AS COM
EXPERTOS EN COMPLIANCE

Asociación Española de Compliance

Galardón "Memorial José Manuel Maza"

2023

GANADOR

APROXIMACIÓN A LAS OBLIGACIONES DE COMPLIANCE PARA UN PROVEEDOR DE SERVICIOS DE ACTIVOS VIRTUALES

ROBERTO ANTONIO SÁNCHEZ LUCENA

www.asociacioncompliance.com

Asociación Española de Compliance

Galardón "Memorial José Manuel Maza"

APROXIMACIÓN A LAS OBLIGACIONES DE COMPLIANCE PARA UN PROVEEDOR DE SERVICIOS DE ACTIVOS VIRTUALES

Roberto Antonio Sánchez Lucena

Resumen: Los avances tecnológicos proyectados sobre la economía han convertido a los denominados *criptoactivos* en una revolución dentro del sector financiero. Este trabajo analiza un conjunto de riesgos corporativos surgidos de un entorno trepidante, desprovisto de regulación y a la zaga de un progreso tecnológico aventajado a requisitos legales y compromisos asumidos desde las organizaciones. La propuesta de *Reglamento MiCA* adquiere protagonismo como base cuya integración junto a una serie identificable de *obligaciones de compliance* se orienta a prevenir, detectar y ofrecer respuesta a múltiples riesgos intrínsecos a la operativa de una plataforma de intermediación de activos virtuales, desde la perspectiva sistemática de gestión de cumplimiento refundida por la reciente Norma ISO 37301.

Palabras clave: compliance, criptoactivos, blockchain, proveedores de servicios de activos virtuales, responsabilidad.

Abstract: The technological advances projected on the economy have turned the so-called crypto-assets into a revolution within the financial sector. This paper analyzes a set of corporate risks arising from a fast-paced environment, devoid of regulation lagging behind technological progress ahead of legal requirements and commitments assumed by organizations. The proposal for a MiCA Regulation acquires prominence as a basis whose integration together with an identifiable series of compliance obligations is aimed at preventing, detecting and responding to multiple risks intrinsic to the operation of a virtual assets brokerage platform, from the systematic perspective of compliance management consolidated by the recent ISO 37301 Standard.

Key words: compliance, crypto-assets, blockchain, virtual assets service providers, legal implications.

"Y porque lo he visto todo lo podré certificar a Vuestra Alteza".
Vasco Núñez de Balboa, *Carta al Rey de España* (1515).

ÍNDICE

I. INTRODUCCIÓN……4

II. DIGITALIZACIÓN DEL SISTEMA FINANCIERO Y EVOLUCIÓN DE LOS RIESGOS EMPRESARIALES……..……..5

2.1.1. Perspectiva nacional……..……..……..……..6
2.1.2. Perspectiva internacional……..……..6
2.2. DEFINICIONES……..7
2.2.1. Tecnología de registro descentralizado……..…..7
2.2.2. Criptoactivo……..……..……7
2.2.3. Proveedor de servicios de activos virtuales……..……8
2.3. SEGURIDAD JURÍDICA COMO SEGURIDAD RAZONABLE……8

III. OBLIGACIONES DE COMPLIANCE PARA LOS PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES……9

3.1. PROVEEDORES DE SERVICIOS Y LSSI……..10
3.2. PROVEEDORES DE SERVICIOS Y LPBCFT……..……11
3.2.1. Obligaciones del Proveedor……..……..…..11
3.2.2. GAFI y la Recomendación número 16 (travel rule)……..…..12
3.2.3. Régimen sancionador……..……..….12
3.3. PROVEEDORES DE SERVICIOS Y PROTECCIÓN DE DATOS……13
3.3.1. Obligaciones del Proveedor……..……..…..15
3.4. PROVEEDORES DE SERVICIOS Y SEGURO DE R. CIVIL……16
3.5. PROVEEDORES DE SERVICIOS Y CIBERSEGURIDAD……17
3.5.1. Cryptojacking……..……..17
3.5.2. Ransomware……..……..17

IV. AVANCES REGULATORIOS EN ESPAÑA……18

4.1. FISCALIDAD SOBRE LOS CRIPTOACTIVOS……18
4.1.1. Ley del IRPF y obligaciones del Proveedor……...18
4.1.2. LGT y obligaciones del Proveedor……...19
4.1.3. Modelos 172, 173 y 721 para declaración informativa a la AEAT….19
4.2. PUBLICIDAD DE CRIPTOACTIVOS Y CIRCULAR DE LA CNMV……..19
4.3. GESTIÓN DE INVERSIONES: REGISTRO EN EL BANCO DE ESPAÑA……20

V. CONCLUSIONES……...21

VI. BIBLIOGRAFÍA……23

I. INTRODUCCIÓN

La gestión empresarial implica responsabilidades derivadas de la interacción entre objetivos económicos, decisiones bajo un enfoque de riesgo y requisitos procedentes de un entorno cambiante. La proliferación de operadores y la escasa normativa del *sector cripto*[1] aconsejan analizar periódicamente los riesgos vinculados al desenvolvimiento de las *obligaciones de compliance* identificadas por el Órgano de administración (Asociación Española de Compliance [ASCOM], 2017)[2]. Para ello debe garantizarse por principio su *independencia, autoridad, el acceso a información relevante y recursos suficientes* (ASCOM e Instituto de Estudios Económicos 2020, p. 15)[3], especificando esas *obligaciones* (integradas por *requisitos legales* y *compromisos voluntarios* en la norma UNE-ISO 37301:2021[4]) como *"parte del proceso para disponer de un sistema de gestión de compliance adecuado para cada organización"* (CASANOVAS YSLA 2021, p. 101), marco extrapolable a la actividad de un proveedor de servicios de activos virtuales.

Configurado ese *marco de convergencia*, doctrina y jurisprudencia evidencian la magnitud económica de un mercado en expansión -v. gr. el Tribunal General de la Unión Europea denegó recientemente a una empresa radicada en la isla de Malta su pretensión de registrar como nombre comercial el de *"Blockchain Island"*, pues conduciría a identificar dicha isla (dado su marco fiscal favorable a las *tecnologías DLT*) con el nombre comercial de "*Isla del Blockchain*", primándola como **Hub**[5] atrayente de empresas de tecnología blockchain-.

Este trabajo analiza el ordenamiento vigente y las propuestas en trámite del sector, ofreciendo un enfoque basado en la identificación sistemática de las principales obligaciones de compliance de un proveedor de servicios sobre

---

[1] Grupos de Trabajo - Prevención del blanqueo de capitales, Criptoactivos y PBC/FT -ASCOM septiembre 2022- (p. 11).
https://www.asociacioncompliance.com/wp-content/uploads/2022/10/2022-GRUPO-TRABAJO-PREVENCION-DE-BLANQUEO-DE-CAPITALES.pdf

[2] Asignará también *"la prevención, detección y gestión de los riesgos derivados de su incumplimiento a uno o varios Programas de Compliance"*, ASCOM - *Libro blanco sobre la función de Compliance* (p. 21).

[3] Factores de un *Compliance* exitoso identificados en la conferencia anual *CARF Luzern Controlling - Accounting - Risk - Finance 2022* -Universidad de Lucerna, 1 y 2 de septiembre- (pp. 187-189).
https://www.hslu.ch/-/media/campus/common/files/dokumente/w/ifz/seminare-konferenzen/carf/konferenzband-carf-2022.pdf?la=de-ch

[4] Los apartados 3.25 y 4.5 simplifican ambos términos en una acepción amplia de *Compliance* siguiendo la norma ISO 37301:2021. Publicada el 13 de abril de 2021 *"especifica los requisitos y proporciona pautas para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión de cumplimiento efectivo dentro de una organización".*
ISO 37301:2021 - Compliance management systems — Requirements with guidance for use (iteh.ai)

[5] Sentencia TGUE (Sala segunda), de 13 octubre de 2021 *(asunto T-523/20- Setarcos Consulting/EUIPO)* -apdos. 6 y 62- (ECLI:UE:T:2021:691).

criptoactivos, como elemento que facilita la prueba del seguimiento ante su gerencia, empleados y partes interesadas (WESTHAUSEN 2021, p. 184), resaltando la percepción del *compliance* no sólo *"como un factor de coste, sino como un valor añadido (v.gr. para aumentar la competitividad)"* (DURRER y HUNZIKER, 2021)[6].

II. DIGITALIZACIÓN DEL SISTEMA FINANCIERO Y EVOLUCIÓN DE LOS RIESGOS EMPRESARIALES

La innovación tecnológica abarata los costes de los servicios financieros, potencia su accesibilidad y acorta fases burocráticas en un contexto de competencia continuada entre operadores. La incorporación de tecnologías **DLT** (*Distributed Ledger Technology* o tecnologías de registro distribuido, como *Blockchain*) actúa reformulando conceptos tradicionales -v.gr. *dinero*, *autoridad bancaria*, *intermediación financiera*- que adquieren rasgos nuevos al influjo del poder que proporcionan al usuario para operar directamente *-peer to peer-*, posibilitando instrumentos de intercambio menos perecederos que las formas usuales de dinero[7], en un proceso que transita del modelo de *economía tradicional* a otro de *economía digital* (PALOMO-ZURDO y REY-PAREDES 2021, p. 16) expuesto a un novedoso escenario de *riesgo digital* que demanda medidas de prevención del *riesgo financiero, riesgo operativo, riesgo del cliente* y *riesgo de cumplimiento*[8].

