AUTENTICACIÓN REFORZADA DE CLIENTE Y RESPONSABILIDAD EN LA SEGUNDA DIRECTIVA DE SERVICIOS DE PAGO

Strong customer authentication and liability in the second payment services directive

LUCÍA ALVARADO HERRERA

Profesora Titular de Derecho Mercantil. Universidad Pablo de Olavide, de Sevilla
ID orcid.org/0000-0002-9594-1983

Revista de Derecho del Sistema Financiero 5
DOI: https://doi.org/10.32029/2695-9569.01.02.2023
Marzo 2023
Págs. 69–112

RESUMEN: Una de las principales novedades que introdujo la Segunda Directiva de Servicios de Pago fue el incremento de las medidas de seguridad en la prestación de servicios de pago, que se materializó en la exigencia de la denominada autenticación reforzada de cliente para el acceso a las cuentas de pago en línea y para el inicio de operaciones de pago electrónico. Las disposiciones de la Segunda Directiva en materia de autenticación reforzada se han desarrollado a través del Reglamento delegado 2018/389, que concreta los requisitos de este procedimiento de autenticación. Destacan, entre ellos, la obligación que se impone a los proveedores de servicios de pago de disponer de mecanismos de supervisión que les permitan detectar operaciones no autorizadas o fraudulentas y el régimen de las exenciones a la exigencia de autenticación reforzada. En el presente trabajo se abordan los aspectos esenciales de la autenticación reforzada de cliente, así como sus consecuencias en materia de responsabilidad.

ABSTRACT: One of the main innovations introduced by the Second Payment Services Directive was the increase of security measures in the provision of payment services, which materialised in the requirement of the so-called strong customer authentication for access to payment accounts online and for the initiation of electronic payment transactions. The Second Directive provisions on strong authentication have been further developed through Delegated Regulation 2018/389, which specifies the requirements of this authentication procedure. These include the obligation for payment service providers to have in place monitoring mechanisms to detect unauthorised or fraudulent transactions and the regime of exemptions from the strong authentication requirement. This paper addresses the key aspects of strong customer authentication and its liability implications.

PALABRAS CLAVE: Servicios de pago – Autenticación – Autenticación reforzada de cliente – Credenciales de seguridad personalizadas – Responsabilidad.

KEYWORDS: Payment services – Authentication – Strong customer authentication – Personalised security credentials – Liability.

Fecha de recepción: 29-11-2022

Fecha de aceptación: 28-12-2022

I. INTRODUCCIÓN

Los cambios experimentados en los últimos años en los servicios de pago han provocado un aumento de los riesgos asociados a la seguridad de los pagos electrónicos. El incremento de esta modalidad de pagos (impulsado, además, por la pandemia del COVID-19), su mayor complejidad técnica y la introducción en el mercado de nuevos servicios de pago (el servicio de iniciación de pagos y el servicio de información sobre cuentas) y de nuevas entidades prestadoras de estos servicios (proveedores de servicios de pago terceros) pueden influir de forma negativa en la seguridad y fiabilidad de los pagos electrónicos. En un entorno en el que los usuarios utilizan este tipo de pagos de forma generalizada, tanto en las compras presenciales como a distancia (operaciones de comercio electrónico), se hace necesario, de un lado, establecer mecanismos que eviten que se ejecuten operaciones de pago no autorizadas por el cliente y, de otro, dotar a las operaciones de pago no autorizadas de un régimen de responsabilidad adecuado, que tenga en cuenta la diferente posición que en la relación contractual ocupan el usuario del servicio de pago y el prestador del mismo.

Una de las principales novedades introducidas por la Segunda Directiva de Servicios Pago[1] (en adelante, DSP2) es la obligación de que los proveedores de servicios de pago (en adelante, PSP) apliquen la denominada «autenticación reforzada de cliente» (en adelante, ARC[2]) a los pagos electrónicos y a otras operaciones –como el acceso a la cuenta de pago en línea–, lo que implica que se impone a los PSP una determinada forma de autenticación. En la Primera de Directiva de Servicios de Pago (en adelante, DSP1)[3], la autenticación –entendida en general como un procedimiento de validación o acreditación de algo– no había sido objeto de demasiada atención por parte del legislador, más allá de la imposición al proveedor de servicios de pago de la carga de probar que una orden de pago que el cliente negaba haber autorizado había sido correctamente autenticada. No obstante, la aparición de modalidades de fraude en las que se ejecutaban operaciones de pago correctamente autenticadas, porque terceros habían accedido de forma ilegítima a las credenciales del usuario (*phising*, *pharming*, *keylogging*, *sniffing*)[4],

1. Directiva (UE) 2015/2366, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE. La Directiva fue objeto de trasposición al ordenamiento jurídico español mediante el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en adelante, Real Decreto-ley 19/2018). Este, a su vez, fue desarrollado por el Real Decreto 736/2019, de 20 de diciembre, de régimen jurídico de los servicios de pago y de las entidades de pago y por el que se modifican el Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico, y el Real Decreto 85/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito; y por la Orden ECE/1263/2019, de 26 de diciembre, sobre transparencia de las condiciones y requisitos de información aplicables a los servicios de pago y por la que se modifica la Orden ECO/734/2004, de 11 de marzo, sobre los departamentos y servicios de atención al cliente y el defensor del cliente de las entidades financieras, y la Orden EHA/2889/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios.
2. *SCA* por sus siglas en inglés *Strong Customer Authentication*.
3. Directiva 2007/64/CE, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, que fue objeto de trasposición a nuestro ordenamiento mediante la Ley 16/2009, de 13 de noviembre, de servicios de pago.
4. Sobre el significado y contenido de estas modalidades de fraude *vid.* PÉREZ GUERRA, M., «Ciberdelitos y responsabilidad civil de las entidades financieras a la luz de la jurisprudencia», *Revista de Derecho del Mercado de Valores*, n.º 29, 2021, p. 2. El Departamento de Conducta de Entidades (DCE) del Banco de España señala, en su Memoria de Reclamaciones de 2021 (pp. 240-241), que durante el año 2021 han aumentado las reclamaciones por operaciones fraudulentas en las que se hace uso de técnicas de ingeniería social: *phising* (por correo electrónico), *vishing* (por teléfono) o *smishing* (mediante SMS). En estos casos, el defraudador suplanta la identidad de una empresa (entidad financiera, organismo público, empresa de transportes, etc.) con la finalidad de hacerse con las credenciales del usuario que permiten su autenticación. Otro tipo de fraude detectado por el DCE es el denominado SIM *swapping*, mediante el que un tercero obtiene de forma fraudulenta un duplicado de la tarjeta SIM de forma que pueden recibir los SMS con los OTP (claves de autenticación de un solo uso –*one time password*–) enviadas por el PSP. Sobre el concepto de *phising vid.* MARTÍ MIRAVALLS, J., «Banca on-line y responsabilidad por daños: Análisis crítico de la jurisprudencia

hizo que el legislador contara entre sus prioridades, de cara a la revisión de la DSP1, la de reforzar la seguridad en la prestación de los servicios de pago. Tal y como veremos, el enfoque cambia de forma sustancial con respecto a textos precedentes que se habían ocupado de la autenticación, al hilo de los avances tecnológicos producidos y de la generalización de la banca en línea. Se produce una ampliación del concepto de autenticación en un doble sentido. Primero, porque la autenticación va a aplicarse no sólo a operaciones de pago (es decir, operaciones que implican movimientos de fondos) sino también a otras actividades relacionadas con la gestión de la cuenta de pago y de los instrumentos de pago (acceso a la cuenta, cambios de PIN o de contraseñas, desbloqueo de tarjetas, etc.). Segundo, porque la autenticación se configura como un procedimiento que incluye, además de la comprobación de que la operación fue signada o marcada con las credenciales del usuario, mecanismos de supervisión que permitan detectar operaciones de pago no autorizadas o fraudulentas. Adicionalmente, la regulación en la DSP2 de los servicios de iniciación de pagos y de información sobre cuentas hacía necesario determinar cómo se aplican los procedimientos de autenticación cuando intervienen terceros proveedores y cómo se distribuye en estos casos la responsabilidad derivada de operaciones de pago o accesos a la cuenta no autorizados.

Se observa que las nuevas normas en materia de seguridad no persiguen solo la protección de los usuarios, sino que también buscan un entorno adecuado para el desarrollo del comercio electrónico (considerando 95 de la DSP2). Lo último resulta de especial interés, ya que pone de manifiesto la estrecha conexión que existe entre seguridad en los pagos y comercio electrónico: sin aquella, este no despegará. Y es que la garantía de que los usuarios queden cubiertos de forma satisfactoria en casos de operaciones fraudulentas (en atención a cómo se asignen las pérdidas por fraude) no genera por sí sola confianza en el comercio electrónico, ya que el solo hecho de que aquellas se produzcan desincentiva la contratación electrónica, ante el temor de los usuarios de ser víctimas de un fraude. Es por ello que la prevención, es decir, el establecimiento de mecanismos que permitan minimizar el riesgo de fraude, aparece como una exigencia para la consolidación del comercio electrónico. La DSP2 persigue, además, que los procedimientos de autenticación basados en la ARC estén diseñados de tal forma que proporcionen a los usuarios sistemas de fácil uso (pues, de lo contrario, podría producirse un abandono por parte de aquellos del comercio electrónico)[5] y que no impidan que los proveedores de servicios de pago terceros presten con normalidad sus servicios.

---

reciente en materia de phishing engañoso», en SÁNCHEZ CRESPO (coord.): *Fraude electrónico entidades financieras y usuarios de banca. Problemas y soluciones*, Aranzadi, 2011, pp. 219-221.

5. Como veremos más adelante, la necesidad de lograr un equilibrio entre seguridad y fácil acceso de los usuarios a los pagos electrónicos justifica que se prevean exenciones a la aplicación de la ARC.

La puesta en marcha de la ARC no ha estado exenta de dificultades, tanto técnicas (de hecho, tuvo que prorrogarse el plazo establecido inicialmente en la DSP2 para que las entidades implementaran las nuevas exigencias en materia de autenticación) como de interpretación y de aplicación. De forma particular, las exenciones legales a la aplicación de la ARC han generado dudas de interpretación entre los operadores, que han intentado solventarse mediante aclaraciones de la Autoridad Bancaria Europea (en adelante, ABE) y, recientemente, con la introducción de modificaciones en la norma que desarrolla la ARC. El devenir de la ARC estará marcado por la revisión, ya iniciada, de la DSP2. En efecto, conforme a lo previsto en el artículo 108 de la DSP2, la Comisión debía presentar como muy tarde el 13 de enero de 2021 un informe sobre su aplicación y sus repercusiones, informe al que acompañaría, en su caso, una propuesta legislativa. En septiembre del año 2020 se publicó la Comunicación de la Comisión sobre una Estrategia de Pagos Minoristas[6], que incluía la ARC entre las materias que debían ser tratadas en el proceso de revisión de la DSP2[7]. Por su parte, en octubre de 2021 la Comisión presentó a la ABE una solicitud de asesoramiento (*Call for Advice*) sobre la revisión de la DSP2, especificando aquellas materias sobre las que se pedía el pronunciamiento de la ABE[8], materias entre las que se encontraba de nuevo la ARC. Tras el requerimiento efectuado, la ABE elaboró una *Opinion* publicada en junio de 2022 [*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)*][9], que contiene además un extenso informe con comentarios y propuestas para la Comisión.

II. ANTECEDENTES

1. LA AUTENTICACIÓN EN LA GUÍA JURÍDICA DE LA CNUDMI SOBRE TRANSFERENCIAS ELECTRÓNICAS DE FONDOS

Aunque han transcurrido ya varios años desde la publicación en el año 1987 de la Guía jurídica sobre transferencias electrónicas de fondos[10] y la

6. COM (2020) 592 final, de 24 de septiembre de 2020.
7. El artículo 108 de la DSP2 hace referencia a una serie de materias que debían incluirse en el informe de la Comisión, listado no exhaustivo y que debe ser complementado, a efectos de la revisión de la DSP2, con las áreas identificadas en la Estrategia de Pagos Minoristas.
8. *Call for advice to the European Banking Authority (EBA) regarding the review of Directive (EU) 2015/2366 (PSD2)*, Ref. Ares (2021)6343649, 18 de octubre de 2021. Disponible en *https://www.eba.europa.eu/sites/default/documents/files/document_library/About%20Us/Missions%20and%20tasks/Call%20for%20Advice/2021/CfA%20on%20PSD2/1024411/EBA%20Call%20for%20advice%20final.pdf*. (consultada el 3 de octubre de 2022).
9. EBA/Op/2022/06, 23 June 2022.
10. *Guía jurídica de la CNUDMI sobre transferencias electrónicas de fondos*, Naciones Unidas, Nueva York, 1987. Disponible en *https://uncitral.un.org/sites/uncitral.un.org/*

evolución experimentada por los pagos electrónicos pudiera hacer pensar en la obsolescencia de lo recogido en ella, su lectura atenta permite encontrar aclaraciones e incluso respuestas a los problemas actuales de los pagos electrónicos y, en particular, en materia de autenticación.

La Guía jurídica define la autenticación como «la identificación de un mensaje por medios físicos, electrónicos o de otra índole que permiten al receptor determinar que el mensaje emana de la fuente indicada»[11]. De la definición expuesta pueden extraerse varias conclusiones. Primera, que la autenticación se concibe como una actividad u operación que realiza el emisor del mensaje; segunda, como se trata de una operación de pago, el mensaje que ha de autenticarse es el que contiene la orden de pago; y tercera, que la finalidad de la autenticación es que el receptor del mensaje pueda atribuirlo a quien lo emite. La función de atribución es, en nuestra opinión, la esencia del procedimiento de autenticación. La autenticación no permite verificar que la orden de pago ha sido autorizada, sino que es un procedimiento establecido para que la entidad pueda considerar válida una orden de pago[12]. En este sentido, la Guía jurídica señala que la «autenticación de un mensaje no indica necesariamente que el mensaje recibido estuviera autorizado»[13], pero «le da una forma jurídica que lo hace digno de crédito»[14].

Cuando se trata de órdenes de pago documentadas en papel, la forma normal de autenticar la orden es la estampación de la firma manuscrita del ordenante[15]. En las operaciones de pago electrónico, la firma manuscrita ha de sustituirse por otras formas o medios de autenticación que sean acordes con el formato electrónico de la orden; puede hablarse así de autenticación electrónica como aquella forma de autenticación que permite, en las operaciones de pago electrónico, autenticar las órdenes de pago emitidas precisamente en formato electrónico.

Lo peculiar de la autenticación electrónica es que, mientras la firma manuscrita es personal de un sujeto y no puede estamparse más que por él, los instrumentos de autenticación electrónica (PIN, contraseña, OTP, etc.) pueden utilizarse por personas no autorizadas[16]. Así, la firma manuscrita, o es auténtica o está falsificada; en el primer caso, la autenticación será válida y en el segundo no. Por el contrario, cuando se trata de una

files/media-documents/uncitral/es/lg_e-fundstransfer-s.pdf (consultada el 5 de mayo de 2022).

