Centro de Estudios de Consumo

PUBLICACIONES JURÍDICAS
http://centrodeestudiosdeconsumo.com

DIRECTIVA DE SERVICIOS DE PAGO II, ¿TOTALMENTE SEGURA? EL REGLAMENTO DELEGADO (UE) 2018/389 A EXAMEN

Mikael Leal Coronado*
Doctorando en Derecho Civil
Universidad de Castilla-La Mancha

Fecha de publicación: 24 de junio de 2018

1. INTRODUCCIÓN

Tras unos meses desde la completa derogación de la Directiva 2007/64/CE[1], conocida comúnmente como DSP I, y de la adopción de la nueva Directiva 2015/2366[2], sobre servicios de pago en el mercado interior, denominada DSP II como sucesora de la anterior, numerosos artículos y noticias han surgido en el ámbito de los medios de pago tratando de establecer la repercusión e impacto que ésta tendrá en el terreno de los pagos, e indudablemente en la protección de consumidores y usuarios que se hallan sumidos en este cambio de paradigma al ecosistema digital.

Varios han sido los aspectos destacables[3] de esta segunda Directiva, que ha supuesto una revolución en el sistema de pagos a nivel europeo, en pro de un Mercado Único Digital y de una completa armonización del marco normativo en un escenario en constante movimiento. Pero, sin duda, uno de los puntos de mayor preocupación viene referido al problema de la seguridad, pues el mero hecho de tener que introducir las claves o contraseñas de Banca online en una determinada pasarela de pagos supone una barrera, para muchos, todavía por saltar. Se hace necesario desarrollar los mecanismos oportunos para lograr una correcta identificación de los consumidores, combatir el fraude online y proteger la confidencialidad de los datos bancarios de clientes, especialmente en el ámbito de los pagos electrónicos.

Ello se pretende conseguir a través del Reglamento Delegado (UE) 2018/389[4] de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE)

* ORCID ID: 0000-0001-8055-3518
[1] DOUE núm. 319, de 5 de diciembre de 2007.
[2] DOUE núm. 337, de 23 de diciembre de 2015.
[3] Para un estudio más completo sobre sus aspectos destacables: PACHECO JIMÉNEZ, Mª. N.: "Novedades importantes que nos trae el 2018 en materia de servicios de pago: la transposición de la DSP II y las transferencias instantáneas", en *Centro de Estudios de Consumo* [online], 2018. Disponible en: http://centrodeestudiosdeconsumo.com/images/Novedades_2018_en_servicios_de_pago.pdf
[4] DOUE núm. 69, de 13 de marzo de 2018.

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. El mismo será examinado con detalle en los epígrafes posteriores, analizando las medidas introducidas como refuerzo a la autenticación del cliente y para un mayor nivel de seguridad en los pagos de bienes y servicios en Europa, de cara a la completa aplicación de la DSP II.

2. SEGURIDAD EN EL ÁMBITO DE LOS PAGOS ELECTRÓNICOS. ESTADO DE LA CUESTIÓN

Es patente que los riesgos de seguridad de los pagos electrónicos han ido aumentando en los últimos años debido a la cada vez mayor complejidad técnica de estos, al continuo incremento del volumen de dichos pagos a nivel mundial y a los nuevos modelos de servicios de pago, como se hace constar en el Considerando 7 DSP II. Partiendo de esta premisa, es condición básica para el correcto funcionamiento del mercado de los referidos servicios disponer de medios de pago fiables y seguros. Ello redundará en una adecuada protección frente a los riesgos a los que se exponen los usuarios, pues no hay que olvidar que "los servicios de pago son esenciales para el mantenimiento de actividades económicas y sociales de vital importancia", como sigue estableciendo el Considerando 7 DSP II.

De esta forma se podrá contribuir al desarrollo continuado de un mercado único integrado de pagos electrónicos seguros, el cual se torna "esencial para apoyar el crecimiento de la economía de la Unión y para garantizar que los consumidores, los comerciantes y las empresas en general disfruten de posibilidades de elección y condiciones de transparencia en los servicios de pago, de modo que puedan aprovechar plenamente las ventajas del mercado interior", de conformidad con el Considerando 5 DSP II. Así, resulta de gran importancia la obligación de preservar la seguridad de las credenciales personalizadas para asegurar la protección de los fondos del usuario de servicios de pago y reducir los riesgos de fraude y acceso no autorizado a las distintas cuentas de pago (Considerando 69 DSP II).