Señalada la crisis económica global de 2008 -año de publicación del artículo sobre *Bitcoin*[9]- como desencadenante de la ebullición del concepto de *"criptoactivo"*, algunos autores (OTERO IGLESIAS y OLIVER LLORENTE, 2022) señalan dos posiciones respecto a las ***tecnologías DLT***. Frente a quienes enfatizan las bondades ligadas a su característica *descentralización* capaz de fomentar servicios financieros optimizados a cada usuario, sus detractores subrayan la *incongruencia* que supone soslayar la mediación bancaria clásica para recurrir a otros intermediarios más opacos -al prescindir de profesionales y

[6] El proyecto de investigación *Return on Compliance* impulsado por la Agencia Suiza para la Innovación -*Innosuisse*-, iniciado en noviembre de 2020 y hasta julio de 2023, constituye el primer proyecto científico sólido destinado a *cuantificar* la contribución del *Compliance* sobre el mundo empresarial.
https://www.hslu.ch/de-ch/hochschule-luzern/forschung/projekte/detail/?pid=5709

[7] Resultan conocidas las ideas de Adam Smith -"La riqueza de las naciones" (1776)-, sobre el uso como dinero de moneda metálica por los estados, pues *"los metales pueden ser no sólo conservados con menor pérdida que cualquier otra cosa, puesto que casi no hay nada menos perecedero que ellos"* -p. 57-, declaración confirmada con las actuales representaciones digitales que proporcionan los criptoactivos.

[8] Los *riesgos de cumplimiento* incluyen cambios inesperados provenientes de sanciones legales, menoscabo de la reputación o incumplimiento de requisitos legales (HUNZICKER 2021, pp. 216-217).

[9]Sostiene que "el comercio en Internet ha venido a depender exclusivamente de instituciones financieras que sirven como terceros confiables para el procesamiento de pagos electrónicos. [..] *el costo de la mediación incrementa costos de transacción, limitando el tamaño mínimo práctico por transacción y eliminando la posibilidad de pequeñas transacciones casuales*" -p. 1-
https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

supervisores públicos-, sembrando un terreno idóneo a la posible comisión de estafas y a la financiación de actividades de dudosa legalidad[10].

2.1.1. Perspectiva nacional

Las nuevas formas de intercambio financiero al margen de los cauces reglados *encienden* el aparato legislativo del Estado (Europa Press, 2022 b), que bajo argumentación tan legítima como la protección ante operaciones que puedan repercutir gravemente sobre la economía de los pequeños inversores, va de ordinario ligada a otra urgencia en la consecución de modalidades adicionales de control impositivo sobre transacciones cuya vacío regulatorio pudiera privar de cuantiosos ingresos al erario público.

A ello obedece la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero, cuyo preámbulo -apartado I- prevé garantizar que dicha transformación *"no afecte en modo alguno al nivel de protección al consumidor de servicios financieros, a la estabilidad financiera y a la integridad en los mercados, ni permita la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo"*[11].

Desde esta perspectiva tuitiva el último Informe de Estabilidad Financiera, de 11 de noviembre (Banco de España [BdE], 2022), sugiere la importancia de un sistema singularizado de compliance para las organizaciones[12] que desarrollan operaciones financieras cuando destaca, entre las principales causas de pérdidas operacionales durante el primer semestre de 2022, los fallos cometidos en el cumplimiento de obligaciones fiduciarias con sus clientes, ocasionando pérdidas que ascienden al 61% del total experimentado en el sector financiero tradicional; mientras que en el sector cripto once *hackeos* han producido pérdidas por valor de 718 millones de dólares durante la primera mitad de octubre de 2022[13].

---

[10] Actualmente en trámite parlamentario, se prevé la modificación del Código Penal para la transposición de directivas contra el fraude y la falsificación de medios de pago distintos del efectivo, e incluir los criptoactivos y los monederos electrónicos como nuevos medios de comisión de los delitos de falsedades y estafa (exposición de motivos -apdo. III-).
https://www.congreso.es/public_oficiales/L14/CONG/BOCG/A/BOCG-14-A-101-1.PDF#page=1

[11] https://www.boe.es/boe/dias/2020/11/14/pdfs/BOE-A-2020-14205.pdf

[12] Una encuesta del *Aalen Management Institute* (AAUF) y la Universidad suiza de Lucerna (Ulrich, P. y Kratt, M., 2021), propone dos enfoques sobre las funciones de gobierno de la organización, denominados *"Tres líneas de defensa"* y *"Garantía combinada"*. Poco conocidos aún, prevén su progresiva implementación dada la necesidad de minimizar riesgos corporativos ante un futuro incremento de requisitos legales.

[13] Página 92.
https://www.bde.es/f/webbde/Secciones/Publicaciones/InformesBoletinesRevistas/InformesEstabilidadFinancera/22/IEF_Otono2022.pdf

2.1.2. Perspectiva internacional

Pretende auspiciarse un entorno flexible entre autoridades nacionales propicio a los proveedores que reconsidere *"las restricciones al flujo de capital en un mundo más digital, y se necesita colaboración y cooperación transfronteriza para abordar los desafíos tecnológicos, legales, regulatorios y de supervisión"* (Fondo Monetario Internacional [FMI], 2021)[14]. Este *ecosistema digital* persigue atajar cuatro riesgos fundamentales (FMI, 2021):

1) *Riesgos operativos y cibernéticos*, como caídas del sistema y episodios de suplantación de perfiles de clientes de billeteras -*wallets*-[15].
2) *Riesgos de gobernanza ligados a la prescindencia de intermediarios centrales*, incluyendo falta de transparencia en la emisión de activos virtuales dificultando la medición de riesgos.

3) *Anonimato facilitado por las tecnologías DLT*. La trazabilidad no evita obstáculos a la hora de identificar a los intervinientes ante un marco regulatorio en estado embrionario y en vías de armonización.

4) *Limitada información* procedente de los proveedores y *heterogeneidad* de jurisdicciones concurrentes, que complica la *trazabilidad fiscal* de sus operaciones[16].

2.2 Definiciones

2.2.1. Tecnología de registro descentralizado

Según el acuerdo provisional de 10 de octubre (Parlamento Europeo, 2022 c) sobre la propuesta MiCA (Parlamento Europeo, 2022 a), la "*«tecnología de registro descentralizado» debe definirse de la manera más amplia posible"*[17] y concebirse conforme al Reglamento sobre un régimen piloto relacionado con la Tecnología de registro descentralizado (Parlamento Europeo, 2022 b). Este Reglamento entiende por tal la que permite el uso de registros descentralizados,

[14] Informe sobre estabilidad financiera mundial del Fondo Monetario Internacional (octubre 2021) -introducción, ap. XV-.
[15] La *valoración* de los criptoactivos constituye uno de los mayores desafíos, derivado de su negociación en mercados frecuentemente no regulados y expuestos a una manipulación de precios en el contexto de procesos operativos inadecuados -pp. 33 y 34-.
https://www.bis.org/bcbs/publ/d533.pdf
[16] Según la OCDE *"las características del sector cripto han reducido la visibilidad de las administraciones tributarias sobre las actividades relacionadas con los impuestos dentro del sector, aumentando la dificultad de verificar si las obligaciones tributarias asociadas se informan y evalúan adecuadamente"* -p. 9-.
https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf
[17] Considerando 8.

definidos como "*repositorio de información que lleva registros de operaciones y se comparte a través de un conjunto de nodos de red TRD y está sincronizado entre dichos nodos, utilizando un mecanismo de consenso"* -artículo 2-, definición análoga a la manejada doctrinalmente (GONZÁLEZ-MENESES 2017, p. 40)[18].

2.2.2. Criptoactivo

Constituye *"una representación digital de un valor o derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o similar"* (Parlamento Europeo 2022 c, art. 3.1.2). La naturaleza disruptiva de dicha tecnología subyace en el alto grado de *provisionalidad* de las definiciones esenciales del sector[19]. La normativa deberá prevenir el blanqueo de capitales y la financiación del terrorismo[20], resultando indispensable para comprender su definición final la que sobre «activos virtuales» establecen las recomendaciones del Grupo de Acción Financiera Internacional (Grupo de Acción Financiera Internacional [GAFI], 2022 a), según las cuales constituye *"una representación digital de valor que se puede comercializar o transferir digitalmente, y se puede usar para fines de pago o inversión"*[21].

2.2.3. Proveedor de servicios de activos virtuales

La Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores, sobre publicidad de criptoactivos como objeto de inversión, los define como *"cualquier persona física o jurídica cuya actividad profesional o empresarial consista en proveer uno o varios servicios sobre criptoactivos a terceras partes de forma profesional"* -artículo 2.i)-, definición reflejada en el acuerdo provisional sobre MiCA de octubre de 2022 -artículo 3.1 apartado 8-, cuya actividad requerirá *"domicilio social en un Estado miembro"* previamente autorizado por la autoridad nacional competente -considerando 50-.