11. *Vid.* «Autenticación», en *Guía jurídica*…, cit., p. 8.
12. *Vid.* GEVA, B., *Bank Collections and payment transactions. A comparative legal analysis*, Oxford University Press, 2011, pp. 394-395.
13. *Vid.* «Autenticación», en *Guía jurídica*…, cit., p. 8.
14. *Vid. Guía jurídica*…, cit., p. 37, párrafo 26.
15. *Vid. Guía jurídica*…, cit., p. 38, párrafo 30.
16. La afirmación debe matizarse en el sentido de que determinados instrumentos de autenticación (por ejemplo, los basados en rasgos biométricos) no parecen permitir usos por terceros no autorizados.

autenticación electrónica, es posible que un tercero no autorizado tenga acceso a los instrumentos de autenticación y los aplique a una concreta orden de pago. En este caso, la autenticación será válida pero la orden de pago no puede considerarse autorizada porque el titular de los fondos no ha dado su consentimiento (autenticaciones no autorizadas). Se plantea así un problema específico de las órdenes de pago electrónicas: órdenes correctamente autenticadas, ya que se ha identificado la orden de pago con los instrumentos de autenticación acordados entre el ordenante y la entidad, pero que, al haber sido autenticadas por un tercero no autorizado, deben considerarse no autorizadas[17]. Surge entonces la cuestión, que será tratada más adelante, de cómo distribuir las pérdidas ocasionadas por la ejecución de órdenes de pago correctamente autenticadas pero que no han sido autorizadas por el titular de los fondos[18].

2. LA AUTENTICACIÓN EN LA LEY MODELO DE LA CNUDMI SOBRE TRANSFERENCIAS INTERNACIONALES DE CRÉDITO

La Ley Modelo de la CNUDMI sobre transferencias internacionales de crédito, aprobada en mayo de 1992, se elaboró para dar respuesta a la creciente electronificación de las transferencias internacionales de fondos y al aumento de las transferencias de crédito frente a las de débito. Pues bien, entre las cuestiones que aborda el texto se encuentra la de determinar los casos en los que el expedidor de una orden de pago queda obligado por ella, estableciendo un régimen jurídico para los supuestos en los que la autenticación se ha realizado por medios electrónicos.

El artículo 2.º, letra i) de la Ley Modelo define la autenticación como «un procedimiento, establecido por un acuerdo, para determinar si una orden de pago o la alteración o revocación de una orden de pago fue emitida por la persona indicada como expedidor». Comparte con la definición ofrecida por la Guía jurídica sobre transferencias electrónicas de fondos la finalidad perseguida con la autenticación: determinar el origen (la fuente) de una orden de pago, si bien los términos en que se expresa son más amplios y permite incluir dentro de la autenticación, al calificarla ya de *procedimiento*, no solo la actuación del emisor del mensaje de identificar el mensaje sino la posterior de la entidad de verificar o comprobar esa identificación. Esta idea de la autenticación como procedimiento de verificación es la que se ha plasmado, como veremos, en la DSP1 y en la DSP2.

17. Sobre esta cuestión *vid. Guía jurídica*…, cit., p. 39, párrafos 33-35. En este sentido señala GEVA (*Bank Collections*…, cit., pp. 393-394) que el concepto de operación no autorizada va ligado al acceso ilegítimo de un tercero (empleado o familiar del usuario, o un extraño) a los medios de autenticación del usuario.
18. Cobra aquí especial importancia la actuación del banco y del cliente para evitar las autenticaciones no autorizadas y la adopción de mecanismos o procedimientos por parte de la entidad para detectar autenticaciones no autorizadas.

De particular interés resulta el contenido del artículo 5.º de la Ley Modelo, ya que establece los casos en los que un expedidor de una orden de pago queda obligado por ella. Tras señalar en su apartado primero que el expedidor queda obligado por las órdenes de pago emitidas por él (es decir, por las órdenes que haya autorizado), establece en el apartado segundo el régimen aplicable a órdenes de pago no autorizadas (no emitidas por el ordenante) pero que estén sujetas a autenticación. Lo relevante del régimen previsto es que, en ciertos casos, el expedidor de una orden de pago va a quedar obligado por órdenes de pago no autorizadas por él, como excepción a la regla general de que sólo quedará obligado por aquellas operaciones de pago para las que haya dado su consentimiento (que haya autorizado). Así, el expedidor de la orden quedará obligado por la orden de pago no autorizada si: a) la operación de pago está sujeta a un procedimiento de autenticación distinto de la mera comparación de firmas; b) la autenticación constituye, dadas las circunstancias del caso, un método razonable de protección contra las órdenes de pago no autorizadas[19]; y c) el banco receptor cumple lo dispuesto en materia de autenticación. Puede decirse que la autenticación crea una apariencia de validez de la orden que permite al banco receptor actuar conforme a lo establecido en ella. Ahora bien, la atribución al expedidor de la orden de pago correctamente autenticada pero no autorizada cuenta con una importante excepción, que pivota sobre cómo se ha producido el acceso al procedimiento de autenticación. Así, el expedidor de la orden de pago no quedará obligado por la orden de pago autenticada pero no autorizada si prueba que la orden de pago la emitió una persona que no es ni ha sido empleado suyo o bien, que teniendo esa persona una relación con el expedidor, tal relación no le permitió tener acceso al procedimiento de autenticación [art. 5.º4, letras a) y b)]. Lo que determina en ambos casos la no atribución de la orden al supuesto expedidor es que el acceso al procedimiento de autenticación no pudo venir desde la esfera de control de aquél, de forma tal que el riesgo de acceso por un tercero a dicho procedimiento se hace recaer sobre el banco receptor, si bien es cierto que la imposición al expedidor de la carga de la prueba puede significar que finalmente tenga que asumir la pérdida. Ahora bien, aun cuando el expedidor logre probar alguna de las circunstancias apuntadas, sí quedará obligado por la orden de pago si el banco receptor prueba que el tercero tuvo acceso al procedimiento de autenticación por negligencia del supuesto expedidor (art. 5.º4, párrafo segundo).

19. En la autenticación realizada por medios electrónicos, es el banco el que determina el procedimiento de autenticación que debe seguirse y, en consecuencia, él debe soportar el riesgo de que se autentiquen operaciones de pago no autorizadas porque el procedimiento de autenticación no sea «comercialmente razonable» (*vid. Nota explicativa de la Secretaría de la CNUDMI sobre la Ley Modelo de la CNUDMI sobre transferencias internacionales de crédito*, apartado 25, disponible en *https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/ml-credittrans-s.pdf,* consultada el 7 de mayo de 2022). Entendemos, además, que debe ser el banco el que debe probar la razonabilidad del procedimiento de autenticación empleado.

Hasta aquí se ha analizado cómo afrontan el problema de la atribución de las órdenes de pago a su expedidor dos significativos textos de la CNUDMI. En general, el expedidor queda obligado por las órdenes de pago que haya autorizado, pero también puede quedar obligado por órdenes de pago que no haya autorizado si estas han sido autenticadas (y se cumplen, además, otras condiciones). Y es que, la autenticación genera una apariencia de validez que legitima al banco para actuar conforme a lo indicado en la orden de pago autenticada[20].

III. AUTENTICACIÓN REFORZADA DE CLIENTE

La DSP1 definía la autenticación como «un procedimiento que permita al proveedor de servicios de pago comprobar la utilización de un instrumento de pago específico, incluyendo sus características de seguridad personalizadas» (art. 4.º19 DSP1). La DSP2 amplía esta definición para abarcar también la verificación de la identidad de los usuarios de servicios de pago. Así, la autenticación se define como un «procedimiento que permita al proveedor de servicios de pago comprobar la identidad del usuario de un servicio de pago o la validez de la utilización de determinado instrumento de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario» (art. 4.º29 DSP2). Por su parte, las credenciales de seguridad personalizadas serían los «elementos personalizados que el proveedor de servicios de pago proporciona al usuario de servicios de pago a efectos de autenticación» (art. 4.º31 DSP2).

Se observa que la autenticación en la Guía jurídica de la CNUDMI sobre transferencias electrónicas de fondos y en la Ley Modelo de la CNUDMI

20. La consideración de las órdenes de pago (o de transferencia de fondos, en la terminología de la Guía jurídica sobre transferencias electrónicas de fondos) como mensajes de datos hizo que cuando se quiso afrontar en el ámbito de la CNUDMI la regulación del comercio electrónico –y en particular, la atribución de los mensajes de datos– se tomara como base el artículo 5.º de la Ley Modelo sobre transferencias internacionales de crédito [*vid. Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre comercio electrónico*, Naciones Unidas, Nueva York, 1999, p. 51, apartado 83 (disponible en *https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf,* consultada el 10 de mayo de 2022; ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, Civitas, 2019, p. 208, nota 14]. El artículo 13, apartado 1 de la Ley Modelo sobre comercio electrónico (Atribución de los mensajes de datos) establece que «(u)n mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador»; es decir, los mensajes enviados efectivamente por el iniciador se atribuyen al iniciador, de la misma forma que en el ámbito de la Ley Modelo sobre transferencias internacionales de crédito, las órdenes de pago emitidas por el expedidor provienen de él y, por tanto, resulta obligado por ellas. Ahora bien, como ocurre con las órdenes de pago electrónicas, también los mensajes de datos están expuestos a ser enviados por personas no autorizadas, planteándose el problema de si y en qué casos pueden los mensajes de datos no enviados por el supuesto iniciador atribuirse a éste (es decir, considerar legítima la actuación del destinatario que actuó sobre lo establecido en el mensaje de datos recibido), cuestión que es abordada en el artículo 13, apartados 3 a 6, de la Ley Modelo sobre comercio electrónico.

sobre transferencias internacionales de crédito no tiene como función propia la identificación de personas, ya que se circunscribe a la identificación de órdenes de pago (mensajes de texto). Lo esencial era la orden de pago y el procedimiento de autenticación como forma de determinar el origen de la orden y su atribución al expedidor. Ciertamente, la autenticación de una orden de pago y su atribución a quien la ha emitido implica de forma indirecta la identificación de quien emite la orden (si el banco recibe una orden autenticada con las credenciales asociadas a X, atribuye la orden a X e identifica a X por las credenciales que ha utilizado), pero entendemos que la función que primaba era la de la atribución de la orden al emisor.

Ahora bien, la posibilidad ofrecida por las entidades a sus clientes de operar a través de la denominada banca electrónica y, más recientemente, a través de aplicaciones móviles, hizo necesario poner el acento en la creación de una identidad digital *ad hoc* para que el cliente pudiera operar con su entidad. Así, tras la previa identificación del usuario, la entidad le facilita unas credenciales a fin de que pueda identificarse (autenticarse) cuando pretende acceder al servicio de banca electrónica o banca móvil.

Se observa, además, que la DSP2 (también la DSP1) alude a la autenticación como un *procedimiento* para que el PSP compruebe la identidad del usuario y la validez de la utilización de un instrumento de pago, y este procedimiento –atendiendo a las nuevas obligaciones de supervisión de las operaciones de pago que la DSP2 impone a los PSP– no se limita al acto de verificar que la orden de pago ha sido autenticada, en el sentido de que se ha identificado la orden de pago o se ha realizado el acceso a la cuenta utilizando las credenciales de seguridad personalizadas. El procedimiento de autenticación comprende también la aplicación de mecanismos que permitan al PSP detectar operaciones de pago no autorizadas o fraudulentas antes de ejecutarlas. Ello resulta de particular relevancia a la hora de realizar la prueba de la autenticación, pues no bastará con que el PSP pruebe que la orden de pago fue correctamente autenticada en el primer sentido aludido, sino que deberá probar, además, que contaba con mecanismos adecuados de detección de órdenes de pago no autorizadas o fraudulentas y que los aplicó.

1. LAS DIRECTRICES SOBRE LA SEGURIDAD EN LOS PAGOS POR INTERNET

La Primera Directiva de Servicios de Pago se mostró pronto insuficiente para dar respuesta a los problemas que en materia de seguridad planteaba la evolución en la prestación de los servicios de pago y, en concreto, el uso cada más frecuente de Internet para acceder a las cuentas de pago y realizar operaciones de pago electrónico de carácter remoto (bien a través de la banca electrónica –transferencias–, bien en las webs de los comerciantes o aplicaciones de pago móvil –fundamentalmente pagos con tarjetas–). Por este motivo, la ABE decidió abordar la cuestión de la seguridad en los pagos

electrónicos en Internet, iniciativa que culminó con la elaboración de unas directrices sobre la seguridad en los pagos por Internet[21]. Las Directrices tenían por finalidad establecer un conjunto de requisitos mínimos relativos a la seguridad de los pagos por Internet en el marco de lo establecido por la DSP1, contemplándose entre estos requisitos la autenticación reforzada de cliente. Ello significa que en muchos Estados miembros se aplicaba la ARC con anterioridad a la entrada en vigor de la DSP2 al amparo de lo previsto en las Directrices, si bien se constató que otros Estados no lo hacían y que el ámbito de aplicación de las Directrices se limitaba a los pagos por Internet, dejando fuera otros tipos de pagos electrónicos (presenciales y a través de apps) y otras actividades (por ejemplo, el acceso a las cuentas de pago). En el proceso de revisión de la DSP1 se evidenció que eran necesarias nuevas normas que tuvieran en cuenta los avances tecnológicos producidos desde la publicación de las Directrices, la regulación de nuevos servicios de pago en la futura DSP2 y los riesgos asociados a los pagos electrónicos en general y a actividades conexas.

En este contexto, la DSP2 encomendó a la ABE la elaboración de proyectos de normas técnicas de regulación (NTR)[22] sobre la ARC (requisitos de la ARC, exenciones de su aplicación, requisitos de las medidas de seguridad para proteger la confidencialidad y la integridad de las credenciales de seguridad personalizadas de los usuarios de servicios de pago) y los requisitos para unos estándares de comunicación abiertos comunes y seguros (art. 98.1 DSP2)[23] y facultó a la Comisión para adoptar actos delegados basados

21. *Directrices definitivas sobre la seguridad en los pagos por Internet*, 19 de diciembre 2014 (disponibles en *https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1004450/44d07cf8-1721-4407-94a6-3a8c256149fa/EBA-GL-2014-12_ES_rev1%20GL%20on%20Internet%20Payments.pdf,* consultada el 15 de mayo de 2022). Las Directrices están basadas en las recomendaciones del Foro sobre Seguridad de los Pagos Minoristas (*Secure Pay*). La Comisión Ejecutiva del Banco de España las adoptó como propias en sesión de 24 de marzo de 2015.
22. *RTS*, por sus siglas en inglés *Regulatory Technical Standards*.
23. La ABE, en la elaboración de las NTR, debía tener presente los objetivos y condiciones marcados por la DSP2 en el apartado segundo del artículo 98: garantizar un nivel adecuado de seguridad para los usuarios de servicios de pago y los proveedores de servicios de pago; garantizar la protección de los fondos y los datos personales de los usuarios de servicios de pago; asegurar y mantener una competencia justa entre todos los proveedores de servicios de pago; garantizar la neutralidad tecnológica y del modelo de negocio; y permitir el desarrollo de medios de pago accesibles, de fácil uso e innovadores. El mandato no está exento de dificultades, ya que los aspectos señalados son en ocasiones contrapuestos (por ejemplo, un mayor nivel de seguridad implica en muchas ocasiones una menor «usabilidad» del instrumento de pago).

    Sobre el proceso de elaboración de las normas técnicas de regulación pueden consultarse los siguientes documentos de la ABE: *Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2*), EBA/DP/2015/03, 8 December 2015 (disponible en *https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1303936/13129941-7581-4473-a767-52ec002bd00a/EBA-DP-2015-03%20%28RTS%20on%20SCA%20and%20CSC%20under%20PSD2%29*.

en dichas normas (art. 98.4 DSP2), lo que se tradujo en la aprobación del Reglamento delegado 2018/389, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros[24] (en adelante, Reglamento delegado). El 14 de octubre de 2021, la ABE derogó las Directrices sobre la seguridad en los pagos por Internet, que de *facto* habían sido reemplazadas por la DSP2 y por el Reglamento delegado[25].

---

pdf?retry=1, consultada el 3 de junio de 2022); *Consultation Paper on the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2*, EBA-CP-2016-11, 12 August 2016 (disponible en *https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1548183/679054cf-474d-443c-9ca6-c60d56246bd1/Consultation%20Paper%20on%20draft%20RTS%20on%20SCA%20and%20CSC%20%28EBA-CP-2016-11%29.pdf?retry=1,* consultada el 3 de junio de 2022); *Final Report. Draft Regulatory Technical Standards on Strong Customer Authenticantion and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)*, EBA/RTS/2017/02, 23 February 2017 (disponible en *https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf?retry=1*, consultada el 3 de junio de 2022).