El problema se acrecienta cuando el pago se ejecuta a través de proveedores de servicios de pago de terceros, como los servicios de iniciación de pagos[5] y de información sobre

[5] Los servicios de iniciación de pagos son aquellos que permiten *"iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago"* (*ex* art. 4.15 DSP II), desempeñando, por tanto, "una función en el comercio electrónico al proporcionar un soporte lógico que sirve de puente entre el sitio web del comerciante y la plataforma bancaria en línea del proveedor de servicios de pago gestor de cuenta del ordenante, con el fin de iniciar pagos por transferencia a través de internet" (Considerando 27 DSP II).

cuentas[6], introducidos en la nueva DSP II, a través de los cuales proveedores de terceros tendrán acceso a ciertos datos bancarios de clientes. Los Bancos tradicionales tendrán que permitir el acceso de dichos proveedores a las cuentas de sus clientes -en caso de que se haya dado el oportuno consentimiento por parte de los mismos-, ya sea para consultar la información sobre sus cuentas y productos bancarios, ya sea para realizar pagos, sin que haya necesidad de formalizar un contrato entre el Banco y el proveedor de servicios[7].

En este contexto la DSP II facultó a la Comisión para la adopción de normas técnicas de regulación (RTS[8]), teniendo como base el proyecto presentado por la Autoridad Bancaria Europea (ABE)[9]. Así se observa en el Considerando 107 DSP II, al establecer que, para garantizar una aplicación coherente de la misma, "la Comisión debe poder confiar en los conocimientos y el apoyo de la ABE, que debe tener la responsabilidad de elaborar directrices y preparar proyectos de normas técnicas de regulación sobre aspectos de seguridad de los servicios de pago, en particular en relación con la autenticación reforzada de clientes […]. La Comisión debe estar facultada para adoptar esos proyectos de normas técnicas de regulación".

Mención expresa a estas normas técnicas de regulación sobre autenticación y comunicación se hace en el art. 98 de la DSP II, al disponer en su apartado 1 que la ABE se encargará de elaborar proyectos de normas técnicas de regulación dirigidas a los proveedores de servicios de pago del art. 1.1 de la DSP II. En ellas habrá de especificar, entre otros: las condiciones de autenticación reforzada de clientes; las exenciones para su aplicación; los requisitos de las medidas de seguridad para proteger la confidencialidad e integridad de las credenciales personalizadas de los usuarios; los requerimientos para unos estándares de comunicación abiertos, comunes y seguros a fin de una correcta identificación, autenticación, notificación e información; además de medidas de seguridad entre proveedores de servicios de pago gestores de cuenta[10], proveedores de servicios de iniciación de pagos, proveedores de servicios de información sobre cuentas, ordenantes, beneficiarios y demás proveedores de servicios de pago.

---

[6] Los servicios de información sobre cuentas son aquellos servicios *"en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago"* (*ex* art. 4.16 DSP II); accediendo a esa información "mediante interfaces en línea del proveedor del servicio de pago gestor de cuenta, lo que permite al usuario del servicio de pago tener en todo momento una visión global e inmediata de su situación financiera" (Considerando 28 DSP II).

[7] PACHECO JIMÉNEZ, Mª. N.: "Novedades importantes que nos trae el 2018 en materia de servicios de pago…", *op. cit*., p. 5.

[8] RTS, por sus siglas en inglés: *Regulatory Technical Standards.*

[9] *Vid.* http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm (Consultado 17/06/2018)

[10] Un proveedor de servicios de pago gestor de cuenta es *"un proveedor de servicios de pago que facilita a un ordenante una o varias cuentas de pago y se encarga de su mantenimiento"*, atendiendo a la definición dada en el art. 4.17 DSP II.

