuentas de pago contratadas telemáticamente, se seguirá el calendario correspondiente a la plaza en la que esté ubicada la sede social del proveedor de servicios de pago con el que se hubieren contratado».

Otra posibilidad es que una orden de pago sea aceptable pero su momento de recepción se haya pospuesto voluntariamente por las partes. En esos casos, no opera la regla general de la irrevocabilidad de la orden de pago, porque se concede al usuario la posibilidad de revocarla hasta el final del día hábil anterior a la fecha pactada de recepción y comienzo de ejecución (art. 52 RDLSP), de modo que surgiría el deber para el proveedor de cancelar la ejecución de una orden de pago recibida y aceptada que haya sido válidamente revocada por el usuario.

Cuando el usuario no tenga la condición de consumidor o de microempresa se permite el establecimiento unas reglas diferentes a las previstas en los arts. 36.3 y 52 RDLSP tanto sobre la retirada del consentimiento como sobre la revocabilidad de la orden de pago (por disposición del art. 34.1 RDLSP). En realidad, que la regla general sea la irrevocabilidad guarda más relación con el funcionamiento de los sistemas de pago, en los que la retrocesión de las operaciones raramente está automatizada y suele suponer un perjuicio a nivel operativo, que con la relación contractual entre el PSP y el usuario. De modo que, incluso cuando el usuario sea consumidor o microempresa, no es del todo descartable que en el contrato marco se alteren estas condiciones, aunque en este caso siempre en favor del usuario, como medida comercial por parte del proveedor que, en su caso, deberá concluir los acuerdos precisos a nivel de sistema de pago o fuera de ellos con otros PSPs para no perturbar el funcionamiento de aquellos, o bien ofrecer la posibilidad de revocación solo en operaciones a cuentas que él mismo gestione.

No obstante, en ocasiones esta medida de la irrevocabilidad podría tener una función más general y trascendente que parece no haber sido inicialmente prevista por el legislador, quien plantea el funcionamiento de las operaciones de pago «con independencia de cualesquiera obligaciones subyacentes entre el ordenante y el beneficiario». Se trata, precisamente, del momento de cumplimiento de dicha obligación. Que en el tráfico esté generalmente aceptado el resguardo de una operación de pago como prueba del cumplimiento tiene mucho que ver con la irrevocabilidad de la orden de pago. Sin embargo, esta conveniente —pero hasta cierto punto forzada— independencia de la relación de servicios de pago con las subyacentes impide poder establecer positivamente esta presunción, aunque *de facto* sí opere como una *iuris tantum*.

Respecto del supuesto en el que servicio prestado consiste en la ejecución de una operación que se basa en una cuenta de pago, en este mismo proceso de recepción, aceptación e iniciación pueden surgir, además, otras obligaciones para el proveedor. Y es en este momento cuando cobra importancia el régimen de acceso a la cuenta de pago del usuario. La prestación de determinados servicios de pago regulados requiere que un PSP acceda a los datos de una cuenta de pago titularidad

de su usuario, mantenida por otro proveedor al que se hace referencia como proveedor de servicios de pago gestor de cuenta (PSPGC). Tanto en relación a los proveedores que emiten instrumentos de pago basados en tarjeta como a los de iniciación de pagos o de información sobre cuentas, el PSPGC está obligado a facilitar su acceso en diferente medida, según el servicio en cuestión, siempre que la cuenta sea accesible en línea —lo que, a día de hoy, en España, es prácticamente siempre—. Debe confirmar de forma inmediata la disponibilidad de los fondos, siempre que se cumplan las condiciones previstas en el art. 37 RDLSP, cuando un PSP emisor de instrumentos basados en tarjeta así lo solicite. En relación a los TPPs debe permitirles acceder a la cuenta designada por el usuario, pues la propia norma configura expresamente como un derecho del usuario la utilización de estos servicios terceros (arts. 38.1 y 7 RDLSP).

En cuanto a la solicitud de disponibilidad de los fondos hecha por un PSP emisor de tarjetas, esta debe venir avalada por el consentimiento explícito del usuario transmitido al proveedor de servicios de pago gestor de cuenta antes de la primera solicitud de confirmación. La respuesta debe limitarse a un «sí» o a un «no», sin facilitar más datos en relación a la cuenta de pago del ordenante y sin bloquear los fondos correspondientes. El PSP emisor tiene obligación de recabar el consentimiento explícito del usuario —se entiende, en el propio contrato de emisión—, identificarse ante el PSPGC, solicitar confirmación solo a efectos de la operación concreta cada vez y por el importe determinado y limitar el uso de los datos a la ejecución de la parte de la operación que le corresponde, sin estar habilitado para usarlos con finalidades diferentes.

La cuestión del acceso de los TPPs a las cuentas de los usuarios abiertas en otro proveedor de servicios de pago gestor de cuenta es quizás de las que más ha llamado la atención desde el proceso de elaboración de la Segunda Directiva de servicios de pago. Por su novedad, pero sobre todo por el impacto que tiene en la competencia en el mercado. Es la gran medida para «nivelar el campo de juego» —como se podría traducir literalmente la manida expresión europea—, es decir, para establecer cierta igualdad de condiciones entre proveedores. Con la singularidad de que, a pesar de tratarse de servicios de pago regulados, la particularidad de cada uno de esos servicios implica diferencias operativas importantes entre modelos de negocio, operativas que complican la consecución de esa libre competencia que en otros sectores puede ser más fácil de conseguir cuando la identidad entre productos o servicios es mayor.

Dentro del sector de los pagos, a menudo los servicios se interconectan, cada uno añade un determinado valor añadido a la cadena, no teniendo sentido sin la preexistencia de otro servicio diferente. Como

denominador común de muchos de ellos está, por supuesto, la cuenta de pago, sin la cual —salvo algunas excepciones—, la ejecución de la operación de pago en los términos del art. 1.2.c) RDLSP no tiene sentido³⁵. Asimismo, la mayoría de contratos de instrumento de pago están vinculados a una cuenta. Y ahora, los servicios de iniciación y de información sobre cuentas, también.

Lo más llamativo de esta cuestión es que el mercado evolucionó hacia la aparición de nuevos operadores, con modelos de negocio radicalmente diferentes a los de los operadores preexistentes que, dicho sea de paso, a menudo estaban encasillados. Simplificándolo mucho, pero como visión representativa del mercado, podría decirse que durante años hubo tres tipos de entidades que, en mayor o menor medida, tenían *de facto* funciones diferenciadas para los usuarios. Las entidades de crédito eran la opción clásica, tu proveedor «para todo», percibido como seguro, serio, fiable. Las entidades de dinero electrónico, que a pesar de nacer como un subtipo de entidades de crédito pronto demostraron no tener más que ver con estas que cualquier otra entidad financiera; de ahí la escisión de su régimen jurídico. Eran la alternativa para internet, y después también para viajar (por ejemplo, *PayPal* y *Revolut* nacieron como entidades de dinero electrónico, aunque ahora ambas son entidades de crédito). Servicios más limitados pero que con rapidez fueron evolucionando hasta lograr ofrecer comodidad, facilidad y precios mucho más competitivos para el concreto nicho de mercado que pretendían cubrir. Y a todo ello se suman las entidades de pago, reconocidas desde 2007 a nivel europeo, que tradicionalmente han centrado sus modelos de negocio en los envíos de dinero, en el sentido más clásico del servicio, las remesas.

Por supuesto, desde hace años contamos —y cada vez más— con otros operadores que prestan servicios estrechamente relacionados a los de pago: los establecimientos financieros de crédito, las entidades de cambio de divisa y, más recientemente, algunos proveedores de servicios de criptoactivos. Pero de momento, aunque quizá por poco tiempo, puede aún trazarse una línea diferenciadora entre el papel que estas entidades desempeñan en el mercado, y el resto de entidades financieras. Si acaso los establecimientos financieros de crédito estarían colindando, —por supuesto cuando se trate de entidades híbridas—, pero en este ámbito su actividad se centra hoy por hoy en los préstamos rápidos y al consumo, siendo los servicios de pago una prestación accesoria a estos³⁶.

³⁵ Recuérdese que el art. 1.2.c) RDLSP se refiere a la ejecución de operaciones de pago a través de transferencia, adeudo domiciliado y tarjeta.

³⁶ A salvo de esta generalización, las financieras de las grandes superficies y grandes distribuidores cuya actividad principal aúna indisolublemente la concesión de crédito y la prestación de servicios de pago, especialmente a través de la emisión de instrumentos de pago y crédito.

Dentro del sector de los servicios de pago en sentido estricto, comenzaron a aparecer, como se decía, nuevos operadores enfocados a momentos específicos de la cadena de pago o, mejor, de la propia relación contractual del servicio de pago, que pretendieron llenar un vacío existente en el mercado. Son los proveedores de servicios de información sobre cuentas y los de iniciación de pagos, que llegan para cubrir una necesidad que quizás en un momento inicial solo algunos usuarios tenían —especialmente allí donde las tarjetas son más caras, para el caso del servicio de iniciación, y donde los usuarios disponen de más cuentas en diversos proveedores, para los de información—, pero que una vez que se extienden aportan un valor añadido, porque ofrecen nuevos servicios a un coste muy reducido —en ocasiones, ni siquiera monetario— y que, además, permite a los usuarios una alternativa rápida y fácil de usar³⁷ para procesos que, de otro modo, presentaban algunos inconvenientes. Y de nuevo ahora, en la siguiente etapa de evolución del mercado, esto es exactamente lo que está pasando con las *BigTech* que desarrollan aplicaciones de digitalización de instrumentos de pago³⁸.