En relación con la seguridad de los pagos electrónicos, la DSP2 encomendó además a la ABE la elaboración de Directrices sobre el establecimiento, la aplicación y la supervisión de las medidas de seguridad (art. 95 DSP2) y sobre clasificación, notificación y evaluación de incidentes (art. 96 DSP2). En cumplimiento de este mandato, la ABE ha elaborado los siguientes documentos, de los que se citan las versiones más recientes: *Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad*, ABE/GL/2019/04, 28 noviembre 2019 (disponible en *https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2*, consultada el 4 de junio de 2022) y *Directrices revisadas sobre la notificación de incidentes graves de conformidad con la Directiva de servicios de pago (PSD2)*, ABE/GL/2021/03, 10 de junio de 2021 (disponible en *https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2*, consultada el 4 de junio de 2022).

24. DOUE L 69, de 13 de marzo de 2018. La fecha inicialmente prevista para su aplicación era el 14 de septiembre de 2019 (art. 38 Reglamento delegado) si bien, ante la falta de preparación del sector, la ABE permitió que las autoridades nacionales competentes otorgaran un tiempo adicional limitado al 31 de diciembre de 2021. *Vid.* CANO PELÁEZ, J. y MONTOLIO CALEAGA, A., «El nuevo régimen jurídico de servicios de pago», en ORTEGA BURGOS (dir.): *Mercados regulados*, Tirant lo Blanch, 2021, p. 94; Nota informativa del Banco de España, de 18 de octubre de 2019, sobre el plazo y procedimiento para completar la migración a la aplicación de la autenticación reforzada del cliente (SCA) en los pagos de comercio electrónico basados en tarjetas (disponible en *https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/Briefing_notes/es/notabe181019.pdf*; consultada el 10 de enero de 2022).
25. La Comisión Europea ha aprobado un nuevo Reglamento delegado por la que se modifica el Reglamento delegado 2018/389. El análisis de las modificaciones que se introducen se realizará con ocasión del estudio de las exenciones a la aplicación de la ARC (epígrafe III. 6.1.).

2. DEFINICIÓN Y ELEMENTOS DE AUTENTICACIÓN

La DSP2 define la ARC como «la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), que son independientes –es decir, que la vulneración de uno no compromete la fiabilidad de los demás–, y concebida de manera que se proteja la confidencialidad de los datos de autenticación» (art. 4.º30)[26]. La ARC se diferencia del procedimiento ordinario de autenticación por la obligación de utilizar más de un factor de autenticación[27]. Además, los elementos de autenticación deben pertenecer al menos a dos categorías distintas[28] y la aplicación de la ARC tendrá como resultado la generación de un código de autenticación[29]. Toda autenticación que no cumpla con los requisitos señalados no será ARC, pero podrá ser un medio válido de autenticación para aquellas operaciones (de pago o no) en las que no se exija la ARC, bien porque no se contemplen en el artículo 97 de la DSP2 (que recoge las operaciones en las que deberá aplicarse la ARC), bien porque estando incluidas el PSP aplique una exención.

Entre los elementos que implican conocimiento se incluyen las contraseñas, PIN (*Personal Identification Number*, por sus siglas en inglés),

---

26. La definición ofrecida en la DSP2 coincide prácticamente con la establecida en las *Directrices definitivas sobre la seguridad en los pagos por Internet* (p. 6, apartado 12), si bien estas, con una finalidad didáctica, ofrecen ejemplos de las distintas categorías de elementos. El artículo 3.º5 del Real Decreto-ley 19/2018 reproduce el contenido del apartado 30 del artículo 4.º de la DSP2, con la salvedad de que al final del precepto emplea la expresión «datos de identificación» en lugar de «datos de autenticación». Señala al respecto ALAMILLO DOMINGO [«Autenticación reforzada y aseguramiento de la identidad del consumidor», en CUENA CASAS – IBÁÑEZ JIMÉNEZ (dirs.): *Perspectiva legal y económica del fenómeno FinTech*, Wolters Kluwer, 2021, p. 696] que la expresión «datos de identificación» es coherente con el procedimiento de identificación previsto en el Reglamento eIDAS, del que la autenticación es una parte.
27. *Cfr.* ALAMILLO DOMINGO, I., «Autenticación reforzada…», cit., p. 696.
28. La ABE ha señalado que es necesario que los dos factores pertenezcan a categorías distintas. Si se utilizan más de dos elementos de autenticación, la exigencia mencionada se traduce en que al menos dos de los elementos de autenticación empleados deben pertenecer a categorías diferentes (*vid. Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, EBA/OP/2018/4, 13 June 2018, p. 7, apartados 33 y 34, disponible en *https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf?retry=1*, consultada el 2 de marzo de 2022).
29. Art. 4.º del Reglamento delegado. Señala al respecto ALAMILLO DOMINGO («Autenticación reforzada…», cit., p. 701) que este código, cuya exigencia no aparece en la definición de ARC de la DSP2, es el elemento que acredita que la ARC se ha producido. Sobre los requisitos que debe reunir el código de autenticación *vid.*, más ampliamente, el contenido del artículo 4.º del Reglamento delegado y las observaciones de ALAMILLO DOMINGO, cit., pp. 701-702. Sobre la independencia de los elementos de autenticación, y en especial sobre la utilización de dispositivos polivalentes, *vid.* artículo 9.º del Reglamento delegado.

preguntas basadas en conocimiento, frases de contraseña, patrones (por ejemplo, la memorización por el usuario del trazo de deslizamiento)[30]. Dado que el conocimiento es definido como algo que «solo» conoce el usuario, el número de la tarjeta, el código de verificación (CVV) y la fecha de caducidad impresos en una tarjeta física no constituyen conocimiento, ya que no son datos que únicamente conoce el usuario[31]. Lo mismo puede aplicarse a los nombres de usuario y a los correos electrónicos. Son, por tanto, elementos que no pueden integrar una ARC.

Por lo que respecta a los elementos de autenticación que implican posesión, la ABE ha realizado dos matizaciones relevantes: primero, la posesión puede ser tanto de elementos físicos (como un teléfono móvil, una tableta, un *token* o *wereables* –relojes, pulseras–) como de otros que no lo son (por ejemplo, una *app*, un navegador web); y, segundo, en ambos casos es necesaria una evidencia de la posesión, es decir, que deben arbitrarse mecanismos que garanticen que quien posee el dispositivo (físico o no) es el usuario autorizado y no un tercero. Esta evidencia de la posesión puede obtenerse mediante una contraseña de un solo uso (OTP) generada o recibida en el dispositivo, un SMS[32], una notificación *push*, una firma electrónica, un código de respuesta rápida (QR) o los códigos de seguridad dinámicos de una tarjeta[33].

La inherencia[34] comprende tanto la biometría biológica (huella dactilar, iris, retina, voz, venas) como la biometría de comportamiento (dinámica de pulsación de teclas, frecuencia cardíaca)[35] y requiere de dispositivos o softwares que permitan su lectura.

30. *Vid.* ABE, *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, EBA/OP/2019/06, 21 June 2019, p. 8, apartado 32. Disponible en *https://www.eba.europa.eu/sites/default/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf,* consultada el 2 de marzo de 2002.
31. *Vid.* ABE, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., p. 7, apartado 35.
32. En el caso de los SMS, la ABE ha aclarado que el elemento de posesión no es el SMS, sino la tarjeta SIM asociada al número de teléfono (*vid. Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, cit., p. 6, apartado 25).
33. Las tarjetas de coordenadas no son elemento ni de conocimiento ni de posesión. Resulta de gran utilidad la consulta de la tabla elaborada por la ABE en la que se incluye un listado no exhaustivo de elementos que pueden integrar las tres categorías (conocimiento, posesión e inherencia). La ABE advierte que la tabla se ha realizado teniendo en cuenta la realidad de la práctica existente en el mercado en el momento de la elaboración de la *Opinion*, por lo que no descarta que en futuro puedan incorporarse nuevos elementos en atención al desarrollo de aquél (*vid. Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, cit., p. 7).
34. Según la ABE, la inherencia se refiere a propiedades físicas de partes del cuerpo, características fisiológicas y procesos de comportamiento creados por el cuerpo, y cualquier combinación de estos (*vid. Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, cit., p. 4, apartado 18).
35. *Vid.* ABE, *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, cit., p. 5, apartado 19. En el apartado 20 aclara que la

3. OPERACIONES SUJETAS

Frente a la libertad de forma de la autenticación prevista en la DSP1 –matizada por la recomendación de aplicar la ARC al amparo de las *Directrices definitivas sobre la seguridad de los pagos por Internet*–, la DSP2 impone a los PSP una determinada forma de autenticar al usuario y a las operaciones de pago –mediante ARC– en determinados casos: cuando el ordenante accede a su cuenta de pago en línea, inicia una operación de pago electrónico o realiza por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos (art. 97.1 DSP2). Debe señalarse que, de conformidad con lo previsto en el artículo 61 de la DSP2, la obligación de aplicar la ARC no está reservada para aquellos casos en los que el ordenante sea un consumidor[36], sino que se extiende a todos los usuarios de servicios de pago (entendiendo por usuario de servicios de pago la persona física o jurídica que utiliza un servicio de pago, ya sea como ordenante, beneficiario o ambos –art. 4.º10 DSP2–)[37].

Por lo que se refiere al acceso a la cuenta de pago en línea [art. 97.1.a) DSP2][38], la obligación de aplicar la ARC existe tanto si es el usuario quien accede directamente a su cuenta como si el acceso se realiza a través de un proveedor de servicios de pago tercero: el proveedor de servicios de información sobre cuentas. En cuanto al inicio de una operación de pago electrónico [art. 97.1.b) DSP2][39], deben incluirse las operaciones de pago

---

memorización del trazo de deslizamiento no constituye un elemento de inherencia sino de conocimiento (algo que solo el usuario conoce).

36. Por consumidor se entiende la «persona física que, en los contratos de servicios de pago objeto de la presente Directiva, actúa con fines ajenos a su actividad económica, comercial o profesional» (art. 4.º 20 DSP2). Se observa, además, que aun cuando el artículo 97 emplea el término «ordenante», serías más apropiado utilizar la palabra «usuario», ya que cuando se accede a una cuenta de pago no se está dando ninguna orden de pago.
37. El artículo 61 de la DSP2 permite que cuando el usuario no tenga la condición de consumidor, las partes (usuario y PSP) puedan acordar que no se apliquen determinados preceptos del Título IV (Derechos y obligaciones en materia de prestación y utilización de servicios de pago), no encontrándose entre los artículos disponibles los relativos a la ARC (arts. 97 y 98). No obstante, sí se incluyen los artículos 71 (notificación de operaciones no autorizadas), 72 (prueba de la autenticación) y 74 (responsabilidad del ordenante en caso de operaciones no autorizadas) que, como veremos, tienen relevancia en la responsabilidad que se deriva de autenticaciones no autorizadas. El artículo 61 DSP2 permite a los Estados miembros que en sus normas de transposición establezcan que las disposiciones del Título IV se apliquen a las microempresas (personas físicas profesionales o empresarios y personas jurídicas de muy pequeña dimensión) de la misma forma que a los consumidores, facultad de la que ha hecho uso el Real Decreto-ley 19/2018 (art. 34). Sobre el concepto de microempresa *vid.* artículo 3.º 25 del Real Decreto-ley 19/2018.
38. Se trata de supuestos en los que el usuario accede a su cuenta a través de un dispositivo: ordenador, móvil, tarjeta, cajero automático, etc. (*vid.* ABE, *Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication*…, cit., p. 12, apartado 27.i).
39. La DSP2 no define qué es una «operación de pago electrónico», lo que puede dificultar la concreción de las operaciones incluidas en el ámbito del artículo 97.1.b)

iniciadas por el ordenante (transferencias de crédito)[40] o por el ordenante a través del beneficiario (pagos con tarjeta). Y ello tanto si el medio de pago utilizado es dinero bancario como si trata de dinero electrónico[41] (salvo, en este último caso, cuando se trate de un instrumento de dinero electrónico de carácter anónimo)[42]. Las operaciones de pago electrónico comprenden también las transferencias iniciadas por el ordenante a través de un proveedor de servicios de pago tercero: el proveedor de servicios de iniciación de pagos. El apartado segundo del artículo 97 establece un requisito adicional cuando la operación de pago electrónico sea remota, entendiendo por «operación remota de pago» la que se realiza a través de Internet o por un dispositivo que pueda utilizarse para la comunicación a distancia (art. 4.º6 DSP2), es decir, sin la presencia física simultánea del PSP y del usuario[43]. Pues bien, en estos casos, la ARC debe incluir elementos que asocien dinámicamente la operación de pago a un importe y a un beneficiario determinados[44]. Por último, los PSP están obligados a aplicar la ARC a las operaciones realizadas por el usuario a través de un canal remoto que no

DSP2. La ABE entiende que, de cara a la revisión de la DSP2, y teniendo en cuenta que la definición de lo que se considera una operación de pago electrónico puede ser compleja, propone modificar la redacción del artículo 97.1.b), de forma que se aplique a los casos en que el ordenante inicie una operación de pago (se suprimiría «electrónico») y que se especifique qué operaciones de pago no están sujetas a la ARC (*vid. Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366*…, cit., pp. 14-15, apartado 1.7).

40. Si la transferencia se realiza una vez que el usuario ha accedido a su cuenta de pago en línea –aplicando la ARC– se plantea la cuestión si para iniciarla sería necesaria una nueva ARC o bastaría con la ARC que dio acceso a la cuenta de pago. La ABE considera que debe exigirse una nueva ARC para la transferencia, salvo que se aplique alguna de las exenciones previstas en el Reglamento delegado (*Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., p. 8, apartado 36).
41. *Vid.* ABE, *Final Report. Draft Regulatory Technical Standards on Strong Customer Authenticantion*…, cit., p. 7, apartado 13.
42. *Vid.* considerando 8 del Reglamento delegado.
43. El artículo 4.º34 de la DSP2 define un medio de comunicación a distancia como «cualquier medio que, sin la presencia física simultánea del proveedor de servicios de pago y del usuario de servicios de pago, pueda emplearse para la celebración de un contrato de servicios de pago». De aquí puede desprenderse que el carácter remoto de la operación se refiere a la ausencia de presencia física simultánea de las partes en la operación. Por ello, los pagos *contactless* en un punto de venta físico no serán remotos, aun cuando el dispositivo (por ejemplo, el móvil) puede utilizarse para la comunicación a distancia, porque en el caso concreto existe esa presencia física simultánea de las partes. No obstante, la ABE considera que la DSP2 no es clara al respecto y propone introducir modificaciones en la definición de operación remota de pago (*vid. Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366*…, cit., pp. 16-17, apartados 51-57).
44. *Vid.* considerando 95 de la DSP2. Los requisitos de la vinculación dinámica se desarrollan en el artículo 5.º del Reglamento delegado. Sobre las conexiones entre esta vinculación dinámica y las exigencias legales de la firma electrónica avanzada del Reglamento eIDAS *vid.* ALAMILLO DOMINGO, I., «Autenticación reforzada…», cit., p. 703.

constituyen una operación de pago (en cuanto que no originan movimientos de fondos) pero que pueden entrañar riesgo de fraude en el pago u otros abusos [art. 97.1.c) DSP2]. Entre estas operaciones habrían de incluirse los cambios de contraseña de acceso a la banca en línea, el cambio del PIN de la tarjeta, el registro de los datos de tarjetas en una solución de monedero electrónico, la creación de listas blancas que exoneren de la aplicación de la ARC, la activación o desactivación de funcionalidades de pago, etc.[45]. Por lo que respecta a las domiciliaciones, estas quedan fuera del supuesto contemplado en el artículo 97.1.b) DSP2, ya que no se trata de una operación de pago iniciada por el ordenante. Ahora bien, sí encajarían en el artículo 97.1.c) las *órdenes* de domiciliación cursadas electrónicamente por el ordenante, por lo que aquellas deben realizarse utilizando la ARC[46].