Y todo ello con las siguientes finalidades: *"a) garantizar un nivel adecuado de seguridad para los usuarios de servicios de pago y los proveedores de servicios de pago, mediante el establecimiento de requisitos eficaces y basados en el riesgo; b) garantizar la protección de los fondos y los datos personales de los usuarios de servicios de pago; c) asegurar y mantener una competencia justa entre todos los proveedores de servicios de pago; d) garantizar la neutralidad tecnológica y del modelo de negocio; e) permitir el desarrollo de medios de pago accesibles, de fácil uso e innovadores"*, según se establece en el apartado 2 del mencionado artículo 98 DSP II.

Sumado a lo anterior, estas medidas de seguridad deben ser compatibles y proporcionales al nivel de riesgo que conlleva el concreto servicio de pago, utilizando adecuadamente las credenciales de seguridad. De esta forma se limitarán los riesgos de captación de datos a través de suplantación de identidad u otras actividades fraudulentas, además de adoptarse medidas que protejan la confidencialidad e integridad de sus credenciales (Considerando 96 DSP II). Por esta razón, la ABE tiene que evaluar la extensión de la privacidad, detectando los riesgos asociados para cada una de las modalidades técnicas disponibles, así como las soluciones que se podrían acordar para reducir las amenazas en la protección de datos, como señala el Considerando 94 DSP II.

Estas normas técnicas de regulación se han plasmado en el Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017. Las medidas de seguridad contenidas en este Reglamento se derivan de dos objetivos clave de la DSP II, a saber: otorgar más protección al consumidor, lo cual se logrará mejorando el nivel de seguridad de los pagos y transacciones electrónicas; y aumentar la competencia e igualdad de condiciones en un mercado en constante evolución[11].

Puesto que la DSP II requiere que los proveedores de servicios de pago diseñen e implementen un sistema de autenticación fuerte de clientes, estas normas precisan de una combinación de al menos dos elementos independientes antes de que se efectúe el pago; a la vez que se especifican una serie de requisitos para conseguir normas de comunicación comunes y seguras entre Bancos y firmas de tecnología financiera[12]. A este respecto, las nuevas reglas no permitirán el acceso a datos de los clientes a través del "*screenscraping*[13]", sino que los Bancos tendrán que aplicar un canal de comunicación que faculte a los proveedores de servicios de pago de terceros a acceder a los datos

[11] *Vid.* http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm (Consultado 17/06/2018).
[12] *Vid.* http://europa.eu/rapid/press-release_IP-17-4928_es.htm (Consultado 17/06/2018).
[13] A través de la técnica del *"screenscraping"*, un tercero puede hacer copia de la información contenida en el sitio web haciéndose pasar por un usuario ordinario; utilizándose en la mayoría de los casos por empresas no bancarias -especializadas en servicios financieros- para tener acceso a los datos de clientes bancarios, siempre que se tenga el permiso de éstos últimos y la empresa se encuentre autorizada o registrada ante la autoridad competente. *Vid*. https://www.bbva.com/es/psd2-acceso-datos-clientes-punto-mira/ (Consultado 18/06/2018).

necesarios para prestar el servicio, permitiendo identificarse entre sí y comunicarse por medio de mensajes seguros en cualquier momento[14].

3. REGLAMENTO DELEGADO (UE) 2018/389

3.1. Contextualización

Una vez establecido el marco general en materia de seguridad, cabe centrarse ahora en las concretas medidas dispensadas en el Reglamento Delegado (UE) 2018/389[15], por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, en lo concerniente a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicaciones abiertos, comunes y seguros (en adelante Reglamento).

Partiendo de lo anterior, y atendiendo a la necesidad de que los servicios de pago electrónicos han de prestarse con la adecuada protección y adopción de tecnologías que permitan una autenticación segura, minimizando así el riesgo de fraude, resulta "necesario precisar los requisitos de autenticación reforzada[16] de clientes que deben aplicarse cada vez que un ordenante acceda a su cuenta de pago en línea, inicie una operación de pago electrónico o lleve a cabo mediante un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos". Es más, esa autenticación ha de incluir mecanismos de supervisión para poder detectar intentos de utilización de las credenciales de seguridad, y debe aseverar que quien se dispone a emplear el servicio de pago es su usuario legítimo y da consentimiento a la transferencia de fondos y el acceso a su información, como señala el Considerando 1 del Reglamento.