Y esto sucede al mismo tiempo que se están difuminando las fronteras otrora claras entre las funciones que cubrían los servicios prestados por los operadores tradicionales y las de los nuevos operadores, siguiendo la estela del comercio electrónico, la movilidad personal de la ciudadanía y la usabilidad de internet. Como proceso paralelo y estrechamente relacionado con éste, la información y los datos personales y no personales, desempeñan cada vez un papel más relevante como motor económico de la actividad de las entidades financieras. Y los nuevos servicios de iniciación y de información apuntan directamente a la información financiera y de consumo de los usuarios.

Deviene entonces imprescindible la previsión de un régimen especial de acceso de estos nuevos proveedores a las cuentas de los usuarios porque, obviamente, los operadores asentados —fundamentalmente entidades de crédito— no iban a ceder voluntariamente uno de sus activos de mayor valor³⁹ a nivel minorista. Por lo que, aunque no es el objeto de estudio principal de este trabajo, este régimen no se concibe solo como la articulación de un derecho del usuario a utilizar estos nuevos

³⁷ ZUNZUNEGUI, F., «La digitalización...», *op. cit.*, p. 6.

³⁸ Y que además cuentan con significativas ventajas competitivas: economías de escala, su enorme base de clientes, la ingente cantidad de valiosa información sobre las preferencias, hábitos y comportamientos de los consumidores, y la posibilidad de controlar las experiencias de compra de muchos de ellos... (*vid.* a este respecto VIVES, X., «La banca frente a la disrupción digital» en *Papeles de economía española*, núm. 162, 2019, pp. 2-13 [p. 6] y POZZOLO, A. F., «PSD2 and the transformation of the business model of payment services providers» en *op. cit.*, pp. 39-42).

³⁹ ZUNZUNEGUI, F., «La digitalización...», *op. cit.*, p. 3 y ALONSO LEDESMA, C., «La desintermediación...», *op. cit.*, p. 498.

servicios, sino como una medida de eliminación de obstáculos a la libre competencia⁴⁰. Y para comprender y valorar el régimen de acceso debe tenerse en cuenta que implica la forzada colaboración de competidores en el mercado, sin necesidad de un vínculo jurídico contractual *ex arts. 7 y 38.5 RDLSP*. Colaboración que no necesariamente deba ser entre un «pequeño» proveedor tercero fintech y una entidad de crédito, pues cada vez es más habitual que grandes compañías, especialmente las propias entidades de crédito, ofrezcan estos servicios, sobre todo, el de información sobre cuentas.

Respecto al régimen jurídico del acceso a las cuentas del usuario, como en tantos otros aspectos, el legislador español no ha hecho sino incorporar sin cambios sustanciales lo previsto en la Directiva que buscaba, fundamentalmente, atajar los problemas de seguridad que las prácticas comunes de estos prestadores estaban generando, al replicar al usuario para acceder a la información⁴¹, en una suerte de suplantación consentida que dificultaba a los gestores de cuenta la identificación de las amenazas reales.

Como punto en común, más allá de la accesibilidad en línea de la cuenta, ambos servicios tienen su prestación, generalmente, a través del uso de las credenciales de seguridad personalizadas del usuario, pues son la llave de entrada a su(s) cuenta(s) de pago, algo que sucede en cualquier caso con el consentimiento explícito del usuario. Por tanto, la utilización de estos servicios supone la cesión de unos datos que el usuario está obligado contractual y legalmente a proteger: tal cesión prevista en la norma, queda condicionada a la réplica para el proveedor tercero de la obligación de protección de las credenciales del usuario y el establecimiento de canales seguros de comunicación con este para su transmisión [arts. 38.3.b) y 39.1.b)⁴² RDLSP]. La exigencia de consentimiento explícito no es tan vacua como pudiera parecer, pues excluye la posibilidad de otros intermediarios —salvo supuestos de externalización válida— entre el usuario y los proveedores de servicios de pago terceros.

En el caso de los servicios de iniciación, la relación directa entre el PSIP y el ordenante supone la clave entre la diferencia de un pago con tarjeta o instrumento similar y uno utilizando un servicio de iniciación.

⁴⁰ Lo cual se complementa, para el resto de servicios, con las previsiones de los arts. 8 y 9 RDLSP (al respecto, *vid.* BUESO GUILLÉN, P.-J., «Servicios de pago, sistemas de pago...», *op. cit.*, pp. 222 a 225).

⁴¹ CONESA, C.; GORJÓN, S. y RUBIO, G., «Un nuevo régimen...», *op. cit.*, pp. 91-92, autores que detallan el régimen previsto en el Reglamento Delegado.

⁴² En este artículo, igual que sucede en el art. 67.2.b) DSP2, hay un claro error de redacción dado que se refiere en último lugar a la obligación del propio PSIC de comunicarse consigo mismo a través de canales seguros y eficientes: «cuando las transmita [las credenciales del usuario] el proveedor de servicios de información sobre cuentas, la transmisión se realice a través de canales seguros y eficientes» (cursiva añadida).

El modelo «clásico» de este servicio supone que PSIP actúa por cuenta del beneficiario⁴³, pero a través de la relación jurídica directa que entabla con el usuario quien consiente expresa y directamente la actuación del iniciador, mientras que en un clásico pago por tarjeta, el adquirente del beneficiario no entabla relación jurídica directa con el usuario.

Elementos esenciales de este régimen, que afecta también a la responsabilidad potencial de los proveedores, son, por un lado, la obligación de los proveedores de servicios de pago terceros de identificarse ante el gestor de cuenta; por otro, la de este de establecer canales seguros de comunicación con estos proveedores⁴⁴.

Al proveedor de servicios de iniciación de pagos se le prohíbe entrar en posesión de los fondos de los usuarios, así como modificar el importe, el destinatario o cualquier otro elemento de la operación. Por la propia naturaleza del servicio que prestan, estas prohibiciones se consideran innecesarias en el caso de los proveedores de servicios de información sobre cuentas.

El resto de obligaciones previstas para los proveedores de servicios de pago terceros tienen que ver con la protección de los datos tanto de carácter personal como financiero. Al proveedor de servicios de iniciación de pagos se le prohíbe almacenar datos de pago sensibles del usuario⁴⁵ y solicitar al usuario datos distintos de los necesarios para prestar el servicio de iniciación del pago, lo que parece expresión del principio de protección de datos de minimización⁴⁶ [art. 38.3.f) RDLSP]. Por su parte, el PSIC está obligado acceder únicamente a la información de las cuentas de pago designadas por el usuario y las operaciones de pago correspondientes y a no solicitar datos de pago sensibles vinculados a las cuentas de pago [art. 39.1.d) y e) RDLSP]. El alcance de esta prohibición no está muy claro, teniendo en cuenta que las credenciales de seguridad son datos de pago sensibles y necesariamente el proveedor de servicios de información sobre cuentas debe acceder a ellas para prestar el servicio. Ha de interpretarse pues, que esta prohibición encuentra como límite la voluntad del usuario, por lo

⁴³ GIMIGLIANO, G., «Title III “Transparency of conditions...», *op. cit.*, p 119.

⁴⁴ Conforme a los arts. 30 a 35 Reg SCA SCS. La cuestión de las APIs genera no pocos problemas, al punto que la ABE constituyó un grupo de trabajo específico al respecto que periódicamente va emitiendo aclaraciones sobre la implementación de este régimen (*vid.* <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/eba-working-group-on-apis-under-psd2>).

⁴⁵ Art. 3.12 RDLSP: «Datos de pago sensibles: datos, incluidas las credenciales de seguridad personalizadas, que pueden ser utilizados para cometer un fraude. Por lo que respecta a las actividades de los proveedores de servicios de iniciación de pagos y los proveedores de servicios de información sobre cuentas, el nombre del titular de la cuenta y el número de la misma no constituyen datos de pago sensibles».

⁴⁶ El principio de minimización de datos, positivizado en el art. 5.1.c) RGPD, implica que solo pueden tratarse los datos de carácter personal adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

que lo que estará prohibido es solicitar al proveedor de servicios de pago gestor de cuenta datos sensibles de las cuentas que no hayan sido requeridos por el usuario o, en su caso, solicitar al usuario mismo más datos de pago sensibles de los estrictamente necesarios para la prestación del servicio. En este punto cobra sentido el que no se prohíba al proveedor de servicios de información sobre cuentas almacenar datos de pago sensibles, en tanto su servicio, prestado con carácter duradero al usuario, requiere almacenar, al menos, sus credenciales de seguridad como requisito *sine qua non* para la ejecución del contrato.

La última prohibición impuesta a los proveedores terceros es una expresión del principio de finalidad del tratamiento en materia de protección de datos⁴⁷, pero no está exenta de dudas. Se les prohíbe utilizar, almacenar o acceder a ningún dato para fines distintos de la prestación de sus respectivos servicios, solo que en el caso de los proveedores de servicios de información sobre cuentas [art. 39.2.f) RDLSP] se añade un último inciso que no se incluye en el art. 38.2.g) RDLSP: «de conformidad con las normas sobre protección de datos». El hecho de que no se incluya este matiz en el régimen de acceso en caso del servicio de iniciación pero sí en el de información sobre cuentas lleva a pensar que se trata de una prohibición absoluta⁴⁸, porque el RGPD sí permite el tratamiento de datos para finalidades diversas e incluso la reutilización de los datos originalmente recabados para una finalidad para otras ulteriores. Eso sí: cumpliendo con el régimen de protección de datos previsto para ello. Pero creemos que esta interpretación es incoherente y no necesariamente justa. Porque a ningún otro proveedor de servicios de pago se le prohíbe utilizar su actividad como medio para recabar datos aplicables a funciones distintas de la de prestación de su servicio, se insiste, cumpliendo escrupulosamente la legalidad vigente en materia de protección de datos. Estamos ante una traba desmesurada para los proveedores de servicios de iniciación de pagos que los coloca en clara desventaja competitiva. Y además es incoherente porque, si se plantea como una medida de protección del usuario, carece de sentido no imponerla también a los proveedores de servicios de información sobre

⁴⁷ El principio de finalidad del tratamiento o de limitación de la finalidad implica que los datos de carácter personal solo serán «recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines» (art. 5.1.b) RGPD).