El PSP, en los casos señalados y salvo que pueda hacer uso de alguna exención, está obligado a aplicar la ARC. Ello ha supuesto un enorme esfuerzo de adaptación de quienes intervienen en la cadena de pago, pero se facilita la prueba de la autenticación, en la medida en que el PSP, cuando aplique la ARC, no tendrá que probar que el procedimiento de autenticación es adecuado ya que se presume que la ARC lo es.

4. ENTIDAD OBLIGADA

El proveedor de servicios de pago que debe aplicar la ARC es el PSP del usuario que accede a la cuenta de pago o que inicia la orden de pago; es decir, el PSP que emite las credenciales de seguridad personalizadas. En el ámbito de los servicios de iniciación de pagos (SIP) y de los servicios de información sobre cuentas (SIC) son los proveedores de servicios de pago gestores de cuenta (PSPGC) los que emiten estas credenciales y, por tanto, los que tienen la obligación de aplicar la ARC. Los PSP pueden acordar con terceros (proveedores de servicios de *wallet*, proveedores de servicios de iniciación de pagos –PSIP– y proveedores de servicios de información sobre cuentas –PSIC–), que sean estos y no el PSP (PSPGC en el caso de servicios de iniciación de pagos y de información sobre cuentas) quienes realicen la autenticación en nombre del PSP o del PSPGC, y que entre ellos acuerden el sistema de responsabilidad[47]. En estos casos de delegación de la ARC, el PSP del ordenante y/o titular de la cuenta (PSPGC, en caso de servicios de iniciación de pagos o de información sobre cuentas) sigue siendo responsable frente a este (por operaciones no autorizadas en las que no se exigió la ARC), pero podrá repetir la pérdida de los terceros (proveedores de servicios de *wallet*, PSIP o PSIC), si así lo han acordado.

45. *Vid.* ABE, *Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication*…, cit., p. 12, apartado 27.iii.
46. *Vid.* ABE, *Consultation Paper on the draft Regulatory Technical Standards specifying the requirements on strong customer authentication*…, cit., p. 9, apartado 18.
47. *Vid.* ABE, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., p. 8, apartado 38.

5. LOS MECANISMOS DE SUPERVISIÓN DE OPERACIONES DE PAGO NO AUTORIZADAS O FRAUDULENTAS

Como se ha señalado, en el procedimiento de autenticación existe el riesgo de que se produzcan autenticaciones no autorizadas porque un tercero acceda a las credenciales de seguridad del usuario y las utilice para acceder a la cuenta o expedir órdenes de pago. Es por ello que el procedimiento de autenticación debe incluir mecanismos de supervisión que permitan detectar estas autenticaciones no autorizadas[48]. La cuestión es relevante, en la medida en que la diligencia del PSP se valorará teniendo en cuenta no sólo si verificó el uso de los elementos de autenticación acordados para el acceso a la cuenta o para emitir la orden de pago sino, además, si contaba con mecanismos de supervisión adecuados y si, en el caso concreto, aplicó dichos mecanismos. Pues bien, el artículo 2.º del Reglamento delegado, bajo el título «Requisitos generales de autenticación», se ocupa de esta cuestión, señalando que los PSP «dispondrán de mecanismos de supervisión de las operaciones que les permitan detectar operaciones de pago no autorizadas o fraudulentas». La redacción del precepto puede crear confusión acerca de si los PSP tienen que contar o no con mecanismos de supervisión para los accesos a las cuentas, ya que el acceso, no es, en puridad una operación de pago. Pues bien, la ABE ha interpretado –de una forma un tanto forzada, a nuestro entender– que el acceso a las cuentas queda incluido en el ámbito de aplicación del artículo 2.º[49]. Y decimos forzada no porque no sea adecuado que los mecanismos de supervisión contemplen también los accesos fraudulentos o no autorizados a las cuentas de pago –que es lo es–, sino porque por mucho que se quiera, la acción de acceder a una cuenta no es una operación de pago.

El Reglamento delegado dispone que los mecanismos de supervisión han de basarse en el análisis de las operaciones de pago o de los accesos de la cuenta sobre la base de un uso normal de las credenciales de seguridad personalizadas y que deberán tener en cuenta los siguientes factores de riesgo: listas de elementos de autenticación comprometidos o sustraídos; el importe de cada operación de pago; supuestos de fraude conocidos en

48. En el considerado primero del Reglamento delegado se dice expresamente que «(e)l procedimiento de autenticación debe incluir, en general, mecanismos de supervisión de las operaciones para detectar los intentos de utilizar las credenciales de seguridad personalizadas del usuario de servicios de pago que hayan sido objeto de extravío, robo o apropiación indebida».

49. *Vid.* ABE, *Final Report. Draft Regulatory Technical Standars amending the Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliamente and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication*, EBA/RTS/2022/03, 5 April 2022, pp. 54-55, response 26. Disponible en *https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2022/EBA-RTS-2022-03%20RTS%20on%20SCA%26CSC/1029858/Final%20Report%20on%20the%20amendment%20of%20the%20RTS%20on%20SCA%26CSC.pdf*., consultada el 30 de abril de 2022.

la prestación de servicios de pago[50]; señales de infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación; y, 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 (art. 2.º2 Reglamento delegado).

6. EXENCIONES DE APLICACIÓN

Con la finalidad de que los PSP ofrezcan a los usuarios servicios de pago de fácil uso e innovadores, la DSP2 admite que en determinados casos los PSP puedan dejar de aplicar la ARC (considerando 96). Así, dispone [art. 98.1.b)] que las normas técnicas de regulación deben establecer las exenciones a la aplicación de la ARC atendiendo a los siguientes factores: el nivel de riesgo del servicio de pago, el importe o la frecuencia de la operación –o ambas–, y el canal de pago utilizado (art. 98.3). El Reglamento delegado se ocupa de estas exenciones en el Capítulo III (arts. 10 a 21), donde se concretan los supuestos en los que los PSP podrán no aplicar la ARC: información de cuentas de pago (art. 10); pagos sin contacto en el punto de venta (art. 11); terminales no atendidas para tarifas de transporte o pagos de aparcamiento (art. 12); beneficiarios de confianza (art. 13); operaciones frecuentes (art. 14); transferencias de crédito entre cuentas mantenidas por la misma persona física o jurídica (art. 15); operaciones de escasa cuantía (art. 16); pagos corporativos seguros (art. 17); y operaciones remotas de pago electrónico de bajo riesgo (art. 18). Es posible que una misma operación puede encajar en más de una exención de las señaladas; en este caso, el PSP debe elegir, si desea hacer uso de una exención, cuál de ellas aplica[51].

Debe ponerse el acento en que no se trata de casos en que la norma exonera de cumplir con la ARC, sino de supuestos en los que los PSP podrán, si lo desean, no aplicarla[52]. El carácter voluntario de las exenciones se justifica en el hecho de que cuando el PSP no aplica la ARC haciendo uso de una exención, asumirá la pérdida ocasionada por la ejecución de una operación no autorizada salvo que el ordenante haya actuado de forma fraudulenta, por excepción al régimen general en materia de operaciones no autorizadas en el que el usuario responde, además de en los casos de

50. Este elemento es importante, ya que permite afirmar que los PSP deberán adoptar medidas de prevención ante los supuestos de fraude conocidos, lo que les exige estar actualizados e ir adaptando dichas medidas ante la aparición de nuevas modalidades de fraude.
51. *Vid.* ABE, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., p. 9, apartado 41.
52. Como se verá seguidamente, el Reglamento delegado se ha modificado recientemente, de forma que en ciertos casos será obligatorio no aplicar la ARC (es decir, será obligatorio para los PSP aplicar la exención).

actuación fraudulenta, si incurrió en negligencia grave o dolo en el cumplimiento de sus obligaciones (art. 74 1 y 2 DSP2)[53].

El PSP facultado para aplicar la exención es el PSP del ordenante, entendiendo por tal el titular de la cuenta a la que se accede en línea o el ordenante del pago electrónico. Como excepción a lo apuntado, el PSP del beneficiario[54] podrá aplicar la exención en alguno de los siguientes casos de pagos con tarjeta: pagos sin contacto en el punto de venta (art. 11); pagos en terminales no atendidas para tarifas de transporte o pagos de aparcamiento (art. 12); operaciones frecuentes (art. 14); pagos remotos de escasa cuantía (art. 16); y pago remotos de bajo riesgo (art. 18)[55]. Ahora bien, en todos los casos señalados, la decisión última sobre aplicar o no la exención recae en el PSP del ordenante; es decir, que aun cuando el PSP del beneficiario aplique una exención, siempre el PSP del ordenante podrá exigir la ARC para ejecutar la operación de pago (si es técnicamente posible) o rechazar el inicio de la operación de pago[56]. Ahora bien, si el PSP del ordenante decide autorizar la operación de pago sin ARC porque el PSP del beneficiario aplicó la exención, el PSP del beneficiario será responsable de la posible pérdida frente al PSP del ordenante, si bien este seguirá siendo responsable frente a su ordenante en los términos establecidos en el artículo 74.2 DSP2[57]. Cuando interviene un PSP tercero (PSIC o PSIC), la facultad de aplicar o no la exención sigue siendo del PSPGC, ya que él es el responsable del proceso de autenticación y ese proceso incluye la decisión de aplicar o no la exención[58].

Una de las cuestiones que suscita el régimen de las exenciones es si el PSP que se acoge a una de ellas y no aplica la ARC debe, sin embargo, seguir algún proceso de autenticación. El supuesto sería comparable a aquellos casos en los que la DSP2 no exige la ARC, es decir, casos distintos a los señalados en el artículo 97.1 DSP2. Pues bien, fuera de los supuestos en los que se exige la ARC, la DSP2 no establece de forma expresa la

53. Sobre esta cuestión *vid.*, más ampliamente, el epígrafe IV.4.
54. La decisión sobre aplicar o no la ARC no puede recaer nunca en el beneficiario (*vid.* ABE, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., p. 8, apartado 40).
55. *Vid. Table 2. Summary table on who may apply an exemption*, en ABE, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., p. 9.
56. *Vid.* ABE, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., p. 9.
57. *Vid.* ABE, Q&A 2018_4042 (disponible en *https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4042;* consultada el 2 de febrero de 2022). La ABE entiende que el supuesto planteado requiere ser clarificado en la revisión de la DSP2, en los términos señalados en el Q&A 4042 (*vid. Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366*…, cit., p. 67).
58. *Vid.* ABE, *Final Report. Draft Regulatory Technical Standards on Strong Customer Authenticantion*…, *cit*., p. 75, cuestión 54; ABE, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., p. 8, apartado 39.

obligación del PSP de autenticar al usuario o la orden de pago, quizás porque entiende que es bastante improbable que un PSP ejecute una operación de pago o permita un acceso a la cuenta antes comprobar que el usuario está legitimado para acceder o que la orden es emitida por el titular de la cuenta[59]. Además, la DSP2 impone al PSP la prueba de la autenticación, y ello para todos los supuestos en los que el usuario niegue haber autorizado una orden de pago. Esta exigencia probatoria no se limita a los supuestos en los que la DSP2 impone la aplicación de la ARC, de lo que puede deducirse que, a efectos de responsabilidad, el PSP, por su propio interés, contará siempre con procedimientos de autenticación del usuario y/o de las órdenes de pago que este emita[60].

La aplicación concreta de una exención por parte del PSP se encuentra condicionada a que la operación (de pago o de acceso a la cuenta) haya pasado el filtro de los mecanismos de supervisión de los que debe disponer el PSP, conforme a lo previsto en el artículo 2.º del Reglamento delegado. Ello se desprende del contenido de los preceptos que regulan las exenciones (casi todos ellos establecen que el PSP tendrá la posibilidad de no aplicar la ARC «siempre que se cumplan los requisitos establecidos en el artículo 2.º», lo que significa que, aun cuando la operación concreta encaje en alguno de los supuestos de exención previstos, el PSP no podrá hacer uso de ella si, tras aplicar los mecanismos de supervisión, existe el riesgo de que la operación sea fraudulenta o no esté autorizada.

6.1. Acceso a la cuenta de pago en línea

Como se ha señalado, la DSP2 exige la aplicación de la ARC cuando el usuario accede a su cuenta de pago en línea [art. 97.1.a) DSP2], y esto tanto si el acceso se produce de forma directa como si se hace indirectamente, a través de un PSIC. La exención recogida en el artículo 10 del Reglamento delegado bajo el título «Información de cuentas de pago», prevista para ambos tipos de acceso, consiste en que el PSP (PSPGC, en el caso de acceso indirecto por prestación del servicio de información sobre cuentas) podrá no aplicar la ARC cuando la información a la que se tiene acceso es limitada: el saldo de la cuenta [art. 10.1.a)] u operaciones de pago ejecutadas en los últimos 90 días [art. 10.1.b)].

Esta exención simplifica la consulta por parte del usuario del saldo de su cuenta o de la información reciente de la misma sobre operaciones de pago realizadas, ya que de otra forma tendría que autenticarse mediante ARC cada que vez que accediera a la cuenta (lo que puede ser bastante

59. Esta cuestión será tratada más ampliamente en el epígrafe IV.2.
60. En este sentido, la ABE ha indicado que la ausencia de ARC no es sinónimo de una falta absoluta de autenticación y que se considera que el PSP aplicará alguna forma de autenticación (*vid.* ABE, *Final Report. Draft Regulatory Technical Standards on Strong Customer Authenticantion*…, cit., p. 80, cuestión 64).

frecuente). Pero más relevante aún –y este parece ser el motivo principal por el que se estableció esta exención– es que, sin ella, se dificultaría la prestación del servicio de información sobre cuentas[61].

Ahora bien, aun en estos casos en los que el acceso a la cuenta va a permitir «visualizar» sólo la información apuntada, los PSP tendrán que aplicar la ARC en dos casos: la primera vez que el usuario accede en línea a su cuenta de pago (tanto si es para la consulta de saldo como para las operaciones recientes) y cuando hayan transcurrido más de 90 días desde que el PSP aplicó la ARC (sólo para consulta de operaciones recientes). Por tanto, si el acceso es únicamente para obtener información sobre el saldo bastará una única ARC[62]. Si, además de, o en lugar del saldo, se accede a información sobre operaciones de pago, habrá que aplicar la ARC: a) siempre, si el usuario puede acceder a información sobre operaciones de pago realizadas en un plazo superior a 90 días; b) cuando hayan transcurrido 90 días desde la última ARC, si la información se refiere a operaciones realizadas en un plazo inferior a 90 días[63].

La exención prevista en el artículo 10 del Reglamento delegado ha provocado, en el ámbito de la prestación del servicio de información sobre cuentas, diversas disfunciones debido a la falta de uniformidad en su aplicación. Y es que, al configurarse la exención como una facultad y no como una obligación, existen PSPGC que no la han aplicado (es decir, exigen la

61. Precisamente, los problemas que la aplicación de la exención ha provocado en el servicio de información sobre cuentas evidenció la necesidad de introducir modificaciones en la misma, que se han plasmado en la reciente reforma del artículo 10 del Reglamento delegado, de la que se tratará en las próximas líneas.