Con ese fin, y en concreto para reducir el riesgo de que los elementos que posibilitan la aplicación de una correcta autenticación reforzada de clientes sean revelados, divulgados a terceros no autorizados y utilizados por ellos, es imprescindible exigir características de seguridad que sean adecuadas "para los elementos de autenticación reforzada de clientes categorizados como conocimiento (algo que solo conoce el usuario), como la duración o la complejidad, para los elementos categorizados como posesión (algo que solo posee el usuario), como especificaciones algorítmicas, longitud de la clave y entropía de la información, y para los dispositivos y programas informáticos que leen los elementos

[14] *Vid.* http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm (Consultado 18/06/2018).
[15] Basado en los proyectos de normas técnicas de regulación que fueron presentados por la Autoridad Bancaria Europea a la Comisión (Considerando 29 Reglamento).
[16] La autenticación reforzada de clientes ya es definida en el artículo 4.30 DSP II 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"*.

categorizados como inherencia (algo que es el usuario), como especificaciones algorítmicas, sensores biométricos o elementos de protección de plantilla". Así se desprende del Considerando 6 del Reglamento, que continúa afirmando la obligatoriedad de garantizar la independencia de cada uno de estos elementos para evitar que la vulneración de uno de ellos comprometa la fiabilidad de los demás.

No hay que olvidar que los requisitos de autenticación reforzada de clientes deben posibilitar la innovación en las diferentes soluciones tecnológicas para hacer frente a la aparición de nuevas amenazas en la seguridad de los pagos online (Considerando 2 Reglamento). A esto se añade la obligación de "introducir requisitos relativos a la creación y entrega seguras de las credenciales de seguridad personalizadas y su asociación con el usuario de los servicios de pago, además de fijar las condiciones para la renovación y la desactivación de dichas credenciales". Y ello porque las medidas de seguridad que protegen la confidencialidad y la integridad de las credenciales, además de los dispositivos y programas informáticos de autenticación, tienen que limitar los riesgos de fraude que eventualmente se puedan producir por medio de un uso o acceso no autorizado o fraudulento de instrumentos y cuentas de pago, como se hace constar en el Considerando 18 del Reglamento.

Por último, es esencial garantizar una comunicación eficaz y segura entre las distintas partes, siendo necesario "especificar los requisitos que todos los proveedores de servicios de pago pertinentes deben cumplir para alcanzar unos estándares de comunicación abiertos comunes y seguros" (Considerando 19 Reglamento).

3.2. Aspectos destacables del Reglamento

Ahondando en el estudio del Reglamento, y tras haber reseñado sus consideraciones más relevantes, conviene remarcar el objeto propuesto en su art. 1, esto es, el establecimiento de requisitos que deben cumplir los proveedores de servicios de pago en la aplicación de medidas de seguridad para:

- *"aplicar el procedimiento de autenticación reforzada de clientes […]";*

- *"eximir de la aplicación de los requisitos de seguridad de la autenticación reforzada de clientes, bajo determinadas condiciones limitadas y basadas en el nivel de riesgo, el importe de la operación de pago y la frecuencia con que se repite, y el canal de pago empleado para la ejecución de dicha operación";*

- *"proteger la confidencialidad y la integridad de las credenciales de seguridad personalizadas del usuario de servicios de pago";*

- *"establecer estándares abiertos comunes y seguros para la comunicación entre los proveedores de servicios de pago gestores de cuenta, los proveedores de servicios de*

> *iniciación de pagos, los proveedores de servicios de información sobre cuentas, los ordenantes, los beneficiarios y otros proveedores de servicios de pago en relación con la provisión y la utilización de servicios de pago […]".*

A raíz de lo anterior, en cuanto a las medidas de seguridad para la aplicación de la autenticación reforzada de clientes, el art. 4.1 del Reglamento preceptúa que *"la autenticación se basará en dos o más elementos categorizados como conocimiento, posesión e inherencia y tendrá como resultado la generación de un código de autenticación"*, el cual *"únicamente será aceptado por el proveedor de servicios de pago una sola vez cuando el ordenante lo use para acceder a su cuenta de pago en línea, para iniciar una operación de pago electrónico o para llevar a cabo cualquier acción a través de un canal remoto que pueda entrañar un riesgo de fraude en el pago u otros abusos".* Será necesario, además, que se garantice por parte de los proveedores de servicios de pago que de la divulgación del código de autenticación no se pueda derivar información sobre ninguno de los elementos de conocimiento, posesión e inherencia; que no pueda crearse un nuevo código basado en el conocimiento de otro código anterior; y, a su vez, que el código no se pueda falsificar, como se estipula en el art. 4.2 del Reglamento.

