LIBRO BLANCO DE REGTECH

La industria RegTech española y su marco regulatorio

Junio 2022

Con la colaboración de

CUATRECASAS

Con el patrocinio de

cecabank

ASOCIACIÓN ESPAÑOLA FINTECH e INSURTECH

Con la colaboración de

CUATRECASAS

Con el patrocinio de

cecabank

Agradecimientos

Asociados de Onboarding Digital

ARIADNEXT

Mitek

ADALIA

Smart Biometrik

Alice

BIOMETRIC VOX

uanataca trust service provider

SIL

TALENTOMOBILE

Electronic IDentification

tecalis

FINVERIS

logalty

veridas

Asociados RegTech

camerfirma AN INFOCERT COMPANY

CUSTOMER COMMS

NEOCHECK

regtech

Suade

Junio 2022 · Madrid, España

LIBRO BLANCO REGTECH

Índice

Prólogo de Cuatrecasas

Dentro de la amplitud del ecosistema FinTech, existe un segmento de proveedores de servicios que ha tenido una menor visibilidad hasta el momento: el sector RegTech.

Quizá una de las razones de esta menor visibilidad pueda encontrarse en la heterogeneidad de los servicios y la naturaleza de sus integrantes (desde pequeñas compañías tecnológicas hasta entidades bancarias), a pesar de que todos ellos comparten un mismo propósito esencial: ayudar a las entidades financieras a cumplir puntualmente con sus obligaciones legales de una forma eficiente.

Los servicios RegTech destinados a entidades financieras incluyen, entre otros, la implementación de procesos de identificación de clientes (*know-your-customer*), de prevención del fraude y firma electrónica, así como la generación automatizada de reportes periódicos a las autoridades de supervisión. A través de estos servicios, las entidades financieras pueden mejorar sustancialmente la eficiencia de procesos que tradicionalmente se han percibido como meros centros de coste, así como beneficiarse de herramientas para la creación de valor, la adopción de decisiones mejor informadas y la implementación de una cultura preventiva en la gestión de riesgos.

Al colaborar con las entidades financieras en la generación de reportes de información periódica cada vez más complejos, las entidades RegTech pueden contribuir a que las autoridades de supervisión reciban puntualmente información precisa y completa sobre el sector financiero, contribuyendo a una mejor supervisión del mismo.

Los clientes de las entidades financieras también pueden resultar, indirectamente, beneficiarios de los servicios RegTech, dado que éstos mejoran la experiencia de usuario mediante la puesta en práctica de procedimientos ágiles y sencillos de alta e identificación de clientes o de firma de documentación a través de medios electrónicos.

Precisamente por la relevancia que todos estos servicios tienen ya en el sector financiero en su conjunto, las entidades RegTech merecen tener visibilidad y voz de manera autónoma, siendo éste el principal objeto de este Libro Blanco.

En este sentido, además de transmitir las inquietudes y propuestas de mejora del sector RegTech, este Libro Blanco pretende aportar mayor luz sobre el impacto estructural que pueden tener las soluciones RegTech en el negocio de las entidades financieras, más allá de la mejora de la eficiencia operativa y el ahorro de costes.

CUATRECASAS

Miguel Sánchez Monjo y Héctor Bros
Socios de Cuatrecasas

BIENVENIDA de Rodrigo García de la Cruz

La industria financiera es uno de los sectores más regulados que hay en Europa y, particularmente, en España. Esta regulación trae consigo, seguridad, protección y confianza para el usuario financiero y gracias a ella las entidades financieras, tanto las tradicionales como las novedosas FinTechs, ganan reputación, notoriedad y buena imagen dentro del imaginario colectivo de la población española.

Desde la AEFI siempre hemos apoyado la necesidad de regulación y supervisión que protejan y empoderen al sector y la creación de marcos de actuación que generen nuevas oportunidades a la innovación en general y al ecosistema FinTech en particular. Por ejemplo, la AEFI ha sido el actor más activo en la puesta en marcha del *Sandbox* Regulatorio Español, de la correcta implantación de la PSD2 o de la llegada de las Leyes Crea y Crece y la de Fomento del ecosistema de las empresas emergentes, más conocida como Ley de *Startups*.

Con este objetivo de llegada a los legisladores, reguladores y supervisores, la asociación ha materializado las necesidades, barreras y reivindicaciones a lo largo de 7 Libros Blancos que han sido presentados y puestos a disposición del público contribuyendo a la divulgación de nuestro ecosistema.

Comenzamos en 2017 con la publicación del Libro Blanco de FinTech, hicimos pública la necesidad de crear un *Sandbox* Regulatorio Español mediante la presentación de un documento concienzudo que sirvió, entre 2017 y 2018, para que el Gobierno entendiera la importancia de esta iniciativa. En 2018, lanzamos una Guía de Buenas Prácticas en el sector para fortalecer la buena imagen de nuestros asociados. El Libro Blanco de InsurTech fue publicado en 2019 de la mano de la Dirección General de Seguros y Fondos de Pensiones. Un mes antes de que comenzara la pandemia, en 2020, la CNMV colaboró con nosotros en la presentación del Libro Blanco de WealthTech. Y durante el 2020, viendo la eclosión que había tenido el sector de los pagos, redactamos el Libro Blanco de PayTech junto a Banco de España. En el primer trimestre de 2022, el Libro Blanco de *Lending Online* vio la luz para hacer énfasis en un sector absolutamente necesario para cubrir las necesidades de los ciudadanos.

En junio de 2022, tenemos el placer de compartir un octavo documento, el Libro Blanco de RegTech, redactado por nuestro colaborador Cuatrecasas y alimentado por los asociados de las verticales de RegTech y *Onboarding* Digital de la AEFI, y con las aportaciones y patrocinio de Cecabank.

Este documento visibiliza cómo ha proliferado el sector RegTech en España, uno de los más complejos e intensivos en regulación, pero también uno de los más necesarios e innovadores. Este sector se está convirtiendo en un el compañero de viaje perfecto para cumplir con toda la normativa, legislación y necesidades legales que les son exigidas a las empresas de la industria financiera en general y a las FinTechs en particular.

Este Libro Blanco es el primer documento, tanto a nivel nacional como europeo, que refleja la realidad de un sector muy potente en nuestro entorno de la Unión Europea y que muestra cuál es la situación real de las empresas españolas ante las diversas situaciones que encorsetan los comportamientos de las RegTechs. Este sector debe ser apoyado y aupado por la industria financiera, los reguladores, legisladores y supervisores porque es de básica necesidad para que la transformación digital sea un hecho consolidado y seguro para todos los actores. Desde la AEFI, creemos firmemente en los espacios colaborativos y cooperativos y mediante la publicación de este libro tendemos puentes que se dirijan a esos entornos favorables.

Este Libro Blanco tienes tres objetivos principales:

1. La visibilidad de un sector, el de RegTech, que contribuye a la correcta ejecución del cumplimiento normativo en la industria financiera. Este sector demuestra cómo la transformación tecnológica supone un paso absolutamente beneficioso para la protección de los usuarios financieros, bien sean empresas o particulares.

2. El análisis y estudios de los marcos regulatorios que afecta a este sector, las barreras que encuentran a la hora de desarrollar bien su trabajo.

3. La propuesta de mejora de las dificultades regulatorias, de arranque y desarrollo para las empresas que se dedican a ayudar a las entidades financieras a cumplir con la regulación.

El contenido de este Libro Blanco realiza una perfecta fotografía de la visión general del sector RegTech, desde sus orígenes hasta el panorama nacional e internacional del sector. También clasifica todos los modelos de negocio que conforman el sector con el objetivo de que el lector encuentre nuevas oportunidades en este entorno. Otro bloque fundamental es el marco regulatorio del que dependen las RegTechs y las barreras y dificultades que encuentran. Por último y en línea con todos los Libros Blancos de la AEFI, se presentan una serie de propuestas para la mejorar del entorno y medidas que, sin duda, contribuirán a que España se posicione como experto y líder ante nuestros vecinos europeos.

Por último, me gustaría transmitir mi sincero agradecimiento a todas las personas que han trabajado de forma constante en este documento; gracias a este equipo se ha logrado un libro revelador y útil para entender mejor al sector de la financiación alternativa.

Un agradecimiento al patrocinador de nuestra iniciativa, Cecabank, y a todo su equipo humano que ha contribuido a que este documento salga a la luz, en especial a Julio César Fernández, Director de la División Desarrollo de Negocio y Soporte Operativo y a Massimo Salerno, Director de la División de Servicios de Tesorería, Riesgos y *Reporting*.

Este documento no habría sido posible sin nuestro magnífico equipo redactor de Cuatrecasas, Héctor Bros y Miguel Sánchez Monjo, socios del despacho, y Claudia Morgado, abogada especialista en IT.

Y por supuesto, a Leyre Celdrán y Kassandra Hernández, el auténtico motor de la AEFI que ha conseguido unir a los principales *stakeholders* del sector para crear entre todos este documento único.

Animo al lector a que conozca a este sector de cerca y que visualice cómo desde el ecosistema FinTech, las empresas que lo componen realizan una función fundamental para mejorar e impulsar la notoriedad, visibilidad y buenas prácticas de toda la industria financiera. Bienvenidos al Libro Blanco de RegTech.

Rodrigo García de la Cruz
Presidente
Asociación Española de FinTech e InsurTech

1. INTRODUCCIÓN

El presente Libro Blanco ofrece una visión general del estado actual del ecosistema RegTech en España, así como de los retos y oportunidades que se presentan para dicho sector, atendiendo especialmente a la aceleración de la digitalización empresarial potenciada por la crisis sanitaria del Covid-19 y a la proliferación normativa que atañe a dicho sector de los últimos años.

En primer lugar, el Libro Blanco realiza una breve descripción del origen del RegTech y su estado actual, indaga sobre el significado del término RegTech y expone la categorización de las distintas áreas que lo integran.

Seguidamente, hace un breve repaso del marco regulatorio actual en el que se enmarca y las principales leyes que han motivado el nacimiento, consolidación y posterior expansión del sector.

Finalmente, expone las barreras normativas y las principales inquietudes del sector, todo ello con el propósito de, por un lado, definir un conjunto de recomendaciones dirigidas a lograr posibles mejoras que contribuyan al desarrollo y crecimiento de la industria RegTech en nuestro país, y, por otro lado, generar una mayor visibilidad, confianza y consciencia de su importancia para el tráfico económico en la era digital.

2. VISIÓN GENERAL DEL SECTOR REGTECH

2.1. RegTech: concepto y alcance

El neologismo RegTech proviene de la combinación de los términos ingleses *regulation* y *technology* y se refiere a la aplicación de innovaciones tecnológicas para dar respuesta a las obligaciones de cumplimiento normativo a las que están sujetas un amplío abanico de sociedades, sobre todo del sector financiero[1].

En este sentido, el RegTech constituye un conglomerado de empresas que suscitan interés de los reguladores, bancos centrales, y entidades financieras tradicionales, principalmente en materia de consultoría de riesgos y cumplimiento normativo.

En particular, el sector RegTech está formado por sociedades que desarrollan y explotan aplicaciones tecnológicas o herramientas informáticas para facilitar a otras el cumplimiento de sus obligaciones legales y procesos regulados, así como para incrementar la seguridad de las operaciones electrónicas.

Las compañías destinatarias de los servicios RegTech pueden pertenecer a diferentes sectores, si bien este Libro Blanco hará especial énfasis a entidades del sector financiero.

La Autoridad de Conducta Financiera de Reino Unido (*Financial Conduct Authority* o, por sus siglas en inglés, *FCA*) define el sector RegTech como un subconjunto de FinTech que se centra en tecnologías que pueden facilitar el cumplimiento de los requisitos regulatorios de forma más eficiente y eficaz que si se realiza con las capacidades existentes[2] (*FCA* 2016).

Tradicionalmente, la lucha contra el fraude y el blanqueo de capitales y la financiación del terrorismo (*BC/FT*), así como la identificación de clientes, constituyen las principales áreas en la aplicación de soluciones RegTech. Sin embargo, tales aplicaciones van más allá y la optimización en la gestión de los datos con los que opere una empresa se ha convertido en la aplicación más prominente de las herramientas RegTech. En este sentido, las empresas financieras están en pleno proceso de digitalización, lo cual ha supuesto un tsunami de datos relativos a personas, productos, servicios, y procesos de negocio, cuya gestión necesita soluciones específicas y adaptadas a las nuevas circunstancias del sector (Butler y O'Brien 2019).

No existe, como es evidente, un solo tipo de RegTech. Su funcionamiento está sujeto a las diversas áreas regulatorias a las que se pretende dar solución, convirtiéndose en un espacio heterogéneo.

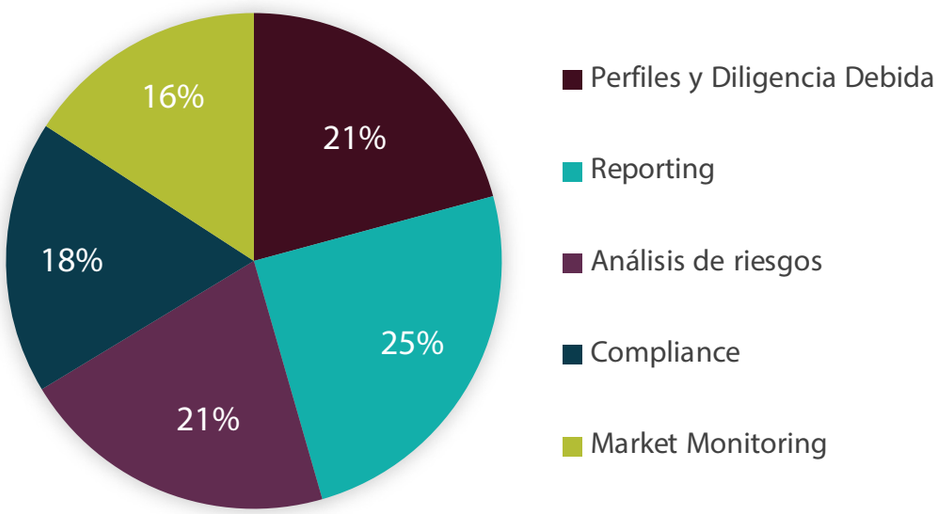
[1] A nivel terminológico, resulta relevante la distinción entre los términos RegTech y Suptech. Este último puede considerarse como la otra cara de la moneda del RegTech, al referirse al uso de aplicaciones de RegTech por las autoridades supervisoras.

[2] En el texto original: "*RegTech is a sub-set of FinTech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities.*".

Según *Thomson Reuters* (*Thomson Reuters Regulatory Intelligence* 2021), el mercado RegTech podría dividirse entre las siguientes áreas: riesgo y gestión del cumplimiento normativo, gestión de identidades, *reporting* a los organismos de supervisión, gestión del fraude e inteligencia regulatoria.

Asimismo, el Centro de Finanzas Alternativas de *Cambridge* (*Cambridge Centre for Alternative Finance*) ha identificado los siguientes segmentos de mercado donde interviene el sector RegTech (Shizas 2019)[3]:

SEGMENTOS DE MERCADO



No obstante, atendiendo a las actividades de los asociados de la AEFI y teniendo en cuenta las particularidades del sector RegTech en España, a los efectos de este Libro Blanco, los subsectores más relevantes pueden clasificarse en las siguientes posibles categorías:

(a) **RegTech de PBC:** servicios relacionados con la aplicación de las medidas previstas en la normativa de prevención de blanqueo de capitales y financiación del terrorismo, aportando soluciones tecnológicas para facilitar la implementación, principalmente, de las medidas de diligencia debida propias de dicha normativa;

[3] Dichos segmentos cubren, en esencia, las siguientes actividades:
(i) **Categorización de perfiles y Diligencia Debida:** la clasificación de diferentes perfiles de clientes en función de su riesgo, sobre la base de las medidas de diligencia debida contempladas en la normativa aplicable en materia de *BC/FT*, es un elemento esencial del día a día de las empresas sujetas a dichas normas.
(ii) ***Reporting:*** recopilar información de fuentes diversas para cumplir con las obligaciones de reporte periódico de las entidades reguladas.
(iii) **Análisis de riesgos:** uso de big data para evaluar el riesgo de fraude, abuso de mercado, BC/FT u otras conductas ilícitas en las transacciones.
(iv) ***Compliance:*** facilitar y supervisar los cambios regulatorios, asegurando que las políticas y controles internos se adaptan en cada momento a la normativa vigente.
(v) ***Market Monitoring:*** uso de datos de diversas fuentes externas para medir los resultados a nivel de mercado a partir de las normas y políticas internas.

(b) **RegTech de Servicios de Confianza y de Prueba Electrónica:** servicios de identificación y firma electrónica y otros servicios de confianza.

(c) **RegTech de Gobierno Corporativo, Gestión de Riesgos y Cumplimiento Normativo**

(d) **RegTech de *Reporting:*** servicios de asistencia, principalmente a las entidades financieras, para dar cumplimiento a las obligaciones de remisión de información periódica a las autoridades de supervisión; y

(e) **Otras RegTech:** servicios de asistencia en el cumplimiento de la regulación de otros ámbitos (por ejemplo, ciberseguridad, prevención del fraude, gestión de comunicaciones electrónicas, etc.).

Las actividades y características de estas cinco categorías de entidades RegTech serán analizadas en mayor detalle en el apartado 3 del presente Libro Blanco.

2.2. Orígenes

Si bien la aparición de algunas entidades del sector RegTech puede situarse a principios del siglo XXI[4], su punto de inflexión tuvo lugar con la proliferación normativa que continuó a la quiebra de *Lehman Brothers* en septiembre de 2008. Dicho proceso de elaboración normativa (conocido como "tsunami regulatorio"), aún en desarrollo, ha incrementado sustancialmente el nivel de regulación del sector financiero, llevando a las entidades financieras a buscar formas eficientes de cumplimiento normativo, incluyendo mediante el uso de tecnología.