62. Esta es la interpretación que cabe realizar del apartado segundo del artículo 10, ya que dice literalmente que «los proveedores de servicios de pago no estarán exentos de la aplicación de la autenticación reforzada de clientes cuando se cumpla alguna de las siguientes condiciones: a) que el usuario de servicios de pago esté accediendo en línea a la información especificada en el apartado 1 por primera vez; b) que hayan transcurrido más de 90 días desde la última vez que el usuario de servicios de pago accediera en línea a la información especificada en el apartado 1, letra b), y se aplicara la autenticación reforzada de clientes». No obstante, la intención era la de exigir la renovación de la ARC cada 90 días también cuando el acceso a la cuenta es sólo para la consulta del saldo, lo que ha llevado, como se indicará más adelante, a modificar la redacción del precepto. Cuando en algún momento de esos 90 días el usuario se autentique mediante ARC –por ejemplo, porque un acceso a la cuenta en principio exento presenta riesgo de fraude–, el PSP podrá «poner el contador a cero», e iniciarse así un nuevo período de 90 días. Y ello con independencia de los canales utilizados por el usuario para acceder a la cuenta (*vid. Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., p. 9, apartado 44).

63. La ABE ha clarificado que, en los casos en que un mismo PSP ofrece servicios de iniciación de pagos y servicios de información sobre cuentas, la aplicación de la ARC para iniciar un pago a través del PSP tercero dentro de esos 90 días no interrumpe el plazo; es decir, los 90 días deben contarse desde la última vez que se aplicó la ARC para prestar el servicio de información de cuentas y no desde el ulterior en que se aplicó para iniciar la operación de pago (*vid. Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., pp. 9-10, apartado 44).

ARC cada vez que el usuario accede a su cuenta de pago en línea); otros que la han aplicado por el período máximo fijado (es decir, exigen la ARC cada 90 días) y otros que la exigen en períodos inferiores (por ejemplo, cada 30 días), agravándose la situación si la agregación se refiere a cuentas mantenidas por el usuario con distintos PSPGC (cada PSPGC podrá aplicar la exención por el período máximo, por un plazo inferior, o no aplicarla).

A la vista de esta situación, y con la finalidad de que la exención del artículo 10 no constituya un obstáculo para el desarrollo de servicios de pago innovadores –como es el servicio de información sobre cuentas– pero a la vez no se menoscabe la seguridad en la prestación de estos servicios, la ABE inició un proceso de modificación del artículo 10[64], que se ha plasmado finalmente en el Reglamento Delegado 2022/2360, de 3 de agosto, por el que se modifican las normas técnicas de regulación establecidas en el Reglamento Delegado (UE) 2018/389 en lo que respecta a la exención de 90 días para el acceso a las cuentas, y cuyas líneas esenciales pasamos a exponer[65].

La nueva regulación diferencia ahora entre si el acceso a la cuenta de pago se ha realizado de forma directa por el usuario (art. 10)[66] o a través

64. De acuerdo con lo previsto en el artículo 98.5 de la DSP2, la ABE debe examinar periódicamente las normas técnicas de regulación y, si es preciso, deberá actualizarlas con la finalidad de tener en cuenta las innovaciones y la evolución tecnológica.

65. El Reglamento fue publicado en el Diario Oficial de la Unión Europea de 5 de diciembre de 2022 y será aplicable a partir del 25 de julio de 2023 (art. 3.º). Como documentos preparatorios pueden consultarse los siguientes: ABE, *Consultation Paper On Draft Regulatory Technical Standards amending the Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication*, EBA/CP/2021/32, 28 October 2021 (disponible en *https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2021/Consultation%20on%20amending%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2/1022909/Consultation%20Paper%20on%20the%20amendment%20of%20the%20RTS%20on%20SCA%26CSC%20under%20PSD2.pdf*, consultada el 15 de diciembre de 2021); y ABE, *Final Report. Draft Regulatory Technical Standards amending the Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication* (*cit*).

66. «Artículo 10. Acceso a la información sobre la cuenta de pago proporcionado directamente por el proveedor de servicios de pago gestor de cuenta.

1. Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes, siempre que se cumplan los requisitos establecidos en el artículo 2, cuando un usuario de servicios de pago acceda en línea a su cuenta de pago directamente, a condición de que el acceso se limite a uno de los siguientes elementos en línea y no se divulguen datos de pago sensibles:

a) el saldo de una o varias cuentas de pago designadas;

b) las operaciones de pago ejecutadas en los 90 últimos días a través de una o varias cuentas de pago designadas.

2. No obstante lo dispuesto en el apartado 1, los proveedores de servicios de pago no estarán exentos de la aplicación de la autenticación reforzada de clientes cuando se cumpla alguna de las siguientes condiciones:

de un PSIC (nuevo art. 10 bis)[67]. En ambos casos el PSPGC está obligado a aplicar la ARC cuando el usuario accede a su cuenta por primera vez [art. 10.2.a) para el acceso directo y art. 10.2.b) para el acceso a través de un PSIC][68]; o cuando ha trascurrido un determinado período de tiempo desde la aplicación de la ARC, que se ha ampliado tanto para el acceso directo como para el indirecto a 180 días, frente a los 90 días previstos anteriormente[69]. Se observa, además, que la aplicación de la ARC transcurrido un período de tiempo no se limita ya a la consulta de operaciones realizadas, sino que se extiende a la consulta del saldo[70].

---

a) que el usuario de servicios de pago acceda en línea a la información especificada en el apartado 1 por primera vez;

b) que hayan transcurrido más de 180 días desde la última vez que el usuario de servicios de pago accediera en línea a la información especificada en el apartado 1, y se aplicara la autenticación reforzada de clientes».

67. «Artículo 10 bis. Acceso a la información sobre cuentas de pago a través de un proveedor de servicios de información sobre cuentas.

1. Los proveedores de servicios de pago no aplicarán la autenticación reforzada de clientes cuando un usuario de servicios de pago acceda a su cuenta de pago en línea a través de un proveedor de servicios de información sobre cuentas, siempre que el acceso se limite a uno de los siguientes elementos en línea y no se divulguen datos de pago sensibles:

a) el saldo de una o varias cuentas de pago designadas;

b) las operaciones de pago ejecutadas en los 90 últimos días a través de una o varias cuentas de pago designadas.

2. No obstante lo dispuesto en el apartado 1, los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes cuando se cumpla una de las condiciones siguientes:

a) que el usuario de servicios de pago acceda en línea a la información especificada en el apartado 1 por primera vez a través del proveedor de servicios de información sobre cuentas;

b) que hayan transcurrido más de 180 días desde la última vez que el usuario de servicios de pago accediera en línea a la información especificada en el apartado 1 a través del proveedor de servicios de información sobre cuentas y se aplicara la autenticación reforzada de clientes».

68. Se mantiene en ambos preceptos el requisito objetivo de la exención, relativo a que la información a la que se accede debe ser limitada (saldo o/y operaciones realizadas en los últimos 90 días).

69. La ABE descartó otras opciones, como establecer un plazo mayor (un año o más) o facultar al usuario para que fuera él quien fijara el plazo para aplicar la ARC. La primera se descartó por aumentar el riesgo de accesos a la cuenta de pago no autorizados o fraudulentos y la segunda porque los criterios para establecer las exenciones vienen establecidos en artículo 98, apartado 3 de la DSP2, y en ellos no se contempla que se deje en manos del usuario la posibilidad de establecer o modular una exención (adicionalmente, esta facultad del usuario podría hacer que fijara plazos no adecuados para el nivel de riesgo de la operación y falta de uniformidad en la aplicación de la exención) [*vid. Consultation Paper on Draft Regulatory Technical Standars amending the Commission Delegated Regulation (EU) 2018/389*…, cit., p. 13, apartados 42-44; *Final Report. Draft Regulatory Technical Standars amending the Commission Delegated Regulation (EU) 2018/* 389…, cit., p. 44, response 12].

70. Ello se desprende de la redacción que se ofrece ahora a los apartados segundo, letra b) del artículo 10 y segundo, letra b), del artículo 10 bis.

La novedad principal de la nueva regulación de la exención consiste en que, para los casos de acceso indirecto a la cuenta de pago –es decir, a través de un PSIC– la aplicación de la exención deja de ser voluntaria y se convierte en obligatoria[71] (para el acceso directo la aplicación de la exención continúa siendo voluntaria). Es decir, en la prestación de servicios de información sobre cuentas, el PSPGC deberá aplicar la ARC en el primer acceso del PSIC a la cuenta de pago y cada 180 días y *no podrá aplicarla* en los sucesivos accesos del PSIC a la cuenta de pago si no han transcurrido más de 180 días desde el último acceso.

Si bien es cierto que la modificación favorecerá la prestación del servicio de información sobre cuentas, el hecho de convertir la exención en obligatoria puede acarrear consecuencias perjudiciales para los PSPGC. Y es que, según dispone el artículo 74.2 DSP2, si el PSP del ordenante (que en este caso sería el PSPGC) no exige la ARC, la responsabilidad del PSPGC por operaciones no autorizadas se agrava, ya que no podrá invocar la negligencia grave o dolo del ordenante en el cumplimiento de sus obligaciones, sino únicamente su actuación fraudulenta. Habría que plantearse, por tanto, si resulta adecuado que los efectos gravosos de la nueva redacción de la exención se hagan recaer en los PSPGC y no en quienes se benefician de ella (los PSIC, que podrán prestar sus servicios de forma más eficiente)[72].

Para paliar de alguna forma las consecuencias negativas del carácter obligatorio de la exención para los PSPGC, el apartado tercero del artículo 10 bis establece la posibilidad de que el PSPGC revierta la exención y aplique la ARC cuando tenga razones objetivamente justificadas y debidamente documentadas de acceso fraudulento o no autorizado a la cuenta de pago[73].

---

71. La ABE consideró que no eran apropiadas otras propuestas realizadas por los operadores del mercado: imponer al PSPGC la obligación de delegar la aplicación de la ARC en el PSIC o establecer que el PSPGC sólo podría solicitar la ARC una vez, en concreto, cuando el usuario conectara sus cuentas al PSIC –no podría pedirla, por tanto, en los sucesivos accesos del PSIC a las cuentas de pago– [*vid. Consultation Paper on Draft Regulatory Technical Standars amending the Commission Delegated Regulation (EU) 2018/389*…, cit., pp. 8-9].
72. *Vid.* ABE, *Final Report. Draft Regulatory Technical Standars amending the Commission Delegated Regulation (EU) 2018/389*…, cit., p. 38, response 5. Sobre esta cuestión *vid.*, más ampliamente, el epígrafe IV.4.
73. Esto puede ocurrir, por ejemplo, cuando los mecanismos de supervisión de operaciones con que cuente el PSPGC (art. 2.º del Reglamento delegado), detecten que existe riesgo de acceso no autorizado o fraudulento [*vid.* ABE, *Consultation Paper On Draft Regulatory Technical Standars amending the Commission Delegated Regulation (EU) 2018/389*…, cit., p. 11, apartado 32]; o cuando el usuario notifique el PSPGC que la seguridad de las credenciales de seguridad personalizadas puede haberse visto comprometida [*vid.* ABE, *Final Report. Draft Regulatory Technical Standars amending the Commission Delegated Regulation (EU) 2018/389*…, cit., p. 53, response 25]. Como pone de manifiesto la propia ABE (*Consultation Paper*, p. 11, apartado 33), en estos casos el PSPGC, además de la posibilidad de revertir la exención y aplicar la ARC, cuenta con la facultad de denegar al PSIC el acceso a la cuenta, de conformidad con lo previsto en el apartado 5 del artículo 68 DSP2.

6.2. Operaciones de pago de escasa cuantía: pagos sin contacto en el punto de venta y operaciones remotas de pago electrónico

El Reglamento delegado permite que los PSP no apliquen la ARC cuando se trate de operaciones de pago de escasa cuantía, a fin de que el usuario ostente un cierto grado de comodidad en la realización de estas transacciones que, por razón de su importe, implican un menor riesgo. El Reglamento aborda la exención en dos preceptos distintos: el artículo 11, que se refiere a pagos sin contacto en el punto de venta (es decir, operaciones presenciales) y el artículo 16, relativo a operaciones de pago electrónico remotas. Ambos tienen en común que permiten al PSP aplicar la exención cuando la operación es de una cuantía reducida, siempre que adicionalmente se cumplan determinados requisitos.

Por lo que se refiere a los pagos sin contacto en el punto de venta[74], la regla general es que el PSP podrá no exigir la ARC cuando el importe de la operación sin contacto no exceda de 50 euros. Ahora bien, la exención decae y, por tanto, el PSP tendrá que aplicar la ARC, si se da alguna de las siguientes condiciones desde la última aplicación de la ARC: a) que la ejecución de la operación de pago sin contacto vaya precedida de operaciones previas sin contacto cuyo importe acumulado exceda de 150 euros, o b) que la ejecución de pago sin contacto sea la sexta operación sin contacto. En estos casos, aunque el importe de la operación de pago no supere los 50 euros, el PSP tendrá que aplicar la ARC.

El artículo 11 no aclara qué ocurre cuando el ordenante inicia pagos sin contacto en el punto de venta desde dispositivos distintos –una tarjeta, un móvil, un reloj–. La cuestión que surge es si, los límites a la aplicación de la exención –150 euros o cinco operaciones– se aplican en atención al dispositivo utilizado o a la cuenta de cargo[75].

De forma similar a los pagos sin contacto en el punto de venta, el artículo 16 del Reglamento delegado permite al PSP no aplicar la ARC en casos de operaciones remotas de pago electrónico de escasa cuantía, fijándose en este caso un importe inferior al previsto para aquellas, en concreto, la operación de pago no podrá exceder de 30 euros. De la misma manera, el PSP tendrá que aplicar la ARC, aunque la operación de pago remota no exceda de 30 euros, si el importe acumulado de las operaciones remotas de pago electrónico previas iniciadas por el ordenante desde la última aplicación de la ARC excede de 100 euros o el número de las operaciones remotas de pago electrónico previas iniciadas por el ordenante desde la

74. Nótese que no se prevé ninguna exención por razón de su cuantía para los pagos con contacto (insertando la tarjeta) en el punto de venta, aun cuando en el proceso de elaboración de las normas técnicas de regulación se sugirió su introducción. La ABE señaló al respecto que no existía justificación para no aplicar la ARC en estos casos (*vid. Final Report. Draft Regulatory Technical Standards on Strong Customer Authenticantion*…, cit., p. 85, cuestión 75).

75. Parece que técnicamente es más fácil actuar a nivel de dispositivo.

última aplicación de la ARC excede de cinco operaciones remotas de pago electrónico individuales consecutivas.

6.3. Terminales no atendidas para tarifas de transporte o pagos de aparcamiento

La exención, prevista en el artículo 12 del Reglamento delegado, se contempla para operaciones de pago electrónico de tarifas de transporte o aparcamiento[76] en una terminal no atendida. Esta exención no figuraba en la primera redacción de las normas técnicas de regulación, incluyéndose posteriormente para evitar los perjuicios que pudieran derivarse de la aplicación de la ARC. Y es que, en efecto, la exigencia de la ARC puede provocar disfunciones en la prestación de estos servicios (colas en los peajes de las autopistas o en los aparcamientos) pudiéndose generar incluso situaciones de peligro para los usuarios (accidentes)[77].

6.4. Beneficiarios de confianza

La exención (art. 13) consiste en que el PSP podrá no aplicar la ARC cuando el beneficiario se encuentre incluido en una lista blanca (es decir, se trate de un beneficiario de confianza) creada por el titular de la cuenta de pago. Ahora bien, el PSP tendrá que aplicar la ARC cuando el titular de la cuenta cree o modifique (añadiendo o eliminando beneficiarios) la lista blanca. La existencia de esa lista no obliga al PSP a aplicar la exención, sino que constituye un requisito previo para que el PSP pueda aplicarla. De otra manera, se estaría obligando al PSP a aplicar una exención y, por tanto, a asumir el riesgo de operaciones de pago no autorizadas en las que haya mediado negligencia grave o dolo del ordenante. Esta exención no se limita a las transferencias de crédito sino que se aplica también a los pagos con tarjeta siempre y cuando exista la confirmación del ordenante[78].