---

[18] También DE CORES HELGUERA, 2021, pp. 179-181; y cuyas garantías de *autoría* y *autenticidad* reconoce la jurisprudencia, así la Sentencia A.P. Álava -secc. 1ª- nº 1032/2021, de 21 de diciembre (ECLI:ES:APVI:2021:1302) condiciona su valor probatorio a "la existencia de algún elemento *a través del cual pueda atribuirse su autoría a quien se considere emisor del mismo* algo que, según el Tribunal, puede realizarse mediante "un Código Seguro de Verificación (CSV), bien mediante una firma electrónica soportada por una entidad de verificación (Ley 6/2020 o Reglamento UE 910/2014), *o bien mediante la aplicación de cualquier elemento tecnológico que permita una mínima auditoría de autenticidad (Blockchain)*" -fj. 2º-.

[19] Sabedor el legislador europeo de que las que finalmente se adopten *"marcarán el tipo de activo al que esta regulación se aplicará*" (NOVELLA GONZÁLEZ DEL CASTILLO 2021, p. 120). Para MARTINEZ NADAL (2021, p. 52) la amplitud en la definición persigue abarcar todos los criptoactivos situados fuera del ámbito de aplicación de la legislación sobre instrumentos financieros que puedan surgir.

[20] Considerando 8.

[21] *"Normas internacionales sobre la lucha contra el blanqueo de capitales y la financiación del terrorismo"* -p. 132-.
https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

2.3. Seguridad jurídica como seguridad razonable

Las organizaciones deben poder planificar sus actividades a partir de un sistema normativo predeterminado –art. 9.3 CE-, precisando tanto el *conocimiento* de las normas vigentes como un nivel mínimo de *estabilidad*[22] en estas. Dicho mandato no equivale a la indefinida preservación del ordenamiento vigente que "*se establece en un momento histórico dado, en relación con derechos o situaciones determinadas*"[23]. La seguridad jurídica no representa, pues, un valor absoluto porque *"el legislador del pasado no puede vincular al legislador del futuro*" hasta el extremo de operar una petrificación del ordenamiento que iría contra la protección de la confianza legítima[24].

Existe un estrecho paralelismo entre este principio general del derecho y el *principio de seguridad razonable* implícito al estándar ISO 37301:2021, sobre Sistemas de gestión de Compliance -incorporado al catálogo nacional como UNE-ISO 37301[25]-, y que la doctrina considera contrapuesto al de *seguridad absoluta* (CASANOVAS YSLA 2021, p. 58), razón por la que tanto el estándar ISO 37301:2021 como su antecedente ISO 19600:2014[26] "plantean en su Introducción *«minimizar» no cumplimientos (no eliminarlos)* y también emplean ocasionalmente el vocablo «reducir», con ese mismo sentido"[27].

Así cabe entender la previsión contemplada en las sucesivas propuestas de MiCA cuando proclama que "*el primer objetivo es la seguridad jurídica*"[28], demandando un marco que ahuyente el peligro de incoherencia entre Estados miembros (Europa Press, 2022 a), y evite una fragmentación normativa *"que falsearía la competencia en el mercado único, dificultaría la expansión transfronteriza de las actividades de los proveedores de servicios de criptoactivos y daría pie al arbitraje regulador"*[29], criterio sostenido doctrinalmente

---

[22] Memoria del Consejo de Estado, año 1992 -pp. 110 a 128-. https://www.consejo-estado.es/wp-content/uploads/2021/05/MEMORIA-1992.pdf

[23] Sentencia del Tribunal Constitucional nº 227/1988, de 29 de noviembre -fj. 10º- (ECLI:ES:TC:1988:227).

[24]Sentencia del Tribunal constitucional nº 51/2018, de 10 de mayo -fj. 5º- (ECLI:ES:TC:2018:51).

[25] Según el Reglamento (UE) 1025/2012 del Parlamento europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea, esta *"incrementa la seguridad y el valor para los consumidores"* -considerando 3-. https://www.boe.es/doue/2012/316/L00012-00033.pdf

[26] En un contexto de *mejora* del sistema de gestión recogido en dicho estándar ISO 19600:2014 -capítulo 10-, que la ISO 37301:2021 integra como principio *"mostrándose así la organización más exigente en cuanto a la interpretación y la aplicación de las obligaciones de compliance que le afectan"* (CASANOVAS YSLA 2021, p. 312).

[27] Nota 68, Guía práctica de compliance según la Norma ISO 37301:2021 -p. 59-.

[28]Página 3. https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0003.02/DOC_1&format=PDF

[29]Considerando 4 -Acuerdo provisional sobre MiCA, de 10 de octubre de 2022-. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13198_2022_INIT&from=ENf

al señalar la trascendencia del principio de confianza legítima como motor de certidumbre que "*aleja las inseguridades que dificultan el tráfico jurídico*" (GÓMEZ JIMÉNEZ 2021, p. 76).

III. OBLIGACIONES DE COMPLIANCE PARA LOS PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES

Concebido el *Compliance* como *"un proceso continuo y el resultado de que una organización cumpla con sus obligaciones"*[30] podríamos precisar, en línea con el Consejo de Estabilidad Financiera (FSB) y su reciente propuesta de marco internacional sobre operaciones con criptoactivos, que *"los marcos regulatorios y de supervisión efectivos deben basarse en el principio de «misma actividad, mismo riesgo, misma regulación». Cuando los criptoactivos y los intermediarios realicen una función económica equivalente a la que realizan los instrumentos e intermediarios del sector financiero tradicional, deben estar sujetos a una regulación equivalente"*[31].

En tal sentido debe repararse en el Libro IV del Código Civil (CC)[32] "De las obligaciones y contratos", interpretando conjuntamente el art. 1.089 CC, a cuyo tenor *"las obligaciones nacen de la Ley, de los contratos y cuasicontratos"*; el art. 1.091 CC, reconociendo fuerza de ley a las obligaciones suscritas por las partes -*pacta sunt servanda*-, y el art. 1.256 CC que proclama el principio de la *necessitas* como esencia de la obligación, derivando nuestro Tribunal Supremo de la concurrencia entre *"la lex contractus, el principio pacta sunt servanda y la necessitas"*[33] el nexo vinculante de toda obligación fruto de la autonomía de la voluntad.
En el ámbito de relaciones *proveedor-usuario* los términos suscritos se complementarán con el régimen aplicable que recogerá el Reglamento MiCA[34], que dedica sus capítulos 2 y 3 a las obligaciones establecidas sobre todos los proveedores, proporcionando un *framework* o regulación caracterizada porque *"encierra y resume en una sola y única fuente normativa de primer nivel (reglamento) lo que contemplan las disposiciones de la Directiva 2014/65/UE (MiFID II) y las del reglamento delegado 565/2017"* (PARACAMPO 2021, p. 264).

[30] Norma UNE-ISO 37301:2021 sobre Sistemas de gestión del *compliance* -p. 7-. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0065822
[31] Página 4, https://www.fsb.org/wp-content/uploads/P111022-2.pdf
[32] Real Decreto de 24 de julio de 1889 de publicación del Código Civil.

[33]Sentencia del Tribunal Supremo nº 175/2015, de 27 de marzo -fj. 2º- (ECLI:ES:TS:2015:1094) –entre otras-.
[34]MiCA planea aplicarse a quienes realicen *"emisión, oferta al público y admisión a negociación de criptoactivos o que proporcionen servicios relacionados con criptoactivos en la Unión".* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13198_2022_INIT&from=EN

La actual propuesta MiCA toma como referente la Directiva MiFID II[35] *"creando un sistema paralelo, revisado con enfoque tecnológico, para aquellos criptoactivos que no pueden considerarse instrumentos financieros".*

3.1. Proveedores de servicios y LSSI

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico[36] (LSSI) se aplica *"a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos"* -artículo 2.1-, concretando su anexo como "prestador" a la persona, física o jurídica, que proporciona un servicio de la sociedad de la información, esto es *"todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario"*, configurando una lista abierta de actividades ampliable en atención a la versatilidad de la definición misma de "servicio de la sociedad de la información", permitiendo otros a condición de que "representen una actividad económica" -apartado a), párrafo 3-.

La organización deberá conservar -art. 10 LSSI- información general disponible al público *"de manera permanente, fácil, directa y gratuita"*, extremando la supervisión sobre (i) el nombre o denominación social, CIF, domicilio y dirección de correo electrónico, teléfono, fax u otros medios de contacto directos y efectivos, (ii) datos de inscripción registral de que derive su personalidad jurídica, (iii) precios de sus productos y servicios, tipo impositivo aplicable, y posibles gastos de envío, y (iv) códigos de conducta a que se halle adherido y modo de consultarlos electrónicamente. Debe constar el consentimiento del usuario para dirigirle comunicaciones comerciales -at. 21 LSSI-; en la práctica muchas comunicaciones por correo electrónico incluyen un enlace que posibilita rechazar futuros envíos.

La inobservancia de tales *deberes de control* depara la aplicación de un régimen de responsabilidad *conectado a la naturaleza del servicio prestado*, concluyendo nuestra jurisprudencia[37] que, en tanto no se presten servicios de intermediación, será aplicable el art. 13.1 LSSI, es decir el régimen general de responsabilidad civil, penal o contencioso-administrativa vigente, y no el diseñado en los arts. 14 a 17 LSSI con especialidades para los prestadores de servicios de mediación financiera, elemento relacional clave a examinar en cada caso.