⁴⁸ Así lo interpretan MCINNES, S. y SAMPEDRO, L., EU: *The interplay of PSD2 and GDPR – some select issues*, 2019, p. 5. Aunque también es posible que la cuestión deba formularse a la inversa y la pregunta sea por qué en el art. 39 RDLSP sí se incluye, mientras que en el art. 38 RDLSP, no. De acuerdo con el art. 15 RDLSP, el art. 65 RDLSP dedicado a la protección de datos, no se aplica a las entidades prestadoras del servicio de información sobre cuentas (en exclusiva). Pero, aun así, esto no deja de plantear nuevas dificultades de aplicación homogénea: el art. 65 RDLSP solo ha transpuesto a medias el art. 94 DSP2 y, además, de acuerdo con el Comité Europeo de Protección de Datos, las reglas de estos preceptos en materia de protección de datos tienen naturaleza contractual en estrecha relación con la protección de los datos de carácter personal de los usuarios, pero no son reglas especiales.

cuentas que acceden a mucha más información que los proveedores de servicios de iniciación de pagos.

Por tanto, solo caben dos interpretaciones posibles: o se trata de un error del legislador que debe ser corregido aplicando el régimen general de protección de datos o, detrás de este régimen discriminatorio hay intereses no declarados que pondrían seriamente en cuestión la libre y leal competencia en el mercado de servicios de pago.

En otro orden de cosas, son claras las obligaciones del proveedor de servicios de pago gestor de cuenta en relación a la utilización por parte del usuario de los servicios de pago complementarios⁴⁹. Además de garantizar una comunicación segura con los proveedores de servicios de pago terceros, los gestores de cuenta deben facilitar o poner a disposición del proveedor de servicios de iniciación de pagos toda la información sobre el inicio y ejecución de la operación de pago, en coherencia con el servicio de iniciación que, además de la fase aquí abordada, implica confirmar al beneficiario que la operación de pago se ha iniciado correctamente y que se cumplen los presupuestos para su ejecución (básicamente, la disponibilidad de los fondos). También tienen obligación de tratar las órdenes de pago transmitidas a través de los servicios de iniciación sin discriminación respecto de las transmitidas directamente por el ordenante (misma prioridad, plazos de ejecución, gastos aplicables, etc.), e igualmente las peticiones de datos transmitidas a través de un proveedor de servicios de iniciación de pagos, salvo —en ambos casos— que concurran causas objetivas que lo justifiquen.

Ahora bien, se permite al proveedor de servicios de pago gestor de cuenta que deniegue el acceso a la cuenta de pago a los proveedores terceros «por razones objetivamente justificadas y debidamente documentadas relacionadas con el acceso no autorizado o fraudulento a la cuenta de pago por parte del proveedor de servicios de pago que preste el servicio de información sobre cuentas o el proveedor de servicios de iniciación de pagos, en particular con la iniciación no autorizada o fraudulenta de una operación de pago» (art. 40.5 RDLSP), si bien entonces deberá informar al ordenante con anterioridad a la denegación, si es posible o, en caso contrario, inmediatamente después. Cuando cese la justificación, el gestor de cuenta deberá permitir el acceso a la cuenta de pago.

4. Ejecución y prueba de la operación de pago

La recepción y aceptación de la orden de pago autorizada y no revocada en los términos expuestos desencadena la obligación general de ejecución que, a su vez, se compone de otras más específicas.

⁴⁹ Art. 38.4 RDLSP.

En primer lugar, una que viene de antaño es la referida al deber todo proveedor de servicios de pago que intervenga en la ejecución de transferir la totalidad de su importe, absteniéndose de deducir gasto alguno de su cuantía (art. 53 RDLSP)⁵⁰. Solo para las operaciones en las que un proveedor actúe por cuenta de su usuario en calidad de beneficiario se permite el pacto de deducción de los propios gastos y comisiones. Ha de llamarse la atención sobre la obligación que se impone al PSP del ordenante de garantizar que el beneficiario recibe el importe total de la operación (art. 53.3 RDLSP), ya que supone un criterio de atribución de responsabilidad. Sin perjuicio de los eventuales derechos de repetición que procedan, es el PSP del ordenante el responsable de que a lo largo de toda la cadena de ejecución —exceptuando al beneficiario— no se detraiga suma alguna del importe movilizado. Por tanto, este precepto debe ser leído en conjunto con el régimen de responsabilidad por operaciones ejecutadas incorrectamente, como se verá en el capítulo siguiente.

Las otras tres obligaciones derivadas propiamente de la ejecución se refieren al plazo, a la determinación de la fecha de valor y a la puesta a disposición de los fondos (arts. 54 a 58 RDLSP). Estas reglas son aplicables con independencia de la condición del usuario y, por tanto, imperativas también, aunque no se trate de un consumidor o de una microempresa. En cambio, para alterar su ámbito de aplicación se tiene en cuenta la moneda en la que se denomine la operación de pago, lo que conecta este régimen directamente con la construcción de la unión económica y monetaria y con la consecución del mercado único de pagos en la UE.

Los supuestos en los que el régimen previsto legalmente es obligatorio son las operaciones de pago en euros y las operaciones de pago nacionales en la moneda de un Estado miembro que no forme parte de la zona del euro. Y además, aquellas a las que se refiere el art. 54.1.c) RDLSP⁵¹ separadamente y de forma un tanto confusa, que son una especie de híbrido de las anteriores. Por un lado, las operaciones transfronterizas en euros que, tras su movilización completa, se convierten a la moneda de un Estado miembro que no forme parte de la zona euro y, por otro, las operaciones de pago domésticas denominadas bien en euros, bien en la moneda distinta de un Estado miembro, que impliquen la conversión de moneda a la otra correspondiente.

⁵⁰ Antes de la armonización de la legislación de servicios de pago, había sido un problema común que los proveedores descontasen del importe de la operación los correspondientes gastos y comisiones aplicables a su usuario, de modo que el beneficiario recibía un pago incompleto.

⁵¹ El art. 54.1.c) sujeta a las reglas del RDLSP aquellas «operaciones de pago que solo impliquen una conversión de moneda entre el euro y la moneda de un Estado miembro que no forme parte de la zona del euro, siempre que la correspondiente conversión se lleve a cabo en el Estado miembro que no forme parte de la zona del euro y, en el caso de operaciones de pago transfronterizas, la transferencia transfronteriza se realice en euros».

Cuando no se trate de una de estas operaciones, las reglas de esta sección admiten pacto en contrario, a falta del cual se aplicarán supletoriamente. En estos casos solo es obligatorio respetar el régimen de la fecha de valor y puesta a disposición de los fondos. Ello implica que la fecha de valor del abono en la cuenta del beneficiario se corresponderá con el día en que el importe entró en posesión de su proveedor de servicios de pago, y que los fondos estén disponibles para el beneficiario inmediatamente después de su abono contable (art. 58 RDLSP). La obligación de disponibilidad inmediata se exceptúa cuando el proveedor del beneficiario deba proceder a la conversión de la moneda de la operación, siempre que no se trate de una conversión entre el euro y la divisa de un Estado miembro o entre las divisas de dos Estados miembros, en cuyo caso sigue siendo obligatoria. Por lo demás, las partes podrán pactar un régimen distinto al previsto legalmente, con la única limitación de que el plazo de ejecución no puede exceder de cuatro días hábiles si se trata de una operación de pago transfronteriza dentro de la UE (art. 54.2 *in fine* RDLSP).

Con carácter general, el plazo de ejecución de una operación de pago basada en cuenta es el de un día hábil⁵²; para ser exactos, el importe correspondiente debe abonarse en la cuenta del proveedor del beneficiario, a más tardar, al final del día siguiente hábil a la recepción de la orden de pago. Ello es así consideración aparte de los posibles acuerdos de horas límite de recepción de órdenes de pago *ex art. 50.1.II RDLSP*.

Pero este plazo puede alargarse cuando la orden de pago se inicie en papel, en cuyo caso el plazo de ejecución podrá ser de dos días hábiles —aunque a mi juicio, hoy en día, es difícilmente justificable que operativamente sea necesario más tiempo para ejecutar la orden—. En el art. 55.3 RDLSP se establece la regla de que el hecho de que la operación de pago se inicie por el beneficiario o a través de él no implica un mayor plazo de ejecución, sino que es obligación —en fase de iniciación— del proveedor de servicios de pago transmitirla de acuerdo a los plazos convenidos con el beneficiario para permitir la ejecución del pago en la fecha pactada.

⁵² El art. 86 DSP2 permitía a los Estados miembros establecer plazos máximos de ejecución de operaciones de pago nacionales inferiores a los indicados en los arts. 82 a 84 DSP2, transpuestos en los arts. 55 a 58 RDLSP, pero el legislador español no ha hecho uso de esta opción, a diferencia de otros legisladores nacionales. Por ejemplo, en Croacia las operaciones nacionales ejecutadas por proveedores de servicios de pago que pueden participar en los sistemas de pago de importancia sistémica (es decir, entidades de crédito y bancos centrales) deben ejecutarse el mismo día hábil en el que la orden de pago es recibida. Es decir, el proveedor de servicios de pago del ordenante debe acreditar los fondos en la cuenta de pago del proveedor del beneficiario el mismo día de recepción de la orden de pago [art. 54(3) *Zakon o platnom prometu* – Ley de los sistemas de pago 2018], *vid.* PARAĆ VUKOMANOVIĆ, I., «Transposition of the PSD2 into Croatian national legislation» en GIMIGLIANO, G. y BOŽINA BEROŠ, M. (eds.) *The Payment...*, *op. cit.*, pp. 264-281 (p. 271).