76. Se ha planteado si dentro de esta exención encajarían las operaciones realizadas en terminales no atendidas para pagos de tarifas de aparcamiento que incluyan la recarga de vehículos eléctricos. La ABE (Q&A 2020_5224, disponible en *https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5224,* consultada el 15 de septiembre de 2021) entiende que, dado que el elemento prevalente es el aparcamiento, el supuesto quedaría dentro del ámbito de aplicación del artículo 12 y, por tanto, el PSP podría no aplicar la ARC (se requiere, lógicamente, que ambos servicios –aparcamiento y recarga– se paguen en la misma terminal). En los casos en los que se trate solo de una recarga (de forma parecida al pago de combustible en una gasolinera) no podría aplicarse el artículo 12, pero podrían aplicarse otras exenciones (por ejemplo, el artículo 11 relativo a los pagos sin contacto).

77. Vid. considerando 11 del Reglamento delegado; ABE, Final Report. Draft Regulatory Technical Standards on Strong Customer Authenticantion…, cit., p. 10, apartado 25.

78. *Vid.* ABE, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, cit., p. 10, apartado 45. En el mismo apartado la ABE ha aclarado que PSP del beneficiario no puede aplicar esta exención. La inclusión de un comerciante como beneficiario de confianza en una lista blanca puede realizarse en el mismo momento de la compra en línea (el titular de la tarjeta marca una casilla en la que se le pregunta si quiere añadir al comerciante como beneficiario de confianza).

6.5. Operaciones frecuentes

El Reglamento delegado prevé una exención para las operaciones frecuentes (art. 14), entendiendo por tales las que formen parte de una serie de operaciones de pago con el mismo importe y el mismo beneficiario. Puede tratarse de transferencias periódicas o de pagos recurrentes iniciados por el beneficiario, si bien en este último caso no se incluyen las domiciliaciones, pero sí los pagos recurrentes con tarjeta. Sí se requiere la ARC para la primera operación de la serie.

6.6. Transferencias de crédito entre cuentas mantenidas por la misma persona física o jurídica

Aun cuando no se desprende del título del artículo, es necesario, según su contenido (art. 15), no sólo que ordenante y beneficiario sean la misma persona sino, además, que la transferencia se realice entre cuentas mantenidas en un mismo PSP. Nos encontramos, por tanto, en una exención aplicable a las conocidas como operaciones de traspaso. Para el resto de las transferencias internas (es decir, entre cuentas mantenidas en el mismo PSP, pero a favor de un beneficiario distinto del ordenante) sigue vigente la regla general de aplicar la ARC salvo que el supuesto encaje en los artículos 13, 14 o 18.

6.7. Pagos corporativos

Esta exención, regulada en el artículo 17, no se recogía en el proyecto de normas técnicas de regulación presentado por la ABE, sino que fue añadida por la Comisión. La exención cubre las operaciones de pago electrónico realizadas a través de los protocolos o procedimientos de pago que usan normalmente las empresas (la exención sólo se aplica cuando el ordenante no sea un consumidor)[79], siempre y cuando la autoridad competente considere que dichos protocolos o procedimientos garantizan unos niveles de seguridad al menos equivalentes a los previstos en la DSP2[80].

6.8. Operaciones remotas de pago electrónico de bajo riesgo

Esta exención (arts. 18 a 20 del Reglamento delegado) se basa en un análisis del riesgo de la operación y permite que el PSP no aplique la ARC a operaciones remotas de pago electrónico (transferencias de crédito y pagos con tarjeta) cuando el riesgo sea bajo. La aplicación de esta exención

79. Sería el caso de las *lodged cards* utilizadas por las empresas para la gestión de los pagos de viaje de sus empleados.
80. *Vid.* PASTOR SEMPERE, C., «El 'mercado único digital' de los micropagos», en MARTÍ MIRAVALLS (dir.): *Problemas actuales y recurrentes en los mercados financieros. Financiación alternativa, gestión de la información y protección del cliente*, Aranzadi, 2018, p. 231.

posibilita, de esta manera, que un PSP autorice un pago electrónico remoto de importe superior a 30 euros (art. 16 del Reglamento delegado) sin exigir la ARC (pagos en un solo *click*). Para que el nivel de riesgo sea bajo deben cumplirse todas las condiciones siguientes: a) que el índice de fraude sea equivalente o inferior al índice de fraude de referencia especificado en el Anexo del Reglamento; b) que el importe de la operación no supere el valor umbral de exención («VUE»), también especificado en el Anexo; c) que el PSP no haya detectado, como consecuencia de la realización de un análisis del riesgo de la operación en tiempo real, elementos que permitan sospechar que la operación no ha sido autorizada o que es fraudulenta[81].

En el caso de operaciones de pago con tarjeta, a fin de evaluar el riesgo y poder aplicar la exención, el comerciante (beneficiario) podría proporcionar al emisor de la tarjeta (PSP) información sobre la transacción, incluida su propia evaluación del riesgo. Otra opción sería que el comerciante proporcionara a su entidad (entidad del adquirente) la información referida para que este sea quien aplique la exención (los beneficiarios no pueden aplicar la exención, aunque sí puede hacerlo su PSP –proveedor de servicios de pago del adquirente–).

IV. RESPONSABILIDAD

En las líneas que siguen se aborda la cuestión de la responsabilidad que deriva de autenticaciones no autorizadas que se traducen en la emisión y ejecución de una orden de pago no autorizada. Para ello se analizarán las obligaciones de los usuarios y de los proveedores de servicios de pago en materia de autenticación, el grado de diligencia exigible y la atribución de la carga de la prueba.

1. UNA CUESTIÓN PREVIA: OPERACIONES NO AUTORIZADAS Y AUTENTICACIONES NO AUTORIZADAS

El artículo 64 de la DSP2 establece que «(l)os Estados miembros velarán por que las operaciones de pago se consideren autorizadas únicamente cuando el ordenante haya dado su consentimiento a que se ejecute la operación de pago», añadiendo que «en ausencia de consentimiento, la operación de pago se considerará no autorizada». La autorización, por tanto, va ligada a la existencia del consentimiento del usuario para una concreta operación de pago. Para comprobar la existencia de dicho consentimiento

81. El artículo 18.2 c) del Reglamento delegado concreta cuáles son estos elementos: i) gastos o pautas de comportamiento anormales en el ordenante; ii) información inusual sobre el dispositivo o programa informático de acceso del ordenante; iii) infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación; iv) supuestos conocidos de fraude en la prestación de servicios de pago; v) una ubicación anormal del ordenante; y vi) una ubicación de alto riesgo del beneficiario.

se aplica el procedimiento de autenticación pero, tal y como se indicó a la hora de analizar la autenticación en el ámbito de la Guía jurídica de la CNUDMI sobre transferencias electrónicas de fondos y de la Ley Modelo de la CNUDMI sobre transferencias internacionales de crédito, la autenticación por medios electrónicos genera el riesgo de que existan autenticaciones no autorizadas porque un tercero haya tenido acceso a las credenciales de seguridad personalizadas de los usuarios. Por tanto, la autenticación no es un medio que asegure en todo caso la existencia del consentimiento del usuario y, por tanto, que este haya autorizado la operación[82]. Es un instrumento o mecanismo, establecido en favor del PSP, para que pueda considerar legítima su actuación cuando ejecuta una operación de pago que, precisamente por haber sido autenticada, genera la apariencia de la existencia de dicho consentimiento. La responsabilidad derivada de operaciones autenticadas, pero no autorizadas (porque el usuario no ha dado su consentimiento) habrá de establecerse atendiendo a diversos factores, siendo uno de ellos analizar en qué medida la autenticación no autorizada se produjo como consecuencia del incumplimiento del usuario y/o del PSP de sus obligaciones en materia de autenticación.

2. OBLIGACIONES DE LOS PROVEEDORES DE SERVICIOS DE PAGO Y DE LOS USUARIOS EN MATERIA DE AUTENTICACIÓN

La DSP2 no recoge expresamente la obligación de los PSP de autenticar a los usuarios o a las órdenes de pago, si bien esta afirmación debe matizarse para los supuestos en los que resulta de obligada aplicación la ARC pues, al exigirse una forma determinada de autenticación, indirectamente se está imponiendo a los PSP la obligación de autenticar. Ahora bien, esta obligación puede inferirse de la condición de comisionista del PSP derivada del contrato de cuenta corriente existente entre este y el usuario. En efecto, el PSP, en tanto, que comisionista obligado a prestar el servicio de caja, debe seguir las instrucciones de su cliente y, por tanto, debe asegurarse de que efectivamente las instrucciones proceden de aquél, para lo que debe aplicar el procedimiento de autenticación[83]. Además, el procedimiento de autenticación, que es elegido por el PSP, debe ser comercialmente razonable. Para los casos en los que se exige la ARC, este requisito se entiende cumplido si el PSP diseña un procedimiento de autenticación que se ajuste a los parámetros establecidos para dicha forma de autenticación en la DSP2

82. En este sentido, la AP de Alicante (Sección 8.ª) n.º 107/2018 de 12 de marzo (AC 2018, 818) señala que la responsabilidad no puede atribuirse al supuesto ordenante de una transferencia «por entenderse ésta autorizada al haberse realizado de acuerdo con los sistemas de autenticación del banco».

83. La sentencia de la AP de Toledo (Sección 2.ª) n.º 221/2020 de 30 de noviembre (JUR 2021, 39946) señala en su fundamento de derecho segundo, que es responsabilidad del banco, en tanto que comisionista, conservar intacta la cuenta del usuario, lo que implica «en primer lugar, y como obligación básica, el vigilar que las operaciones ordenadas lo sean por el legitimado para emitir órdenes de pago».

y en el Reglamento delegado. Por lo que respecta al alcance de la obligación de autenticación, esta no se limita a la comprobación de la identidad del usuario o de la validez de la utilización de un instrumento de pago, sino que abarca también la obligación de contar y aplicar mecanismos de supervisión que permitan detectar operaciones de pago no autorizadas y accesos no autorizados a la cuenta de pago, de conformidad con lo previsto en el artículo 2.º del Reglamento delegado. Por último, según establece el artículo 70.1.a) DSP2, es obligación del PSP asegurarse de que las credenciales de seguridad personalizadas sólo sean accesibles para el usuario[84]. Este último precepto ha sido desarrollado por el Reglamento delegado en el Capítulo IV que, tras señalar que los PSP garantizarán la confidencialidad e integridad de las credenciales de seguridad personalizadas durante la fase de autenticación (art. 22.1), establece los requisitos relativos a la creación y entrega de estas credenciales, su asociación al usuario y las condiciones para su renovación y activación (arts. 23 a 27).

Por lo que respecta al usuario, el artículo 69 de la DSP2 le impone las siguientes obligaciones, cuyo incumplimiento puede derivar en autenticaciones no autorizadas de usuarios o de operaciones de pago: hacer uso del servicio de pago en las condiciones pactadas con el PSP (se menciona expresamente la obligación de adoptar todas las medidas razonables a fin de proteger las credenciales de seguridad personalizadas) y notificar a su PSP o a quien este designe, el extravío, robo o apropiación indebida del instrumento de pago o de las credenciales de seguridad personalizadas –aun cuando no se haya producido una operación no autorizada– o la utilización no autorizada del instrumento de pago[85]. La notificación debe realizarse

84. El artículo 70 DSP2 contiene otras obligaciones del PSP que tienen también relevancia en la atribución de la responsabilidad por operaciones no autorizadas: abstenerse de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso sustitución del instrumento de pago; garantizar que en todo momento están disponibles medios adecuados que permitan al usuario notificar el extravío, robo o apropiación indebida del instrumento de pago o de las credenciales de seguridad personalizadas; e impedir cualquier utilización del instrumento de pago una vez efectuada dicha notificación.

85. Entendemos que este deber de notificación es distinto del que establece el artículo 71 de la DSP2. Este se refiere a la notificación de operaciones no autorizadas, mientras que el artículo 69 contempla la notificación de hechos (extravío, robo, apropiación indebida) *que pueden derivar* en que se ejecuten operaciones no autorizadas (más dudas ofrece, sin embargo, la referencia a la «utilización no autorizada del instrumento de pago»). Así, un usuario puede haber cumplido con la obligación de notificar una operación no autorizada *ex* artículo 71 (sin demora injustificada en cuanto tuvo conocimiento de la misma) pero haber incumplido la de notificar el extravío, por ejemplo, de la tarjeta. La obligación de notificar las operaciones no autorizadas surge, por tanto, desde el momento en que efectivamente el usuario tuvo conocimiento de la operación no autorizada (por ejemplo, cuando examinó los extractos de cuenta o cuando recibió un mensaje del banco informándole de un determinado cargo) y no desde el momento en que se efectuó el adeudo en su cuenta. Ahora bien, la norma establece un plazo para efectuar la notificación o, dicho en otros términos, un plazo *para que el usuario conozca la operación no autorizada* y la notifique al banco. Se impone, de esta manera, un deber de diligencia al usuario de comprobar la justificación de las operaciones

sin demora indebida, en cuanto el usuario tenga conocimiento de alguno de los hechos apuntados. Del cumplimiento de estas obligaciones responde el usuario, por regla general, en casos de negligencia grave o dolo, si bien existen supuestos, como se verá más adelante, en los que ni si siquiera en estos casos responderá.

3. LA OBLIGACIÓN DE RESTITUCIÓN

Bajo la denominación «Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas», el artículo 73 de la DSP2 impone al PSP del ordenante la obligación de devolverle el importe de la operación de pago no autorizada[86]. Esta restitución deberá hacerse «de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en que haya observado o se le haya notificado la operación». Únicamente cuando el PSP tenga motivos razonables para sospechar la existencia de fraude del usuario[87] y comunique por escrito esos motivos a la autoridad nacional pertinente podrá no efectuar dicha devolución. En nuestra opinión, el precepto no se ocupa de la responsabilidad del PSP, sino que establece una obligación de restitución basada en la mera declaración del usuario de que

realizadas por el banco. Si el usuario no notifica la operación no autorizada conforme a lo apuntado (es decir, sin demora injustificada desde que tuvo conocimiento de la misma y, como máximo, en un plazo de 13 meses), entonces el banco quedará exonerado de su obligación de devolver el importe de la operación no autorizada, conforme establece el artículo 73 DSP2. Y ello por lo establecido en el primer inciso de este precepto, que señala «(s)in perjuicio del artículo 71…». Esto no significa que sea el usuario quien finalmente deba asumir la pérdida, pero sí que el banco podrá retener los fondos correspondientes al importe de la operación aun cuando no exista sospecha de fraude del usuario. La posición del banco se verá, además, reforzada, ya que la falta de comunicación del usuario podrá constituir una prueba de su negligencia.

86. El artículo 72 añade que el PSP, en su caso, restituirá la cuenta de pago al estado en que se habría encontrado de no haberse efectuado la operación no autorizada, lo que implicaría, la devolución del principal de la operación, los intereses de demora y las comisiones cobradas por la posición deudora y los intereses que la cantidad adeudada incorrectamente podría haber generado en la cuenta de pago (*vid.* ROJO ÁLVAREZ-MANZANEDA, R., *La utilización fraudulenta de las tarjetas de pago*, Thomson Reuters Aranzadi, 2011, p. 85).

87. Que se trata de la sospecha de fraude del usuario y no de cualquier fraude cometido se infiere no tanto de la redacción del precepto como del considerando 71 de la DSP2, que señala que «(n)o obstante, cuando haya una sospecha fundada de que una operación no autorizada es el resultado de una conducta fraudulenta del usuario de servicios de pago […]». La ABE entiende que la redacción actual del artículo 73 debe ser modificada, a fin de dejar claro que el fraude relevante a efectos de su aplicación es el fraude del usuario de servicios de pago [*vid.* Informe anexo a la *Opinion* de la ABE de 23 de junio de 2022 (*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366*…, cit., p. 68, apartados 289-292]. Se ha señalado que, en función de lo que se entienda por «motivos razonables», el PSP podrá retener los fondos con mayor o menor facilidad [*vid.* REQUEIJO TORCAL, A., «Derechos y obligaciones en relación con la prestación de servicios de pago», en URÍA FERNÁNDEZ – CARPINTERO PÉREZ (coords.): *Servicios de pago: adaptación a la Directiva PSD II*, Claves Prácticas Francis Lefebvre, Madrid, 2018 pp. 96-97].