---

[35]Directiva 2014/65/UE, del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE Texto pertinente a efectos del EEE.
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014L0065

[36]Traspuso la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, sobre determinados aspectos jurídicos de los servicios de la sociedad de la información y el comercio electrónico.
https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=uriserv:OJ.L_.2000.178.01.0001.01.SPA

[37] STS nº 668/2018 -Sala 1ª, secc. 1ª- de 23 de noviembre -fj. 3º- (ECLI:ES:TS:2018:3905).

3.2. Proveedores de servicios y LPBCFT

La Directiva (UE) 2018/843, que modifica la Directiva (UE) 2015/849 sobre prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, pretende abarcar todos los posibles usos de las monedas virtuales[38], lo que aconseja implementar programas de compliance para prevenir, controlar y minimizar los perjuicios que acarrearía la desatención de las responsabilidades de control e información atribuidas al proveedor de servicios de cambio (*exchanges*) y de custodia de monederos electrónicos (*wallets*). En este sentido *Global Digital Finance* (GDF)[39] viene trabajando en la adaptación al sector cripto del procedimiento de *diligencia debida* del sector financiero tradicional, basado en el cuestionario del *Grupo Wolfsberg*[40], orientado a facilitar la comprensión de los riesgos implícitos a las operaciones financieras y mejorar los controles que permitan cumplir los estándares del sector.

3.2.1. Obligaciones del Proveedor

Implican recabar información para identificar al cliente junto al "*propósito y la índole prevista de la relación de negocio"*[41]. Esta diligencia, que no elimina por completo el anonimato de una transacción –en tanto podría ser directamente realizada entre usuarios- puede en la práctica dificultar los flujos de capital ilícito por tales plataformas, proporcionando un grado aceptable de transparencia en espera de futuras medidas al respecto en el marco de las Unidades de Inteligencia Financiera nacionales[42]. La Directiva (UE) 2018/843, traspuesta mediante el Real Decreto-ley 7/2021, de 27 de abril (RDL 7/2021), modifica la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y financiación del terrorismo (LPBCFT).

El RDL 7/2021 ahora obliga a *"los proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos"* -art. 2.1.z) LPBCFT-, proclamando su deber de registro en el Banco de España, responsable de supervisar el cumplimiento de las condiciones requeridas para el acceso y mantenimiento en este de *"las personas físicas o jurídicas que, cualquiera que sea su nacionalidad, ofrezcan o provean en España servicios de los descritos en los apartados 6 y 7 del artículo 1 de la ley".*

---

[38] Considerandos 8 a 10.

[39] https://www.gdf.io/working-group/kyc-aml-ctf/

[40]https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%27s_CBDDQ_Capacity_Building_Guidance_Final%20V1.1%20160420.pdf

[41] Artículo 13.1.c) de la *Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo, sobre prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.*
https://eur-lex.europa.eu/eli/dir/2015/849/oj/spa

[42]Considerando 9 -Directiva (UE) 2018/843-.

Deberán (i) identificar a la persona con quien entablen relación de negocio, (ii) realizar seguimiento permanente del mismo, y (iii) aplicar medidas de diligencia debida, debiendo poder probar su adecuación al fin perseguido -arts. 3 a 16-. El Grupo de Acción Financiera Internacional, que en junio actualizó sus Estándares sobre *activos virtuales y proveedores de servicios de activos virtuales* (Grupo de Acción Financiera Internacional [GAFI], 2022 b), introduce algunas precisiones sobre la *Recomendación número 16*.

3.2.2. GAFI y la Recomendación número 16 (travel rule)

Contempla la obligación de recabar, mantener y transmitir información sobre el origen y beneficiario de transferencias de activos virtuales (Centro de Cambridge para Finanzas Alternativas [CCAF], 2020) para identificar y comunicar transacciones sospechosas, pudiendo adoptar su bloqueo y prohibición cuando rebasen el umbral de los 1000 euros, en atención al mayor riesgo ligado a estos activos dada su naturaleza transfronteriza y aún escasa regulación[43].

Esta Recomendación, introducida en el ordenamiento mediante el Reglamento (UE) 2015/847 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, sobre información que acompaña a las transferencias de fondos, amplía su aplicación a los proveedores de servicios de activos virtuales, que deberán adjuntar dicha información para su transmisión a la autoridad competente.

A ello responde la propuesta de Reglamento sobre información que acompaña a las transferencias de fondos y de determinados criptoactivos, cuya versión presentada en octubre de 2022 (Consejo de la Unión Europea, 2022) proyecta hacer extensivo a estos proveedores ese deber informativo ya vigente para los proveedores de servicios de transferencias electrónicas -considerando 2-.

Se pretende eliminar el umbral cuantitativo mínimo recogido en la *Recomendación número 16* de modo que, para las transferencias de criptoactivos, deba informarse de todas *con independencia de su cuantía*. Si bien esto puede facilitar el cumplimiento y la gestión de riesgos por los proveedores, excede el rigor propio de las recomendaciones del GAFI[44], siendo susceptible de ocasionar que los usuarios de criptoactivos que utilicen monederos privados

[43]Para el CCAF resulta difícil de implementar porque *"requiere el establecimiento de estándares técnicos comunes (v.gr. mensajería) para agilizar y estandarizar la transmisión de información del originador a sus beneficiarios, así como el desarrollo de soluciones tecnológicas para que los proveedores cumplan con la regla de viaje a nivel mundial"* -p. 55-.
https://www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf

[44]Pretende promover la *travel rule* mediante debates sobre buenas prácticas transfronterizas, comprendiendo "*i) medidas de monitoreo y mitigación de riesgos que involucran transacciones entre VASP y billeteras no alojadas; ii) interoperabilidad de las soluciones tecnológicas Travel Rule; iii) umbrales de minimis; y iv) normas de protección de datos"* -p. 23-.
https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf

autocontrolados sean fiscalizados más severamente que quienes continúen haciendo uso de efectivo en sus transacciones. A este propósito *rigorista* obedece la nota publicada por el Consejo de la Unión Europea[45], subrayando "la necesidad de aplicar requisitos estrictos de transparencia a las *transferencias de criptoactivos desde el primer euro*".

3.2.3. Régimen sancionador

La regulación vigente debe complementarse con el próximo Reglamento sobre información que acompaña a las transferencias de fondos y de determinados criptoactivos. Los Estados -artículo 22.1- además de sanciones penales, pueden regular otras de naturaleza administrativa, si bien *"las sanciones y medidas previstas serán* ***eficaces, proporcionadas y disuasorias****".* Son estas las tres notas características del régimen sancionador europeo en materia fiscal, inspirado en un principio recogido en el considerando 41 del citado Reglamento (Consejo de la Unión Europea, 2022) que debe observarse por el legislador en línea con la Comunicación de la Comisión de 8 de diciembre de 2010, titulada *«Regímenes sancionadores más rigurosos en el sector de servicios financieros»*[46]*.* Todo control sobre las medidas implementadas debe poder asegurar la *ponderación* de la gravedad que implica la infracción en que puede incurrirse.

Las sanciones -en coherencia con la Directiva (UE) 2015/849- podrán abarcar (i) una declaración pública sobre infractor y naturaleza de la infracción; (ii) requerimiento de cese de la conducta absteniéndose de repetirla; (iii) retirada o suspensión de la autorización previa para el ejercicio de actividades; (iv) prohibición temporal de ejercer funciones directivas por el infractor; (v) multas administrativas máximas de, al menos, el doble del beneficio procedente de la infracción -art. 59.2-. En todo caso este catálogo podrá ampliarse a escala nacional para atender las especialidades de cada mercado, presupuesto a que responde la vigente LPBCFT -artículos 50 a 65-.

3.3. Proveedores de servicios y protección de datos

Este análisis debe abordarse examinando las implicaciones que la normativa de protección de datos proyecta sobre *Blockchain* como tecnología vehicular del activo virtual. Según ERBGUTH y GALILEO FASCHING (2017, p. 560) debe

[45]https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CONSIL:ST_9697_2022_REV_1&from=EN

[46] Según el Informe del Grupo de Alto Nivel sobre Supervisión Financiera en la UE, de 25 de febrero de 2009: *«Es indispensable que dentro de la UE y en otras partes todos los supervisores puedan echar mano de regímenes sancionadores suficientemente convergentes y estrictos, con la capacidad de disuasión necesaria»* -apartado 201-.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0716&from=CS
https://www.esrb.europa.eu/shared/pdf/de_larosiere_report_es.pdf?f1c7edf9533e93b9b6201b53a588bc6c

distinguirse al *responsable* en función de su capacidad de efectiva determinación de los *medios* y *fines* del tratamiento[47], partiendo de unas tecnologías originariamente obstativas al ejercicio de derechos como el derecho al olvido -art. 17 RGPD-[48].

La última versión sobre MiCA (Parlamento Europeo, 2022 c), dentro de su Título V "Autorización y condiciones de ejercicio de la actividad de los proveedores", mantiene la protección de datos cuando un proveedor *externalizase* algunas operaciones, no eximiéndole ello de tomar medidas adecuadas para prevenir riesgos operativos potenciales *"siendo plenamente responsables del cumplimiento de todas sus obligaciones en virtud del presente título"*, debiendo asegurarse de que los terceros cumplen la normativa *"en materia de protección de datos que se aplicaría si los terceros estuvieran establecidos en la Unión"* -art. 66.1 apartado g)-.