En relación a la inmediata puesta a disposición de los fondos se establece una excepción para los supuestos en los que el beneficiario no recibe el pago en una cuenta, y se le otorga a su proveedor de servicios de pago un día hábil adicional para poner los fondos a su disposición (art. 56 en relación al art. 55 RDLSP). Igualmente, se matiza que en los casos en los que —esta vez solo— un consumidor o microempresa ingrese efectivo en una cuenta de pago en la moneda de dicha cuenta, la disponibilidad de los fondos debe ser también inmediata desde la misma recepción por el proveedor, que además debe fijar la fecha de valor del ingreso en el mismo día. Cuando el usuario tenga otra condición, se permite que la puesta a disposición se produzca al día siguiente, al igual que la fijación de la fecha de valor.

En cuanto a las posibles vicisitudes que puedan afectar a la ejecución de una operación de pago, cualquiera que sea el instrumento utilizado, el art. 44 RDLSP determina, de forma imperativa, si el usuario es consumidor o microempresa, y dispositiva, en otro caso, que recaerá sobre el PSP la carga de acreditar que la operación discutida —por presunta falta de autorización o por ejecución incorrecta— fue autorizada por el usuario mediante la correspondiente autenticación del mismo y, en su caso, del instrumento utilizado; registrada con exactitud y contabilizada por el PSP; y «que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago»; así como, en su caso, que el usuario cometió fraude o negligencia grave (art. 44.1 RDLSP). A estos efectos, se obliga al proveedor a conservar la documentación y registros correspondiente durante al menos seis años, estableciéndose implícitamente el derecho del usuario a consultarlos. Y se matiza que el mero registro de la operación no constituye prueba de autorización por parte del usuario. Cuando en la ejecución de la operación intervenga un proveedor de servicios de iniciación de pagos, también sobre él recaerá la carga de la prueba de aquellos aspectos en el ámbito de su competencia.

Precisamente para evitar el posible acaecimiento de ciertos supuestos patológicos se recogen en el art. 42 RDLSP una serie de obligaciones que, de acuerdo con la definición de instrumentos de pago, deben entenderse aplicables a tarjetas o similares, así como a las transferencias, a los adeudos y a cualesquiera otros procedimientos que permitan la iniciación de operaciones de pago *ex. art.* 3.23 RDLSP. El proveedor tiene la obligación de cerciorarse de que las credenciales de seguridad personalizadas solo sean accesibles para el usuario; de garantizar que estén disponibles los medios adecuados y gratuitos para que el usuario pueda cumplir con sus obligaciones de notificación (en caso de operaciones no autorizadas o defectuosas, pérdida o sustracción de instrumentos de pago, etc.) y, en su caso, solicitar un desbloqueo legítimo; así como de facilitar, también gratuitamente, medios tales que permitan al usuario demostrar que ha notificado el extravío, sustracción o utili-

zación no autorizada del instrumento durante los 18 meses siguientes a la misma. Igualmente, en estos casos, deberá impedir la utilización del instrumento de pago una vez recibida la notificación del usuario.

También se les prohíbe enviar al usuario instrumentos de pago no solicitados, salvo que sea para sustituir uno caducado ya en posesión del cliente, o que en el contrato marco se haya pactado la posibilidad de sustitución cuando el nuevo instrumento incorpore nuevas funcionalidades. Y en caso de que en el contrato se haya pactado la posibilidad de bloquear el instrumento de pago de forma justificada, será obligación del proveedor comunicar al usuario tal bloqueo, a ser posible, con carácter previo y, si no, inmediatamente después, en los términos del art. 40.3 RDLSP, pasados los motivos que justificaron el bloqueo, o a petición del usuario deberá proceder al desbloqueo o a la sustitución del instrumento de pago sin coste alguno.

Un supuesto especial es el que se refiere a las operaciones con tarjeta en las que el importe exacto se desconoce en el momento en que el ordenante da su consentimiento para la ejecución de la operación de pago. Por ejemplo, en gasolineras automáticas, en contratos de alquiler de vehículos, reservas de hotel o máquinas de *vending*. En estos casos, independientemente de la condición del usuario, el art. 47 RDLSP establece que el proveedor de servicios de pago del ordenante solo puede bloquear fondos en la cuenta de pago del ordenante si este último ha consentido en la cantidad exacta de fondos que ha de bloquearse. Recibida la información sobre el importe exacto de la operación, debe liberar los fondos «sin demora [...] y, como muy tarde, inmediatamente después de haber recibido la orden de pago».

La última cuestión es la relativa al régimen de devolución (arts. 48 y 49 RDLSP), que tiene el carácter de dispositivo cuando el usuario no sea consumidor o microempresa. Hay dos supuestos en los que el usuario de servicios de pago tiene derecho a solicitar la devolución de una operación de pago iniciada por el beneficiario o a través del mismo. El primero, es aquel en el que la autorización de la operación no especificaba, en el momento en que se dio, el importe exacto de la operación de pago y el importe final superó el que el ordenante podía esperar razonablemente teniendo en cuenta las anteriores pautas de gasto, las condiciones del contrato marco y las circunstancias pertinentes al caso. La peculiaridad es que corresponderá al usuario la carga de acreditar que se cumplen estas condiciones, siempre que así lo pida el PSP. Por ejemplo, un recibo de suministros básicos muy elevado. Además, cuando haya habido cambio de divisa y se haya utilizado el tipo de cambio de referencia acordado, los incrementos en este no pueden motivar la solicitud de devolución.

El segundo supuesto, incondicionado y sometido únicamente a un plazo límite para solicitarlo, son los adeudos domiciliados en euros

regulados por el Reglamento SEPA; de hecho, el origen de este régimen es precisamente dicho reglamento. La motivación de prever este derecho de devolución para el primer supuesto, en contraposición, es la protección del usuario ante operaciones inusualmente altas en aquellos Estados miembros en los que la moneda no es el euro⁵³ aunque, por extensión, es aplicable a cualquier adeudo nacional no SEPA.

El plazo para solicitar la devolución es de ocho semanas desde la fecha del adeudo y, tras la solicitud, el PSP dispone de 10 días hábiles para devolver el importe íntegro de la operación de pago o, únicamente en caso de los primeros, comunicar al usuario las razones objetivas que justifican la denegación e indicar los procedimientos de reclamación, judiciales y extrajudiciales, a disposición del usuario, pues no es posible la denegación de devolución de los adeudos directos SEPA (art. 49.2 RDLSP).

Finalmente, se prevé la posibilidad de excluir el derecho de devolución en el contrato marco cuando el ordenante haya dado su consentimiento directamente al proveedor de servicios de pago y, en su caso, el PSP o el beneficiario hayan informado al usuario, con al menos cuatro semanas de antelación a la fecha prevista de ejecución, sobre la operación de pago en cuestión (art. 48.4 RDLSP).

III. OBLIGACIONES DEL USUARIO DE SERVICIOS DE PAGO

A diferencia de la larga lista de obligaciones y cargas que se establecen para los proveedores de servicios de pago, en la contratación de servicios de pago los usuarios no tienen muchas obligaciones más allá del pago de los gastos y comisiones pactadas y, en su caso, de las que deriven de las normas sobre prevención del blanqueo de capitales y de la financiación del terrorismo.

Por supuesto, dentro de los límites establecidos por la ley, en el contrato se podrán establecer algunas obligaciones accesorias y, en todo caso, el medio de comunicación que hayan de utilizar las partes, que también vinculará al usuario, salvo en el caso de ejercicio del derecho de resolución como se ha indicado en el capítulo anterior.

También deberán preverse de forma expresa en el contrato, en su caso, los límites de gasto aplicables a las operaciones de pago iniciadas a través de determinados instrumentos, en cuyo caso el usuario deberá actuar conforme al acuerdo alcanzado con su proveedor de conformidad

⁵³ Considerando 76 RDLSP.

con el art. 40 RDLSP⁵⁴. Asimismo, de lo expuesto en el apartado anterior, se desprende la prohibición para el usuario de revocar o solicitar la devolución de la operación fuera de los casos antedichos. Pero, en la práctica, todas estas cuestiones comportarán más una imposibilidad operativa que una circunstancia que el usuario pueda controlar y acabe ocasionando su responsabilidad.

Las únicas obligaciones en sentido estricto que la ley establece para el usuario son las tendentes a evitar casos de fraude. Así, está obligado a utilizar los instrumentos de pago de conformidad con las condiciones acordadas con su proveedor, tomando «todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas» y, en caso de extravío, sustracción o apropiación indebida del instrumento o de su utilización no autorizada, deberá notificarlo al proveedor, «sin demora indebida en cuanto tenga conocimiento de ello» (art. 41 RDLSP).

La indeterminación del plazo de notificación es una de las cuestiones abiertas que generan mayor inseguridad jurídica, si bien es cierto que el art. 43 RDLSP da un criterio legal máximo. Este precepto condiciona el derecho del usuario a obtener la rectificación de una operación no autorizada o ejecutada incorrectamente a la comunicación de la misma al PSP «sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 60, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo»⁵⁵. Ahora bien, la exigibilidad de estos plazos se supedita a que el proveedor de servicios de pago haya proporcionado la información correspondiente a la operación de pago concreta, de acuerdo con sus obligaciones de transparencia e información en ejecución del contrato (art. 43.1. II RDLSP)⁵⁶. De esta obligación, se deriva implícitamente la de consulta periódica de los movimientos de la cuenta como expresión de la debida diligencia del usuario, cuestión que habrá de ser valorada en su caso por los tribunales⁵⁷.