En particular, la Unión Europea viene llevando a cabo una importante labor legislativa[5] en ámbitos tales como la lucha contra el fraude y la prevención del *BC/FT*, el reporte sistemático sobre la base de principios de transparencia[6], el impulso en el uso de servicios electrónicos de confianza en las transacciones *online* o el tratamiento de datos biométricos para la autenticación de identidades en el contexto digital[7].

Todo ello ha propiciado el crecimiento del RegTech y su expansión hacia nuevos modelos de negocio dirigidos a facilitar el cumplimiento normativo a una gran diversidad de sectores tales como el financiero, el de los fondos de inversión o el asegurador.

[4] Puede citarse, por ejemplo, el impulso derivado, en este ámbito, de la aprobación por parte de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) de las primeras leyes modelo sobre comercio electrónico (1996) y firma electrónica (2001).

[5] Todas estas menciones a regulaciones de la Unión serán abordadas en mayor detalle en el apartado 4.

[6] Por ejemplo, en materia de instrumentos financieros complejos, los Reglamentos EMIR y SFTR imponen obligaciones de información con respecto a la conclusión de derivados y las llamadas *securities financial transactions*.

[7] Nace igualmente en esta época el concepto de "espacio de pruebas controladas" también conocido como el *sandbox*, que permitirá a las empresas testear mecanismos innovadores en un entorno vivo. El objetivo del espacio *sandbox* es equilibrar la protección de los consumidores y el cumplimiento de las regulaciones.

Mención particular merece el efecto que colateralmente ha tenido, en el uso de la tecnología, la crisis sanitaria del Covid-19. Desde su inicio, y debido al distanciamiento social y a las restricciones a la movilidad, se han puesto en evidencia más que nunca los beneficios, eficiencias y distintos casos de uso del sector RegTech. Se analizará dicho impacto con mayor detalle en el apartado 2.4 siguiente.

2.3. La puesta en valor de los servicios de RegTech

Desde un punto de vista simplista, puede considerase que la actividad de las entidades del sector RegTech está vinculada fundamentalmente a cuestiones de cumplimiento normativo, por ejemplo, análisis y gestión de riesgos, identificación de clientes en el proceso de alta, recopilación de firmas en documentos legales, reporte regulatorio a autoridades, etc. En definitiva, a áreas tratadas tradicionalmente como meros centros de costes administrativos sin más valor que el de asegurar el cumplimiento de la normativa aplicable.

Es cierto que los servicios de las entidades RegTech tienen como uno de sus propósitos la reducción de costes de diversa índole y la mejora de la eficiencia operativa de las entidades. No obstante, tampoco debe ignorarse ni minusvalorar su capacidad tanto para crear valor dentro de las entidades financieras que los utilizan como para promover la transformación del negocio de éstas.

Las entidades financieras tienen identificados, por lo general, los beneficios que pueden ofrecerles las soluciones RegTech, si bien, como se analizará más adelante, aún existe cierto desconocimiento sobre el impacto real que dichas soluciones puede tener el negocio de las entidades, más allá del ahorro de costes y la mejora de la eficiencia.

A continuación, se exponen brevemente los beneficios que pueden ofrecer herramientas tecnológicas proporcionadas por el sector RegTech a las entidades financieras.

2.3.1. Cultura preventiva y gestión de riesgos

Las entidades RegTech ayudan a las entidades financieras en el cumplimiento de sus diferentes obligaciones legales y a mejorar sus procesos de diferente índole. Esto se traduce, en la práctica, en la implementación de medidas encaminadas a reducir el riesgo legal y operativo de las entidades.

En este sentido, los servicios de RegTech pueden ayudar a promover la instauración de una cultura interna dentro de las entidades con un enfoque preventivo más profundo. De ese modo, se consigue generar una mayor consciencia de la importancia de la gestión de riesgos y se obtiene una seguridad a las entidades en lo que respecta al cumplimiento de la normativa.

2.3.2. Mejora de la eficiencia y ahorro de costes

Entre los beneficios esenciales que ofrecen los servicios de RegTech, destacan la mejora de procesos (y la consiguiente eficiencia operativa), así como la reducción de costes. Ambos beneficios se generan

de manera sucesiva: en la medida en que se implementan procesos más eficientes, se consigue un ahorro de costes de diferente naturaleza.

La mejora de la eficiencia deriva principalmente de la estandarización y automatización que conlleva la puesta en práctica de los procesos tecnológicos ofrecidos por las entidades RegTech.

En este sentido, la conversión de procesos manuales en tecnológicos y automáticos permite la reducción de costes de mano de obra, agiliza su desarrollo y reduce el número de errores que puedan producirse. Además, dichos procesos pueden encadenarse unos a otros dentro de las entidades, permitiendo un flujo operativo mucho más integrado dentro de éstas.

De esta forma se incrementa el conocimiento de los órganos de gobierno en cuestión de riesgo y Cumplimiento, permitiendo así una correcta toma de decisiones en los diferentes niveles de la compañía. Ejemplo de esto son las soluciones de GRC que, además de mejorar los sistemas de control interno, permiten la gestión de riesgos, facilitan la trazabilidad y veracidad de la información y la supervisión de las autoridades reguladoras.

Las ventajas de esta integración son múltiples: desde la generación de información importante para la toma de decisiones de negocio (véase siguiente apartado), hasta la detección de origen de posibles incidencias en cualquiera de los pasos del proceso.

De hecho, para la mayoría de los proveedores de servicios de la industria RegTech, la eficiencia y efectividad de procesos gravita sobre el modelo de soluciones *Sofware-as-a-Service* (*SaaS*), esto es, la integración de las soluciones RegTech en los sistemas de las entidades a través de interfaces de programación de aplicaciones (*application programming interfaces*, conocidas como *API*) (EBA 2021).

Entre las diferentes aplicaciones de estas mejoras, puede citarse, por ejemplo, la generación de información para el *reporting* regulatorio a las autoridades de supervisión. La implementación de procesos automatizados puede permitir que la diferente información que se genere dentro de la entidad desde cualquier fuente, alimente directamente los ficheros de reporte que deban remitirse a los reguladores, ahorrando tiempo y costes y evitando errores de traslación de información.

La siguiente figura ilustra un ejemplo de cómo las aplicaciones de RegTech permiten integrar diferentes procesos dentro de una misma entidad aportando valor en cada eslabón de la cadena:

2.3.3. Soporte para decisiones de negocio

Como se indicaba anteriormente, las soluciones ofrecidas por el RegTech pueden también generar valor añadido para las entidades en el marco de su proceso de desarrollo de negocio.

Los (grandes) volúmenes de datos que recopilan y gestionan los procesos de RegTech no sólo sirven para asegurar el cumplimiento de la regulación, sino también para generar información valiosa para la adopción de posibles decisiones con impacto en el negocio y en la cuenta de resultados.

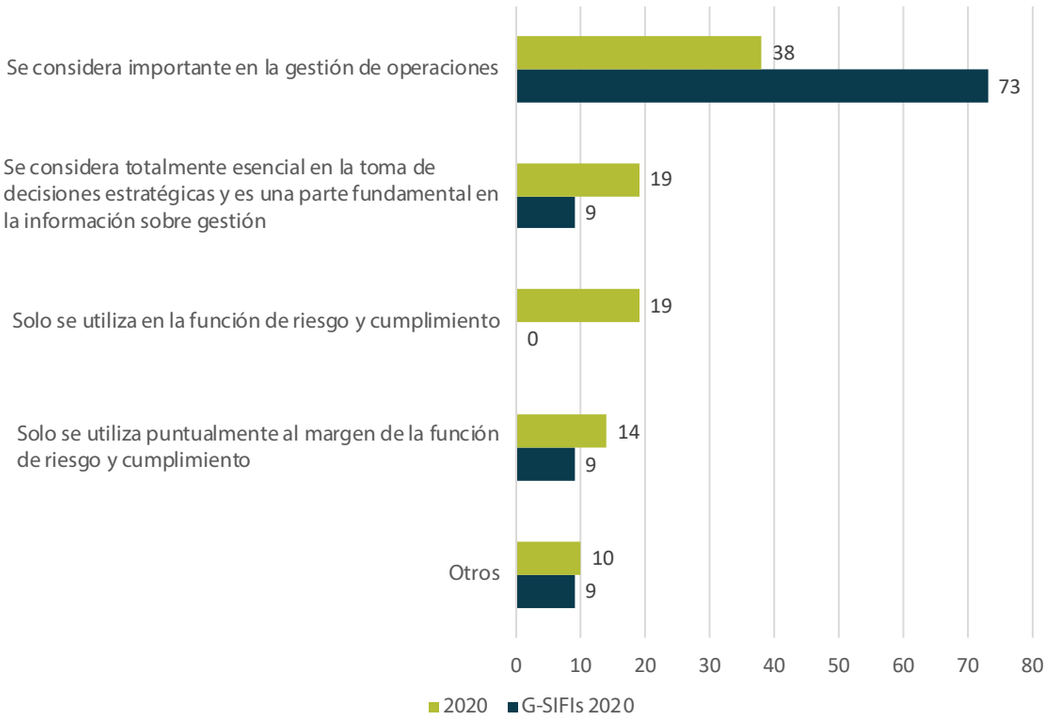
En efecto, los sistemas de RegTech pueden identificar tendencias de comportamiento en los clientes que pueden explotarse por parte de la entidad, así como riesgos no detectados inicialmente (por ejemplo, en materia de prevención del fraude y de *BC/FT*). Además, algunas de las soluciones de RegTech permiten el tratamiento de información en tiempo real, lo que permite tener una imagen más precisa de determinados aspectos de la entidad financiera.

Las plataformas de RegTech son capaces igualmente de generar información adicional para las entidades. Por ejemplo, la sustitución de procesos manuales de identificación y autenticación del cliente por sistemas automatizados y plataformas tecnológicas integradas puede permitir que se solicite a los clientes una valoración del proceso de alta y autenticación, estableciéndose un modelo de *feedback* continuo por parte de los clientes que resulte valioso para la mejora de procesos y la experiencia de usuario.

Además, el tratamiento de información dentro del ámbito de RegTech puede conjugarse también con otras técnicas de gestión y explotación de datos, como el uso de *Big Data* o de *machine learning*, tanto para la corrección de ratios de error como para la generación de nueva información.

A pesar de la importancia y beneficios que lo anterior puede tener para las entidades financieras, aún no existe una percepción clara y extendida entre las entidades de la capacidad que tiene el sector RegTech para apoyar en la definición estratégica del negocio. Así lo refleja la encuesta realizada por *Thomson Reuters* (*Thomson Reuters Regulatory Intelligence* 2021), donde el 73% del grupo de las instituciones de servicios financieros de importancia sistémica (*SIFI*, por sus siglas en inglés) considera las soluciones RegTech importantes para la gestión operativa, si bien sólo el 9% las considera esenciales para la toma de decisiones estratégicas.

¿CUÁL ES EL RESULTADO DEL USO DE REGTECH EN SU EMPRESA?



Fuente: *Thomson Reuters Regulatory Intelligence: Fintech, RegTech and the Role of Compliance in 2021*, redactado por *Susannah Hammond y Mike Cowan*. Disponible en: https://legal.thomsonreuters.com/en/insights/reports/fintech-RegTech-compliance-report-2021.

2.3.4. Adaptación al entorno

En línea con lo descrito en el apartado anterior, y la capacidad del sector RegTech de influir en la estrategia y el negocio de las entidades, cabe destacar también la ayuda que dicho sector puede prestar a las entidades financieras en su adaptación al entorno, así como a las demandas de sus clientes.

El caso paradigmático de esta ayuda es la implementación de procesos electrónicos de alta de clientes (identificación) y contratación a distancia, así como de sustitución del soporte papel en las

comunicaciones con clientes. Más allá de que estos procesos ya venían siendo una demanda tanto del propio entorno socioeconómico (mejora de la sostenibilidad y el ahorro de costes) como de los clientes (por ejemplo, por la forma que tienen los clientes más jóvenes de interactuar con sus entidades financieras totalmente a distancia y electrónica), la crisis sanitaria del Covid-19 ha acelerado su implementación urgente por cuestiones de necesidad, tal y como se expondrá con más detalle en el siguiente apartado.

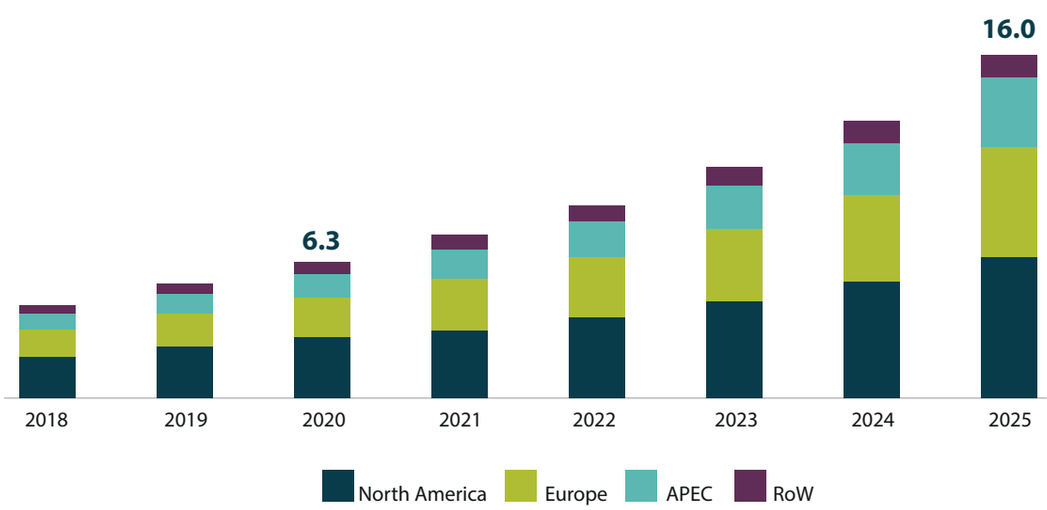
2.4. Estado actual del sector

2.4.1. Panorama internacional y nacional

De acuerdo con un estudio realizado por el Observatorio de Innovación y Tendencias RegTech de *Finnovating* (*Finnovating 2018*), desde 2013, la financiación global en RegTech ha alcanzado cifras que superan los 5 mil millones de dólares.

En el gráfico siguiente, podemos observar una tendencia creciente desde 2018 hasta la actualidad alcanzando cifras en torno a los 6,3 mil millones de dólares en 2020 y un pronóstico que apunta a que en 2025 se haya alcanzado unas cifras que ronden los 16 mil millones de dólares.

REGTECH MARKET, BY REGION (USD BILLION)



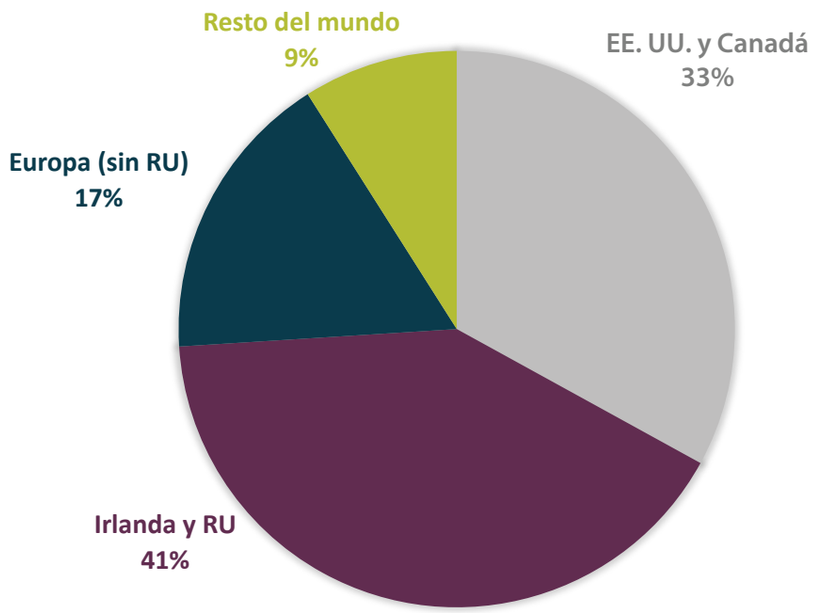
Fuente: *MarketsandMarkets Analysis.* Disponible en: https://www.marketsandmarkets.com/Market-Reports/RegTech-market-63447434.html.

Dichos datos nos llevan a afirmar que el sector RegTech está llamado a crecer significativamente y de forma constante a nivel mundial durante los próximos años. En el gráfico anterior, se categorizan

los países en los siguientes bloques: Norte América, Europa, los países de la coalición económica de Asia-Pacífico (o por sus siglas en inglés, "*APEC*") y los países del resto del mundo (o por sus siglas en inglés, "*RoW*").

En la siguiente figura, además, se observa que el sector tiene una presencia notable en las principales capitales donde el mercado financiero tiene mayor volumen de negocio, tales como Reino Unido e Irlanda (41%), Estados Unidos y Canadá (33%). En Europa, en cambio, el surgimiento de este sector ha sido más tardío, por lo que no extraña que, en 2017, su presencia girase en torno al 17%.

REGTECH EN EL MUNDO POR ZONA GEOGRÁFICA



España, por su parte, no fue pionera en la implantación de RegTech a diferencia de Estados Unidos o Reino Unido. Sin embargo, en los últimos años ha promovido un clima regulatorio favorable para el surgimiento o consolidación de nuevas *startups* orientadas a la prestación de estos servicios y para la transformación o diversificación de muchas empresas que ya existían hacia la vertiente RegTech. De hecho, algunos de los principales *players* en el mercado español surgieron como *spin offs* del sector bancario o asegurador, o mutaron desde la prestación de otra clase de servicios electrónicos hacia el terreno de los servicios RegTech.

En España, además, destaca especialmente la proliferación en los últimos años de *startups* dirigidas a ofrecer al mercado sistemas de firma electrónica o al envío de comunicaciones certificadas que garantizan la integridad y el origen de las transacciones o la verificación y autenticación de identidades de personas por medios electrónicos (es decir, los generalmente denominados como "servicios electrónicos de confianza").