Tal precepto proyecta la aplicación a este sector de la división entre *Responsables* y *Delegados de tratamiento* -ex capítulo IV, arts. 24 a 31 RGPD-. El proveedor suscribirá un contrato con los terceros intervinientes concretando las actuaciones a seguir por quienes traten datos personales[49], con las especialidades del artículo 26 RGPD en caso de colaboración entre varios responsables (esto es, entre varios proveedores), expresando "*las funciones y relaciones respectivas de los corresponsables en relación con los interesados"* (art. 26.2 RGPD).

Otra novedad se encuadra en el artículo 95, sobre publicación *on line* de las sanciones por infracción del Reglamento, que incluirá los datos personales identificativos del infractor y que durante un plazo mínimo de cinco años se mantendrá en la web, matizando que podrán aplicarse plazos inferiores. A mi juicio -salvo que se tase legalmente- será necesario ponderar caso por caso desde cada autoridad sancionadora nacional, algo que, a la larga, podría ocasionar diferencias interpretativas en detrimento de la seguridad jurídica a nivel europeo de no fijarse criterios estables. El Supervisor Europeo de Protección de Datos, en su Opinión 9/2021, de 24 de junio, respecto a la propuesta MiCA (SEPD 2021, p. 10), sobre tales riesgos ya recomendó que se sustituyese el período de conservación de "al menos cinco años" -artículo 95.4- por un *período máximo de conservación* de los datos especificado.

---

[47]Así cuando *"los proveedores de servicios encargados tienen el control, deben ser considerados responsables. Si el mismo usuario realiza las transacciones, es el propio usuario el responsable*". https://erbguth.ch/ZD12-2017.pdf

[48]Para asegurar su observancia se trabaja en una solución eficiente basada en *"un diseño único que permite eliminar datos de la cadena de bloques "silenciosamente", sin interacción de otros nodos de la blockchain, y sin impacto en el rendimiento de la escritura de datos en la base de datos",* Godyn M. *et al.*, *Nature* (2022) -p. 11-.
https://doi.org/10.1038/s41598-022-19341-y

[49] Artículo 28.3 RGPD.

Nuestra doctrina (BRITO IZQUIERDO 2021, p. 335) aconseja fijar taxativamente un plazo que permita dar cumplimiento al principio de limitación de conservación de los datos personales -art. 5.1.e) RGPD-. Es aquí relevante el Informe Jurídico 2019-0148[50] de la Agencia Española de Protección de Datos (AEPD, 2020) que no considera posible determinar anticipadamente los plazos de conservación que hayan de aplicarse en todos los supuestos que pueden suscitarse en la práctica, así que de cara al cumplimiento de la obligación de bloqueo por el responsable de tratamiento -es decir, por el proveedor de servicios de criptoactivos- deberán valorarse dos datos clave (i) plazo prescriptivo de las acciones ejercitables en función de la naturaleza de la relación jurídica preexistente, y (ii) normas sectoriales aplicables a la actividad, conforme al principio proclamado en el título preliminar del Código Civil que prioriza la norma especial sobre la norma general *-lex specialis derogat generalis-.*

3.3.1. Obligaciones del Proveedor

Sus deberes de supervisión y control (pudiendo prevenir sanciones que, en el caso de las multas administrativas, pueden alcanzar los 20 millones de euros o un montante de hasta el 4% del volumen de negocio anual total -art. 83 RGPD-) implican:

1) Documentar la observancia de los principios sobre tratamiento y responsabilidad proactiva –arts. 5.1 y 5.2 RGPD- a disposición de la autoridad nacional competente (AEPD), designando un *Delegado de Protección de datos* -arts. 37 a 39 RGPD- según la naturaleza de la actividad, el montante económico y los riesgos asociados a la tecnología empleada.

2) Contar con base legitimadora del tratamiento, generalmente constituida por el consentimiento plasmado en el contrato (art. 1261 CC) -arts. 6 y 7 RGPD-.

3) El proveedor que obtuviera los datos directamente del cliente, debe informarle de (i) la identidad del responsable del tratamiento, (ii) su finalidad, y (iii) posibilidad de ejercer los derechos reconocidos en los artículos 15 a 22 RGPD. De no obtenerlos directamente, le informara además de (i) las categorías de datos tratados, y (ii) fuentes de procedencia -art. 11 LOPDGDD[51]-.

4) Una política de privacidad *desde el diseño y por defecto* adaptada al servicio prestado -art. 25 RGPD- mediante plataformas *on line* provistas de canales permanentes de comunicación con el cliente, siendo recomendable también un

[50] Para la AEPD *"corresponde al responsable del tratamiento -que ha determinado su finalidad- decidir cuándo los datos han dejado de ser necesarios para la finalidad para la cual fueron recabados -decayendo la posibilidad de su tratamiento-, si bien, en algunas ocasiones, es el legislador quien fija un plazo de conservación determinado en relación con supuestos o materias concretas"* -p. 26-.
https://www.aepd.es/es/documento/2019-0148.pdf

[51] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

protocolo ante deficiencias y brechas de seguridad[52] -sección 2, capítulo IV RGPD-.

5) Evaluar los riesgos conectados al tratamiento con tecnologías DLT -art. 35.1 RGPD- en la gestión del proveedor, pudiendo hacer indispensable una evaluación de impacto[53] para extraer conclusiones sobre medidas técnicas y organizativas apropiadas para prevenirlos -art. 25 RGPD y art. 28.1 LOPDGDD-.

6) El tratamiento con tecnologías DLT constituye uno de los "*factores de riesgo identificados en el tratamiento que no están señalados específicamente en el RGPD o en su desarrollo"* (AEPD 2021, p. 93), siendo la principal amenaza su falta de transparencia respecto a los actores involucrados en las operaciones, pudiendo repercutir sobre todas las dimensiones del sistema de seguridad (confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad). Los datos podrían permanecer en la blockchain durante un lapso temporal no sujeto, en principio, a control del proveedor, lo que no se compadece adecuadamente con el principio de limitación de conservación de los datos a observar desde la organización -art. 5.1.e) RGPD-.

7) Estrechamente relacionado con el cumplimiento de los deberes de diligencia establecidos en la LPBCFT -artículo 4 bis-, toda organización sometida a la misma deberá obtener, conservar y actualizar los datos identificativos de la persona física que ostente su titularidad real –art. 4 bis, apartado 4- durante un plazo de 10 años desde el cese de dicha titularidad.

---

[52] Según la *Guía para la notificación de brechas de datos personales,* de 25 de junio de 2021 -AEPD- *"los artículos 33 y 34 RGPD exponen la necesidad de que las organizaciones integren, dentro de sus políticas de información, un proceso de gestión de brechas de datos personales que concrete cómo la organización va a dar cumplimiento a sus obligaciones con respecto a las brechas*", que *"vendría a completar el proceso de gestión de incidentes de la organización".* -p. 6-.
https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

[53] La *Guía del riesgo y evaluación de impacto en tratamientos de datos personales*, de 29 de junio de 2021 –AEPD-, de conformidad con el Esquema Nacional de Seguridad precisa que la protección de las claves criptográficas se extenderá a todo su ciclo de vida, debiendo emplearse algoritmos acreditados por el Centro Criptológico Nacional, y equipos cuyas funcionalidades y nivel de seguridad hayan sido evaluados conforme a normas europeas o internacionales, como la ISO/IEC 15408 o análogas -p. 119-.
https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

3.4. Proveedores de servicios y seguro de responsabilidad civil

La propuesta MiCA establece *requisitos prudenciales* -artículo 60- debiendo el Proveedor disponer permanentemente de un capital mínimo variable según la operativa autorizada a desempeñar[54]:

1) Recepción, transmisión y ejecución de órdenes por cuenta de terceros; asesoramiento, gestión de carteras, y transferencia y colocación de criptoactivos: 50.000 euros.
2) Proveedores que presten cualquier servicio anterior, junto con el de custodia y administración de criptoactivos por cuenta de terceros, e intercambio de criptoactivos: 125.000 euros.
3) Proveedores que presten cualquiera de los indicados en el apartado 2, junto con el servicio de explotación de una plataforma de negociación de criptoactivos: 150.000 euros.

La prestación escalonada de servicios adicionales a los inicialmente autorizados requerirá un aumento de los requisitos patrimoniales mínimos (PARACAMPO 2021, p. 272). La póliza cubrirá las pérdidas derivadas de la falta de diligencia profesional respecto a la *"protección de los criptoactivos y fondos de los clientes"*[55]. El escaso desarrollo de las pólizas para criptoactivos se relaciona directamente con la falta de regulación sobre estos[56], afirmando nuestra doctrina que actualmente *"las bolsas de criptomonedas no están obligadas a asegurar los fondos de los clientes de la misma manera que los bancos y corredores del sector financiero tradicional.*

Es la excepción, no la regla, que un asegurador ofrezca un seguro de criptoactivos" (MUÑOZ VILLARREAL 2021, p. 319), aconsejándose no obstante la contratación de un seguro, de conformidad con la práctica asumida en el sector financiero tradicional (*"misma actividad, mismo riesgo, misma regulación"*[57]).