⁵⁴ Al hilo del contenido del contrato ya ha dicho, pero merece la pena recordarlo, que el PSP puede reservarse el derecho a bloquear el instrumento de pago de forma justificada, pero entonces deberá informar al ordenante en la forma convenida.

⁵⁵ Así lo ha interpretado el TJUE, que ha declarado que la rectificación de la operación solo es posible si el usuario la notifica a su proveedor de servicios de pago a más tardar en los trece meses siguientes a la fecha de adeudo correspondiente (FD 33, Sentencia del TJUE de 2 de septiembre de 2021, *Caisse régionale de Crédit agricole mutuel (CRCAM)*, C-337/20, ECLI:EU:C:2021:671).

⁵⁶ El tenor literal del precepto no es el más claro, pero el segundo párrafo del mismo 43.1, parece dejar claro que el plazo se refiere a la notificación efectuada por el usuario. Con todo, este precepto plantea dudas interpretativas severas al ponerlo en relación con el régimen de responsabilidad (*vid. infra* en el epígrafe dedicado a las operaciones de pago no autorizadas).

⁵⁷ En la doctrina Austriaca, en relación a la transposición de la Segunda Directiva de servicios de pago en la ZaDiG 2018, pueden encontrarse dos corrientes divergentes al respecto de la obligación del usuario de monitorizar el instrumento de pago. Para algunos autores, forma parte

IV. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DEL USUARIO

1. Cuestiones abiertas sobre la interacción entre las normas de servicios de pago y las de protección de datos de carácter personal

Cuando el usuario sea persona física, independientemente de que se trate de un consumidor o de un empresario individual, como en la prestación de cualquier otro servicio, el proveedor de servicios de pago será, además, responsable del tratamiento de sus datos de carácter personal⁵⁸. Esta materia se encuentra armonizada a nivel europeo mediante el Reglamento General de Protección de Datos (RGPD)⁵⁹ que en España ha sido desarrollado por la Ley Orgánica 3/2018, de 5 de diciembre,

de su diligencia debida. Para otros, sin embargo, de la forma en que el art. 63 ZaDiG 2018 (que transpone el art. 69 DSP2 y sería el homólogo al art. 41 RDLSP —«(2) *The payment service user shall notify the payment service provider or the body designated by the payment service provider without undue delay on becoming aware of loss, theft, misappropriation or any other unauthorised use of the payment instrument*»—), no puede concluirse que sea obligación del usuario la comprobación constante de las operaciones realizadas con un instrumento de pago, en la medida en que no se enumera expresamente y el precepto contiene un alista *numerus clausus* de obligaciones para el usuario (*vid.* MIERNICKI, M., «Implementation of the PSD2 in Austria» en GIMIGLIANO, G. y BOŽINA BEROŠ, M. [eds.] *The Payment...*, *op. cit.*, pp. 245-263 [p. 246-247]). En España, sin embargo, la interpretación del art. 41.b) en relación al art. 43 RDLSP aboca a la conclusión expresada *supra*.

⁵⁸ Los datos personales se definen como toda información sobre una persona física identificada o identificable al que se denomina en la legislación europea «el interesado», siendo identificable aquella persona cuya identidad pueda determinarse, directa o indirectamente —por ejemplo, mediante un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona— (art. 4.1 RGPD). Es decir, el «interesado» es la persona física a la que se refieren los datos personales (RECIO GAYO, M., *El ejercicio de los derechos de protección de datos y su aplicación práctica*, Bosch, Madrid, 2019, p. 24). El tratamiento de datos personales es «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción» (art. 4.2 RGPD). Por otro lado, se considera responsable de dicho tratamiento a la persona física o jurídica que determine los fines y medios del tratamiento (art. 4.7 RGPD), es decir, que decida sobre la finalidad para la cual se vayan a tratar los datos de los interesados (para qué) y sobre la forma en que se va a llevar a cabo dicho tratamiento (cómo). Sobre estos conceptos, en la doctrina *vid.* ROMEO CASABONA, C. M., «Datos personales (comentario al artículo 4.1 RGPD)» y DAVARA RODRÍGUEZ, M. A. «Tratamiento (comentario al artículo 4.2 RGPD)», ambos en TRONCOSO (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales*, tomo I, Civitas, Cizur Menor, 2021, pp. 573-590 y 591-600, respectivamente.

⁵⁹ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

Simplificando esta compleja cuestión, puede decirse que el sistema de protección de datos personales descansa sobre dos pilares fundamentales: la necesidad de que el tratamiento sea lícito, leal y transparente; y el principio de responsabilidad proactiva⁶⁰, que consiste en que el responsable del tratamiento cumpla el régimen legal y, además, sea capaz de demostrar dicho cumplimiento (art. 5 RGPD). En torno a estos dos pilares, se detallan una serie de principios que informan todo el marco jurídico aplicable⁶¹.

La interacción de las normas de servicios de pago y las de protección de datos de carácter personal plantea algunas dificultades específicas debidas, algunas, al hecho de que la Segunda Directiva de servicios de pago contiene normas aparentemente especiales en relación a la protección de datos en sede de prestación de estos servicios y, otras, a la propia naturaleza de los servicios de pago⁶².

Las normas aparentemente especiales son los arts. 66, 67 y 94 DSP2. A este último, de vital importancia, se le dedica el siguiente subepígrafe. En relación con los arts. 66 y 67 DSP2, transpuestos al ordenamiento jurídico español en los arts. 38 y 39 RDLSP, ya se ha puesto de manifiesto la aparente discordancia que existe entre estos y el art. 6 RGPD. Una interpretación literal de la ley de servicios de pago lleva a concluir que los proveedores de servicios de iniciación de pagos, a diferencia del resto de los proveedores de servicios de pago, no pueden utilizar los datos recabados en la prestación de servicios de iniciación con fines ulteriores. Y ello a pesar de que, con carácter general, el RGPD sí permite ese tratamiento ulterior siempre y cuando sea lícito

⁶⁰ *vid.* NÚÑEZ GARCÍA, J.L., «Responsabilidad y obligaciones del responsable y del encargado de tratamiento» en RALLO (dir.), *Tratado de Protección de Datos*, Tirant lo Blanch, Valencia, 2019, pp. 353-386 (pp. 353-358).

⁶¹ Se trata de los principios de limitación de la finalidad, de minimización de datos, de exactitud, de limitación del plazo de conservación, y de integridad y confidencialidad (art. 5 RGPD), *vid.* TRONCOSO REIGADA, A., «Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al art. 4 LOPDGDD)», en TRONCOSO (dir.), *Comentario al Reglamento...*, *op. cit.*, pp. 847-908 (pp. 855 y ss.); PUENTE ESCOBAR, A., «Principios y licitud del tratamiento» en RALLO (dir.), *Tratado de Protección...* *op. cit.*, pp. 115-168.

⁶² Algunas de estas dificultades fueron puestas de manifiesto aún en relación a la derogada Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por GONZÁLEZ FUSTER, G., «EU Data Protection and Future Payment Services» en GIMIGLIANO, G. (ed.), *Bitcoin and mobile payments. Constructing a European Framework*, Studies in Financial Services Technology, Palgrave Macmillan, Londres, 2016, pp. 181-202 (p. 189); y en relación al RGPD, por Sophia in't Veld, parlamentaria europea por Países Bajos que a principios de 2018 envió una carta al Comité Europeo de Protección de datos en relación a algunas cuestiones relativas a la interacción entre el RGPD y la DSP2. A dicha carta, contestó el Comité el 5 de julio de 2018 mediante otra, disponible en: https://edpb.europa.eu/sites/default/files/files/news/psd2_letter_en.pdf.

de conformidad con el art. 6.4 RGPD que, en esencia, requiere que este otro tratamiento se base en el consentimiento del usuario o que sea compatible con aquel para el que se recabaron los datos inicialmente. Compatibilidad que debe valorarse teniendo en cuenta, principalmente, la relación entre los fines de ambos tratamientos, el contexto en que se hayan recogido los datos personales, la naturaleza de los datos personales, las posibles consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas (por ejemplo, el cifrado de los datos o la seudonimización)⁶³.

Como se ha adelantado en un epígrafe anterior, la valoración que se hace de estas supuestas normas especiales es negativa, en la medida en la que desnivelan las condiciones de competencia en el mercado de servicios de pago e, indirectamente, perjudican por ello al usuario. A mi juicio, los arts. 38 y 39 RDLSP no son normas de carácter especial y deben interpretarse conforme al régimen general de protección de datos, sin que se entienda que prohíben ningún tratamiento que sí permite el RGPD. En este sentido, las Directrices del Comité Europeo de Protección de Datos⁶⁴ sobre la interacción de la DSP2 y el RGPD han establecido un criterio intermedio según el cual los proveedores de servicios de pago terceros solo pueden proceder a un tratamiento ulterior de los datos personales de los usuarios de servicios de pago con su consentimiento, pero no sobre la base del test de compatibilidad entre los fines iniciales y los ulteriores al que se refiere el art. 6.4 RGPD⁶⁵.