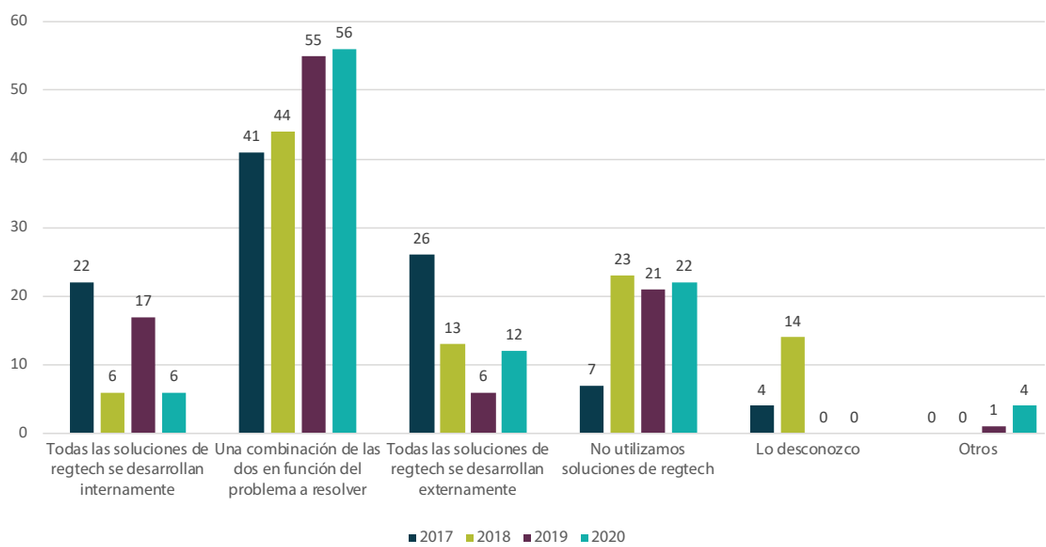
De hecho, en consonancia con lo anterior, la recientemente aprobada Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, enfatiza que España es actualmente el país de la Unión Europea con más prestadores de servicios electrónicos de confianza, tal y como se desprende del listado español de prestadores cualificados (*Trusted Services List o TSL*) del Ministerio de Asuntos Económicos y Transformación Digital[8].

2.4.2. Barreras de entrada

A pesar del crecimiento y consolidación del sector, el ecosistema RegTech se enfrenta a un conjunto notable de barreras de entrada y obstáculos para su evolución.

En este sentido, el siguiente estudio realizado por *Thomson Reuters* durante los años 2017 y 2020 (*Thomson Reuters Regulatory Intelligence 2021*) muestra que no existe un patrón estable respecto a si las soluciones RegTech son mayoritariamente desarrolladas internamente por las empresas o si son encargadas a proveedores externos. Las tendencias durante dichos años han variado y lo que se observa es que, en la mayoría de los casos, las empresas optan cada vez más por confiar en una combinación de las dos vías en función del problema a resolver.

¿DESARROLLA SOLUCIONES DE REGTECH INTERNAMENTE O BUSCA SOLUCIONES EXTERNAS?



Fuente: *Thomson Reuters Regulatory Intelligence: Fintech, RegTech and the Role of Compliance in 2021*, redactado por *Susannah Hammond y Mike Cowan.* Disponible en: https://legal.thomsonreuters.com/en/insights/reports/fintech-RegTech-compliance-report-2021.

[8] Consúltese el listado de prestadores de servicios de confianza inscritos en el Listado del Ministerio de Asuntos Económicos y de Transformación Digital disponible en: https://sede.serviciosmin.gob.es/es-es/firmaelectronica/paginas/Prestadores-de-servicios-electronicos-de-confianza.aspx.

Dicho resultado respalda la teoría de que las soluciones RegTech requieren de un grado elevado de personalización y adaptación concreta a las necesidades de cada empresa. Ello implica que su adopción requiere ciertos tiempos e interacciones entre las partes, lo cual impide en muchos casos que su implementación pueda realizarse de forma ágil, como si de herramientas estandarizadas se tratase.

Por ejemplo, la adopción de sistemas de firma electrónica requiere un tiempo de análisis previo a la implementación, y un periodo razonable de adaptación del personal, especialmente para procurar que todos los usuarios se familiaricen con el proceso y conozcan sus nuevos deberes y responsabilidades. Existen estudios que afirman que la duración media de una implementación de este tipo en empresas pequeñas es de 2,3 meses, en medianas de 5,5 meses y en grandes de hasta 9 meses[9].

Asimismo, los asociados de la AEFI inciden en la problemática que suponen los elevados costes de las tasas de certificación o cualificación que muchos de los proveedores deben asumir para poder acreditar el cumplimiento de los estándares más exigentes. Estos estándares además no siempre son uniformes entre los distintos países, lo cual incrementa más los costes de estas entidades, especialmente si persiguen operar de forma internacional. Según la EBA, la ausencia de armonización entre los distintos Estados Miembros constituye una barrera de entrada en un Mercado Único (EBA 2021).

A lo largo de este libro haremos hincapié en diferentes barreras de entrada y en la forma de superarlas.

2.4.3. El auge del RegTech durante la crisis sanitaria del Covid-19

La crisis sanitaria del Covid-19 ha tenido un impacto positivo en la industria RegTech, principalmente motivado por los siguientes factores:

- Aumento del 20% del uso canales digitales para los servicios financieros entre los usuarios (*Lemerle, Patnaik, Ring, Sayama y Sieberer 2020*).

- Mayor gestión de los riesgos de conducta de los usuarios a través de la integración digital. Rastrear el comportamiento de los clientes y proporcionar una mayor transparencia en los aspectos de interacción digital se ha convertido en un área de crecimiento para este sector.

- Aprobación de normativa de impulso de la digitalización de procesos empresariales. En este sentido, en los últimos 12 meses se han producido más de 1.300 cambios normativos propiciados por los reguladores en relación con la crisis sanitaria del Covid-19 (EBA 2021).

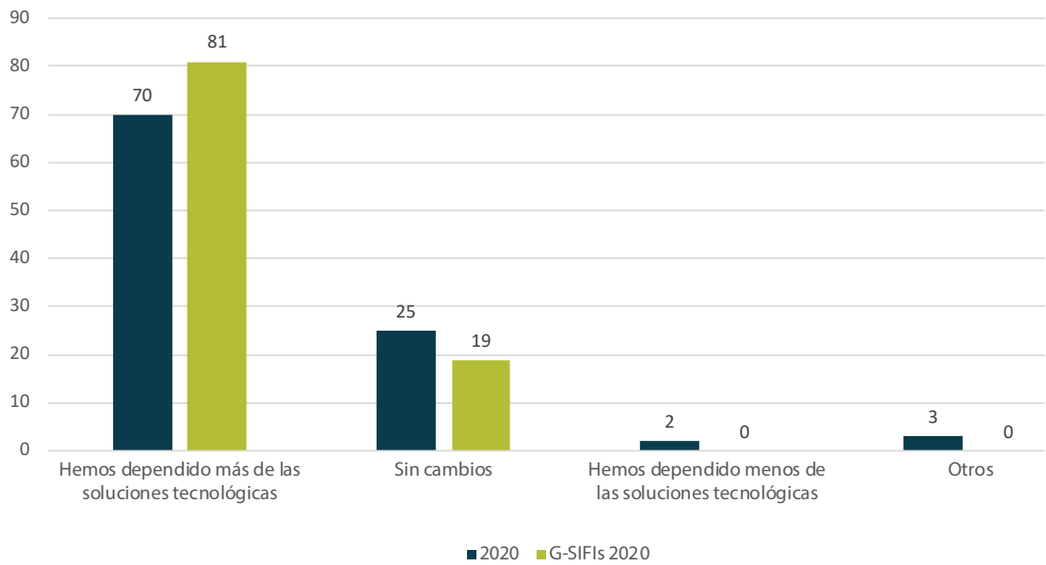
Precisamente, esta crisis sanitaria ha derivado igualmente en un incremento de la confianza en el sector RegTech para mitigar los retos específicos en materia de cumplimiento, y en particular, en lo que se refiere a la vigilancia para evitar el abuso y la manipulación de los mercados. De hecho, en abril del 2020 fue alertado por el Grupo de Acción Financiera Internacional (organismo internacional contra la lucha del Blanqueo de capitales y Financiación del Terrorismo) la exacerbación del fraude

[9] Datos obtenidos de la organización *Finances Online Research* en su publicación titulada "*47 Essential e-Signature Statistics:2020 Market Share Analysis & Data*" accesible en financesonline.com.

y delincuencia financiera, alentando la necesidad de incorporar mayor vigilancia para mitigar estos riesgos resultantes y acrecentados por la pandemia (FATF 2020).

A partir de una encuesta realizada por *Thomson Reuters* (*Thomson Reuters Regulatory Intelligence* 2021), el 81% del grupo SIFI encuestado ha manifestado que en el año 2020 se ha producido un incremento de confianza en soluciones tecnológicas. Por su parte, un 19% no ha experimentado la misma transformación.

¿CÓMO HA AFECTADO A SU EMPRESA LA PANDEMIA POR LA COVID-19 EN CUANTO AL USO DE SOLUCIONES TECNOLÓGICAS?



Fuente: *Thomson Reuters Regulatory Intelligence: Fintech, RegTech and the Role of Compliance in 2021*, redactado por *Susannah Hammond y Mike Cowan*. Disponible en: https://legal.thomsonreuters.com/en/insights/reports/fintech-RegTech-compliance-report-2021.

3. VERTICALES INTEGRANTES DEL SECTOR REGTECH

El sector RegTech constituye un conjunto diverso de entidades dedicadas a servicios de diferente naturaleza. Dichos servicios van desde el desarrollo de herramientas específicas destinadas a funciones de cumplimiento normativo, hasta la prestación de servicios considerados regulados (como es el caso de los servicios electrónicos de confianza).

La oferta de servicios ofrecidos por el sector RegTech es muy amplia y se encuentra en constante evolución. Dicho crecimiento viene motivado por las diferentes innovaciones que surgen en el tiempo, por las nuevas necesidades que tienen las entidades financieras o sus clientes y por las nuevas obligaciones legales que continuamente se introducen en el ordenamiento jurídico.

Tal y como se apuntaba en el apartado 2.1 de este Libro Blanco, pueden distinguirse cinco tipos principales de entidades RegTech:

A continuación, se ofrece una visión general de las distintas categorías que operan en el mercado español.

3.1. RegTech de PBC. Prevención de blanqueo de capitales y financiación del terrorismo

De conformidad con el reciente análisis publicado por la Autoridad Bancaria Europea ("*EBA*", por sus siglas en inglés) en junio de 2021 sobre las entidades RegTech en el sector financiero europeo (*EBA* 2021), el segmento de RegTech más activo en la Unión Europea es el relativo a la prevención de

blanqueo de capitales y financiación del terrorismo ("*PBC* y *FT*"), tanto desde el punto de vista de la demanda de servicios como de su oferta.

En particular, el estudio muestra que, de las entidades RegTech que respondieron a la encuesta realizada por la *EBA*, el 39% de dichas empresas prestaba soluciones de *BC* y *FT*, mientras que una amplia mayoría del 76% de las entidades financieras participantes manifestaron tener experiencia en la contratación de soluciones tecnológicas de *BC* y *FT* ofrecidas por entidades RegTech.

Dentro de estas soluciones, destacan las relativas al desarrollo de medidas de diligencia debida, utilizadas tanto para el proceso de alta de clientes (*onboarding*) como para la monitorización continuada de la información disponible sobre clientes y su operativa.

En ocasiones, los sujetos obligados en materia de *BC* y *FT* suelen quedarse con una visión estática de sus clientes, obtenida al inicio de la relación contractual. Esta imagen, además de poder quedar desactualizada, puede ser incompleta, por ejemplo, como consecuencia de la comisión de errores al recopilar inicialmente la información del cliente, o de una custodia deficiente a lo largo de la vigencia de la relación.

No es extraño, por tanto, que las medidas de diligencia debida desarrolladas por las entidades puedan presentar, en determinados casos, ineficiencias o errores, que quedan de manifiesto en el marco de auditorías externas o de requerimientos e inspecciones de las autoridades competentes de supervisión.

Las entidades del RegTech pueden ayudar a corregir estos procesos mediante la implementación de soluciones tecnológicas (*Software as a Service, SaaS*) integradas con el sistema del sujeto obligado, y accesibles a través de Internet o de interfaces de programación de aplicaciones (*API*). Estas soluciones permiten identificar a los clientes de una forma completa y segura, monitorizar y actualizar dicha información de manera continuada en el tiempo, así como presentar todos estos datos de una manera inmediata a los sujetos obligados.

En este sentido, las entidades RegTech de *PBC* pueden prestar servicios tales como:

- La implementación de medidas de diligencia debida a clientes, a través de mecanismos de video-conferencia o video-identificación, que serán analizados más adelante en el apartado de normativa.

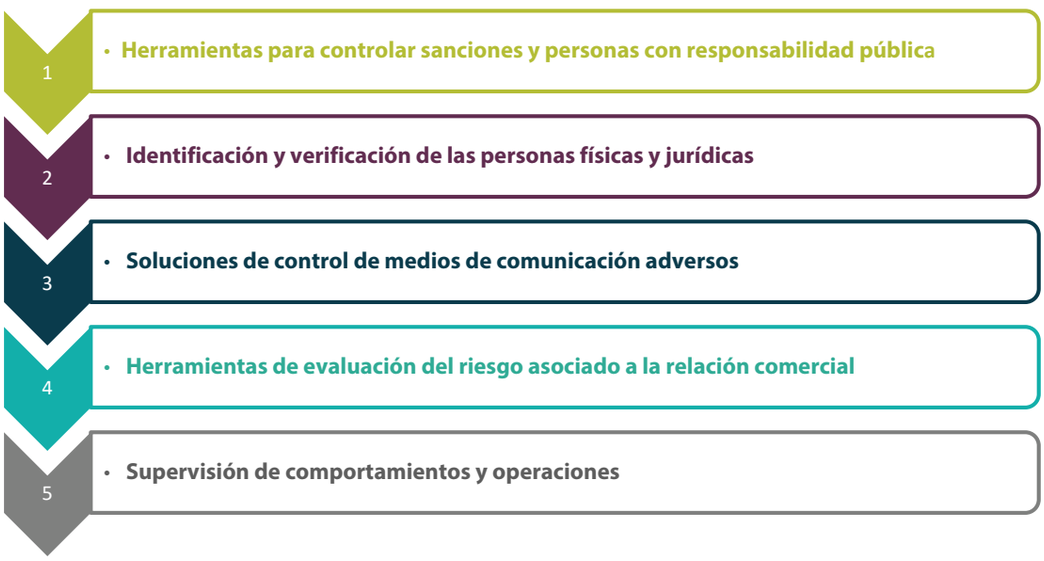
- La recolección de información de clientes en el proceso de alta para su tratamiento y cruce con bases de datos públicas o privadas. Por ejemplo, se utilizan fuentes de noticias para detectar referencias a clientes en investigaciones de orden penal o administrativo, o bien bases de datos para verificar la posible condición del cliente como persona de responsabilidad pública o para identificar otros atributos que podrían llevar a asignarle un perfil de riesgo elevado en materia de *PBC* y *FT*. Asimismo, en este ámbito, se realiza el cruce inicial y periódico de los datos del cliente contra listas oficiales de sanciones y organizaciones y grupos terroristas.

- Análisis y monitorización de transacciones y operaciones realizadas por clientes con el fin de poder identificar indicios o patrones de potenciales actividades sospechosas relacionadas con el

blanqueo de capitales o la financiación del terrorismo, incluyendo la creación, gestión y tratamiento de alertas automáticas.

- La prevención del fraude. Estos servicios pretenden facilitar la implementación de medidas de control interno en el seno de una entidad con el fin de prevenir y mitigar posibles riesgos derivados de la comisión de delitos o fraudes por parte de directivos o empleados de la entidad. En este sentido, destacan las soluciones tecnológicas relativas a la prevención de riesgos penales.

La combinación de estos servicios y herramientas permite resolver una de las debilidades que presentan algunos sujetos obligados en cuanto a la integración y consolidación de información. Las entidades RegTech de *PBC* permiten recopilar, tratar y gestionar de forma agregada toda la información de los clientes y de su operativa, desde su alta en la entidad hasta el cese de la relación de negocio, tal y como se muestra en el siguiente gráfico:



En definitiva, esta categoría de entidades de RegTech pueden ofrecer a sus clientes entidades financieras las siguientes ventajas y beneficios:

- Asegurar y reforzar el cumplimiento de la regulación en materia de PBC y FT.
- Mejorar la gestión de riesgos y de los sistemas de prevención.
- Aumentar la eficiencia y simplificación operativa.
- Mejorar la trazabilidad de la información y de procesos.
- Digitalizar la información y la custodia documental.

3.2. RegTech de Servicios de Confianza. Servicios de identificación y firma electrónica y otros servicios de confianza

3.2.1. Firma electrónica y otros servicios electrónicos de confianza

Los servicios electrónicos de confianza son una categoría amplia de servicios electrónicos regulados en el Reglamento (UE) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE[10](el "**Reglamento eIDAS**") y prestados hoy día en España por un gran número de operadores del sector RegTech.

Son servicios que proporcionan, entre otras muchas ventajas, seguridad y confianza a las transacciones electrónicas y que se consideran parte de los generalmente denominados servicios de la sociedad de la información.

En la siguiente tabla se resumen los tipos y las principales características y finalidades de los principales servicios de confianza:

CREACIÓN, VERIFICACIÓN Y VALIDACIÓN DE FIRMAS ELECTRÓNICAS
Existen tres tipos de firma electrónica: • La firma electrónica básica, cuya definición coincide con la definición general de firma electrónica; • La firma electrónica avanzada, que debe cumplir con los requisitos del artículo 26 del Reglamento eIDAS; y • La firma electrónica cualificada[11]
CREACIÓN, VERIFICACIÓN Y VALIDACIÓN DE SELLOS ELECTRÓNICOS
Los sellos electrónicos sirven para sellar documentos, como contratos u órdenes de pedido, de forma remota, proporcionando garantías sobre el origen y la integridad de los datos sellados.
CREACIÓN, VERIFICACIÓN Y VALIDACIÓN DE SELLOS DE TIEMPO ELECTRÓNICOS
Sirven para conocer el tiempo exacto y por quién fue firmado o sellado un contrato u orden de pedido y así poder realizar un mejor seguimiento, ahorrando tiempo y costes.