---

[54] Anexo IV de la *Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos, por el que se modifica la Directiva (UE) 2019/1937.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13198_2022_INIT&from=EN

[55] Artículo 60.5 apartado f).

[56] Según *Evertas* obedece a tres factores (i) tamaño relativamente pequeño del mercado de criptoactivos, (ii) falta de experiencia en suscripción de seguros sobre activos digitales, y (iii) escasa familiaridad de las pólizas de seguro con el espacio criptográfico. https://www.evertas.com/ https://www.actuarialpost.co.uk/article/huge-lack-of-capacity-in-insurance-sector-for-cryptoassets-17886.htm

[57] https://www.fsb.org/wp-content/uploads/R111022-2.pdf

3.5. Proveedores de servicios y ciberseguridad

Sobrevuela este sector un dilema constante derivado de la máxima que estatuye al consumidor en soberano del mercado (VON MISES 2018, p. 328): *mayor seguridad o mayor control*, de modo que *"de momento, los actores que participan en este mercado prefieren el riesgo que conlleva la volatilidad, al riesgo que supone una monitorización fiscal"* (TEJERINA RODRÍGUEZ 2021, p. 297). La cibercriminalidad no constituye un problema nuevo; convertidos los equipos informáticos en *instrumento criminógeno creciente* respecto a delitos patrimoniales (ROMEO CASABONA (1988, p. 21) plantean un reto *"que se materializa de forma continua, y victimiza cada vez de manera más importante a miles de instituciones, empresas y ciudadanos"*[58], proviniendo aquí las principales amenazas para el sistema financiero del denominado *Cryptojacking* y del *Ransomware*.

3.5.1. Cryptojacking

Definido como *"el uso ilegítimo de un equipo por parte de los cibercriminales para realizar el proceso de obtención de criptomonedas y obtener el total de las ganancias"* (Centro Criptológico Nacional 2018, p. 4), recurre como principales vías de infección al (i) *Phishing*, mediante engaño al propietario, (ii) *Exploit kits*, detectando brechas de seguridad, (iii) *ataques de fuerza bruta*, (iv) *código dañino*, (v) *Internet of Things*, (vi) *cryptominers en la web*, (vii) *dispositivos móviles*, y (viii) *vulnerabilidades* en equipos desactualizados.

3.5.2. Ransomware

A diferencia del Cryptojacking, el Ransomware conlleva mayor *visibilidad* al cifrar la información del equipo, imposibilitándolo y reclamándose un rescate a cambio de su liberación, razón por la que el Cryptojacking suele preferirse en los últimos años pues *"los cibercriminales ven en esta práctica una forma más discreta y menos dañina de ganar dinero"* (Centro Criptológico Nacional 2021, p. 28).

La ciberseguridad exigible a los proveedores -art. 16.2.n), propuesta MiCA- impone que en la solicitud de autorización a la autoridad nacional competente deba incluirse la *"descripción de los procedimientos y sistemas para salvaguardar la seguridad, en particular la ciberseguridad, la integridad y la confidencialidad de la información, conforme a lo contemplado en el artículo 30, apartado 10"*, remisión realizada al Reglamento del Parlamento Europeo y del Consejo sobre resiliencia operativa digital para el sector financiero, cuyo artículo 2.1.f) prevé su aplicación a *"proveedores de servicios de criptoactivos*

[58]Página 7, Orden PCI/487/2019, de 26 de abril, que publica la Estrategia Nacional de Ciberseguridad 2019.
https://www.boe.es/buscar/pdf/2019/BOE-A-2019-6347-consolidado.pdf

autorizados en virtud de un Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937 («Reglamento relativo a los mercados de criptoactivos»), y emisores de fichas referenciadas a activos"[59].

Habida cuenta que, conforme a la propuesta de Reglamento del Parlamento Europeo y del Consejo que modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento de un marco europeo para una *identidad digital*, se prevé que *"el almacenamiento seguro de materiales criptográficos pase también a ser un asunto sometido a certificación de ciberseguridad"*[60], deberán implementarse sistemas de seguridad informática acordes al Esquema Nacional de Ciberseguridad[61].

IV. AVANCES REGULATORIOS EN ESPAÑA

4.1. Fiscalidad sobre los criptoactivos

La naturaleza jurídica y la función de un activo virtual en cada operación determinarán la relevancia fiscal de las operaciones efectuadas con los activos contemplados en MiCA (CEDIEL y PEREZ POMBO 2021, p. 348), generando la realización del "hecho imponible"[62] la consecuente obligación de tributar[63] conforme a la Ley General Tributaria (LGT). La Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, que traspone la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016, sobre normas contra las prácticas de elusión fiscal, conlleva dos reformas sustanciales.

---

[59] *Reglamento DORA* (cuya Acta final ha sido firmada el 14 de diciembre de 2022). https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52020PC0595R(01)&qid=1671289211718

[60] https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/es/pdf

[61] Relacionada con la contratación de un seguro ante posibles riesgos, el CCAF reconoce que *"la seguridad del almacenamiento de criptoactivos no debe dejarse solo en manos de sistemas de seguridad de TI bien diseñados. El seguro de fondos es un componente clave de una buena oferta de servicios"* -p. 62-. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study/

[62] Para el Parlamento europeo *"la dinámica de los mercados de criptoactivos hace urgente la entrada en vigor de normas que definan el tipo de fiscalidad que debe aplicarse, la definición del «hecho imponible», el momento en que se genera un hecho imponible y su valoración"* -considerando 24-. https://www.europarl.europa.eu/doceo/document/TA-9-2022-0335_ES.pdf

[63] Artículo 20.1 de la LGT 58/2003, de 17 de diciembre. https://www.boe.es/buscar/pdf/2003/BOE-A-2003-23186-consolidado.pdf

4.1.1. Ley del IRPF y obligaciones del Proveedor

La disposición adicional decimotercera de la Ley 35/2006[64], introduce dos obligaciones informativas[65] sobre tenencia y operaciones con criptomonedas. Los proveedores de servicios de cambio de moneda virtual y custodia de claves criptográficas privadas para la tenencia y uso de criptomonedas, deberán informar a la Agencia Tributaria sobre los saldos que, a 31 de diciembre, mantengan sus titulares, junto a la identidad de estos y de los autorizados y beneficiarios de tales saldos.

4.1.2. LGT y obligaciones del Proveedor

Según la disposición adicional decimoctava de la Ley 58/2003, de 17 de diciembre, General Tributaria, los proveedores informarán sobre las monedas virtuales situadas en el extranjero, sancionándose su omisión con multa que oscilará entre 1.500 y 10.000 euros como umbrales mínimos, dependiendo de si se ha cumplimentado defectuosamente o se ha incumplido la obligación de informar.

4.1.3. Modelos 172, 173 y 721 para declaración informativa a la AEAT

Finalizado el plazo de aportaciones[66] respecto al proyecto de Orden Ministerial[67] que aprueba los modelos 172 (declaración sobre saldos en monedas virtuales), y 173 (declaración sobre operaciones con monedas virtuales), deberán presentarse ambos con periodicidad anual, desde enero de 2023 respecto al ejercicio 2022 y mediante mensaje informático en los términos fijados en los anexos I y II de dicha Orden Ministerial. A ambos se suma el modelo 721[68] para declaración sobre monedas virtuales en el extranjero, a presentar entre el 1 de enero y el 31 de marzo de 2023 con la información a suministrar del ejercicio anterior.

---

[64] Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas. https://www.boe.es/buscar/act.php?id=BOE-A-2006-20764

[65]https://sede.agenciatributaria.gob.es/Sede/ayuda/manuales-videos-folletos/manuales-practicos/patrimonio-2021/capitulo-3-determinacion-base-imponible/formacion-patrimonio-bruto/monedas-virtuales.html

[66] https://www.hacienda.gob.es/es-ES/Normativa%20y%20doctrina/NormasEnTramitacion/Paginas/normasentramitacion.aspx

[67] https://www.hacienda.gob.es/Documentacion/Publico/NormativaDoctrina/Proyectos/27062022-ProyectoOM-modelo-172-173.pdf

[68] https://www.hacienda.gob.es/Documentacion/Publico/NormativaDoctrina/Proyectos/28062022-Proyecto-OM-modelo-721.pdf

4.2. Publicidad de criptoactivos y Circular de la CNMV

No obstante la redacción final que reciba MiCA[69], esta publicidad presenta mayor desarrollo a nivel estatal, resultando conveniente analizar cada ordenamiento nacional para profundizar en los requisitos establecidos sobre su creación (OTERO COBOS 2021, p. 201). En nuestro país la Comisión Nacional del Mercado de Valores y el Banco de España han venido advirtiendo[70] de los riesgos de *volatilidad*, *complejidad* y *escasa transparencia* que supone esta inversión, demandando medidas de supervisión y control proporcionadas a los mismos.