Si bien este criterio puede servir para aliviar los efectos perjudiciales sobre la competencia de una interpretación estricta de los arts. 66 y 67 DSP2, no parece que tal conclusión cuente con una justificación suficientemente argumentada⁶⁶. Debe llamarse la atención sobre el hecho de que, de acuerdo con su art. 1, el RGPD no pretende solo «la protección de las personas físicas en lo que respecta al tratamiento de los datos personales» sino también garantizar «la libre circulación de tales datos» (ap. 1), al punto de que «[l]a libre circulación de los

⁶³ Directriz 60, COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Directrices 6/2020 sobre la interacción de la Segunda Directiva sobre servicios de pago y el Reglamento general de protección de datos. En general, sobre estas directrices *vid.* DIVISSENKO, N., «Title IV, Chapter 4 “Data Protection”» en GIMIGLIANO, G. y BOŽINA BEROŠ, M. (eds.) *The Payment...*, *op. cit.*, pp. 179-188 (pp. 185 y ss.); sobre la seudonimización *vid.* ROMEO CASABONA, C. M., «Datos personales (comentario al artículo 4.1 RGPD)» en TRONCOSO (dir.), *Comentario al Reglamento...* *op. cit.*, pp. 613-628.

⁶⁴ *Ibid.* Sobre el origen y naturaleza del Comité Europeo de Protección de Datos *vid.* CERVERA NAVAS, L., «El Comité Europeo de Protección de Datos» en RALLO (dir.), *Tratado de Protección...* *op. cit.*, pp. 655-670.

⁶⁵ Directriz 23, sobre la interacción de la Segunda Directiva sobre servicios de pago y el Reglamento general de protección de datos.

⁶⁶ En este sentido, también CYNDECKA, M., «The Interplay between the Framework for Payment Services and Data Protection: A Piece of European Community Identity» en GIMIGLIANO y CATTELAN (eds.), *Money Law...*, *op. cit.*, pp. 37-56 (pp. 45-47).

datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales». Por tanto, puede afirmarse que el objetivo de este Reglamento es garantizar el equilibrio entre la tutela de la privacidad de los ciudadanos y la fluidez de los datos personales, convertidos a día de hoy en un activo fundamental, tanto desde el punto de vista del mercado como, en general, para el propio funcionamiento de nuestra sociedad. Además, el RGPD (2016) es posterior a la Segunda Directiva de servicios de pago (2015). Del planteamiento del Comité Europeo de Protección de Datos se deduce la no consideración de los arts. 66 y 67 DSP2 como *lex specialis*, ya que su literalidad llevaría a concluir que el tratamiento ulterior está prohibido en todo caso⁶⁷. Entonces, debería considerarse que el RGPD, en tanto que ley posterior, ha derogado tácticamente las limitaciones contenidas en los art. 66 y 67 DSP2. Pero las Directrices no llegan a esta conclusión. Por el momento, no ha habido pronunciamientos judiciales ni de las autoridades de protección de datos en esta materia, pero parece que sería conveniente aprovechar la revisión de la Segunda Directiva de servicios de pago para abordar estas cuestiones.

Por otro lado, entre las cuestiones abiertas en la interacción entre la DSP2 y el RGPD derivadas de la naturaleza de los servicios de pago, destaca el problema del tratamiento de categorías especiales de datos y el del tratamiento de los datos personales de las «partes silenciosas». Su estudio en profundidad supera el objeto de este trabajo, pero merece la pena hacer siquiera sea un breve comentario, porque también a este respecto convendría mayor aclaración que la proporcionada por las Directrices del Comité Europeo de Protección de Datos⁶⁸.

Los datos personales pertenecientes a categorías especiales son aquellos que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física (art. 9.1 RGPD)⁶⁹. Es indudable que multitud de operaciones de pago

⁶⁷ Tampoco se repara en la evidente diferencia de redacción entre ambos preceptos. Recuérdese que, tras prohibir la utilización de los datos de los usuarios para fines distintos de la prestación del servicio de información sobre cuentas, el art. 67.2.f) DSP2 hace expresa alusión a las normas sobre protección de datos —lo que podría servir de base para justificar la aplicación del art. 6.4 RGPD—, mientras que el art. 66.3.g) DSP2 no contiene tal referencia, limitándose a establecer la antedicha prohibición.

⁶⁸ En relación a estos problemas y su impacto sobre los proveedores de servicios de pago terceros, *vid.* CYNDECKA, M., «The Interplay...», *op. cit.*, pp. 48-52.

⁶⁹ REBOLLO DELGADO, L., «Las condiciones de tratamiento de categorías especiales de datos (comentario al artículo 9 RGPD y 9 LOPDGDD)»; GÓMEZ SÁNCHEZ, Y., «Categorías especiales de datos personales: los datos de origen étnico o racial, los datos genéticos, los datos biométricos, los datos relativos a la salud, los datos relativos a la vida sexual y la orientación

pueden revelar, si no claramente, al menos indiciariamente este tipo de datos sensibles. Piénsese, por ejemplo, en el pago de una cuota sindical o de una afiliación a un partido político. Otro ejemplo: hoy en día, no es nada infrecuente que los proveedores de servicios de pago traten los datos biométricos de los usuarios como medida de seguridad para el acceso a los servicios en línea. Con carácter general, el tratamiento de estos datos está prohibido salvo que concurra una de las circunstancias «habilitantes» del art. 9.2 RGPD que, en lo que aquí interesa, se reducen al consentimiento expreso del usuario. *A priori*, ello implica que el proveedor de servicios de pago debe recabar un consentimiento expreso adicional ante el eventual tratamiento de datos de pago sensibles. El problema es que en las Directrices sobre interacción entre el RGPD y la DSP2 parecen adoptarse criterios más estrictos que en otras anteriores⁷⁰, planteando algunas dificultades para entender lícito el tratamiento de categorías especiales de datos en sede de prestación de servicios iniciación de pagos y de información sobre cuentas, cuyos proveedores deben evitar dicho tratamiento. A mi juicio, ello es prácticamente imposible. El ejemplo más representativo es el del proveedor de servicios de información sobre cuentas: no se concibe cómo puede evitar el tratamiento de categorías especiales de datos cuando el usuario le pide información sobre varias cuentas en las que, por seguir con el ejemplo anterior, tiene domiciliado el pago de su cuota sindical y de la afiliación a un partido político. Pero, además, negarse al tratamiento de esos datos puede implicar el incumplimiento de las obligaciones que le imponen la normativa de pagos y el contrato con el usuario. En estos casos, parece que la única solución —posible pero, desde luego, no incuestionable— es acudir a la circunstancia habilitante del art. 9.2.g) RGPD y entender que el tratamiento de dichos datos es necesario por razones de interés público⁷¹, en concreto, el buen funcionamiento de

sexual (comentario al artículo 9.1 RGPD)» y GONZÁLEZ-POL GONZÁLEZ, I., «Los datos reveladores de las opiniones políticas como categorías especiales de datos personales. El tratamiento de datos personales en el ejercicio de la acción política (comentario al artículo 9.1 RGPD)» todos en TRONCOSO (dir.), *Comentario al Reglamento...*, *op. cit.*, pp. 1013-1040, 1041-1066 y 1067-1064, respectivamente.

⁷⁰ *Ibid.*, pp. 52-54. En concreto, GRUPO DE TRABAJO DE ART. 29, Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018 (directriz C). El Grupo de Trabajo del artículo 29 (GT Art. 29) fue el grupo de trabajo europeo independiente que se ocupó de las cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD), momento en el que fue sustituido por el Comité Europeo de Protección de Datos (*European Data Protection Board*).

⁷¹ Art. 9.2.g) RGPD: «el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado».

los servicios y sistemas de pago⁷², cuya justificación se hallaría en el considerando 5 de la PSD2, que considera crucial para el crecimiento económico de la UE «el desarrollo continuo de un mercado interior integrado para la seguridad de los pagos electrónicos» y afirma que «los servicios de pago son esenciales para el funcionamiento de actividades económicas y sociales vitales». Es evidente que nos encontramos ante otra cuestión que debe ser revisada.

Por último, el tratamiento de datos personales de las «partes silenciosas» es el referido a las personas que no tienen una relación contractual con el proveedor de servicios de pago, pero cuyos datos deben ser tratados para ejecutar el contrato con el usuario. Por ejemplo, en una transferencia entre particulares, el proveedor del ordenante debe tratar los datos personales del beneficiario, con quien no le une ningún contrato. Con carácter general, este tratamiento será lícito conforme al legítimo interés del proveedor en cumplir sus obligaciones contractuales para con su usuario [*ex art. 6.1.f) RGPD*]. En este punto, las Directrices son imprecisas en relación a la prueba de equilibrio que debe realizarse para asegurar que los intereses de la parte silenciosa no prevalecen sobre los del proveedor⁷³ y, de nuevo, son aparentemente más exigentes con los proveedores de servicios de pago terceros que con el resto de proveedores de servicios de pago⁷⁴. Sin embargo, el mayor problema lo plantea, otra vez, el tratamiento de categorías especiales de datos. Volviendo al ejemplo anterior, el proveedor de servicios de pago de un sindicato trata datos sensibles de todos los afiliados a dicho sindicato y, evidentemente, es inviable exigir que recabe el consentimiento de cada uno de ellos. Otro ejemplo podría ser el del proveedor de una clínica de salud privada. Por ahora, la única alternativa viable es la indicada *supra*: reputar lícito el tratamiento sobre la base del interés público en el buen funcionamiento de los servicios y sistemas de pago.

2. Breve análisis del art. 94 DSP2 y de su coherencia con el Reglamento General de Protección de Datos

El art. 94 DSP2 regula algunos aspectos en relación con la protección de datos personales de los usuarios de servicios de pago. Su apartado primero aclara que los Estados miembros deben autorizar el tratamiento los datos personales de los usuarios por parte de los proveedores de servicios de pago y de los sistemas de pago cuando sea necesario a fin de garantizar la prevención, la investigación y el descubrimiento del fraude en los pagos. Aclaración que no está de más, pero pudiera

⁷² CYNDECKA, M., «The Interplay...», *op. cit.*, p. 56.

⁷³ Directriz 20, sobre la interacción de la Segunda Directiva sobre servicios de pago y el Reglamento general de protección de datos.