[10] Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

[11] Aunque no se denegarán efectos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada, únicamente se reconocerán a la firma electrónica cualificada efectos jurídicos equivalentes a la firma manuscrita.

SERVICIOS DE ENTREGA ELECTRÓNICA CERTIFICADA Y EMISIÓN DE CERTIFICADOS
Permiten a distintas partes intercambiar datos por medios electrónicos y aportar pruebas relacionadas con su envío y recepción. Además, estos servicios protegen los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizadas.
AUTENTICACIÓN DE SITIOS WEB
Tienen como objetivo mostrar la fiabilidad de la web de una empresa y proteger el nombre de dominio contra el *phishing* o contra sitios web falsos.
PRESERVACIÓN DE FIRMAS, SELLOS O CERTIFICADOS ELECTRÓNICOS
Estos servicios están relacionados o tienen como finalidad garantizar el grado de confianza de un firma o sello cualificado a través del tiempo.

3.2.2. Los servicios de identificación electrónicos

Asimismo, el Reglamento eIDAS regula los llamados servicios de identificación electrónica (los "**Servicios eID**"), esto es, aquellos que consisten en el proceso de *"utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica"*[12].

Los servicios de identificación electrónica únicamente son regulados en cierta medida, especialmente en el contexto del acceso por parte de ciudadanos a servicios prestados en línea por un organismo del sector público en un Estado miembro. Si bien, está previsto un nuevo paradigma europeo de identificación digital que revolucione todo el sector y extienda sus posibilidades al sector privado y a multitud de nuevos casos de uso.

La normativa actualmente vigente ha previsto la utilización de los medios de identificación electrónica expedidos por los Estados, por mandato de los Estados o reconocidos por los Estados, también en las transacciones entre privados. Por este motivo, en el ámbito del cumplimiento resultan cada vez más importantes. Estos medios de identificación ofrecen niveles de seguridad variables, llegando al nivel alto, en el que encontramos el uso de la autenticación multifactorial, frecuentemente con apoyo en la biometría.

La Agencia Española de Protección de Datos (la "**AEPD**") ha aclarado que es necesario distinguir entre el concepto de "Identificación biométrica" y "autenticación/verificación biométrica" (AEPD 2020). En este sentido, el primer proceso consistiría en el proceso de búsqueda de equivalencias uno-a-varios (reconocer a un individuo particular entre un grupo), mientras que el segundo sería el de búsqueda

[12] Artículo 3.1 del Reglamento eIDAS.

de correspondencias uno-a-uno (comparar los datos del individuo únicamente con los datos asociados a la identidad reclamada). Según la AEPD, un sistema de autenticación fuerte es aquél que exige que se proporcione, al menos, dos de los siguientes factores: algo que se sabe, algo que se tiene o algo que se es (biometría) (AEPD 2020).

Tanto la identificación electrónica como los servicios de confianza pueden ayudar a las empresas y a sus negocios a:

- Evitar el *phishing* e incrementar la confianza de sus consumidores;
- Cumplir con requerimientos de la normativa de prevención de blanqueo de capitales;
- Proporcionar confianza respecto del origen de los documentos;
- Reducir el tiempo en el intercambio de documentación;
- Proteger contra la pérdida, robo, daño o alteraciones de un documento;
- Reducir los costes mediante procesos simplificados y monitorizar o hacer seguimiento de los recorridos de un determinado documento;
- Proporcionar una mayor y mejor rendición de cuentas; y
- Ampliar la base de clientes comerciales.

Los procesos de transformación digital en sectores regulados como el bancario y el financiero necesariamente pasan por ser servicios que ofrezcan garantías legales, así como la necesidad de generar confianza entre terceras partes en el desarrollo de sus actividades económicas. En este sentido, los servicios electrónicos de confianza permiten articular un sector financiero y bancario digital y ágil. Por ejemplo, las Normas Técnicas Reguladoras de la Autoridad Bancaria Europea crearon el puente perfecto entre el Reglamento eIDAS y la Directiva PSD2, estableciendo que la identificación de *Third Party Providers, "TPP"* debe basarse en un certificado cualificado tal y como se define en el Reglamento eIDAS.

3.3. RegTech de Gobierno Corporativo, Gestión de Riesgos y Cumplimiento Normativo

Durante los últimos años se ha incrementado el número de regulaciones impuestas por las autoridades con el fin de mejorar la ética y transparencia en el seno de las compañías, además de mitigar los casos de fraude y corrupción en Europa. Esto supone que las empresas necesiten estar en constante adaptación para gestionar adecuadamente la normativa.

Por tanto, la rapidez y optimización de las empresas en la adaptación de la normativa aplicable es un factor clave que les permite evitar riesgos de cualquier índole.

El GRC (Gobierno Corporativo, Gestión de Riesgos y Cumplimiento Normativo) surge, precisamente, ante la necesidad de optimizar los procesos de adaptación a la normativa y aunar la identificación, gestión, análisis y prevención de los riesgos de una compañía, ya sean riesgos legales, penales,

económicos, reputacionales o cualquier tipo de riesgo que pudiera poner en peligro la estabilidad de la compañía.

Sin embargo, debemos destacar que uno de los objetivos principales de las RegTech en GRC es, además de la prevención, la mejora de la ética, transparencia y sostenibilidad del ecosistema empresarial. Es evidente que el conjunto de las medianas y grandes compañías posee un gran peso en la sociedad actual, por lo que debemos persistir en crear una cultura adecuada y sostenible desde el seno del negocio.

3.3.1. Gobierno Corporativo

Es el conjunto de mecanismos implementados en una organización para asegurar que la información que llega a los órganos de decisión es suficiente, completa, correcta y puntual. En este sentido, las RegTech de GRC, mediante las soluciones tecnológicas y adaptadas a cada negocio, aúnan toda la información en tiempo real.

3.3.2. Gestión de Riesgos

La identificación, análisis y tratamiento de los riesgos que puedan afectar de forma adversa a la estrategia de la organización y a su capacidad para operar, es fundamental para asegurar su sostenibilidad en el tiempo.

Las entidades RegTech de GRC ayudan a gestionar estos complejos procesos de gestión de riesgos mediante la implementación de soluciones tecnológicas integradas en las empresas. Estas soluciones permiten identificar de forma temprana los posibles riesgos y mitigarlos de forma efectiva optimizando los recursos.

3.3.3. Cumplimiento Normativo

El Cumplimiento Normativo o *Compliance* es el conjunto de normas y políticas internas que aseguran el correcto cumplimiento de las regulaciones y leyes que resulta de aplicación al negocio por parte de la organización que la forma.

Además, el conjunto de procesos, compromisos y valores internos que conforman la cultura y la ética de la organización también está gestionada bajo el paraguas del Cumplimiento Normativo. La cultura y ética dentro de las compañías asegura el correcto comportamiento de cada una de las personas que forman parte del equipo y se debe considerar siempre este punto como factor clave en este apartado.

A continuación, se identifican los tipos de servicios y soluciones que prestan las entidades RegTech en relación al GRC:

- Control Interno,
- Gestión de Riesgos,
- Auditoría Interna,
- Planes de Prevención Penal,

- Ciberseguridad,
- Gestión del riesgo de Protección de Datos,
- Planes de Continuidad del negocio
- Sistemas Internos de Información.

Entre las ventajas y beneficios de las entidades RegTech de GRC, encontramos una amplia variedad de puntos a tener en cuenta. La implementación de estas soluciones puede ayudar a las empresas a:

- Identificar, analizar y prevenir los riesgos en una etapa temprana, pudiendo así aplicar controles debidos de forma eficaz y óptima, además de minimizar riesgos en la compañía que puedan afectar al correcto funcionamiento de la misma.

- Mantener el control del negocio, ya que permitir tener una definición clara de los roles y responsabilidades en cada una de las áreas.

- Evitar que la entidad pueda ser sancionada por la comisión de fraude, corrupción u otros delitos, minimizando el coste económico y reputacional que esto conlleva.

- Acelerar el proceso de transformación digital en diferentes áreas de la compañía, lo que hace más eficiente la labor de los equipos de *Compliance*.

- Lograr un sistema de canales de comunicación dentro de la compañía amplio y eficaz que mejore la transparencia de la misma.

- Lograr una visibilidad y trazabilidad de todas las partes de los procesos dedicados al GRC, evitando la pérdida de información en caso de que, a futuro, pudiera ser de interés.

- Cumplimiento de la normativa aplicable con garantía de seguridad y protección de datos.

3.4. RegTech de *Reporting*. Asistencia en reportes regulatorios ante las autoridades de supervisión

Las entidades RegTech de *reporting* son aquellas que están especializadas en ofrecer a las entidades financieras soluciones tecnológicas destinadas al cumplimiento de sus obligaciones de reporte regulatorio (*reporting*), es decir, de entrega de información periódica a las diferentes autoridades de supervisión, tales como el Banco de España, el Banco Central Europeo (BCE), la Comisión Nacional del Mercado de Valores (CNMV) o la Dirección General de Seguros y Fondos de Pensiones (DGS).

Estas obligaciones de información periódica a los supervisores han sido objeto de importante desarrollo en los últimos años, incrementándose notablemente el volumen y complejidad de la información objeto de reporte. Como se analizará en el apartado de regulación de este Libro Blanco, cada bloque normativo aplicable al sector financiero (CRD y CRR, MiFID, UCITS, AIFMD, EMIR, SFTR,

Solvencia II, etc.) incluye un conjunto de obligaciones de reporte a los reguladores, ya sea de manera armonizada a nivel europeo o bien estrictamente local.

De acuerdo con el estudio publicado por la EBA en junio de 2021, únicamente el 11% de las empresas dedicadas a los servicios de RegTech a nivel europeo se especializan en la prestación de servicios de reporting a reguladores (EBA 2021). En este sentido, el segmento de reporte regulatorio es uno de los segmentos menos desarrollados entre los principales que conforman el sector RegTech de la Unión Europea, siendo especialmente destacable que más de la mitad de las soluciones tecnológicas en esta materia son desarrolladas a nivel interno por la propia entidad regulada (EBA 2021).

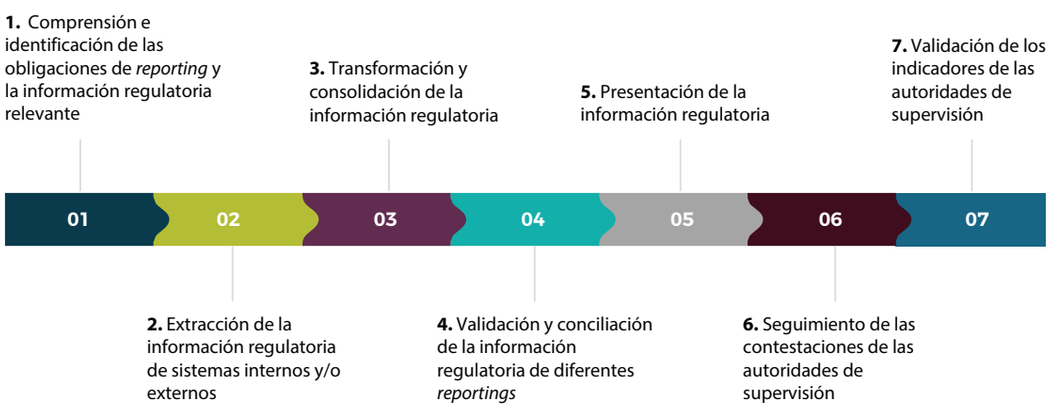
La explicación de lo anterior se encuentra en la complejidad inherente a la prestación de estos servicios. Mientras que ciertos reportes pueden resultar más fáciles de generar y completar, no siendo estrictamente necesario (o especialmente ventajoso) la implementación de soluciones de RegTech, existen otros reportes de una elevada complejidad regulatoria, técnica y operativa (p.ej. los relativos a información financiera de las entidades de crédito) que requieren la existencia de equipos altamente especializados y con elevados conocimientos técnicos para poder completarlos de una manera correcta. Estos equipos forman parte, normalmente, de las propias entidades sujetas a la obligación de *reporting*, de forma que éstas mismas generan internamente sus procesos para la preparación de los reportes y su envío al regulador.

Por ello, únicamente pueden prestar estos servicios de reporte regulatorio (complejo) aquellos prestadores de servicios que dispongan de capacidad y calidad técnica suficiente en esta materia, lo cual supone una elevada barrera de entrada en este segmento de RegTech.

Además, esa capacidad técnica no solamente debe ser predicable en lo que respecta a la capacidad de cumplimentar los reportes, sino también de, por ejemplo, establecer medidas de automatización para su generación, traslado a los ficheros informáticos exigidos por el regulador en cuestión y remisión, de una manera fluida y sin incidencias, a éste. En este sentido, los prestadores de servicios de reporte regulatorio utilizan sistemas de automatización robótica de procesos, computación en la nube (*cloud computing*) o de aprendizaje automático (*machine learning*).

En definitiva, aparte de los conocimientos, se debe presuponer a los prestadores de estos servicios cierta capacidad operativa y tecnológica como para poder poner en funcionamiento sistemas de tratamiento de información eficientes y de cierta sofisticación, reduciendo aún más las posibilidades de entrada en este nicho del RegTech.

Desde un punto de vista gráfico, puede mostrarse la cadena de proceso de *reporting* a través de las siguientes fases (EBA 2021):



Con todo, la implementación de soluciones tecnológicas proporcionadas por las empresas de RegTech de *reporting* pueden ofrecer a las entidades reguladas las siguientes ventajas:

- Reforzar el cumplimiento de las obligaciones de *reporting* regulatorio a través de plataformas de información integrada.
- Facilitar el manejo de la información de la entidad y mejorar la calidad y precisión de la misma.
- Sustituir procesos manuales por otros automatizados, con menores márgenes de error.
- Estimular la interoperabilidad entre los sistemas internos de la entidad y las plataformas de las autoridades de supervisión.

3.5. Otras RegTech

Como se ha descrito en el apartado 2.1 de este Libro Blanco, el sector RegTech puede ofrecer una amplia variedad de servicios de diversa naturaleza.

Además de los cuatro grupos principales descritos anteriormente, existen otras empresas dentro del sector RegTech especializadas en otros ámbitos y servicios entre los cuales destacan los siguientes:

- Ciberseguridad. En este ámbito, se ofrecen soluciones tecnológicas para prevenir ataques cibernéticos (*hacking*) u otras incidencias de seguridad en los sistemas de tecnología de la información, a fin de evitar robos de información sensible de la entidad y sus clientes o la paraliza-

ción de los sistemas internos de la entidad en cuestión. Está previsto que en los próximos años se amplíe el catálogo de exigencias técnicas y jurídicas de la normativa de ciberseguridad. Ello especialmente tras la trasposición en España de la Directiva NIS[13] (en referencia a la fórmula en inglés relativa a sistemas y redes de información -*Network and Information Systems*-), la cual está previsto que sea actualizada a medio plazo por la Directiva NIS 2. También en el ámbito financiero, se espera un cambio significativo con la aprobación de la propuesta de Reglamento (UE) sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014 (el "**Reglamento DORA**").

- Gestión de comunicaciones electrónicas. Dentro de la tendencia de implementar procesos sostenibles con el medio ambiente, existen prestadores de servicios RegTech especializados en la generación, tratamiento y envío de comunicaciones electrónicas a clientes, mediante la implementación y adaptación de procesos automáticos de auto cumplimentación de contratos y documentos con transcendencia legal, así como su remisión a clientes por medios telemáticos.

- Gestión automatizada fiscal y contable. Las soluciones tecnológicas que ofrecen las empresas de RegTech en este ámbito se centran principalmente en facilitar el cumplimiento de obligaciones fiscales por parte de los contribuyentes, por ejemplo, respecto de la correcta cumplimentación de declaraciones y formularios, llevanza de contabilidad de forma automatizada, control y gestión de facturas, entre otros.

4. MARCO LEGAL ACTUAL

4.1. Normativa de prevención del blanqueo de capitales y la financiación del terrorismo

Como se ha apuntado anteriormente, una parte relevante del sector RegTech está formada por entidades especializadas en aplicaciones destinadas a facilitar el cumplimiento de la normativa de prevención del blanqueo de capitales y la financiación del terrorismo (PBC y FT).

En España, la normativa de referencia es la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo (la **"LPBC"**)[14], desarrollada por el Real Decreto 304/2014,

[13] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Dicha directiva fue transpuesta en España por el RD-ley 12/2018 y recientemente ha sido complementada a su vez por el RD 43/2021.

[14] Dicho marco legal nacional ha sufrido diversas modificaciones a lo largo de los últimos años, con motivo de la transposición de las seis Directivas europeas en materia de prevención de blanqueo en esta materia. La última modificación ha tenido lugar en 2021 con la aprobación del Real Decreto-Ley 7/2021, de 27 de abril.

de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (el "**Reglamento LPBC**").

Dicha normativa se encuentra armonizada a nivel de la UE, en virtud de las diferentes Directivas que se han ido aprobando en los últimos años en materia de PBC y FT[15].

Asimismo, está prevista la aprobación de un paquete de medidas nuevas relacionadas con la normativa de PBC y FT en el marco del proyecto *Security Union Strategy* 2020-2025[16], que podrían armonizar y reforzar el conjunto de obligaciones tanto de los sujetos obligados como de los organismos supervisores durante los próximos años.

4.1.1. Medidas de diligencia debida

Entre las principales obligaciones legales en materia de PBC y FT, se encuentra el deber de los sujetos obligados de identificar a las personas físicas o jurídicas con quienes pretendan establecer relaciones de negocios o intervenir en cualesquiera operaciones.