El Real Decreto-ley 5/2021, de 12 de marzo, de medidas extraordinarias para la solvencia empresarial, introdujo un nuevo artículo 240 bis en el Real Decreto Legislativo 4/2015, de 23 de octubre, que aprueba el texto refundido de la Ley del Mercado de Valores (este Real Decreto Legislativo será sustituido por la futura *Ley de los Mercados de Valores y de los Servicios de Inversión*, con importantes reformas sobre *compliance* para los proveedores[71]), facultando a la CNMV para establecer mecanismos de control administrativo sobre la publicidad de los criptoactivos como objeto de inversión. Su Circular 1/2022, de 10 de enero, se centra *"exclusivamente sobre los requisitos que deberá cumplir la actividad publicitaria"*[72], obligando a (i) proveedores de servicios de criptoactivos cuando los publiciten, (ii) proveedores de servicios publicitarios, y (iii) cualquier persona física o jurídica que realice, por iniciativa propia o por cuenta de terceros, esta publicidad -norma 4-.

Deberá advertirse de que *"la inversión en criptoactivos no está regulada, puede no ser adecuada para inversores minoristas y perderse la totalidad del importe invertido"*, acompañando un enlace con información adicional identificado así:

---

[69] *Vid.* artículos 7.2, 15.3 y 46.9.

[70] Comunicado CNMV, de 8 de febrero de 2018; comunicado conjunto CNMV-BdE, de 9 de febrero de 2021; y comunicado de 17 de marzo de 2022, emitido por la CNMV, el BdE y la Dirección General de Seguros y Fondos de Pensiones, reiterando las advertencias emitidas desde la Autoridad Bancaria Europea, la Autoridad Europea de Valores y Mercados, y la Autoridad Europea de Pensiones y Seguros de Jubilación, sobre los riesgos de operar con criptoactivos y el grave peligro para las expectativas de un usuario atraído por una publicidad en ocasiones engañosa e incompleta.
https://www.cnmv.es/Portal/verDoc.axd?t=%7B9c76eef8-839a-4c19-937f-cfde6443e4bc%7D
https://www.cnmv.es/Portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D
https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/22/presbe2022_19.pdf
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Warnings/2022/ESAs%20warning%20on%20crypto%20assets/Translations/1028369/ESA%202022%2015%20Joint%20ESAs%20warning%20on%20crypto-assets_ES.pdf

[71] Así los artículos 306 y 321 prevén mejorar las funciones supervisoras y sancionadoras de la CNMV para proteger a los inversores en criptoactivos, cuya entrada en vigor se prevé hacer coincidir con la del Reglamento MiCA -DF 9ª-.
https://www.congreso.es/public_oficiales/L14/CONG/BOCG/A/BOCG-14-A-114-1.PDF

[72] https://www.boe.es/boe/dias/2022/01/17/pdfs/BOE-A-2022-666.pdf

"es importante leer y comprender los riesgos de esta inversión" -norma 5-. Incorpora, además, un régimen obligatorio de *comunicación previa* para toda campaña publicitaria masiva -superior a 100.000 personas- debiendo aportarse el *documento de comunicación previa de campaña publicitaria masiva de criptoactivos* disponible en la web de la CNMV[73], junto con (i) datos descriptivos del tipo de criptoactivo o servicio, público destinatario y medios empleados para publicitarlos, y (ii) datos de cada mensaje comercial, sus advertencias y el formato para transmitirlo -norma 7.2-.

La CNMV podrá requerir información pertinente para valorar el cumplimiento de la Circular -norma 6.2-, debiendo la organización mantener un registro de todas las campañas seguidas en los últimos dos años, comprendiendo (i) fechas de inicio y cierre, ámbito territorial y subjetivo, medios y soportes publicitarios empleados, y porcentaje esperable de población receptora, (ii) mensaje comercial y sus advertencias, junto al formato para su lectura o reproducción, y (iii) proveedor del servicio publicitario a usar.

4.3. Gestión de inversiones: Registro en el Banco de España

El RDL 7/2021 establece nuevas obligaciones registrales a cargo de quienes desempeñen operaciones con moneda virtual, introduciéndose en la LPBCFT una nueva disposición adicional segunda que impone el registro en el Banco de España[74] de quienes ofrezcan o provean servicios descritos en los apartados 6 y 7 del artículo 1 LPBCFT de (i) compraventa de criptomonedas mediante la entrega o recepción de euros u otra moneda de curso legal o dinero electrónico aceptado como medio de pago en el país emisor, y (ii) custodia de claves criptográficas privadas en nombre del cliente para la tenencia, almacenamiento y transferencia de monedas virtuales[75].

Constituye infracción muy grave -apdo. 5º, D.A. 2ª- cualquiera de estas operativas sin estar inscrito en el Registro del Banco de España, competente para sancionar conforme al título IV de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. No obstante, la Resolución de 16 de diciembre de 2021 de la Dirección General de Seguridad Jurídica y Fe Pública, del Ministerio de Justicia[76], considera dicha inscripción una exigencia administrativa que, dada la limitada legislación vigente sobre entidades que operan con monedas virtuales (y mientras no exista desarrollo normativo más pormenorizado), *debe sujetarse a un criterio restrictivo* y no susceptible de

[73] https://sede.cnmv.gob.es/ov/Documentos/FormularioCriptoactivos.pdf

[74]https://sedeelectronica.bde.es/sede/es/menu/tramites/autorizaciones-de-entidades-de-credito-y-otros/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos.html

[75]Cabe distinguir en MiCA (IBÁÑEZ JIMÉNEZ 2021, p. 225) tres subcategorías de gestión a cargo de la organización (i) *gestión económica* (art. 41), (ii) *gestión tecnológica* (arts. 3.1.11 y 68), y (iii) *gestión de activos* (arts. 30, 31 y 33) integrando gestión de claves privadas y protocolos para validación de operaciones.

[76] https://www.boe.es/boe/dias/2021/12/29/pdfs/BOE-A-2021-21753.pdf

interpretación extensiva más allá de los supuestos tasados en la propia LPBCFT[77].

V. CONCLUSIONES

PRIMERA. - Descartada una expectativa de *seguridad absoluta* cabe mantener otra de riesgo mínimo para una Organización en el normal desempeño de sus obligaciones, según se concluye del análisis convergente del principio general de seguridad jurídica -art. 9.3 CE-, con el principio de *seguridad razonable* en materia de Compliance -implícito al estándar ISO 37301:2021-.

SEGUNDA. - En virtud de la LSSI, se deben supervisar y controlar un conjunto de obligaciones generales que incluyen poner a disposición del destinatario *información clara, comprensible e inequívoca* sobre los trámites a seguir para celebrar el contrato, mediante técnicas adecuadas al medio de comunicación utilizado.

TERCERA. - La organización debe implementar medios adecuados al cumplimiento de los *deberes de diligencia debida* previstos en la normativa de prevención del blanqueo de capitales y financiación del terrorismo, dirigidos a:

a) identificar formalmente a la persona física y jurídica con quien se entablen relaciones de negocio,
b) realizar un seguimiento permanente de tal relación de negocio,
c) aplicar medidas de diligencia debida, debiendo poder probar su adecuación al logro de los fines propuestos.

CUARTA. - Resulta recomendable una política de privacidad desde el diseño y por defecto en función del servicio a prestar con criptoactivos, así como un protocolo para *minimizar riesgos* ante deficiencias y brechas de seguridad en el tratamiento de los datos de los clientes con tecnologías DLT.

QUINTA. - Dada su previsión en MiCA, el logro de renombre como organización confiable aconseja la suscripción de una póliza de seguro con una entidad autorizada conforme a la *Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre acceso a la actividad de seguro y reaseguro (Solvencia II)*, ante potenciales pérdidas derivadas de la falta de diligencia profesional respecto a la protección de los criptoactivos y los fondos manejados.

SEXTA. - Deben implementarse procedimientos y sistemas informáticos de *salvaguarda de la seguridad, la integridad y la confidencialidad de la información*,

[77]https://www.dpoitlaw.com/la-direccion-general-de-seguridad-juridica-y-fe-publica-resuelve-que-el-deber-de-inscripcion-en-el-registro-de-exchangers-del-banco-de-espana-lpbcft-10-2010-d-a-2a-ha-de-interpretarse-con-criter/

homologando su operatividad al Reglamento sobre resiliencia operativa digital para el sector financiero (Reglamento DORA)[78].

SÉPTIMA. - Aprobados los modelos 172, 173 y 721 sobre declaración informativa de *saldos* y *operaciones* con monedas virtuales, debe implantarse un protocolo adecuado para suministrar información a la AEAT, siguiendo el procedimiento previsto en los artículos 16 y 17 de la Orden HAP/2194/2013, de 22 de noviembre.

OCTAVA. - La responsabilidad última sobre publicidad se reconduce a la advertencia de que la inversión en criptoactivos no está aún regulada exhaustivamente, pudiendo resultar inadecuada para inversores minoristas y ocasionar la pérdida total de su inversión -Circular CNMV 1/2022-.

NOVENA. - La inscripción en el *Registro de Exchanges* del Banco de España para operaciones de *cambio* de moneda virtual, y *custodia* de claves criptográficas privadas, debe interpretarse ajustada a tales operaciones en sentido restrictivo.

DÉCIMA. – Pese a que la falta de un marco general europeo puede generar desconfianza obstaculizando el crecimiento del mercado de criptoactivos, los proyectos en tramitación adoptando como referente al sector financiero tradicional (que evocan el principio *"misma actividad, mismo riesgo, misma regulación"*), unido a la implementación de *modelos de compliance* singularizados a cada organización, ahuyentan los peligros de diversidad e incoherencia interestatal dotando de *previsibilidad razonable* al sector cripto.