⁷⁴ *Ibid.* Directrices 21 a 25.

también ser superflua, ya que el art. 6.1.c) RDLSP prevé la licitud de todo tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable de dicho tratamiento, y los proveedores de servicios de pago están obligados por las normas especiales de servicios de pago a aplicar medidas de seguridad y de prevención y análisis de riesgos (arts. 66 RDLSP y 18 RTS SCA-SCS). En cualquier caso, esta previsión del art. 94.1 DSP2 sirve para evitar posibles prácticas supervisoras divergentes en la materia por parte de las autoridades nacionales de protección de datos. El último inciso de este apartado simplemente señala —aunque con una redacción mejorable— que cualquier tratamiento en sede de prestación de servicios de pago debe llevarse a cabo conforme a las reglas generales de protección de datos⁷⁵.

Es el segundo apartado de este artículo, así como, en general, la transposición de todo el precepto al ordenamiento jurídico español, lo que plantea ciertos problemas de incongruencia que, a mi juicio, urge subsanar.

Por un lado, el art. 94.2 DSP2 introduce una nueva regla respecto al régimen previsto en la Primera Directiva de servicios de pago, imponiendo que «[l]os proveedores de servicios de pago únicamente obtendrán, tratarán y conservarán los datos personales necesarios para la provisión de sus servicios de pago, únicamente con el consentimiento expreso del usuario del servicio de pago». *A priori*, podría parecer que, por alguna razón, el legislador europeo ha querido establecer una regla de carácter especial que limita la posibilidad de tratamiento de datos personales en relación con la comercialización y prestación de servicios de pago: la prohibición de un tratamiento ulterior, con finalidad distinta a la prestación de servicios de pago, y la necesidad de que la base jurídica del tratamiento sea, en todo caso, el consentimiento expreso del usuario. Pero cuando se consulta la documentación correspondiente a la elaboración de la Segunda Directiva de servicios de pago no se encuentra una justificación clara del por qué este cambio de criterio respecto de la Directiva de 2007. El ap. 2 de lo que ahora es el art. 94 DSP2 se introdujo próximo a finalizar el proceso prelegislativo,

⁷⁵ En este punto, la referencia a la legislación europea anteriormente vigente (la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y el Reglamento (CE) núm. 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos), debe entenderse actualizada y hecha al Reglamento General de Protección de Datos de 2016. Sobre la transposición en España del régimen de la Directiva mediante Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal *vid.* APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor, 2002, *passim*.

en el texto de compromiso final⁷⁶, sin que conste ningún explicación adicional o cambios sustanciales en los considerandos de la norma que permitan entender el objetivo o razón del precepto. A decir verdad, más bien parece que esa relación entre la necesidad del consentimiento expreso del usuario y la protección de datos tenía un objeto mucho más definido: la prestación de servicios de información de cuentas y de iniciación de pagos⁷⁷.

Aunque la —evidente— necesidad de consentimiento del usuario para la intervención de un proveedor tercero es una exigencia que se ha mantenido, en el texto finalmente aprobado no hay referencia alguna a la conexión de esta específica cuestión con la protección de datos personales (ni en el preámbulo, ni en la parte dispositiva de la norma), de modo que no es posible asegurar a ciencia cierta que este sea el origen del art. 94.2 DSP2, si bien ello podría explicar su extraño contenido.

Se considera extraño porque difiere sustancialmente de las reglas generales de protección de datos. En primer lugar, al exigir que los proveedores de servicios de pago únicamente obtengan, traten y conserven los datos personales para la provisión de sus servicios, el art. 94.2 DSP2 parece prohibir cualquier posibilidad de tratamiento ulterior que, como se ha explicado anteriormente, sí se permite, previo cumplimiento de ciertos requisitos, en virtud del art. 6.4 RGPD. Como se desprende de lo referido en el apartado anterior, las Directrices del Comité Europeo de Protección de Datos parecen permitir el tratamiento ulterior en los términos generales del RGPD —más allá de las limitaciones indicadas *supra* en relación a los servicios de iniciación de pagos y de información sobre cuentas—, sin dar ninguna argumentación sobre cómo ello debe conciliarse con el tenor literal del primer inciso del art. 94.2 DSP2.

En segundo lugar, este artículo de la norma de pagos parece extraño por la exigencia de consentimiento expreso del usuario como medida de protección de datos. Ciertamente, todo tratamiento de datos personales debe fundamentarse en una de las bases jurídicas previstas en el art. 6

⁷⁶ CONSEJO DE LA UNIÓN EUROPEA, *Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC - Confirmation of the final compromise text with a view to agreement*, 2 de junio de 2015.

⁷⁷ Aunque en los sucesivos cambios de redacción de la norma durante el proceso legislativo acabó desapareciendo con este tenor literal, el considerando 51 de la Propuesta de Segunda Directiva [COM (2013) 547 final] se refería a la necesidad de que los proveedores de servicios de pago terceros cumplieren con las obligaciones de protección de datos y, acto seguido, exigía que los usuarios diesen su consentimiento expreso para el acceso a su cuenta de pago. Razón por la no puede descartarse que este sea el origen del art. 94.2 DSP2, aunque en la generalización se haya desvirtuado.

RGPD⁷⁸. Lo primero que debe tenerse en cuenta es que el consentimiento del interesado es solo uno de los posibles fundamentos para el tratamiento de sus datos de carácter personal, pero no es el único ni necesariamente el más frecuente. Incluso puede que, al contrario, los estrictos requisitos exigidos por el art. 7 RGPD y las directrices que lo interpretan⁷⁹ para que el consentimiento sea válido, implican que cuando sea posible basar el tratamiento en alguna de las otras causas de licitud enumeradas en el art. 6 RGPD, ello redunde en una mayor capacidad del proveedor para acreditar el cumplimiento de sus obligaciones (responsabilidad proactiva) y, por tanto, sea más eficiente escogerla, en lugar del consentimiento del interesado.

Con carácter general, en sede de prestación de servicios de pago —y, en realidad, de cualquier servicio—, el tratamiento de datos personales será lícito en tanto necesario para la ejecución de un contrato en el que el interesado es parte [art. 6.1.b) RGPD]. Pero el art. 94.2 DSP2 parece exigir que para que el tratamiento sea lícito, deba basarse en el consentimiento del usuario [art. 6.1.a) RGPD].

Sin embargo, por el momento, debe concluirse que este precepto de la Segunda Directiva de servicios de pago no tiene carácter de ley especial en materia de servicios de pago. Primero, porque el propio Considerando 89 DSP2 señala que «cuando a efectos de la presente Directiva hayan de tratarse datos personales, deben especificarse los fines precisos, mencionarse la base jurídica pertinente y cumplir los requisitos de seguridad pertinentes establecidos en la Directiva 95/46/CE [ahora RGPD]». De modo que si deben especificarse los fines y la base jurídica pertinente no parece que el art. 94.2 DSP2 haya de ser entendido en el sentido de que veta la posibilidad de un tratamiento distinto a la estricta prestación de servicios de pago ni, menos aún, que la causa de licitud del tratamiento deba ser el consentimiento.

La duda que surge entonces es la de para qué sirve ese consentimiento que exige el art. 94.2 DSP2, y esta es precisamente la gran cuestión abierta en materia de interacción de la Directiva con el RGPD.

⁷⁸ AA.VV., PIÑAR (dir.) y RALLO (coord.), *Memento práctico de protección de datos*, Francis Lefebvre, Madrid, 2019, pp. 55-67; SEMPERE SAMANIEGO, F., «La licitud del tratamiento. (Comentario al artículo 6 RGPD y al artículo 8 LOPDGDD y disposición adicional duodécima LOPDGDD)» en TRONCOSO (dir.), *Comentario al Reglamento...*, op. cit., pp. 925-944.

⁷⁹ GRUPO DE TRABAJO DE ART. 29, Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, adoptadas el 28 de noviembre de 2017 y revisadas por última vez y adoptadas el 10 de abril de 2018; en la doctrina, *vid.* VILASAU SOLANA, M., «El consentimiento general y el de menores» en RALLO (dir.), *Tratado de Protección...*, op. cit., pp. 197-250 (pp. 197-233); CASTILLO VÁZQUEZ, I-C., «Consentimiento (comentario al artículo 4.11 RGPD)» y «Requisitos del consentimiento utilizado como fundamento jurídico para el tratamiento de los datos de carácter personal (comentario al artículo 7 RGPD y al artículo 6 LOPDGDD)», ambos en TRONCOSO (dir.), *Comentario al Reglamento...* op. cit., pp. 679-692 y 954-956, respectivamente.

A mi juicio, este apartado no aporta nada útil, más bien al contrario, genera más inseguridad jurídica que protección de algún tipo. Las Directrices del Comité Europeo de Protección de Datos han tratado de dotar de cierto sentido a la exigencia de «consentimiento expreso» del usuario del art. 94.2 DSP2 declarando que se trata de un requisito adicional de carácter contractual⁸⁰ «que debe interpretarse en el sentido de que, al celebrar un contrato con un proveedor de servicios de pago en el marco de dicha Directiva, los interesados deben ser plenamente conscientes de las categorías específicas de datos personales que se tratarán. Además, tienen que ser informados de la finalidad específica (del servicio de pago) para la que se tratarán sus datos personales y tienen que aceptar de manera expresa estas cláusulas. Dichas cláusulas deben distinguirse claramente de las demás cuestiones tratadas en el contrato y el interesado las deberá aceptar expresamente»⁸¹. No alcanza a entenderse en qué se diferencia esa finalidad del «consentimiento expreso» exigido por la DSP2 de la del «consentimiento» de los arts. 6.1.a) y 7 RGPD. En cualquier caso, parece evidente que para el Comité Europeo de Protección de Datos el art. 94 DSP2 no tiene la consideración de *lex specialis* frente al RGPD. En mi opinión, ello debería llevar a otro planteamiento: la posibilidad de que el art. 94 DSP2 quedara tácitamente derogado con la aprobación del RGPD, en lo que a este último se oponga (todo su apartado 2). Pero en las directrices no se expresa esta posibilidad, ni siquiera hipotéticamente.