En un primer nivel, los sujetos obligados deben proceder a la identificación formal de sus clientes, mediante la comprobación de su identidad a través de documentos fehacientes, tales como el documento nacional de identidad (DNI), el pasaporte o la tarjeta de residencia para el caso de las personas físicas, o documentos públicos acreditativos de existencia y determinados datos, para el caso de las personas jurídicas[17].

Asimismo, los sujetos obligados tienen la obligación de identificar al titular real (es decir, la persona o personas físicas por cuya cuenta se pretenda establecer una relación de negocios o que directa o indirectamente posean el 25% del capital o derechos de voto de una persona jurídica).

Igualmente, la normativa exige la solicitud y comprobación de otra información, como, por ejemplo, el propósito o índole prevista de la relación de negocios del potencial cliente (que, principalmente, se traduce en conocer su actividad profesional o empresarial).

Todos estos procesos de identificación se enmarcan en las medidas de *know-your-customer* (*KYC*) aplicadas por las entidades. Dentro de estas medidas, se encuentra la exigencia de identificar personas que tengan, o hayan podido tener, responsabilidades públicas (conocidas como "*PEPs*", *politically exposed persons*), las cuales suponen un mayor riesgo a efectos de PBC y FT.

---

[15] En este sentido, se habla de las cinco Directivas europeas en materia de PBC y FT. La primera de ellas fue Directiva 91/308/CEE del Consejo, de 10 de junio de 1991, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales, siendo el resto modificación o derogación de las anteriores, hasta la actual Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE (conocida como Quinta Directiva de PBC y FT.

[16] Véase el paquete de la propuesta de medidas en: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

[17] La obligación de identificación formal debe ponerse en relación también con el deber de las entidades de crédito de solicitar el número de identificación fiscal (NIF) a sus clientes, conforme a la disposición adicional sexta de la Ley 58/2003, de 17 de diciembre, General Tributaria.

4.1.2. Identificación en operaciones no presenciales o a distancia

Dentro de los ámbitos en los que las entidades RegTech de PBC pueden aportar un mayor valor añadido es el relativo a la identificación de clientes a distancia o a través de canales no presenciales.

En efecto, con el auge de la contratación electrónica, en general, y en el sector financiero, en particular, la aplicación de medidas de identificación de clientes a través de sistemas electrónicos supone una cuestión esencial para las entidades. Esto es así no sólo por una cuestión de mero cumplimiento normativo de la normativa de PBC y FT, sino también por las implicaciones que puede tener a nivel de experiencia de uso. Un sistema de identificación de clientes a distancia que sirva para cumplir adecuadamente la norma, pero que sea incapaz de facilitar que el cliente pueda completar el proceso de una forma rápida y sencilla, puede tener implicaciones graves a nivel comercial y de negocio.

A este respecto, la LPBC, en su artículo 12, establece los medios electrónicos a través de los cuales las entidades pueden identificar formalmente a sus clientes de manera no presencial, tales como:

- La acreditación de la identidad del cliente mediante la firma electrónica cualificada regulada en el Reglamento eIDAS (tal y como más adelante se define). En tal caso, no es necesario solicitar al cliente la copia de su documento de identificación personal, simplificando la interacción con el cliente y el volumen de documentación que deba custodiarse por la entidad.

- La acreditación de la identidad del cliente mediante procedimientos seguros de identificación en operaciones no presenciales que hayan sido autorizados previamente por el SEPBLAC. Estos procedimientos son, hoy en día, dos: (i) la videoconferencia (en tiempo real) con el cliente[18] y (ii) la video-identificación[19].

Cabe destacar que un número relevante de entidades RegTech ofrecen la implementación de estos procedimientos siguiendo los requisitos establecidos por el SEPBLAC. Para que estos procedimientos sean válidos, deben cumplir los requisitos establecidos de forma general por el SEPBLAC para cada uno de ellos, no existiendo ningún tipo de validación previa ni posterior por parte del SEPBLAC de cada una de las soluciones ofrecidas por estos proveedores caso por caso. Es decir, no existe ningún tipo de homologación de procedimientos, soluciones y sistemas por parte del SEPBLAC que confirme la validez y suficiencia de dichos procedimientos.

Se analizarán más adelante en este Libro Blanco las implicaciones que existen hoy en día respecto de estos procedimientos, los retos que presentan para el sector RegTech y las mejoras que éste propone para simplificar el alta de nuevos clientes en las entidades financieras.

[18] Véase los requisitos del SEPBLAC para la identificación no presencial mediante videoconferencia en: https://www.sepblac.es/wp-content/uploads/2018/02/autorizacion_identificacion_mediante_videoconferencia.pdf.

[19] Véase los requisitos del SEPBLAC para la video-identificación en: https://www.sepblac.es/wp-content/uploads/2018/02/Autorizacion_video_identificacion.pdf.

4.1.3. Seguimiento continuo de la relación de negocios

Los sujetos obligados también deben adoptar medidas de seguimiento continuo a lo largo de la relación contractual con los clientes para garantizar que la información que disponen de ellos coincide con la actividad empresarial y profesional real del cliente y su perfil de riesgo.

Esta obligación exige a las entidades establecer mecanismos de monitorización y control de los clientes y su operativa y el análisis constante de fuentes de información públicas o privadas que permitan detectar hechos o circunstancias de los clientes que impliquen una actualización de su perfil de riesgo. Las entidades RegTech ofrecen herramientas de seguimiento de información en este sentido.

4.2. El Reglamento eIDAS y la regulación de los servicios de confianza

Un porcentaje elevado de compañías comprendidas en el sector RegTech prestan alguno o varios de los denominados "servicios electrónicos de confianza" (los "**Servicios de Confianza**" o "**SEC**"). Esta categoría de servicios electrónicos, que comprende varios tipos de servicios entre los que destaca la firma electrónica, y que formaría parte de los generalmente denominados "servicios de la sociedad de la información", fue reconocida y regulada específicamente por el Reglamento eIDAS.

Aunque la Directiva 1999/93/CE ya proporcionó un primer marco comunitario regulador de las firmas electrónicas y de su clasificación, el Reglamento eIDAS vino a reforzar y ampliar el acervo que dicha Directiva representaba. En este sentido, el Reglamento eIDAS supuso la adopción de un marco global transfronterizo e intersectorial al permitir el reconocimiento mutuo de los operadores existentes en los Estados Miembros estableciendo estándares técnicos y niveles de seguridad. El Reglamento eIDAS también eliminó aquellos obstáculos que fragmentaban el mercado único digital en la Unión Europea.

En España, el Reglamento eIDAS ha sido complementado y desarrollado en algunos ámbitos por la Ley 6/2020, de 11 de noviembre reguladora de determinados aspectos de los servicios electrónicos de confianza (la "**LSEC**"). La LSEC dejó sin efectos la anterior Ley 59/2003, de 19 de diciembre, de Firma electrónica, que transponía al ordenamiento jurídico español la derogada Directiva 1999/93/CE, así como el artículo 25 relativo a la intervención de terceros de confianza de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico (la "**LSSI**").

Asimismo, la LSEC introduce algunas disposiciones específicas para completar el Reglamento eIDAS, por ejemplo, en materia de expedición, contenido y duración de los certificados cualificados, requisitos de constitución de garantías económicas para la prestación de servicios cualificados de confianza y la posibilidad de que el órgano supervisor mantenga un servicio de difusión de información sobre los prestadores cualificados que operan en el mercado[20].

[20] Véase nota de pie anterior nº 9.

4.2.1. La regulación de los servicios electrónicos de confianza

En primer lugar, cabe tener en cuenta que los SEC, que se definen por el Reglamento eIDAS[21] como aquellos servicios electrónicos prestados habitualmente a cambio de una remuneración, comprenden la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y los certificados relativos a estos servicios. Asimismo, los SEC incluyen la creación, verificación y validación de certificados para la autenticación de sitios web o la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

En términos generales, el Reglamento eIDAS ofrece un marco jurídico para la prestación de estos servicios, así como para su empleo tanto por parte de personas físicas como jurídicas. La regulación se divide en seis capítulos con diversas secciones en las que se abordan cuestiones tales como las características y tipología de estas clases de servicios, sus distintos niveles de seguridad y confiabilidad jurídica, distinguiendo entre dos tipologías básicas: "cualificados y no cualificados".

La normativa regula igualmente los organismos de supervisión y los controles y requisitos técnicos que tanto los prestadores como sus servicios deberán cumplir, siendo destacable la obligatoriedad de figurar inscrito en las llamadas *trust lists* (listas de confianza) para aquellos prestadores que cuenten con el grado de cualificados.

4.2.2. La regulación de los servicios de identificación electrónica

Igualmente, el Reglamento eIDAS regula los sistemas de identificación electrónica, consistentes en el proceso de "*utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica*"[22]. A diferencia del bloque de los servicios SEC, los servicios de identificación electrónica únicamente son regulados en cierta medida, especialmente en el contexto del acceso por parte de ciudadanos a servicios prestados en línea por un organismo del sector público en un Estado miembro.

En este sentido, el Reglamento eIDAS (Identificación Electrónica) establece, entre otras cuestiones, las bases para el reconocimiento mutuo de los servicios prestados en línea por organismos del sector público en otro Estado miembro a efectos de la autenticación transfronteriza, así como las condiciones para la notificación de los sistemas de identificación electrónica y los distintos niveles de seguridad de dichos sistemas (bajo, sustancial y alto).

Por otro lado, el Reglamento eIDAS también regula la posibilidad de emplear sistemas de identificación electrónica de forma auxiliar a la prestación de los servicios emisión de certificados cuando la identificación del solicitante se lleve a cabo en remoto. En este sentido, el art. 24 d) del Reglamento eIDAS establece las distintas fórmulas para identificar a la persona física, entre las que se incluye, más allá de la identificación presencial, la posibilidad de utilizar otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la

[21] Artículo 3.16) del Reglamento eIDAS.

[22] Artículo 3.1) del Reglamento eIDAS.

presencia física. La seguridad equivalente deberá ser confirmada por un organismo de evaluación de la conformidad.

En implementación de lo anterior, el artículo 7.2 de la LSEC introdujo una disposición por la que se dispuso que "*Reglamentariamente, mediante Orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, se determinarán otras condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física según su evaluación por un organismo de evaluación de la conformidad.(…)*".

En este sentido, el pasado 6 de mayo de 2021, fue aprobada por el Ministerio de Asuntos Económicos y de Transformación Digital la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados[23] (la "**OM ETD/465/2021**"). Dicha OM ETD/465/2021 aplica a los prestadores cualificados públicos y privados establecidos en España y a los residentes o domiciliados en otro Estado miembro pero que tengan establecimiento permanente en territorio nacional.

Entre otras cuestiones, la OM ETD/465/2021 aborda las distintas modalidades de identificación, el proceso de evaluación de la conformidad en el cumplimiento de los requisitos de seguridad y otros deberes de los prestadores de esta clase de servicios (por ejemplo, la obligatoriedad de llevar a cabo un análisis de riesgos de carácter anual de conformidad con la normativa de protección de datos o la necesidad de notificar al órgano supervisor las violaciones de seguridad y pérdidas de integridad que impacten al servicio).

Finalmente, cabe destacar que el pasado 3 de junio de 2021 fue publicada la propuesta de Reglamento del Parlamento Europeo y el Consejo que modifica el Reglamento eIDAS y está comenzando a ser conocido como la "*European Digital Identity Regulation*" (la "**Propuesta de Reglamento EUid**" o "**eIDAS 2**")[24], con el propósito de imponer a los Estados la obligación de expedir Carteras de Identidad Digital que permita a los ciudadanos identificarse de forma segura y uniforme en sus relaciones con entidades públicas y privadas. Una importante cantidad de sujetos privados quedarán sujetos al deber legal de admitir a los ciudadanos el uso de su Cartera, por lo que se facilitará el funcionamiento del Mercado Único Digital. Asimismo, la Propuesta de Reglamento EUid pretende dar un paso adelante hacia la descentralización de los sistemas de verificación de identidad ("*Self Sovereign Identity*").

[23] Durante la crisis sanitaria del Covid-19 y hasta que no fue aprobada dicha orden el Ministerio de Asuntos Económicos y Transformación Digital autorizó provisionalmente la emisión de certificados cualificados mediante identificación digital llevada a cabo a través de sistemas de video identificación que reuniesen un volumen de exigencias superior a los previstos por SEPBLAC para la identificación de usuarios.

[24] *Regulation of the European Parliament and of the Council amending Regulation* (EU) No 910/2014 *as regards establishing a framework for a European Digital Identity*. Disponible en: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation.

4.3. El Reglamento General de Protección de Datos y la privacidad

El Reglamento UE 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (el "**RGPD**") supuso un cambio de paradigma de los prestadores de servicios de la sociedad de la información, incluidas las RegTech.

Dicho marco legal, complementado poco después en España por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDDD), sientan las bases para la protección de las personas físicas en relación con el tratamiento de los datos personales como derecho fundamental, reconocido en la Carta de los Derechos Fundamentales de la UE.

Entre las principales novedades introducidas por el GDPR y que afectan al sector del RegTech, cabe destacar las obligaciones para quienes tratan y determinan el tratamiento de datos de carácter personal y los nuevos derechos para los interesados. En particular, dicho marco regulatorio incentiva la aplicación de la seudonimización para reducir riesgos y establece el deber de llevar a cabo una evaluación de impacto en caso de que se lleve a cabo un tratamiento de datos biométricos que pueda afectar significativamente a los derechos y libertades del individuo.

4.3.1. Consideraciones sobre el tratamiento de datos biométricos

El tratamiento de datos biométricos[25] en el ámbito de la prestación de los Servicios de Confianza e identificación electrónicos, como la huella dactilar o el reconocimiento facial, es uno de los aspectos más discutidos y complejos desde el punto de vista jurídico. Así, el RGPD dispone que serán considerados datos sensibles aquellos datos biométricos cuyo tratamiento con medios técnicos específicos permita la identificación o la autenticación unívocas de la persona física[26]. La regla general es que dicho tratamiento no podrá llevarse a cabo salvo que esté sustentado en las bases jurídicas correspondientes y alguna de las excepciones previstas.

En el informe 36/2020 de la AEPD, referido al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online, se dispuso lo siguiente:

"*(…) esta Agencia considera que se trata de una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo atenderse al caso concreto según los datos tratados, las técnicas empleadas para su tratamiento y la consiguiente injerencia en el derecho a la protección de datos, debiendo, en tanto en cuanto no se pronuncia al respecto el Comité Europeo de*

[25] Artículo 1. 14) del RGPD define los datos biométricos como aquellos "datos personales obtenidos a partir de un tratamiento técnico específicos, relativos a las característias físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos."

[26] Nótese que con carácter general, la AEPD advierte de que únicamente tendrán la consideración especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación (uno-a-uno).

Protección de Datos o los órganos jurisdiccionales, adoptarse, en caso de duda, la interpretación más favorable para la protección de los derechos de los afectados."

En cualquier caso, el tratamiento de datos biométricos requerirá, en la mayoría de los casos, la realización previa de evaluaciones de impacto que permitan analizar la legitimidad del tratamiento y si resulta proporcional, así como las medidas que deban adoptarse para minorar los riesgos a los derechos y libertades de los sujetos afectados.

En junio de 2020, la AEPD publicó el documento titulado 14 equívocos con relación a la identificación y autenticación biométrica (AEPD 2020), en el cual, además de insistir en dilucidar una vez más la diferencia entre identificación y autenticación (ya presentada con anterioridad en el Dictamen 3/2012 del Grupo de Trabajo del art. 29 sobre la evolución de las tecnologías biométricas), expuso su opinión respecto a lo que consideró equívocos extendidos con relación al uso de datos biométricos para fines de identificación y autenticación. Su posicionamiento, claramente desfavorable, supuso un revés para un sector que apuesta por desarrollar tecnologías ágiles y eficaces que resuelvan problemas de interés general.

Por suerte para el sector, posteriormente ha habido nuevos pronunciamientos[27] de la AEPD que avalan el empleo de estas tecnologías para determinados trámites o ámbitos, como, por ejemplo, para el registro de jornadas en el ámbito laboral si se cumplen requisitos estrictos, dando un giro positivo hacia la tendencia que había precedido.

Sin perjuicio de lo anterior, y a los efectos del sector RegTech, el pasado 2 de julio de 2021[28], la AEPD volvió a emitir un informe desfavorable hacia la propuesta que planteaba el tratamiento de datos de reconocimiento facial en el momento del alta de clientes en la oficina o a través de un canal online con el objetivo de verificar su identidad y así realizar las verificaciones oportunas previstas en la LPBC. En esta ocasión, la AEPD consideró que se trata de "[…] sistemas de identificación muy intrusivos para los derechos y libertades fundamentales de las personas físicas".

4.3.2. Consideraciones sobre los encargos de tratamiento de datos

Una de las primeras consideraciones en el ámbito del tratamiento de datos personales en el contexto del empleo de servicios de RegTech es la calificación de los roles de las partes. A diferencia de lo que ocurre en la mayoría de las relaciones entre clientes y prestadores de servicios, en las que el cliente es el "responsable de los datos" mientras que el proveedor es el "encargado de tratamiento", en el ámbito de las RegTech, no siempre es así. Por ejemplo, en el caso de prestadores de servicios de certificación, debe barajarse el intercambio de roles.

Efectivamente, tal y como puso en evidencia la resolución de 5 de noviembre de la AEPD relativa al procedimiento sancionador incoado contra la entidad Empresa de Certificación y Servicios Izenpe, S.A.,

[27] Véase la Resolución de la AEPD de fecha 21 de octubre de 2020.

[28] Véase el informe completo de la AEPD, disponible en: https://www.aepd.es/es/documento/2021-0047.pdf.

existe un debate y una cierta confusión en torno a la distribución de los roles de responsable y encargado de tratamiento de los datos en el ecosistema de prestadores de servicios de certificación e identificación electrónicos. La confusión es aún mayor cuando quienes intervienen son entidades que actúan cómo medios propios en ejecución de encomiendas de las Administración Pública o agentes registradores que actúan en el proceso de identificación.