él no ha autorizado la orden de pago[88], que tendrá carácter provisional hasta que se confirme (y pruebe) por el PSP su actuación diligente y la negligencia grave o dolo del usuario en el cumplimiento de sus obligaciones o el fraude el usuario. Por tanto, el PSP no podrá en este momento alegar que la operación ha sido autenticada correctamente, registrada y contabilizada, y que no se vio afectada por un fallo técnico u otras deficiencias (art. 72 DSP2), sino que tendrá que devolver el importe de la operación al ordenante cuando este niegue que la ha autorizado. La obligación de restitución así establecida no supone que el legislador imponga al PSP el riesgo de todas las autenticaciones que no hayan sido autorizadas por el usuario ya que, como se verá más adelante, el ordenante soporta todas las pérdidas cuando actuó con negligencia grave o dolo en el cumplimiento de sus obligaciones o actuó de manera fraudulenta (art. 74 DSP2). Lo que significa es que, aun cuando la operación haya sido correctamente autenticada y salvo sospecha de fraude del usuario, el PSP debe devolver el importe al ordenante, sin perjuicio de que más adelante, y de conformidad con lo establecido en el artículo 74, pueda recuperar esos fondos[89]. Esta obligación subsiste en los casos en los que la operación de pago se haya iniciado a través de un PSIP (es decir, el PSP del ordenante, como PSPGC, deberá devolverle el importe de la operación de pago), si bien el PSP del ordenante podrá repetir del PSIP si este es responsable de la operación no autorizada (art. 73.2 DSP2).

4. PRUEBA DE LA AUTENTICACIÓN Y RESPONSABILIDAD

La atribución al PSP de la carga de la prueba en materia de autenticación la realiza el apartado primero del artículo 72 DSP2, que establece que los Estados miembros exigirán que «cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada, o alegue que esta se ejecutó de manera incorrecta, corresponda al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago». Se produce, por tanto, una inversión de la carga de la prueba en favor del usuario[90]. Debe advertirse que lo previsto en el artículo

88. De esta opinión parece ser RUIZ MUÑOZ, M., «Obligaciones del proveedor de servicios de pago frente al usuario de los instrumentos de pago (La Directiva y la Ley de servicios de pago, y el Anteproyecto de Ley de Código Mercantil de 2014)», *La Ley Mercantil*, n.º 7, octubre 2014, p. 12 y nota 62.
89. Una opinión distinta mantiene RUIZ MUÑOZ («Obligaciones del proveedor de servicios de pago frente al usuario…», cit., pp. 14 y ss.), que sostiene que en caso de que se verifique la autenticación, decae la obligación de restitución inmediata, pudiendo el PSP optar por devolver la totalidad del importe, devolver el importe con la franquicia de 150 euros (ahora 50 euros) o no devolver nada porque el ordenante deba soportar todas las pérdidas.
90. *Vid.*, entre otros, RUIZ ESPINOSA, J., «Garantías legales en el pago a distancia con tarjeta efectuado por consumidores», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 60, 2022, p. 11.

72 es materia disponible en caso de que el usuario no sea un consumidor (art. 61.1 DSP2), en cuyo caso, el PSP y el usuario podrán acordar que no se produzca dicha inversión de la carga de la prueba[91]. Si interviene un PSIP, la prueba de los hechos apuntados corresponde a él (art. 72.1, párrafo segundo).

Al PSP le corresponde, por tanto, la carga de acreditar su comportamiento diligente en el procedimiento de autenticación[92]. Ello implica que el PSP debe probar que la orden que ejecutó estaba debidamente autenticada con las credenciales de seguridad personalizadas del usuario; que la forma de autenticación era adecuada (ARC, cuando sea exigible, u otra forma de autenticación comercialmente razonable, en otros casos); y que contaba con procedimientos de detección de operaciones de pago no autorizadas[93] y con medidas de seguridad para salvaguardar la confidencialidad

91. Haciendo uso de la habilitación contenida en el artículo 61.3 de la DSP2, que faculta a los Estados miembros a establecer que las disposiciones del Título IV de la DSP2 se apliquen a las microempresas de la misma forma que a los consumidores, el artículo 34 del Real Decreto-ley 19/2018 declara aplicable el artículo 44 (el equivalente al artículo 72 de la DSP2) a las microempresas, por lo que cuando el usuario sea una microempresa también la carga de la prueba recaerá sobre el PSP.
92. *Vid.* sentencia de la AP de Pontevedra (Sección 6.ª), n.º 539/2021 de 21 de diciembre (JUR 2022, 121233), fundamento de derecho tercero, apartado 21.
93. En la sentencia de la AP de Pontevedra (Sección 6.ª), n.º 539/2021 de 21 de diciembre (JUR 2022, 121233) se concluye que el PSP no acreditó la diligencia en el procedimiento de autenticación al no haber adoptado un mecanismo *antiphising*, lo que le vendría exigido por el apartado segundo, letra c) del artículo 2.º del Reglamento delegado, que establece que los mecanismos de supervisión deben tener en cuenta los supuestos conocidos de fraude, y el *phising* lo es. Añade, además, que el envío a los usuarios de correos explicativos y con recomendaciones de actuación para estos tipos de fraude no puede ser considerado un mecanismo *antiphising* (*vid.*, sobre esta sentencia, RUIZ ESPINOSA, J., «Garantías legales en el pago a distancia…», cit., p. 8). En términos parecidos se manifiestan la sentencia de la AP de Alicante (Sección 8.ª) n.º 107/2018 de 12 de marzo (AC 2018, 818) y la sentencia de la AP de Barcelona (Sección 14.ª), n.º 151/2013 de 7 de marzo (JUR 2013, 171665). Esta última señala «que por más recomendaciones que se hagan al usuario o cliente […] es ésta (la entidad) la que ofrece un producto en principio seguro, pero con conocimiento de los distintos riesgos ajenos a un uso del cliente con todas las recomendaciones, por lo que corresponde a la misma adoptar las medidas de seguridad o control necesarias, y renovarse ante los distintos modos de ataque informático» (concluye indicando que la entidad no aportó prueba de la adopción de medidas concretas de seguridad para el fraude de *phising*). En la misma línea, la ABE (*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366*…, cit., pp. 68-69, apartados 293 y 294), pone de manifiesto que en ocasiones los PSP consideran que existe negligencia grave en los casos en los que el usuario es víctima de un fraude en el que se utilizan técnicas de ingeniería social y es manipulado para entregar o desvelar sus credenciales de seguridad personalizadas a un estafador, y considera que esta interpretación no es adecuada conforme al artículo 2.º del Reglamento delegado. La cuestión de si en el *phising* engañoso la actuación del usuario debe ser considerada como negligencia grave ya había sido apuntada por MARTÍ MIRAVALLS («Banca on-line y responsabilidad por daños…», cit., pp. 246-248), que entiende que en la mayoría de los casos será así. Ahora bien, dicha afirmación se realiza en el contexto de la Ley

e integridad de las credenciales de seguridad personalizadas conforme a lo previsto en el Reglamento delegado[94]. La diligencia del PSP será la de un empresario experto, diligencia profesional exigible en tanto que comisionista y depositario de los fondos del usuario[95]. Si el PSP no acredita el cumplimiento de sus deberes de diligencia en la autenticación, tendrá que responder de la pérdida salvo que concurra el fraude del ordenante[96].

Ahora bien, la prueba de los hechos apuntados no significa que la pérdida por la operación de pago no autorizada se atribuya al usuario. Será necesario, además, que el PSP pruebe la negligencia grave o dolo en el cumplimiento de sus obligaciones o el fraude del usuario[97]. Así se desprende de los artículos 74.1 y 72.2 DSP2. El primero de ellos establece que el ordenante soportará todas las pérdidas derivadas de operaciones de pago no autorizadas si «ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 69»[98]. Por

16/2009, de 13 de noviembre, de servicios de pago, que traspuso a nuestro ordenamiento la Primera Directiva de Servicios de Pago. En la actualidad, tras la entrada en vigor de la DSP2 y del Reglamento delegado, y la imposición de la obligación al PSP de contar con mecanismos de detección del fraude, la responsabilidad del PSP se agrava, y no podrá imputarse la pérdida al usuario si el PSP no cumplió con la obligación prevista en el artículo 2.º del Reglamento delegado.

94. No parece ser esta la opinión del Departamento de Conducta de Entidades, que considera la prueba de la autenticación como limitada al hecho de verificar que la operación de pago fue autenticada con las credenciales de seguridad personalizadas del usuario (en el caso examinado, datos de la tarjeta y OTP) (*vid.* Memoria de Reclamaciones de 2021, p. 263, expediente 202125872).

95. *Vid.* sentencia de la AP de Toledo (Sección 2.ª) n.º 221/2020 de 30 de noviembre (JUR 2021, 39946), fundamento de derecho segundo y sentencia de la AP de Madrid (Sección 14.ª) n.º 371/2017 de 11 de diciembre (JUR 2018, 123994), fundamento de derecho tercero; PÉREZ GUERRA, M., «Ciberdelitos y responsabilidad civil…», cit., p. 3.

96. En este sentido se pronuncia la sentencia de la AP de Pontevedra (Sección 6.ª), n.º 539/2021 de 21 de diciembre (JUR 2022, 121233), en el fundamento de derecho tercero, apartado 22.

97. *Vid.* ROJO ÁLVAREZ-MANZANEDA, R., *La utilización fraudulenta*…, cit., pp. 96-97; sentencia de la AP de Pontevedra (Sección 6.ª), n.º 539/2021 de 21 de diciembre (JUR 2022, 121233), fundamento de derecho tercero, apartado 21.

98. En palabras de ROJO ÁLVAREZ-MANZANEDA (*La utilización fraudulenta*…, cit., p. 96), la norma «viene a exigir al titular una diligencia mínima, liberándolo de responsabilidad en los supuestos de culpa leve o simple negligencia, elevando la protección del titular también por el hecho de que en la propia ejecución de una operación de pago no autorizado ha mediado una causa de carácter extraño, la intervención de un tercero». Como excepción a lo apuntado, el usuario responderá hasta un máximo de 50 euros (se ha reducido el importe de 150 euros que establecía la DSP1) en el caso de ausencia de negligencia grave, dolo o actuación fraudulenta (es decir, si actuó diligentemente o con negligencia leve) si la pérdida se debió a la utilización de un instrumento de pago extraviado, robado o sustraído, o a la apropiación indebida del mismo. Todo ello salvo que al usuario no le resulte posible detectar la pérdida, robo o apropiación indebida antes de un pago, o que la pérdida se derive de la acción o inacción de empleados o de cualquier agente, sucursal o entidad a la que se hayan externalizado

su parte, el artículo 72.2 dispone que el PSP «aportará pruebas para demostrar que el usuario del servicio de pago ha cometido fraude o negligencia grave»[99]. Una vez más, debe hacerse una precisión. Y es que, como se indicó anteriormente, el contenido del artículo 72 es disponible para las partes en caso de que el usuario no tenga la consideración de consumidor, disponibilidad que se extiende igualmente al artículo 74 (art. 61.º DSP2)[100]. Por tanto, el PSP y el usuario no consumidor podrán pactar, además de la no inversión de la carga de la prueba, que el usuario responda también en casos de negligencia leve.

Teniendo en cuenta estas precisiones, podemos concluir, por tanto, que el ordenante soportará las pérdidas derivadas de operaciones de pago no autorizadas si se cumplen dos requisitos: primero, que haya actuado de manera fraudulenta o incumpliendo, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 69 y, segundo, que la operación de pago no autorizada haya sido correctamente autenticada (en los términos apuntados) y registrada, y no se haya visto afectada por un fallo técnico u otra deficiencia del servicio prestado por el PSP[101], cuestiones todas ellas que debe probar el PSP. El régimen establecido es, como se deduce, muy beneficioso para los consumidores, en sintonía con los objetivos de la DSP2 de fomentar la protección de los mismos en la prestación de servicios de pago.

Como excepción a la regla general que recoge el apartado primero del artículo 74 de la DSP2 (el ordenante soportará todas las pérdidas derivadas

---

actividades (art. 74.1 DSP2), en cuyo caso ni siquiera tendrá que soportar la pérdida de 50 euros. RUIZ ESPINOSA («Garantías legales en el pago a distancia…», cit., p. 15) señala que la prueba de tales hechos recae en el usuario, lo que entiende no está exento de dificultad.

99. Se ha señalado al respecto, siguiendo a la jurisprudencia (*vid.* PEÑAS MOYANO, M. J., *Régimen jurídico de los servicios de pago en el Derecho español*, Aranzadi, 2020, pp. 113-114; REQUEIJO TORCAL, A., «Derechos y obligaciones…», cit., pp. 97-98; PÉREZ GUERRA, M., «Ciberdelitos y responsabilidad civil…», cit., p. 4) que la DSP2 establece un sistema de responsabilidad cuasi objetiva para los PSP. *Vid.* sentencia de la AP de Asturias (Sección 1.ª), n.º 351/2012 de 18 de septiembre (JUR 2012, 369519), fundamento de derecho tercero; sentencia de la AP de Castellón (Sección 3.ª) n.º 39/2014 de 4 de febrero (JUR 2014, 120627), fundamento de derecho quinto, sentencia de la AP de Alicante (Sección 8.ª) n.º 107/2018 de 12 de marzo (AC 2018, 818). Indica de forma acertada PÉREZ GUERRA («Ciberdelitos y responsabilidad civil…», cit., p. 4), que el ser víctima de un fraude no implica por sí mismo haber actuado con falta de diligencia, a lo que añade que «el extravío (de las credenciales) o el *hackeo* al usuario no supone una falta de diligencia».

100. Haciendo uso de la habilitación contenida en el artículo 61.3 de la DSP2, que faculta a los Estados miembros a establecer que las disposiciones del Título IV de la DSP2 se apliquen a las microempresas de la misma forma que a los consumidores, el artículo 34 del Real Decreto-ley 19/2018 declara aplicable el artículo 46 (el equivalente al artículo 74 de la DSP2) a las microempresas.

101. *Vid.* sentencia de la AP de Pontevedra (Sección 6.ª), n.º 539/2021 de 21 de diciembre (JUR 2022, 121233), fundamento de derecho tercero, apartado 20.

de operaciones de pago no autorizadas si ha actuado de manera fraudulenta o ha incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 69), el apartado segundo del mismo precepto establece un régimen más beneficioso para el usuario si su PSP no exige la ARC. En efecto, dispone el precepto que «(s)i el proveedor de servicios de pago del ordenante no exige autenticación reforzada de cliente, el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta» (el ordenante no respondería, por tanto, en caso de negligencia grave o dolo en el cumplimiento de sus obligaciones). Ahora bien, el precepto suscita ciertas dudas en torno a qué supuestos se aplica, ya que pueden diferenciarse hasta tres casos distintos: a) el PSP del ordenante no exige la ARC porque se trata de supuestos distintos de los que contempla el apartado primero del artículo 97 (es decir, casos en los que no es obligatorio aplicar la ARC); b) el PSP del ordenante no exige la ARC a pesar de estar obligado a ello por tratarse de operaciones u actuaciones incluidas en el apartado primero del artículo 97; c) el PSP del ordenante no exige la ARC amparándose en una exención. En nuestra opinión, la finalidad del precepto es incentivar a los PSP a que cumplan con la obligación de aplicar la ARC, y la atribución de la pérdida al PSP en caso de negligencia grave o dolo del usuario podría interpretarse como una «sanción» por no cumplir con esta obligación. De esta forma, el artículo 74.2 no se aplicaría a los supuestos que hemos englobado bajo la letra a) y sí a los mencionados en la letra b)[102].