Asimismo, los proveedores de servicios de pago, más allá de cumplir los requisitos anteriores, tendrán que satisfacer ciertas medidas de seguridad, establecidas en el art. 5.1 del Reglamento, con base en lo siguiente:

> *"a) que el ordenante sea informado del importe de la operación de pago y del beneficiario;*
>
> *b) que el código de autenticación generado sea específico para el importe y el beneficiario de la operación de pago aceptados por el ordenante al iniciar la operación;*
>
> *c) que el código de autenticación aceptado por el proveedor de servicios de pago se corresponda con el importe específico original de la operación de pago y con la identidad del beneficiario aceptados por el ordenante;*
>
> *d) que cualquier cambio del importe o del beneficiario suponga la invalidación del código de autenticación generado".*

No obstante lo anterior, a lo largo del Capítulo III se señalan una serie de exenciones a la autenticación reforzada de clientes, reguladas pormenorizadamente en los arts. 10 a 18 del Reglamento, y previstas para los siguientes casos: información de cuentas de pago; pagos sin contacto en el punto de venta; terminales no atendidas para tarifas de transporte o pagos de aparcamiento; beneficiarios de confianza; operaciones frecuentes; transferencias de créditos entre cuentas mantenidas por la misma persona física o jurídica; operaciones de escasa cuantía; procesos y protocolos de pago corporativo seguro; así

como análisis del riesgo de la operación; siempre y cuando se den las condiciones establecidas en cada uno de los artículos que regulan las citadas exenciones.

Resulta también relevante la confidencialidad e integridad de las credenciales de seguridad personalizadas de los usuarios de servicios de pago en todas las fases de la autenticación, de manera que los proveedores de dichos servicios, de conformidad con el art. 22.2 del Reglamento, velarán para que *"las credenciales de seguridad personalizadas se enmascaren cuando se muestren y no sean legibles en su totalidad cuando sean introducidas por el usuario de servicios de pago durante la autenticación"*; *"que las credenciales de seguridad personalizadas en formato de datos, así como los materiales criptográficos relacionados con el cifrado de las credenciales de seguridad personalizadas, no sean almacenados en formato de texto común"*; y *"que el material criptográfico secreto quede protegido de una divulgación no autorizada"*.

Igualmente, será indispensable que solo el usuario del servicio de pago esté asociado de manera fiable con sus credenciales de seguridad, así como con los dispositivos y programas informáticos de autenticación (*ex* art. 24.1 Reglamento), y que la entrega al mismo de credenciales, dispositivos y programas de autenticación se produzca de forma segura. Para ello se tendrán en cuenta los riesgos en relación con su uso no autorizado como consecuencia de su extravío, robo o reproducción (*ex* art. 25.1 Reglamento); así como el cumplimiento de las condiciones establecidas en los arts. 26 y 27 para los casos de renovación, destrucción, desactivación y revocación de las credenciales personalizadas de seguridad.

El último de los aspectos novedosos del presente Reglamento viene referido a los estándares de comunicación abiertos, comunes y seguros, siendo preciso que los proveedores de servicios de pago gestores de cuenta pongan en funcionamiento una interfaz de acceso. Ésta podrá ser específica para la comunicación o bien autorizar el uso por los proveedores de servicios de pago referidos en el art. 30.1 del Reglamento de las interfaces utilizadas para la autenticación o comunicación de los propios usuarios del proveedor de servicios de pago gestor de cuenta (*ex* art. 31 Reglamento). Cualquiera que sea la clase de interfaz, deberá cumplir con una serie de requisitos establecidos en el art. 30.2 del Reglamento:

> *"a) que un proveedor de servicios de iniciación de pagos o un proveedor de servicios de información sobre cuentas pueda dar instrucciones al proveedor de servicios de pago gestor de cuenta para iniciar una autenticación basada en el consentimiento del usuario de servicios de pago;*
>
> *b) que las sesiones de comunicación entre el proveedor de servicios de pago gestor de cuenta, el proveedor de servicios de información sobre cuentas, el proveedor de*

servicios de iniciación de pagos y cualquier usuario de servicios de pago de que se trate se establezcan y mantengan durante todo el proceso de autenticación;

c) que la integridad y la confidencialidad de las credenciales de seguridad personalizadas y de los códigos de autenticación transmitidos por el proveedor de servicios de iniciación de pagos o el proveedor de servicios de información sobre cuentas, o a través de ellos, estén garantizadas".

Por lo que se refiere a la seguridad de las sesiones de comunicación, resulta interesante la exigencia de fijar un cifrado seguro entre las partes durante el tiempo de estas sesiones, en las que hay un intercambio de datos a través de Internet, con el objetivo de proteger la confidencialidad y la integridad de los mismos. Con esa finalidad se recaban técnicas de cifrado reforzadas y considerablemente reconocidas, velando por ello proveedores de servicios de pago gestores de cuenta, proveedores de servicios de pago que emitan instrumentos de pago basados en tarjetas, proveedores de servicios de información sobre cuentas y proveedores de servicios de iniciación de pagos, de conformidad con lo establecido en el art. 35.1 del Reglamento.

Para dar cumplimiento a éstas y al resto de novedades recogidas a lo largo del articulado del presente Reglamento, y según se dispone en su art. 38.2, éste será de aplicación a partir del 14 de septiembre de 2019, sin perjuicio del artículo 30 apartados 3 y 5, que serán de aplicación a partir del 14 de marzo de 2019 (*ex* art. 38.3 Reglamento), siendo obligatorio en todos sus elementos y de directa aplicación en cada Estado Miembro.

Con este espacio de tiempo concedido hasta su completa aplicación, se prevé que los Bancos y las distintas firmas de tecnología financiera tengan tiempo suficiente para adaptarse y ajustarse a las normas técnicas instituidas en materia de seguridad[17].

4. CONCLUSIONES

Tras el análisis llevado a cabo como consecuencia del nuevo Reglamento Delegado 2018/389, que viene a completar la Directiva 2015/2366 sobre servicios de pago en el mercado interior, y que encuentra plena alineación con los objetivos establecidos en la misma, resulta ineludible la mejora en la protección del consumidor. Ésta se alcanza a través del fortalecimiento de la seguridad en Internet, y específicamente en el contexto de los pagos electrónicos, permitiendo realizar pagos y transacciones online en entornos seguros que minimicen la posibilidad de sufrir riesgos innecesarios, gracias a los estrictos requisitos que deberán implementar y llevar a cabo los proveedores de servicios de pago.

[17] *Vid.* https://www.bbva.com/es/psd2-europa-aprueba-mayor-seguridad-pagos/ (Consultado 20/06/2018).

Pero, además, supondrá un progreso en la competencia de un sector en constante desarrollo, que a su vez conducirá a la expansión del Mercado Único Digital a escala de la Unión cada vez más eficaz, transparente e inteligente. Ello redundará en una mejor experiencia de consumidores y usuarios de servicios de pago y, a su vez, en mayores oportunidades de negocio e igualdad para Bancos y empresas de tecnología financiera, teniendo como sustento una base firme en materia de medidas de seguridad.

Es pronto para considerar la evolución de estas normas técnicas de regulación recogidas en el nuevo Reglamento, y más todavía cuando nos encontramos en un período transitorio hasta su completa aplicación en septiembre de 2019 y seguimos a la espera de la transposición de la DSP II al ordenamiento jurídico español. En cualquier caso, con estas nuevas normas cada vez estamos más cerca de un marco normativo completo y adecuado a la presente realidad tecnológica que estamos viviendo; lo que no quiere decir que haya que despistarse ni confiarse, pues, en materia de seguridad, nunca podemos estar seguros, valga la redundancia.