Cabe destacar que ni el Reglamento eIDAS, ni la LSEC, dedican excesivos perceptos a dilucidar algunos aspectos relacionados con la distribución de roles en el tratamiento de protección de datos de carácter personal en el ecosistema de prestadores de confianza, más allá de indicar la necesidad general de cumplir estrictamente con el contenido de dicha normativa.

4.4. Reporte regulatorio a supervisores

Las labores de supervisión de las autoridades regulatorias tienen, como una de sus piezas clave, la información que de forma periódica le remiten las entidades sobre su actividad, su situación financiera y sus clientes.

Esta exigencia de remisión de información periódica a los supervisores ha sido objeto de un especial desarrollo a raíz de la crisis financiera de 2008. Una de las debilidades detectadas en el marco de dicha crisis fue precisamente la ausencia de información completa y actualizada de aspectos importantes de las entidades supervisoras (como, por ejemplo, sus niveles de exposición de riesgo, liquidez o apalancamiento).

En este sentido, a día de hoy, las entidades financieras se encuentran con obligaciones de información periódica de todo tipo a su supervisor de referencia.

Los reportes regulatorios han de remitise a través de plantillas estándar establecidas, ya sea en la propia normativa, o bien en las aplicaciones técnicas definidas por el supervisor competente. En este sentido, las entidades de RegTech ofrecen servicios de automatización de procesos para completar esta información, evitando errores humanos a la hora de trasladar la información de la entidad a las plantillas de información y mejorando la eficiencia en términos de tiempo y coste.

Además, la forma de envío de esta información es, casi en su integridad, electrónica, utilizando los formatos de archivos que en cada caso determine el supervisor en cuestión y los sistemas de comunicación electrónica definidos e implementados por éste. Por ello, las entidades RegTech ofrecen, en este ámbito, no sólo servicios para completar formularios y fichas informativas, sino también de volcado de información en los formatos exigidos por el supervisor y de integración tecnológica para asegurar el envío correcto y puntual de información.

A nivel regulatorio, destaca principalmente el volumen de información periódica que han de remitir las entidades de crédito al Banco Central Europeo y al Banco de España sobre aspectos relacionados

con su situación financiera y actividad, p.ej. balance, cuenta de pérdidas y ganancias, préstamos concedidos a clientes, garantías, etc[29].

En el ámbito de supervisión de la CNMV, también destacan las obligaciones de información periodica que, con una frecuencia u otra, han de remitir las empresas de servicios de inversión, las sociedades gestoras de instituciones de inversión colectiva, de entidades de capital riesgo o de entidades de inversión colectiva de tipo cerrado. Dicha información debe enviarse a través del sistema de comunicación electrónica de la CNMV (Sede Electrónica – CIFRADOC)[30].

En el ámbito de los instrumentos financieros, destacan también las obligaciones de comunicación de operaciones con valores e instrumentos financieros -en el marco de las obligaciones establecidas por el Reglamento MiFIR[31]- y con derivados negociados o extrabursátiles (over-the-counter, OTC) en el marco del Reglamento EMIR[32], u operaciones de financiación de valores en el reglamento SFTR[33]. También en lo que respecta a PBC y FT, existen obligaciones de información continua al SEPBLAC. Además del deber de comunicar operaciones sospechosas de blanqueo de capitales o de financiación del terrorismo (comunicación por indicio), las entidades deben reportar al SEPBLAC de forma mensual determinadas operaciones (la llamada declaración mensual obligatoria, o bien, con carácter semestral, la ausencia de éstas, a través de la aplicación DMO 3.0[34]).

4.5. Entornos controlados de pruebas (*sandbox*)

Estos entornos son espacios establecidos y supervisados por organismos reguladores, que permiten a las entidades realizar pruebas y tests de sus productos y servicios con un conjunto reducido de clientes, siempre que dichos productos y servicios ofrezcan un marcado carácter innovador a nivel tecnológico.

[29] Se pueden citar, en este caso y sin ánimo de exhaustividad, las siguientes Circulares del Banco de España: Circular 4/2019, sobre normas de información financiera pública y reservada, y modelos de estados financieros; Circular 2/2019, sobre los requisitos del Documento Informativo de las Comisiones y del Estado de Comisiones, y los sitios web de comparación de cuentas de pago; Circular 4/2017 a entidades de crédito, sobre normas de información financiera pública y reservada, y modelos de estados financieros; Circular 2/2016, sobre supervisión y solvencia, que completa la adaptación del ordenamiento jurídico español a la Directiva 2013/36/UE y al Reglamento (UE) n.º 575/2013; Circular 8/2015, sobre información para determinar las bases de cálculo de las aportaciones al Fondo de Garantía de Depósitos; Circular 2/2015 sobre normas para el envío al Banco de España de las estadísticas de pagos y sistemas de pagos recogidas en el Reglamento (UE) 1409/2013; Circular 5/2012, sobre transparencia de los servicios bancarios y responsabilidad en la concesión de préstamos; o Circular 1/2010, sobre estadísticas de los tipos de interés que se aplican a los depósitos y a los créditos frente a los hogares y las sociedades no financieras.

En términos de *reporting* al Banco Central Europeo, se puede citar el Reglamento (UE) n. º 2015/534 del Banco Central Europeo, sobre la presentación de información financiera con fines de supervisión; o el Reglamento de Ejecución (UE) Nº 680/2014 de la Comisión, de 16 de abril de 2014, por el que se establecen normas técnicas de ejecución en relación con la comunicación de información con fines de supervisión por parte de las entidades.

[30] Principalmente a través de archivos con formato XML.

[31] Reglamento (UE) nº 600/2014 del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativo a los mercados de instrumentos financieros y por el que se modifica el Reglamento (UE) nº 648/2012.

[32] Reglamento (UE) n ° 648/2012 del Parlamento Europeo y del Consejo, de 4 de julio de 2012 , relativo a los derivados extrabursátiles, las entidades de contrapartida central y los registros de operaciones.

[33] Reglamento (UE) 2015/2365 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre transparencia de las operaciones de financiación de valores y de reutilización y por el que se modifica el Reglamento (UE) no 648/2012.

[34] Véase la información y las indicaciones del SEPBLAC relativas a la comunicación sistemática y la aplicación DMO 3.0, disponible en: https://www.sepblac.es/es/sujetos-obligados/tramites/comunicacion-sistematica/.

En nuestro país, este espacio ha sido implementado a través de la Ley 7/2020, de 13 de noviembre para la transformación digital del sistema financiero (la "**Ley 7/2020**").

Únicamente tendrán acceso al *sandbox* aquellos proyectos que cumplan con una serie de requisitos. En este sentido, además de ofrecer una funcionalidad mínima para comprobar su utilidad, deben perseguir alguno de los siguientes objetivos:

(a) Facilitar el cumplimiento normativo mediante la mejora u homogeneización de procesos u otros instrumentos;

(b) Suponer un eventual beneficio para los usuarios de servicios financieros en términos de reducción de los costes, de mejora de la calidad o de las condiciones de acceso y disponibilidad de la prestación de servicios financieros, o de aumento de la protección a la clientela;

(c) Aumentar la eficiencia de entidades o mercados; o,

(d) Proporcionar mecanismos para la mejora de la regulación o el mejor ejercicio de la supervisión financiera.

En el caso de que los promotores cumplan con los requisitos exigidos, solicitarán el acceso al espacio de pruebas a través de la sede electrónica de la Secretaría General del Tesoro y Financiación Internacional, acompañadas de una memoria justificativa en la que se explicará el proyecto, dando paso a una posterior evaluación que, en caso de ser favorable, suscribirá un protocolo de pruebas entre el promotor y la autoridad supervisora responsable del seguimiento por razón de su competencia (Banco de España, CNMV o Dirección General de Seguros y Fondos de Pensiones).

Una vez aprobado el protocolo de pruebas podrán dar comienzo las pruebas que integran el proyecto, bajo la supervisión de la autoridad competente.

Sólo pueden aceptar en el piloto de pruebas aquellos participantes que confirmen su libre voluntad de participar en las pruebas mediante la firma de un documento informativo en el que se describan, entre otros aspectos, las implicaciones y riesgos del piloto. Podrán, no obstante, desistir de participar en la prueba sin ningún tipo de penalización.

Dentro de los proyectos que participan actualmente en el *sandbox*, existen varios que tienen un marcado enfoque de RegTech, al referirse a contratación *online* de productos o biometría y seguridad en el ámbito de PBC y FT, entre otros, y sistemas de GRC. De hecho, el primer proyecto aprobado por el sandbox es una solución RegTech de GRC para el sector asegurador.

El sector confía en que la participación de este tipo proyectos RegTech en el *sandbox* español le conceda una mayor visibilidad y dinamismo, atrayendo talento e impulsando la innovación.

5. RETOS DEL SECTOR

5.1. Retos del segmento RegTech de PBC

A continuación, se resumen brevemente los principales retos a los que se enfrentan las entidades pertenecientes al segmento RegTech de PBC.

Explorar más vías de comunicación con el SEPBLAC y otras autoridades de supervisión.

Las ventajas de una mayor interlocución con el SEPBLAC y otras autoridades de supervisión de las entidades RegTech serían múltiples como, por ejemplo, facilitar el cumplimiento de la normativa, incrementar la seguridad jurídica y adquirir una mayor capacidad de detección de operaciones sospechosas. Los diferentes asociados de la AEFI dedicados al segmento de RegTech de PBC destacan la importancia de trabajar en nuevas vías de comunicación que contribuyan mantener un diálogo más fluido con las autoridades de supervisión.

Una mayor interlocución a través de vías de comunicación de fácil acceso contribuiría al mejor desarrollo de la actividad de las entidades de este segmento, dado que permitiría trasladar adecuadamente al SEPBLAC y a otras autoridades de supervisión las inquietudes y dudas que los sujetos obligados tienen en relación con la normativa aplicable.

Esta interlocución puede desarrollarse por las autoridades no sólo a nivel individual con cada entidad o sujeto obligado, sino también de forma conjunta o en colaboración con asociaciones que puedan canalizar las inquietudes comunes de los sujetos obligados, como la AEFI. Ello facilitaría al SEPBLAC y al resto de autoridades de supervisión la posibilidad de ofrecer respuestas e información de interés generalizado para todo el colectivo de sujetos obligados u otros interesados.

Elaboración de mayores desarrollos regulatorios, directrices y recomendaciones.

La normativa en materia de PBC y FT se encuentra principalmente en la LPBC y su Reglamento. Estas dos normas, por su propia posición en la pirámide normativa, no definen en detalle algunas cuestiones y materias, en las que, desde un punto de vista de cumplimiento normativo, necesitarían un mayor desarrollo de aspectos técnicos para asegurar un adecuado cumplimiento de la norma.

Es cierto que el SEPBLAC tiene publicados en su página web diferentes documentos, tales como recomendaciones sobre medidas de control interno, guías de cumplimiento orientativas sobre aspectos concretos (p.ej., en relación con fideicomisos anglosajones (*trusts*) o las obligaciones aplicables a

fundaciones y asociaciones), buenas prácticas sobre la aplicación de listas de sanciones, así como listados de algunas preguntas frecuentes. Sin embargo, el sector RegTech precisa un mayor volumen de orientaciones y guías prácticas que faciliten la comprensión de los criterios formales de supervisión, así como también directrices, orientaciones o cuestionarios prácticos (*Q&A*) que ayuden a un cumplimiento efectivo de la normativa y las expectativas de las autoridades de supervisión.

Actualización de los sistemas de identificación autorizados por SEPBLAC.

Si bien esta cuestión se desarrollará con más detalle en el apartado 5.2 siguiente en relación con el segmento de RegTech de Servicios de Confianza, los asociados de AEFI dedicados a la implementación de sistemas de video-identificación y otros sistemas de identificación no presencial mediante videoconferencia consideran que debería valorarse la adopción de una decisión de adecuación por parte del SEBPLAC que alinee los requisitos exigidos desde 2016 para la video-identificación y videoconferencia en operaciones en remoto con los exigidos por la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, dado el progreso que ha supuesto la aprobación de la Orden y las ventajas que traería una mayor uniformidad en cuanto a requisitos aplicables.

Homologaciones o auditorías que certifiquen los sistemas de los sujetos obligados.

En línea con lo anterior, en materia de sistemas de identificación de clientes a través de videoconferencia y video-identificación, el SEPBLAC tiene publicados sendos documentos en los que autoriza el uso de estos procedimientos y enumera los requisitos que estos tienen que cumplir para resultar válidos y conformes con la normativa.

A pesar de ello, en la práctica, los prestadores de estos servicios de identificación electrónica en ocasiones no tienen claro si el grado de cumplimiento que tienen los sistemas que ofrecen a sus clientes es acorde a la normativa aplicable. El conjunto de asociados RegTech considera que contar con un proceso de homologación o auditoría de dichos sistemas sería de gran ayuda para dotarles de una mayor confianza jurídica, especialmente en los supuestos de supcontratación o externalización a terceros.

Hasta el momento, estos sistemas de videoconferencia y video-identificación no están siendo sometidos a auditorías previas, ni cuentan con una certificación u homologación diseñada por parte del SEPBLAC. Por un lado, la ausencia de estos requisitos facilita la puesta en práctica de estos procedimientos y elimina las posibles trabas burocráticas y regulatorias para su implementación, pero por otro lado , atendiendo a la relevancia que tienen estos procedimientos para las entidades (para algunas de ellas, la única forma de autenticación inicial con sus clientes), la instauración de alguna forma de homologación o acreditación del cumplimiento de los requisitos por parte del SEPBLAC tendría un impacto positivo.

De esta forma, se propiciaría el surgimiento en el mercado de prestadores de servicios dirigidos a facilitar estos procedimientos con soluciones más seguras, robustas y alineadas con la normativa.

Ausencia de iniciativas de integración de información entre sujetos obligados

En el ámbito de PBC y FT, resulta esencial la obtención de información, no sólo del cliente directamente, sino también de fuentes públicas y privadas que complementen la información facilitada de primera mano por el cliente o desmientan lo indicado por éste.

Desde el segmento de PBC y FT, se echan de menos también la existencia de iniciativas destinadas a que los diferentes sujetos obligados compartan información sobre clientes en cuestiones que tengan trascendencia en materia de PBC y FT. Este tipo de iniciativas no son extrañas en el sector financiero, si bien se centran principalmente en información sobre el nivel de endeudamiento de los clientes (por ejemplo, la Central de Información de Riesgos gestionada por el Banco de España) y no existencia de impagos por parte de los mismos (como es el caso de los ficheros de solvencia gestionados por entidades de naturaleza privada).

La posibilidad de compartir información entre los sujetos obligados en materia de PBC y FT permitiría mejorar la prevención de operativas sospechosas de lavado de dinero o de financiación del terrorismo. En efecto, permitiría una mejor identificación de clientes, la detección de aquellos clientes que pueden plantear un mayor riesgo (aunque ello no se evidencie en los documentos facilitados) y una mayor capacidad de anticipación ante posibles operaciones sospechosas.

Mejoras en el acceso a información sobre titularidad real

La identificación del titular real puede resultar una de las cuestiones más complejas en el proceso de diligencia debida de los sujetos obligados. Éstos tienen la obligación de comprobar que la información que ha sido facilitada por el cliente es consistente con el resto de información proporcionada, así como su grado de veracidad.

En este sentido, resulta también esencial el acceso que puedan tener los sujetos obligados y las entidades de RegTech a fuentes de información fiable en las que figuren los datos de titulares reales de personas jurídicas. A día de hoy, dichas fuentes existen, como es el caso del Registro de Titulares Reales del Colegio de Registradores o la Base de Datos de Titularidad Real del Consejo General del Notariado, si bien ambas con ciertas trabas para su acceso.

La puesta en marcha del Registro de Titularidades Reales, previsto por el Real Decreto-ley 7/2021, de 27 de abril, y gestionado por el Ministerio de Justicia, genera también una cierta preocupación para los asociados de AEFI, en la medida en que sólo se contempla un acceso completo a los sujetos obligados de la LPBC, pero no a los prestadores de servicios de RegTech, que tendrían el mismo nivel de acceso que el de cualquier otro ciudadano.

Retos derivados de la operativa con monedas virtuales y criptomonedas

Con la aprobación del Real Decreto-ley 7/2021, de 27 de abril, los proveedores de servicios de cambio de monedas virtuales (como criptomonedas, tales como *Bitcoin, Ethereum, Dogecoin*, etc.) por moneda fiduciaria y de custodia de monederos electrónicos (*e-wallets*) pasan a ser sujetos obligados de la LPBC.

Si bien esta novedad supone también una oportunidad para las entidades RegTech de PBC, al incrementar el número de sujetos obligados con necesidades de adaptación a la normativa de PBC y FT, implica también nuevos retos.

Los servicios de cambio de monedas virtuales y custodia no deberían presentar grandes diferencias en cuanto a la amplia tipología de clientes con las que ya tratan las entidades financieras, por lo que, en materia de identificación de clientes, los procesos que ya ofrecen las entidades de RegTech podrían instaurarse también en proveedores de servicios de criptomonedas. Sin embargo, aunque la operativa de sus clientes pueda presentar elementos comunes con la de los clientes de entidades financieras, las RegTech de PBC deberán también actualizar y ajustar sus sistemas y procesos para asegurar su capacidad de detección de operaciones sospechosas propias o específicas del ámbito de las criptomonedas.

5.2. Retos del segmento RegTech de Servicios de Confianza

Desconocimiento del sector y falta de formación

Del mismo modo que el resto de los tipos de RegTech, este subgrupo se enfrenta a un primer e importantísimo reto derivado del desconocimiento y la confusión generalizados que envuelve su ecosistema. Preocupa que, tras varios años de legislación, y a pesar del gran número de operadores existentes en el mercado, ni los ciudadanos de a pie, ni tampoco los profesionales, o incluso trabajadores del sector público, parecen conocer y tener claras cuestiones básicas sobre la naturaleza, la tipología o los casos de uso de estos servicios.