Mayores dudas presenta la actuación del PSP que no exige la ARC amparándose en una exención. Si entendemos que resulta de aplicación el apartado segundo del artículo 74 se estaría equiparando la actuación de un PSP que no cumple con su obligación (la de aplicar la ARC) con la de un PSP que sí cumple, ya que no la exige al amparo de una previsión legal. Esta interpretación podría llevar a que los PSP fueran reticentes a hacer uso de las exenciones que permite la norma. Pero, si excluimos estos supuestos, el usuario se vería perjudicado, al tener que responder por negligencia grave o dolo al amparo de una decisión (la de no aplicar la ARC) que no ha sido adoptada por él, pero, además, sobre la que no puede decidir (sólo el PSP del ordenante y, en ciertos casos, el PSP del beneficiario, están facultados para aplicar algunas de las exenciones). En nuestra opinión, y con independencia de que esta cuestión debería ser aclarada en la revisión de la DSP2[103], es el PSP que hace uso de la exención quien debe correr el riesgo

102. Si el PSP del ordenante exige la ARC, pero el beneficiario o el proveedor de servicios de pago del beneficiario no la aceptan, el PSP del ordenante sigue siendo responsable frente al ordenante, pero se impone a aquellos la obligación de reembolsar el importe del perjuicio financiero causado al PSP del ordenante (art. 74.2 *in fine* DSP2).

103. En este sentido se ha pronunciado la ABE (*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366*…, cit., p. 67), que entiende que en el proceso de revisión de la DSP2 debe clarificarse «whether Articles 73 and 74 of PSD2 cover the cases of unauthorised payment transactions for which an SCA exemption has been applied».

de que se ejecute una operación no autorizada a la que no aplicó la ARC, ya que es él quien ha adoptado la decisión. Por tanto, se defiende incluir en el ámbito de aplicación del artículo 74, apartado segundo, los supuestos en los que no se exige la ARC haciendo uso de una de las exenciones. Ahora bien, queda aún por resolver qué sucede en los casos del artículo 10 bis del Reglamento delegado, en los que la no aplicación de la ARC es obligatoria (acceso a una cuenta de pago en línea a través de un PSIC). En nuestra opinión, deben conciliarse dos intereses: los del usuario que, una vez más, es ajeno al procedimiento de autenticación y a sus exenciones; y los del PSP del usuario, al que se le obliga a aplicar una exención. Entendemos que el supuesto debe quedar englobado en el apartado segundo del artículo 74, de forma que el usuario sólo responderá en caso de su propia actuación fraudulenta, pero que el PSP podrá repetir la pérdida del PSIC, que es el proveedor que resulta beneficiado por la existencia de la exención obligatoria. Se propone, por tanto, la misma solución que se ha apuntado para los casos en los que es el PSP del beneficiario quien aplica la exención.

V. LA AUTENTICACIÓN REFORZADA DE CLIENTE EN EL PROCESO DE REVISIÓN DE LA SEGUNDA DIRECTIVA DE SERVICIOS DE PAGO

Como se señaló al inicio de este trabajo, la Segunda Directiva de Servicios de Pago se encuentra actualmente en proceso de revisión. Con respecto a la autenticación reforzada de cliente, la ABE señala que su aplicación ha producido los efectos deseados, en la medida en que el nivel de fraude, tanto por volumen de operaciones como por su valor, es significativamente menor en las operaciones en las que se aplicó la ARC que en las que no fue así[104]. Menciona, no obstante, una serie de cuestiones que deben clarificarse, y para ello recomienda revisar determinados aspectos de la ARC. Por lo que se refiere a su aplicación, propone que la Directiva se ocupe de la delegación de la ARC en terceros (ya sean proveedores de servicios de pago o de servicios tecnológicos), aclare la naturaleza de las exenciones (si son facultativas u obligatorias), y contemple de forma explícita que la ARC tiene carácter gratuito. En relación con los fraudes basados en la utilización de técnicas de ingeniería social, propone que se prevean medidas educacionales y de sensibilización frente al fraude, así como otras que incentiven a los PSP a invertir en mecanismos de supervisión más eficientes y que faciliten el intercambio de información entre los PSP sobre casos de fraude y defraudadores conocidos, y cuentas utilizadas para llevar a cabo los fraudes[105]. Por último, para evitar que ciertos sectores de la población puedan resultar excluidos del mercado de pagos (se considera que los servicios de

104. *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366*…, cit., p. 2.

105. IBERPAY (Sociedad Española de Sistemas de Pago) ofrece el servicio de prevención del fraude denominado «Payguard», que «facilita a los PSP el intercambio de información sobre operaciones de movimientos de fondos no autorizadas, o sospechosas de serlo, con el fin de poder evaluar anticipadamente el riesgo de fraude en los pagos recibidos

pagos son un servicio financiero básico o esencial) como consecuencia de la exigencia de la ARC (que implica el acceso a la tecnología y estar dotado de competencias digitales), propone introducir una disposición que exija a los PSP que, a la hora de ofrecer a sus clientes soluciones de ARC, tengan en cuenta las necesidades de los diversos grupos de población, incluyendo los denominados sectores vulnerables.

Otra de las cuestiones relevantes, ya apuntada en la Estrategia de Pagos Minoristas, es la de la de aprovechar el desarrollo de la identidad digital europea, prevista en la futura modificación del Reglamento eIDAS, a efectos de aplicación de la ARC. Así, en el considerando 28 de la Propuesta de Reglamento[106] se indica que las empresas que prestan servicios bancarios y financieros, entre otras, «deben aceptar el uso de las carteras de identidad digital europea para la prestación de servicios en los casos en los que la legislación nacional, el Derecho de la Unión o una obligación contractual requieran una autenticación reforzada de los usuarios». Se trata, por tanto, de promover el uso de la identidad electrónica y las soluciones basadas en los servicios de confianza, para contribuir al cumplimiento de los requisitos de autenticación reforzada de cliente en lo relativo al inicio de sesión en cuentas y la iniciación de operaciones de pago.

VI. CONCLUSIONES

La introducción de la autenticación reforzada de cliente, a pesar de las dificultades que ha presentado su aplicación, ha supuesto una mejora en la seguridad de los pagos electrónicos y de otras operaciones que conllevan riesgos de fraude. En particular, al configurarse la autenticación como un procedimiento que incluye no solo la obligación de los PSP de comprobar que se han utilizado las credenciales de seguridad personalizadas sino también la obligación de aplicar mecanismos de supervisión que les permitan detectar operaciones de pago no autorizadas o fraudulentas, permite que la posición de los usuarios se ve claramente mejorada, ya que la prueba de la autenticación (que corresponde al PSP, y esto ya aparecía en la DSP1) ha de referirse necesariamente a ambos aspectos. Resulta igualmente favorable al usuario –sobre todo cuando tiene la condición de consumidor– el régimen de responsabilidad establecido para aquellos casos en los que el PSP no exige la ARC.

No obstante, a la vista de las diversas aclaraciones que ha debido realizar la ABE y a las propuestas de modificación vertidas en su *Opinion* de junio de 2022, podemos concluir que el régimen jurídico de la ARC

---

de los clientes, así como comprobar que las cuentas destino beneficiarias de los pagos no están, o han estado, comprometidas en operaciones no autorizadas».

106. Propuesta de Reglamento por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital, COM (2021) 281 final, Bruselas, 3 de junio de 2021.

está aún en fase de construcción. Cuestiones tales como los elementos de autenticación que pueden configurar cada una de las distintas categorías (conocimiento, posesión e inherencia) –vinculadas a los desarrollos tecnológicos–, el régimen de las exenciones a la aplicación de la ARC –que trata de conciliar la seguridad con la comodidad de los usuarios y con la prestación de servicios de pago innovadores–, y el régimen de responsabilidad aplicable cuando el PSP no exige la ARC en virtud de una exención, con independencia de las soluciones que han tratado de apuntarse en este trabajo, deben ser objeto de aclaración y, en ciertos casos, preverse en las propias disposiciones de la DSP2. Todo ello unido a la necesidad de evitar que los nuevos mecanismos de autenticación puedan provocar la exclusión del mercado de pagos de sectores de la población con menos aptitudes tecnológicas o con mayores dificultades de acceso a las tecnologías. Habrá que esperar a la próxima revisión de la DSP2 (y, en su caso, del Reglamento delegado) para ver en qué medida las cuestiones apuntadas van materializándose, así como a las decisiones jurisprudenciales que vayan adoptándose al respecto.

VII. BIBLIOGRAFÍA

ALAMILLO DOMINGO, I., «Autenticación reforzada y aseguramiento de la identidad del consumidor», en CUENA CASAS – IBÁÑEZ JIMÉNEZ (dirs.): *Perspectiva legal y económica del fenómeno FinTech*, Wolters Kluwer, 2021, pp. 687-708.

CLAROS FERNÁNDEZ, R. A., «Transformación digital y medios de pago: una visión práctica a la luz de la PSD2», en PEREA ORTEGA (dir.): *Estudios sobre Derecho Digital*, Aranzadi, 2021, pp. 155-195.

AUTORIDAD BANCARIA EUROPEA, *Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2)*, EBA/DP/2015/03, 8 December 2015. Disponible en *https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1303936/13129941-7581-4473-a767-52ec002bd00a/EBA-DP-2015-03%20%28RTS%20on%20SCA%20and%20CSC%20under%20PSD2%29.pdf*.

– *Consultation Paper on the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2*, EBA/CP/2016/11, 12 August 2016. *Disponible en https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1652933/9014220a-2bea-414e-964c-aa6a8c38da1f/Consultation%20Paper%20on%20RTS%20and%20ITS%20on%20the%20authorisation%20of%20credit%20institutions%20%28EBA-CP-2016-19%29.pdf*–.

– *Final Report. Draft Regulatory Technical Standards on Strong Customer Authenticantion and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)*, EBA/RTS/2017/02, 23 February 2017.

Disponible en *https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf?retry=1*.

– *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, EBA/OP/2018/4, 13 June 2018. Disponible en *https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf?retry=1*.

– *Directrices sobre requerimientos de comunicación de datos de fraude con arreglo al artículo 96, apartado 6, de la PSD2*, EBA/GL//2018/05, 17 septiembre 2018. Disponible en *https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2352765/501f89bd-78f9-4488-9a0e-38ff27d18ff0/Guidelines%20on%20fraud%20reporting%20%28EBA%20GL-2018-05%29_ES.pdf?retry=1*.

– *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, EBA/OP/2019/06, 21 June 2019. Disponible en *https://www.eba.europa.eu/sites/default/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf*.

– *Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad*, ABE/GL/2019/04, 28 noviembre 2019. Disponible en *https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2*.

– *Directrices revisadas sobre la notificación de incidentes graves de conformidad con la Directiva de servicios de pago (PSD2)*, ABE/GL/2021/03, 10 de junio de 2021. Disponible en *https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2*.

– *Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry*, EBA/DP/2022/1, 17 January 2022. Disponible en *https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Discussions/2022/Discussion%20Paper%20on%20the%20payment%20fraud%20data%20received%20under%20PSD2/1026061/Discussion%20Paper%20on%20the%20EBA%27s%20preliminary%20observations%20on%20selected%20payment%20fraud%20data%20under%20PSD2%20as%20reported%20by-%20the%20industry.pdf*.

– *Consultation Paper on Draft Regulatory Technical Standars amending the Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliamente and of the Council with regard*

to regulatory technical standards for strong customer authentication and common and secure open standards of communication, EBA/CP/2021/32, 28 October 2021. Disponible en *https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2021/Consultation%20on%20amending%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2/1022909/Consultation%20Paper%20on%20the%20amendment%20of%20the%20RTS%20on%20SCA%26CSC%20under%20PSD2.pdf*.

– *Final Report. Draft Regulatory Technical Standars amending the Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliamente and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication*, EBA/RTS/2022/03, 5 April 2022. Disponible en *https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2022/EBA-RTS-2022-03%20RTS%20on%20SCA%26CSC/1029858/Final%20Report%20on%20the%20amendment%20of%20the%20RTS%20on%20SCA%26CSC.pdf*.

– *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, 23 June 2022. Disponible en *https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf*.

CANO PELÁEZ, J. y MONTOLIO CALEAGA, A., «El nuevo régimen jurídico de servicios de pago», en ORTEGA BURGOS (dir.): *Mercados regulados*, Tirant lo Blanch, 2021, pp. 89-110.

GEVA, B., *Bank Collections and payment transactions. A comparative legal analysis*, Oxford University Press, 2011.

ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, 3.ª ed., Civitas, 2019.

LORENTE HOWELL, J. L., «Exenciones de la autenticación reforzada en la Directiva de Servicios de Pago», *Actualidad Jurídica Aranzadi*, n.º 930, 2017.

MARTÍ MIRAVALLS, J., «Banca on-line y responsabilidad por daños: Análisis crítico de la jurisprudencia reciente en materia de phishing engañoso», en SÁNCHEZ CRESPO (coord.): *Fraude electrónico entidades financieras y usuarios de banca. Problemas y soluciones*, Aranzadi, 2011, pp. 215-249.

NABALÓN, I., «La identificación electrónica: redefiniendo las reglas del sector financiero», *Papeles de Economía Española*, n.º 162, 2019, pp. 162-174.

PACHECO JIMÉNEZ, M. N., «Nuevas alternativas de pago online: proveedores de servicio de pago externo en un mercado más tecnológico y seguro», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 49, 2019 (recurso electrónico).

PASTOR SEMPERE, C., «El 'mercado único digital' de los micropagos», en MARTÍ MIRAVALLS (dir.): *Problemas actuales y recurrentes en los mercados financieros. Financiación alternativa, gestión de la información y protección del cliente*, Aranzadi, 2018, pp. 215-242.

PEÑAS MOYANO, M. J., *Régimen jurídico de los servicios de pago en el Derecho español*, Aranzadi, 2020.

PÉREZ GUERRA, M., «Ciberdelitos y responsabilidad civil de las entidades financieras a la luz de la jurisprudencia», *Revista de Derecho del Mercado de Valores*, n.º 29, 2021, pp. 1-10.

REQUEIJO TORCAL, A., «Derechos y obligaciones en relación con la prestación de servicios de pago», en URÍA FERNÁNDEZ – CARPINTERO PÉREZ (coords.): *Servicios de pago: adaptación a la Directiva PSD II*, Claves Prácticas Francis Lefebvre, 2018, pp. 85-122.

ROJO ÁLVAREZ-MANZANEDA, R., *La utilización fraudulenta de las tarjetas de pago*, Thomson Reuters Aranzadi, 2011.

RUIZ ESPINOSA, J., «Garantías legales en el pago a distancia con tarjeta efectuado por consumidores», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 60, 2022 (recurso electrónico).

RUIZ MUÑOZ, M., «Obligaciones del proveedor de servicios de pago frente al usuario de los instrumentos de pago (La Directiva y la Ley de servicios de pago, y el Anteproyecto de Ley de Código Mercantil de 2014)», *La Ley Mercantil*, n.º 7, octubre 2014, pp. 1-15.

TAPIA HERMIDA, A. J., «La Segunda Directiva de Servicios de Pago», *Revista Estabilidad Financiera* (Banco de España, Eurosistema), n.º 35, 2018, pp. 57-80.

– «La regulación de los servicios de pago por el Real Decreto-ley 19/2018, de 23 de noviembre. Una visión panorámica», *Revista de Derecho Bancario y Bursátil*, n.º 155, 2019, pp. 9-36 (pp. 1-29 versión web).