Quizás la directriz 38⁸² aporte algunos argumentos para comprender este precepto de la norma europea de servicios de pago, que precisamente conectan con la tesis de que el art. 94.2 DSP2 se elaboró ini-

⁸⁰ Criterio que ya había mantenido anteriormente en la carta en respuesta a Sophia in 't Veld y que, en Austria, ya había sido acogido y puesto en práctica por la autoridad de protección de datos, el Tribunal Federal Administrativo y la doctrina jurídica (*vid.* MIERNICKI, M., «Transposition of the PSD2 in Austria» en BANI, STASIO Y SICARRONE ALIBRANDI [eds.], *The transposition... op. cit.*, pp. 189-206 [pp. 196-200], comentando la aplicación de esta doctrina defendida por los académicos austriacos en el caso que dio lugar a la Sentencia del *Bundesverwaltungsgericht* de 24 de mayo de 2019 [W258 2205602-1]).

⁸¹ Directriz 37, sobre la interacción de la Segunda Directiva sobre servicios de pago y el Reglamento general de protección de datos.

⁸² «Un aspecto central del concepto de “consentimiento expreso”, según el artículo 94, apartado 2, de la DSP2, es la obtención del acceso a los datos personales para su posterior tratamiento y almacenamiento con el fin de prestar servicios de pago. Esto implica que el proveedor del servicio de pago aún no está tratando los datos personales, pero necesita acceder a datos de carácter personal que han sido tratados bajo la responsabilidad de cualquier otro responsable del tratamiento. Si un usuario de servicios de pago celebra un contrato, por ejemplo, con un proveedor de servicios de iniciación de pagos, este proveedor necesita obtener acceso a datos personales del usuario de servicios de pago que se están tratando bajo la responsabilidad del proveedor de servicios de pago gestor de cuentas. El objeto del consentimiento expreso en virtud del artículo 94, apartado 2, de la DSP2 es el permiso para obtener el acceso a dichos datos de carácter personal, para poder tratar y almacenar los datos necesarios para la prestación del servicio de pago. Si el interesado da su consentimiento expreso, el proveedor de servicios de pago gestor de cuentas está obligado a dar acceso a los datos personales indicados».

cialmente para ser aplicado solo en materia de servicios de iniciación de pagos y de información sobre cuentas. De la directriz se desprende que la verdadera utilidad de este apartado es la de amparar la cesión de datos por parte del proveedor de servicios de pago gestor de cuenta al proveedor de servicios de pago tercero. Es decir, en realidad, la exigencia del consentimiento expreso del usuario tiene como finalidad que el gestor de cuenta ceda los datos del usuario, que está obligado a proteger, con la seguridad de que tal cesión ha sido consentida y, de hecho, solicitada por el propio usuario⁸³. Lo cual, por otro lado, tampoco aportaría nada, en tanto la configuración legal del derecho del usuario a la utilización de proveedores terceros ya lleva implícita la base jurídica de tal cesión: el cumplimiento por parte el PSPGC del contrato con el usuario. En cualquier caso, si esta es la *ratio legis* del art. 94.2 DSP2, desde luego debe ser modificado⁸⁴ porque ahora mismo tiene un alcance mucho mayor y, además, sin una utilidad clara.

3. La transposición parcial del art. 94 DSP2 en España

En nuestro ordenamiento jurídico, el art. 94 DSP2 ha sido transpuesto en el art. 65 RDLSP, pero no de forma completa. En realidad, solo transpone el último inciso del art. 94.1 DSP2, es decir, la afirmación general y en nuestra opinión superflua de que las reglas generales de protección de datos personales son aplicables en materia de servicios de pago.

Llama la atención que el art. 65 RDLSP contenga un único párrafo pero numerado con un 1, como si debieran seguirle otros después. De hecho, en el anteproyecto de ley de servicios de pago, efectivamente había un segundo apartado del mismo tenor literal que el tan cuestionado art. 94.2 DSP2 y un tercero que transponía el primer inciso del ap. 1 del mismo artículo, relativo a la habilitación de los proveedores de servicios de pago para el tratamiento de datos personales de sus usuarios cuando sea necesario a fin de garantizar la prevención, la investigación y el descubrimiento del fraude en los pagos. Pero finalmente, el RDLSP fue aprobado con un artículo de protección de datos

⁸³ A una conclusión parecida, aunque valorando más positivamente las Directrices sobre interacción entre la PSD2 y el RGPD parece llegar, DIVISSENKO, N., «Title IV, Chapter 4...», *op. cit.*, p. 187.

⁸⁴ En general, sobre la necesidad de modificar la DSP2 en aras de la coherencia con el RGPD *vid.* AUTORIDAD BANCARIA EUROPEA, *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, EBA/Op/2022/06, 2022, p. 114. Sin embargo, en el estudio de revisión de la Segunda Directiva de servicios de pago se concluye que no es necesaria ninguna modificación (COMISIÓN EUROPEA, DIRECTORATE-GENERAL FOR FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL MARKETS UNION, BOSCH CHEN, I., FINA, D., HAUSEMER, P., ET AL., *A study on the application...*, *op. cit.*, p. 171).

que ni siquiera transpone la mitad de su homólogo europeo⁸⁵. Quizás se consideró que esos dos párrafos eliminados resultaban superfluos o irrelevantes en relación con el RGPD⁸⁶. Ciertamente, tal podría ser el caso en cuanto al tratamiento para la prevención, investigación y descubrimiento del fraude en los pagos, porque la aplicación de las reglas generales de protección de datos no presentadas interpretativas. Pero desde luego, no es el caso de la previsión del art. 94.2 DSP2.

Si la interpretación que de dicho precepto se hace en las Directrices del Comité Europeo de Pagos de 2020 es correcta —y en tanto no haya un pronunciamiento del TJUE que la modifique, así debería entenderse—, resulta que el RDLSP ha dejado de transponer un requisito de carácter contractual impuesto por la Segunda Directiva de servicios de pago que, en este extremo, es de máxima armonización. El problema es que, si se trata de una norma especial de derecho contractual, está llamada a tener efectos jurídico-privados y, entre particulares, no cabe la aplicación directa de una directiva europea.

Cosa distinta es que el art. 94.2 DSP2 pueda —y, a mi juicio, deba— ser cuestionado por no estar clara su utilidad, que urja una interpretación jurisprudencial de su significado y efectos e, idealmente, su modificación (al menos para aclararlo) en la próxima norma europea de servicios de pago.

En la práctica —al menos en la relativa a los contratos marco de servicios de pago regidos por el RDLSP—, lo habitual es que el proveedor de servicios de pago requiera el consentimiento del usuario para el tratamiento de sus datos de carácter personal. Ahora bien, la prestación del consentimiento exigido por el art. 94.2 DSP2 que no requiere el art. 65 RDLSP, dada la transposición parcial, debe tener unos requisitos diferentes a los previstos en el art. 7 RGPD, porque no se trata de lo mismo. El problema es que no está claro cuáles hayan de ser esos requisitos a nivel europeo, en tanto legislación armonizada y, desde luego, tampoco a nivel de nacional, dado que en nuestra legislación ni siquiera se contempla la exigencia del «consentimiento expreso» «contractual» para el tratamiento de los datos personales de los usuarios de servicios de pago.

Entonces, lo que tampoco está claro es a qué está consintiendo el usuario de servicios de pago cuando en un contrato regido por el RDLSP da el consentimiento al tratamiento de sus datos personales. Probablemente sea una mezcla de la exigencia del art. 94.2 DSP2 cumplida voluntariamente por los proveedores aún a falta de correcta transposición al ordenamiento español y uno de los múltiples consen-

⁸⁵ Tampoco en la LOPDgdd se prevé especificidad alguna en cuanto al tratamiento de datos personales en sede de prestación de servicios de pago.

⁸⁶ ZUNZUNEGUI, F., «Luces y sombras...», *op. cit.*, (versión digital).

timientos que puede exigir el RGPD, por ejemplo —según los casos— para el tratamiento de categorías especiales de datos o para el tratamiento ulterior con una finalidad distinta a la prestación de servicios de pago. Pero si este es el caso, ese consentimiento será contrario al art. 7.2 RGPD que exige que, en el contexto de una declaración escrita que también se refiera a otros asuntos, como puede ser la contratación de servicios de pago, la solicitud de consentimiento se presente de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.

En definitiva, tanto el art. 94.2 DSP2 como su falta de transposición en el art. 65 RDLSP generan un nivel de inseguridad jurídica que urge paliar. No puede sino concluirse que lo que se plantea en las normas de servicios de pago como una supuesta medida de tutela de los intereses del usuario, en concreto, de su privacidad, no tiene ningún efecto positivo sobre su protección. Al contrario, puede estar generando situaciones de mayor riesgo si al usuario no se le informa adecuadamente sobre qué es lo que está consintiendo o, cuando menos, puede inducir a confusión.

Por otro lado, la falta de seguridad jurídica derivada de la aparente incoherencia entre el RGPD y la Segunda Directiva de servicios de pago, así como la transposición parcial del art. 94 DSP2 al ordenamiento jurídico español, también perjudica a los proveedores de servicios de pago, a los que resulta difícil poder evaluar adecuadamente el riesgo de cumplimiento legal en este punto, en toda la UE y, en especial, en el mercado español.