Los sujetos a quienes se dirigen estos servicios, o quienes deben recibirlos, manifiestan inseguridad respecto a cuestiones básicas de confiabilidad jurídica. Cuestiones que se suman, además, a la elevada complejidad técnica y sofisticación (en muchos casos) en términos de infraestructura tecnológica que caracteriza el uso de estos servicios.

En efecto, la normativa regula estos servicios de forma teórica, dejando al criterio de expertos técnicos y jurídicos la calificación de estos servicios. El resultado de ello es que se hayan producido interpretaciones dispares y contradictorias en el contexto de la calificación de estos servicios y que incluso los expertos del sector discrepen en aspectos que atañen a la seguridad jurídica y técnica de los usuarios de estos servicios (lo cual, como cabe esperar, redunda en mayor confusión). Tampoco se han producido hasta la fecha suficientes pronunciamientos judiciales que diluciden o ayuden a

esclarecer los claroscuros y ambigüedades que suscita el empleo de los distintos servicios electrónicos de confianza que han proliferado en el mercado.

A tal efecto, este subgrupo de entidades RegTech considera que sería práctico que la autoridad de supervisión, en calidad de organismo público "neutral", publique guías, videos divulgativos o directrices y materiales dirigidos a dar a conocer al público general aspectos básicos y esenciales de la normativa o del Reglamento eIDAS, así como a evitar confusiones o interpretaciones equivocadas a los potenciales usuarios, beneficiarios o afectados por estos servicios.

Los servicios electrónicos de identificación o autenticación de identidad, por su parte, también padecen del desconocimiento generalizado. En este caso, cabe destacar que se trata de una cuestión que deriva del disperso marco regulatorio que reconoce dichos servicios y la falta de claridad respecto a los casos de uso a los que son aplicables. Igualmente, como ha sido objeto de análisis en este Libro Blanco, el sector se enfrenta a la aceptación de los distintos órganos de referencia, entre ellos, el SEPBLAC, el Ministerio de Asuntos Económicos y Transformación Digital y también la AEPD. Por no mencionar el efecto que genera la propuesta de Reglamento EUid, que prevé que se produzca un cambio de paradigma en relación con los métodos de identificación a escala comunitaria en los próximos años.

Este importante reto inquieta significativamente al sector, que siente sobre sus hombros el peso de tener que responsabilizarse casi en exclusiva de la labor informativa de forma dispersa y descoordinada. Todo supone un hándicap y un freno a la evolución y consolidación del sector, y requiere grandes recursos y esfuerzos que desincentiva a todos los eslabones de la cadena del servicio. Es por ello por lo que el sector propone una serie de medidas dirigidas a concienciar sobre este problema y a solicitar apoyo institucional en remediar la situación con carácter urgente. El apartado 6, recoge un conjunto de recomendaciones concretas dirigidas a tal fin.

Falta de una estrategia nacional clara

Otro reto vinculado al anterior es la falta de un posicionamiento definido en términos de estrategia de país.

El sector reclama que se esboce y promueva institucionalmente una estrategia concreta sobre las pautas que deban guiar el empleo de esta clase de servicios por la ciudadanía, las empresas y los servicios públicos, teniendo en cuenta factores generacionales y otros factores relacionados con el interés general de todos los *players* del ecosistema.

Del mismo modo que viene adoptándose desde hace años la estrategia nacional de ciberseguridad promovida por el Centro Criptológico Nacional, o se baraja la estrategia nacional en el ámbito de la Inteligencia Artificial por el Ministerio de Economía, el sector RegTech clama por una estrategia propia (*National Digital Trust Strategy*), tal y como se incluye en el bloque de recomendaciones incluidas en el apartado 6 siguiente.

Falta de supervisión del cumplimiento de la normativa

Ligado con lo anterior, el sector manifiesta tener interés en que el regulador supervise de forma activa el cumplimiento de la normativa que, a día a hoy, requiere el empleo de determinados servicios de identificación o firma electrónica y que, según trasladan, no estarían siendo cumplidos en todos los escenarios o no estarían siendo cumplidos de forma correcta.

La supervisión proactiva por parte de los reguladores y la adopción de medidas sancionadoras ante la falta de cumplimiento de estos requisitos ayudarían a generar conciencia sobre la relevancia de estas exigencias, que a su vez redundaría en un mayor conocimiento y seguridad jurídica del ecosistema. El apartado 6 recoge una recomendación concreta dirigida a solicitar dicha cuestión al regulador.

Necesidad de estar preparados para la implementación del nuevo paradigma de Identidad Digital Europea

Otra cuestión que inquieta al sector es la implementación nacional del nuevo paradigma de identificación digital que baraja la UE tras la publicación de la propuesta de Reglamento (UE) relativa al nuevo marco para la Identificación Digital Europea.

Según los asociados de la AEFI pertenecientes a esta vertical, este nuevo planteamiento requerirá de numerosos esfuerzos coordinados y un trabajo previo y planificado por parte de los expertos del sector privado, que complemente las aportaciones que los Estados Miembros ya están realizado en el marco del eIDAS 2 *toolbox* liderado por *eIDAS Expert Group*, y que debe entregar sus resultados antes de finalizar 2022. En este sentido, el sector reclama la constitución de un Comité de Expertos que trabaje en la futura adaptación nacional del nuevo paradigma, de la mano y en coordinación con el sector y con las instituciones de referencia.

Actualización de los sistemas de identificación autorizados por SEPBLAC

En otro orden de las cosas, el sector RegTech se enfrenta igualmente a un conjunto adicional de retos y reverses que contribuyen a la desaceleración del crecimiento y el despliegue de su pleno potencial.

Un ejemplo de ello es que los numerosos esfuerzos y recursos dedicados a la negociación, diseño y elaboración de la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, no hayan sido reciclados para otros casos de uso en los que dicho marco jurídico represente un progreso y contribuya a dotar el sistema de mayor uniformidad.

En este sentido, los asociados de AEFI consideran que debería valorarse la adopción de una decisión de adecuación por parte del SEBPLAC que alinee los requisitos.

Igualmente sería conveniente valorar la extrapolación de dichos requisitos a otros casos de uso o escenarios en los que estos nuevos sistemas de identificación puedan ser adecuados, así como continuar con la labor de examinar y autorizar otros sistemas o tecnologías que puedan servir para los mismos fines, ser menos intrusivos y proporcionar una seguridad equivalente a la identificación presencial.

Necesidad de adoptar estándares y especificaciones técnicas comunitarios para el reconocimiento de tecnologías como la biometría

El desarrollo de nuevas tecnologías aplicables al ámbito de este tipo de RegTech debe ir acompañado igualmente de un marco jurídico favorable que contribuya a dotar de seguridad y proporcionar pautas claras y especificaciones concretas que sirvan de referencia y orientación para quienes apuesten por estas tecnologías.

Así, existe un panorama incierto respecto a los estándares técnicos fijados por las autoridades locales para dar cobertura al empleo de sistemas basados en biometría, por ejemplo, en el contexto de firmas electrónicas o en el de autenticaciones o verificaciones de identidad.

En este sentido, el sector reclama la adopción a nivel europeo de estándares propios para la homologación de nuevas tecnologías en línea con los estándares de Estados Unidos dictados por el *National Institute of Standards and Technology* (*NIST*).

Necesidad de dotar de mayor confiabilidad jurídica a sistemas basados en nuevas tecnologías homologadas o combinaciones de varias

El fomento de las nuevas tecnologías incorporadas en sistemas de firma electrónica o de identificación digital que sean distintas a la tecnología digital o de criptografía asimétrica que caracteriza los sistemas cualificados (p. ej. las firmas electrónicas basadas en certificados) es también un caballo de batalla para el sector.

En este sentido, el reconocimiento y otorgamiento de confianza jurídica a estos sistemas en equivalencia con los basados en tecnología de cifrado y criptografía asimétrica es otra batalla que promueve la búsqueda de soluciones que amplíen el abanico de opciones y permitan explorar nuevos escenarios de posibilidades para los distintos casos de uso.

Otra recomendación del sector es impulsar una reforma legislativa que otorgue un mayor grado de reconocimiento a sistemas que se basen en estas tecnologías, con una mayor certeza de sus efectos jurídicos.

Necesidad de mejorar el acceso y disponibilidad de bases de datos públicas de consulta y verificación

Algunos proveedores de certificados cualificados han detectado que los servicios de verificación y consulta de las bases de datos en las que se apoyan para ofrecer sus servicios no son todo lo accesi-

bles y rápidos que cabe esperar. Ello ha implicado retrasos e interrupciones en la prestación de sus servicios que dificulta enormemente su labor.

En este sentido, el bloque de recomendaciones del apartado 6 incorpora una propuesta dirigida al Ministerio de Asuntos Económicos y Transformación Digital para la mejora urgente de la disponibilidad y accesibilidad a las bases de datos de la plataforma de intermediación del Servicio de Verificación y Consulta de Datos de la Secretaría de Estado de Digitalización e Inteligencia Artificial a la que se refiere el artículo 11.3 de la Orden ETD/465/2021, de 6 de mayo.

Insuficiente adopción de Servicios de Confianza por parte del cuerpo de notarios y registradores

Otro de los retos del sector está relacionado con el bajo nivel de acogida que los servicios de identificación y confianza electrónicos tienen por parte de instituciones como el cuerpo de notarios y registradores, en el marco de la realización de sus funciones.

La cuestión no es que los notarios o los registradores empleen ellos mismos sistemas de firma electrónica (lo cual ya es así, dado que cuentan con su propio organismo de certificación), sino que acepten el uso de estos servicios por parte de usuarios interesados en el cierre de transacciones, el otorgamiento de documentos públicos o la inscripción de documentos en registros por vía telemática que incorporen firmas electrónicas.

A tal efecto, y sin perjuicio de la reserva de funciones reconocida en la LSEC que establece que "*lo dispuesto en esta ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente la facultad de dar fe en documentos en lo que se refiere al ámbito de sus competencias siempre que actúen con los requisitos exigidos en la ley*"[35], el sector anhela que se produzcan progresos hacia la aceptación de estos sistemas en aras de modernizar, simplificar y agilizar la operativa que caracteriza este eslabón de la cadena y facilitar las trabas administrativas al público en general.

A tal efecto, el recientemente publicado texto del Anteproyecto de Ley de fomento del ecosistema de las empresas emergentes ya incluye una propuesta en esta dirección al establecer que: "*El Consejo General del Notariado y el Colegio de Registradores de España promoverán la adaptación de las aplicaciones informáticas que deban emplear los ciudadanos para relacionarse electrónicamente con los notarios y los registradores con el fin de que sean compatibles con cualquier navegador, admitan todas las firmas y sellos electrónicos incluidos en la "lista de confianza de prestadores de servicios de certificación" y pueda interactuarse con ellas desde dispositivos móviles (…)*"[36].

[35] Véase la disposición adicional primera de la LSEC.
[36] Artículo 16 del Anteproyecto de Ley de fomento del ecosistema de las empresas emergentes, disponible en: https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/210706-APL-START-UPS.pdf.

En este sentido, en el bloque de recomendaciones, se incluye una propuesta dirigida a solicitar precisamente que se promueva esta cuestión con carácter urgente y como aspecto crítico y esencial para el interés público en general.

Escasa oferta de soluciones cualificadas de un solo uso o de tiempo limitado que proporcionen la agilidad y seguridad jurídica que requieren los mercados

Otro de los retos que el sector reconoce tener que afrontar es el desarrollo de soluciones tecnológicas operativas y ágiles que den respuesta a las necesidades de los mercados y a la velocidad y agilidad que requiere el cierre diario de cientos de operaciones mercantiles de toda índole.

El sector es consciente de que aún está pendiente el desarrollo, promoción y adopción de más servicios de confianza "cualificados" y de un solo uso o de duración limitada pensados para contextos en los que, por razones operativas o de carácter internacional, otras alternativas no resulten lo suficientemente ágiles.

Una de las principales quejas del sector profesional y de los usuarios en relación con el uso de sistemas de firma electrónica cualificada es que normalmente se trata de soluciones que requieren de cierto tiempo de asimilación para poder ser adoptadas y comprendidas en el seno empresarial de forma ágil. No se trata de un proceso rápido que pueda completarse y tenerse preparado en veinticuatro horas, sino que requiere de la negociación del sistema, de formación a los afectados, de la realización de trabajos técnicos y de la verificación de las identidades de los usuarios. Aunque la verificación de la identidad pueda realizarse hoy en día mediante sistemas de video-conferencia en los términos de la OM ETD/465/2021, lo cierto es que no se percibe como un ahorro de tiempo suficiente, sino que, la sensación continúa siendo que el proceso es excesivamente largo.

Cierto es también, y cabe reseñar, que, en la mayoría de los casos, el problema deriva de una mala gestión de expectativas y una falta de previsión y entendimiento sobre las diferencias entre el proceso físico y el proceso cibernético. Durante años, en el plano presencial, firmar un documento o identificar a una persona era una cuestión que podía realizarse en minutos, sin necesidad de prepararse y con poco más que un bolígrafo y el tiempo de desplazamiento. Ahora, en el plano cibernético, para poder igualar o superar esa rapidez en la gestión, por ejemplo, de firmas de documentos multi-parte, debe previamente haberse pasado por, primero, un proceso de implementación del sistema en el seno empresarial de todos los intervinientes, y segundo, haberse realizado un proceso de adaptación, lo cual es algo para lo que muchos operadores no están mentalizados y no forma parte de sus expectativas.

Ello hace que en contextos donde el tiempo apremia y haya varias partes, por ejemplo, extranjeras, se planteen grandes inconvenientes y reticencias hacia el empleo de sistemas cualificados que requieran mayores trámites, y se opte por el uso de sistemas más elementales, sacrificándose en dichos casos niveles y capas de seguridad (tanto técnicas como jurídicas), a cambio de rapidez.

Por ello, urge el desarrollo y fomento de soluciones cualificadas, por ejemplo, de un solo uso o de duración limitada, que se adapten a los tiempos y exigencias del mercado y proporcionen las máximas garantías de seguridad y de confiabilidad jurídica, así como mayor flexibilidad, incluso en el plano internacional.

Restricciones derivadas de la intervención de operadores monopolísticos de índole internacional, que no reconocen los estándares del Reglamento eIDAS

Finalmente otro aspecto con componente internacional es el reto relacionado con el reconocimiento por parte de sistemas operativos y navegadores de grandes plataformas en su mayoría con origen en Estados Unidos y como su criterio y sus propias restricciones y políticas afectan y limitan a los prestadores europeos de servicios de autenticación cualificada de sitios web (QWAC).

Por ello, los prestadores afectados insisten en el deber de trabajar en iniciativas coordinadas con la UE para lograr la independencia y reconocimiento automático de los servicios de confianza QWAC por los navegadores y sistemas operativos controlados por grandes plataformas como Google, Microsoft, Apple o Mozilla. Esta situación está suponiendo trabas y restricciones adicionales para el pleno despliegue de estos servicios cualificados e inscritos en las correspondientes *Trust Lists* europeas, pero no por quienes controlan los sistemas operativos. Dichos operadores que actúan como agentes supervisores llevan a cabo actuaciones de veto incluso llegando a desconfiar de dominios que no se adapten a sus propios estándares, generando así una doble carga para los afectados y una sensación de supeditación contraria a las buenas prácticas de mercado y a la libertad de prestación de servicios.

A tal efecto, en el apartado 6, se incluyen recomendaciones dirigidas a explorar fórmulas para remediar esta situación.

5.3. Retos del segmento RegTech de GRC

Mayor exigencia por parte de los supervisores de Cumplimiento Normativo

Uno de los pilares de la regulación financiera consiste en garantizar la trazabilidad de la información. Sin embargo, en ocasiones las entidades mantienen procesos internos en materia de gestión de riesgos, cumplimiento y auditoria interna escasamente digitalizados, lo que dificulta las tareas de supervisión e incrementa el riesgo operacional.

Por esa razón, proponemos que los supervisores sean más estrictos a la hora de exigir que las distintas fuentes de información estén bien conectadas y en este sentido, las herramientas GRC han nacido para ayudar a cumplir con la premisa básica de asegurar la trazabilidad de la información.

Establecer estándares para las soluciones de GRC

Ligado a lo anterior, para que se garanticen que las soluciones de GRC son adecuadas y útiles para cumplir con los objetivos y exigencias normativas, es necesario que se establezcan una serie de condiciones técnicas mínimas de obligado cumplimiento.

Es importante que se estandaricen las características que todos los sistemas de GRC deben cumplir y, de esta manera, las soluciones sean las adecuadas, incluyendo los requerimientos que exige un buen sistema preventivo de ciberseguridad.

Entendemos que el órgano supervisor tendría mucho que aportar a la hora de garantizar la robustez de los sistemas y que estos sean escalables.

No cabe duda de que este reto puede suponer un mayor esfuerzo por parte de las diferentes entidades que implanten un sistema de GRC, pero será la mejor garantía para que realmente aporten valor al conjunto del sistema financiero.

5.4. Retos del segmento RegTech de *Reporting*

Creciente complejidad normativa

El principal reto al que tienen que hacer frente las entidades del segmento de RegTech de *reporting* es la creciente complejidad normativa de las obligaciones de *reporting* a reguladores.

Esta complejidad deriva de diferentes fuentes. En primer lugar, existen bloques normativos relativamente consolidados que sufren modificaciones con relativa frecuencia para la introducción de nuevas obligaciones de información a supervisores (p.ej., véase, por ejemplo, la normativa de servicios de pago, modificada por la Directiva 2366/2015/EU (PSD2), que introduce nuevas obligaciones de información que no existían con la Directiva anterior).

En segundo lugar, aparecen conjuntos normativos novedosos que, además de obligaciones de carácter material, incluyen también obligaciones formales de información. Es el caso, por ejemplo, del Reglamento europeo sobre derivados extrabursátiles (Reglamento (UE) 648/2012 (EMIR)), o bien el Reglamento europeo sobre operaciones de financiación de valores (conocido como SFTR).

Todas estas novedades exigen a los prestadores de servicios de *reporting* un esfuerzo sustancial y constante de actualización normativa que tiene diversas implicaciones para sus actividad. Por un lado, ese esfuerzo de seguimiento de la normativa implica costes fijos de revisión y actualización de conocimientos de diversa índole (jurídicos, tecnológicos, financieros, etc.). Por otro lado, las noveda-

des normativas suponen o bien la modificación de los sistemas y procesos que el prestador de servicios RegTech ya tenía definidos para cumplir con la normativa anterior, o bien el desarrollo de nuevos procesos para adaptarse a conjuntos normativos de nueva creación.

Otro aspecto relevante de la creciente complejidad a la que tienen que hacer frente las entidades RegTech de *reporting* es, en determinadas situaciones, la ausencia de reglas, directrices u orientaciones clara para bajar al detalle las obligaciones legales aprobadas en los diferentes textos normativos. En efecto, dichos textos se limitan a fijar el contenido de los diferentes reportes y su frecuencia, pero sin aclarar aspectos que pueden ser tanto operativos y técnicos, como jurídicos (como, por ejemplo, interpretar el contenido real del reporte exigido por la norma).

Si bien los reguladores hacen esfuerzos para intentar proporcionar ciertos detalles sobre dichos reportes, a través de diferentes herramientas, tales como Reglamentos Delegados o de Ejecución, directrices, recomendaciones, orientaciones, preguntas y respuestas (*Q&A*) o publicación de consultas presentadas por entidades, tales esfuerzos resultan, en algunos casos, insuficientes, no siendo posible conocer con exactitud o seguridad el alcance y significado real de las exigencias legales.

El sector RegTech es consciente de la enorme dificultad de definir tales detalles en materias que son altamente complejas, pero celebraría cualquier avance o iniciativa que permitiera arrojar mayor claridad regulatoria a este respecto.

Creciente complejidad operativa

Aparte de la complejidad normativa, el hecho de que los reportes a los reguladores se remitan, por lo general, a través de medios electrónicos incrementa la complejidad operativa asociada a tales envíos.

Algunos de los reportes regulatorios pueden ser remitidos los reguladores sin complejidad, o con un nivel de complejidad mínimo o razonable. Sin embargo, para reportes más complejos en cuanto a su contenido o frecuencia, no es extraño que vengan también acompañados de una elevada complejidad también operativa, por la dificultad de trasladar la información a las correspondientes plataformas o ficheros informáticos exigidos por los reguladores[37], o por la forma de su remisión (por ejemplo, a través de plataformas que requieren credenciales de seguridad o certificados de autenticación complejos de obtener).

Asimismo, es frecuente también que los propios reguladores modifiquen y actualicen sus propios sistemas y plataformas, mediante la introducción de cambios o mejoras en sus instrucciones técnicas. Esto tiene un doble efecto. Por un lado, implica revisar y comprender el alcance de las nuevas instrucciones técnicas y, por otro lado, desarrollos operativos que, en una instancia final, tienen que ser comprobados y validados por la entidad en cuestión y el supervisor para verificar que funcionan adecuadamente.

[37] Uno de los retos a los que se presenta el reporting regulatorio es, en este sentido, la dificultad de traslado del lenguaje expresado en las diferentes normativas reguladoras al lenguaje de codificación en que se basan las soluciones tecnológicas.

Al igual que con la complejidad normativa, las entidades de RegTech de *reporting* comprenden y aceptan la dificultad operativa de su actividad, pero también sugieren la introducción de medidas y sistemas operativos que les concedan seguridad (técnica y jurídica) y estabilidad tecnológica (con el correspondiente ahorro de costes).

Duplicidad de reportes

En línea con los dos elementos anteriores, y ante la proliferación de normativa regulatoria en diferentes jurisdicciones, no es tampoco infrecuente que las entidades financieras queden sujetas, respecto de un mismo hecho u operación, a obligaciones de información en dos Estados diferentes.

En tales casos, las entidades deben reportar la misma información (o con modificaciones o matices) a dos supervisores a través de sus correspondientes plataformas tecnológicas.

Estas duplicidades pueden no generarse necesariamente en relación con dos supervisores de la UE, pero sí pueden producirse, por ejemplo, en relación con un supervisor de la UE y otro de un tercer Estado (p.ej. Reino Unido).

En estos casos, el prestador de servicios de RegTech de *reporting* puede tener que abstenerse de realizar uno de los dos reportes (por lo general, el relativo al tercer Estado), o bien verse obligado a expandirse internacionalmente para poder tener acceso a otros reguladores si quiere poder tener como clientes a grandes grupos financieros internacionales.

Economías de escala e internacionalización

En relación con esa posible internacionalización del negocio de los prestadores de servicios de RegTech de *reporting*, debe tenerse en cuenta que estos servicios están basados en una estructura de economías de escala.

Al exigir el diseño e implementación de grandes desarrollos complejos, es necesario encontrar el mayor número de aplicaciones para los mismos. Considerando el tamaño del sector financiero en nuestro país, uno de los retos a los que se enfrentarían estos prestadores de servicios es la posible necesidad de internacionalizar su negocio, para acceder a un mayor número de entidades, siempre que puedan aprovechar de una manera eficiente la estructura y desarrollos de los que ya dispongan en España.

5.5. Otros retos

Además de los retos descritos en los apartados precedentes, el RegTech se enfrenta hoy día a otros retos que condicionan la entrada y también la permanencia de los operadores de este sector. A continuación se resumen brevemente algunos de estos restos:

Costes y tasas elevados, en términos comparativos

En este sentido, algunos asociados de AEFI señalan que, en términos relativos, en España los costes o tasas a las que está sujeta su actividad son superiores a los de otros países comunitarios. Por ejemplo, enfatizan que los costes de certificación o de las auditorías para obtener o mantener el grado de cualificación o para acreditar el cumplimiento de los requisitos de eIDAS, son más elevados a nivel local. Ello puede condicionar la decisión de establecer originariamente su sede en España o de si trasladarse a otro país de la UE al cabo de un tiempo, especialmente si otros países ofrecen mejores condiciones. Por ello, algunos asociados del sector abogan por defender la aprobación de incentivos fiscales o facilidades administrativas que contribuyan a generar un clima favorable para la consolidación y expansión del sector en nuestro país.

Elevada competencia internacional

En línea con lo anterior, también hay voces que alertan de que la competitividad internacional es elevada. Existen operadores mundiales que están acaparando un volumen de mercado y una popularidad significativa, especialmente por el ofrecimiento de soluciones del tipo *commodity* que no siempre cumplen con los estándares europeos o que no cuentan con un mecanismo de evidencia jurídica suficiente[38].

La situación dificulta que otros operadores locales de menor envergadura -pero que ofrecen incluso servicios más avanzados tecnológicamente o seguros desde el punto de vista jurídico- tengan la misma visibilidad y reconocimiento. Los asociados alertan de que se trata de una situación desfavorable, no solo para el conjunto de proveedores, sino también para su público objetivo. Argumentan que dichos operadores, en su mayoría, de origen estadounidense, se benefician del grado de desconocimiento de los usuarios, que ignoran los posibles inconvenientes jurídicos o técnicos a los que pueden tener que enfrentarse en el futuro. De nuevo, la situación debe remediarse mediante la divulgación de conocimiento y la formación a todos los distintos eslabones vinculados al ecosistema.

Rapidez y continuo cambio en el marco normativo

Otro gran reto al que se enfrentan las sociedades del sector RegTech es la continua y rápida evolución del marco normativo aplicable a los servicios que prestan. En los últimos años y especialmente durante la crisis sanitaria del Covid-19, la adopción de nuevas regulaciones y requisitos ha determinado, condicionado y moldeado la expansión del sector. Por ejemplo, en el ámbito de la prevención de blanqueo de capitales, este año fue transpuesta en España la Quinta Directiva en materia de PBC mediante la aprobación del Real Decreto-Ley 7/2021, de 27 de abril. Dicha novedad, ha supuesto para los proveedores de RegTech la necesidad de realizar ajustes para adaptar sus servicios a la nueva definición de algunos de los requisitos exigibles.

[38] Véase como ejemplo la sentencia de la Audiencia Provincial de Lleida, Sección 2ª, 74/2021 de 29 de enero. Rec. 158/2020.

Igualmente, en el ámbito de la ciberseguridad, también son varias las propuestas que se barajan en un medio plazo, siendo relevante para el sector financiero la aprobación del Reglamento DORA. Dicha novedad condicionará muy significativamente al sector.

Finalmente, merece la pena destacar la proliferación de normativa en el ámbito de los Servicios de Confianza. Además de la LSEC y la reciente aprobación de la OM ETD/465/2021, se espera que próximamente se produzca un total cambio de paradigma en la identificación digital europea mediante la aprobación del Reglamento EUid, también referido como el esquema del *European Digital Identity and Wallet framework*. Este cambio condicionará significativamente la tecnología empleada hasta la fecha y requerirá la suma de esfuerzos para la adopción de una infraestructura común para todos los Estados Miembros.

Rápida evolución de la tecnología

En la actualidad, existe ya la previsión de una serie de nuevos hitos que seguirán moldeando y condicionando significativamente la evolución y expansión de los casos de uso de este sector. La regulación de las nuevas tecnologías como la inteligencia artificial, las criptomonedas, los llamados Non Fungible Tokens o el blockchain prometen protagonizar, sin lugar a duda, los siguientes episodios de un sector que está llamado a ser crítico para la digitalización empresarial de nuestro país.

6. PROPUESTAS DEL SECTOR REGTECH

A continuación, se exponen, de manera esquemática, las propuestas del sector RegTech representado en la AEFI, para la adopción de medidas, catalogadas en urgentes, importantes y necesarias, en función de la rapidez con la que deban de adoptarse y su relevancia[39].

[39] La categorización de las distintas medidas se basa en una encuesta realizada por Cuatrecasas durante los meses de julio a septiembre de 2021 a los asociados de AEFI.

6.1. MEDIDAS URGENTES

1. Creación de un Comité de Expertos que trabaje en la futura adaptación española al nuevo paradigma de identificación digital que baraja la UE tras la publicación de la propuesta de Reglamento (UE) relativa al nuevo marco para la Identificación Digital Europea. (importante)

2. Habilitación de mayores vías de comunicación con los organismos supervisores, con el fin de permitir realizar consultas y mantener un diálogo más fluido. Esta medida debe tener por objetivo la mejora del nivel de publicaciones relativas a los criterios de los supervisores y a aumentar los canales, guías y directrices para establecer un cuerpo unificado. Además, contribuirá a la disponibilidad, calidad, actualización y unificación de las bases de datos públicas accesibles para las RegTech (p.ej. titularidad real y situación crediticia o de morosidad).

3. Posibilidad de verificación de los sistemas de video-identificación u otros mecanismos que ofrezcan una seguridad equivalente a la identificación presencial por parte del SEPBLAC en su fase de diseño y antes de su implementación en las diferentes entidades.

4. Esbozar y promover institucionalmente una estrategia nacional sobre servicios electrónicos de confianza (*National Digital Trust Strategy*), que fomente su uso.

5. Supervisión institucional por el organismo de referencia del cumplimiento por parte de los sujetos obligados a las exigencias de emplear determinados sistemas para la autenticación de la identidad de sus clientes.

6. Uniformizar los requisitos autorizados por el SEPBLAC en 2016 para la video-identificación en operaciones no presenciales en el contexto del cumplimiento de la normativa de blanqueo de capitales con los exigidos por la Orden Ministerial ETD/465/2021, de 6 de mayo.

7. Implementar infraestructuras tecnológicas por parte de las autoridades de supervisión que faciliten la labor de las RegTech cuando sea necesaria la comunicación vía integración o APIs informáticas.

6.2. MEDIDAS IMPORTANTES

1. Inclusión de otras autoridades de supervisión participantes en la evaluación, aprobación y supervisión de los proyectos de *Sandbox*, tales como la Agencia Española de Protección de Datos, para una mayor transversalidad.

2. Crear institucionalmente un organismo de referencia o una subsecretaría específica que dicte directrices sobre la interpretación legislativa y promueva los distintos casos de uso de los servicios de confianza e identificación electrónicos.

3. Posibilidad de que las entidades RegTech no reguladas puedan ser aptas para que las entidades financieras puedan delegar sus obligaciones de KYC en ellas.

4. Trabajar junto con el regulador en alternativas colaborativas para pequeñas y medianas empresas, que necesitan cumplir con unos requerimientos AML pero que no pueden hacer frente a la inversión tecnológica que ello supone.

5. Fomentar el uso por parte de las autoridades de supervisión de sistemas informáticos de control automatizado del cumplimiento de la normativa tipo SupTech (*Supervisory Technology*) y RegTech de GRC.

6. Impulsar la adopción a nivel europeo de mayores estándares, recomendaciones o especificaciones técnicas para la homologación de nuevas tecnologías en línea con los estándares de Estados Unidos dictados por el *National Institute of Standards and Technology* (*NIST*).

7. Trabajar en iniciativas coordinadas con la UE para lograr la independencia y reconocimiento automático de los servicios de confianza QWAC por los navegadores y sistemas operativos controlados por grandes plataformas como Google, Microsoft, Apple o Mozilla.

6.3. MEDIDAS NECESARIAS

1. Impulsar una reforma legislativa que otorgue una mayor confiabilidad jurídica a los sistemas de firma electrónica e identificación digital basados en tecnologías que combinen sistemas de biometría, IA, *blockchain*, holografía, video- identificación, etc.

2. Impulsar la interoperabilidad semántica en el ámbito de la información regulatoria del sector financiero mediante la creación de un único diccionario de términos comunes para permitir un *reporting* armonizado tanto ante las autoridades de supervisión nacionales como europeas.

3. Mejorar y simplificar el proceso de la "traducción" de la letra de la norma que establece obligaciones de *reporting* regulatorio en las aplicaciones y programas tecnológicas utilizadas para la recopilación de la información y la realización del *reporting*.

4. Promover institucionalmente la formación de todos los agentes involucrados en el ecosistema *eTrust*: funcionarios, jueces, empleados públicos, etc. Así como, promover y difundir el uso de servicios de confianza e identificación electrónicos cualificados de un solo uso para contextos en los que, por razones operativas o de carácter internacional, otras alternativas no resulten lo suficientemente ágiles.

5. Realizar una campaña pública e institucional dirigida a dar a conocer y formar al público sobre la existencia, tipología y usos de servicios de confianza e identificación electrónicos.

6. Impulsar el uso de los servicios de confianza e identificación electrónicos por parte del cuerpo de notarios y registradores en el marco de la realización de sus funciones.

7. Alineación de la Ley de tarjetas de prepago con los requisitos exigidos por la normativa de blanqueo de capitales a los efectos de impulsar el uso de medidas de video-identificación u otros mecanismos que ofrezcan una seguridad equivalente a la identificación presencial.

7. BIBLIOGRAFÍA Y DOCUMENTOS ANALIZADOS

Agencia Española de Protección de Datos (AEPD), 2020. *14 equívocos con relación a la identificación y autenticación biométrica.* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf [consulta: septiembre de 2021].

ALAMILLO DOMINGO, Ignacio, 2019. Identificación, firma y otras pruebas electrónicas: la regulación jurídico-administrativa de la acreditación de las transacciones electrónicas, *Thomson Reuters*.

BUTLER, Tom y O'BRIEN Leona, 2019. Understanding RegTech for Digital Regulatory Compliance. En: LYNN Theo (ed.), et al. *Disrupting Finance: Fintech and Strategy in the 21st Century. Switzerland: Palgrave Pivot, Cham* [consulta: septiembre de 2021]. ISBN 978-3-030-02330-0. Disposnible en: https://link.springer.com/book/10.1007%2F978-3-030-02330-0#about.

European Banking Authority (EBA), 2021. *EBA Analysis of RegTech in the EU Financial Sector.* EBA/REP/2021/17 [en línea] Disponible en: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf [consulta: septiembre de 2021].

Financial Action Task Force (FATF), 2020. Statement by the FATF President: COVID-19 and measures to combat illicit financing. En: *Financial Action Task Force* [en línea]. Disponible en: https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html [consulta: septiembre de 2021].

Financial Conduct Authority (FCA), 2016. *Call for input on supporting the developtment and adopters of RegTech.* [en línea]. Disponible en: https://www.fca.org.uk/publication/feedback/fs-16-04.pdf [consulta: septiembre de 2021].

Finnovating, 2018. *Observatorio de Innovación y Tendencias RegTech 2018* [en línea]. Disponible en: https://www.finnovating.com/wp-content/uploads/2018/01/Informe-RegTech.pdf [consulta: septiembre de 2021].

LEMERLE, Matthieu, PATNAIK, Debasiah, RING, Ildiko, SAYAMA, Hiro y SIEBERER, Marcus, 2020. *No going back: New imperatives for European banking. En: McKinsey & Company* [en línea]. Disponible en: https://www.mckinsey.com/industries/financial-services/our-insights/no-going-back-new-imperatives-for-european-banking [consulta: septiembre de 2021]

SHIZAS, Emmanuel et al., 2019. The Global RegTech Industry Benchmark Report. *Cambridge Centre for Alternative Finance* [en línea]. Disponible en: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/the-global-RegTech-industry-benchmark-report/#.YTHWk2gzaUk [consulta: septiembre de 2021].

Thomson Reuters Regulatory Inteligence, 2021. *Fintech, RegTech and the Role of Compliance 2021*. [en línea]. Disponible en: https://legal.thomsonreuters.com/en/insights/reports/fintech-RegTech-compliance-report-2021 [consulta: septiembre de 2021].

AEFI LIDERANDO LA TRANSFORMACIÓN DE ESPAÑA COMO HUB FINANCIERO MUNDIAL

CREANDO UN ENTORNO FAVORABLE PARA EL DESARROLLO
DE EMPRESAS FINTECH E INSURTECH EN ESPAÑA

Edición 2022

Madrid, Junio 2022

contacto@asociacionfintech.es