[78] https://eur-lex.europa.eu/legal-content/ES/HIS/?uri=CONSIL:ST_11051_2020_INIT

VI. BIBLIOGRAFÍA

AEPD (2020). *Informe del Gabinete Jurídico 2019-0148*. https://www.aepd.es/es/documento/2019-0148.pdf

AEPD (2021). *Guía del riesgo y evaluación de impacto en tratamientos de datos personales.* https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Asociación Española de Compliance (2017). *Libro blanco sobre la función de Compliance*. https://www.asociacioncompliance.com/wp-content/uploads/2017/08/Libro-Blanco-Compliance-ASCOM.pdf

Asociación Española de Compliance e Instituto de Estudios Económicos (2020). *Estudio sobre la función de Compliance en las Empresas españolas 2020*. https://www.asociacioncompliance.com/wp-content/uploads/2020/10/ESTUDIO-ESTADISTICO-COMPLIANCE-FINAL.pdf

Banco de España (2022). *Informe de Estabilidad Financiera-otoño 2022.* https://www.bde.es/f/webbde/Secciones/Publicaciones/InformesBoletinesRevistas/InformesEstabilidadFinancera/22/IEF_Otono2022.pdf

Brito Izquierdo, N. (2021). Criptoactivos y privacidad, en Barrio Andrés, M. (Ed.), *Criptoactivos. Retos y desafíos normativos*. Wolters Kluwer España S.A.

Casanovas Ysla, A. (2021). *Guía práctica de compliance según la Norma ISO 37301:2021.* AENOR Internacional S.A.U.

Cediel, A. y Pérez Pombo, E. (2021). Tributación de los criptoactivos regulados en MiCA, en Madrid Parra, A. y Pastor Sempere, C. (Ed.), *Guía de criptoactivos MiCA*. Thomson-Reuters Aranzadi S.A.U.

Centro Criptológico Nacional (2018). *Informe CCN-CERT IA-25-18 Cryptojacking*. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3027-ccn-cert-ia-25-18-cryptojacking/file.html

Centro Criptológico Nacional (2021). *Informe 2021 CCN-CERT_BP_12_Buenas Prácticas en Cryptojacking.* https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3472-ccn-cert-bp-12-cryptojacking/file.html

Centro de Cambridge para Finanzas Alternativas (2020). *3º Estudio global de evaluación comparativa de criptoactivos.* Universidad de Cambridge. https://www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf

Comité de Basilea de Supervisión Bancaria (2022). *Documento consultivo. Segunda consulta sobre el tratamiento prudencial de las exposiciones a criptoactivos.*
https://www.bis.org/bcbs/publ/d533.pdf

Consejo de la Unión Europea (2022). Texto transaccional final sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la información que acompaña a las transferencias de fondos y determinados criptoactivos (refundición), de 5 de octubre de 2022.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13215_2022_INIT&from=EN

De Cores Helguera, C. (2021). La circulación jurídica y sus señales. De la *traditio* a la Blockchain, en Ibáñez Jiménez, J. (Ed.), *Token Law and Markets*. Editorial Reus S.A.

Durrer, M., y Hunziker, S. (2021). *Retorno del Compliance*. Universidad de Lucerna.
https://www.hslu.ch/de-ch/hochschule-luzern/forschung/projekte/detail/?pid=5709

Erbguth, J. y Galileo Fasching, J. (2017). *¿Quién es responsable de una transacción de Bitcoin? Sobre la aplicabilidad del RGPD a la cadena de bloques.* Revista de protección de datos.
https://erbguth.ch/ZD12-2017.pdf

Europa Press (2022 a). *El alto riesgo de los criptoactivos*. El Economista. https://www.eleconomista.es/opinion-blogs/noticias/11760248/05/22/El-alto-riesgo-de-los-criptoactivos.html

Europa Press (2022 b). *El evento sobre la transformación financiera que coorganiza el Ayuntamiento se presenta en el Congreso.* La vanguardia. https://www.lavanguardia.com/local/sevilla/20220524/8290436/evento-sobre-transformacion-financiera-coorganiza-ayuntamiento-presenta-congreso.html

Fondo Monetario Internacional (2021). *Fondo Monetario Internacional - Informe de Estabilidad Financiera Global octubre 2021. Covid-19, Criptografía y Clima.* https://www.imf.org/en/Publications/GFSR/Issues/2021/10/12/global-financial-stability-report-october-2021

Godyn, M., Kedziora, M., Ren, Y., *et al.* (2022). Análisis de soluciones para el cumplimiento de Blockchain con RGPD. *Nature,* 12, 15021 (2022). https://doi.org/10.1038/s41598-022-19341-y

Gómez Jiménez, M. L. (2021). Seguridad Jurídica y Criptomonedas: desafíos normativos en la era de las gov-coins, en Belando Garín, B. (Ed.), *Las criptomonedas a debate*. Thomson-Reuters Aranzadi S.A.U.

González-Meneses, M. (2017). *Entender el blockchain: una introducción a la tecnología de registro distribuido*. Thomson-Reuters Aranzadi S.A.U.

Grupo de Acción Financiera Internacional (2022 a). *Recomendaciones del GAFI. Estándares internacionales sobre la lucha contra el blanqueo de capitales y la financiación del terrorismo.* https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Grupo de Acción Financiera Internacional (2022 b). *Actualización específica sobre la implementación de los estándares del GAFI sobre activos virtuales/VASP*. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf

Hunziker, S. (2021). *Gestión de riesgos empresariales.* Springer Gabler.

Ibáñez Jiménez, J. (2021). Emisión, representación y gestión de criptoactivos. En Barrio Andrés, M. (Ed.), *Criptoactivos. Retos y desafíos normativos*. Wolters Kluwer España S.A.

Martínez Nadal, A. (2021). Ámbito de aplicación y conceptos esenciales de la propuesta de Reglamento relativo a los mercados de criptoactivos: la noción de criptoactivo y sus subcategorías (arts. 2 y 3), en Madrid Parra, A. y Pastor Sempere, C. (Ed.), *Guía de criptoactivos MiCA*. Thomson-Reuters Aranzadi S.A.U.

Muñoz Villarreal, A. (2021). Ciberiesgos y seguros: Los riesgos de los criptoactivos y su aseguramiento, en Barrio Andrés, M. (Ed.), *Criptoactivos. Retos y desafíos normativos*. Wolters Kluwer España S.A.

Novella González del Castillo, E. (2021). El futuro reglamento europeo para un mercado de criptoactivos (Propuesta MiCA), en Barrio Andrés, M. (Ed.), *Criptoactivos. Retos y desafíos normativos*. Wolters Kluwer España S.A.

OCDE (2022). *Marco de notificación sobre Criptoactivos y modificaciones al estándar común de información*.

https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-tothe-common-reporting-standard.htm

Otero Cobos, M. T. (2021). Régimen de información y transparencia: el libro blanco de criptoactivos, en Madrid Parra, A. y Pastor Sempere, C. (Ed.), *Guía de criptoactivos MiCA*. Thomson-Reuters Aranzadi S.A.U.

Otero Iglesias, M y Oliver Llorente, P (2022). *Criptomonedas, stablecoins y la cripto-economía: el estado de la cuestión*. (Documento de trabajo 2/2022). Real Instituto Elcano. https://www.realinstitutoelcano.org/documento-de-trabajo/criptomonedas-stablecoins-y-la-cripto-economia-el-estado-de-la-cuestion/

Palomo-Zurdo, R. y Rey-Paredes, V. (2021). Las criptomonedas en la sociedad digital: ¿visión o transgresión?, en Belando Garín, B. (Ed.), *Las criptomonedas a debate*. Thomson-Reuters Aranzadi S.A.U.

Paracampo, M.-T. (2021). Marco normativo armonizado sobre los proveedores de criptoactivos, reglas de comportamiento destinadas a proteger al cliente y requisitos organizativos, en Madrid Parra, A. y Pastor Sempere, C. (Ed.), *Guía de criptoactivos MiCA*. Thomson-Reuters Aranzadi S.A.U.

Parlamento Europeo (2022 a). Informe sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937 (COM(2020)0593 – C9-0306/2020 – 2020/0265(COD)) de la Comisión de Asuntos Económicos y Monetarios, de 17 de marzo de 2022.
https://www.europarl.europa.eu/doceo/document/A-9-2022-0052_ES.pdf

Parlamento Europeo (2022 b). Reglamento (UE) 2022/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado y por el que se modifican los Reglamentos (UE) nº 600/2014 y (UE) nº 909/2014 y la Directiva 2014/65/UE.
https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-80826

Parlamento Europeo (2022 c). Acuerdo provisional favorable a la propuesta de Reglamento relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937 (COM(2020)0593 – C9-0306/2020 – 2020/0265(COD)) de la Comisión de Asuntos Económicos y Monetarios, votado el 10 de octubre de 2022.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13198_2022_INIT&from=EN

Romeo Casabona, C. M. (1988). *Poder informático y seguridad jurídica: la función tutelar del derecho penal ante las nuevas tecnologías de la información*. Fundesco.

Smith, A. (2020). *La riqueza de las naciones.* Alianza editorial.

Supervisor Europeo de Protección de Datos (2021). Dictamen de 24 de junio de 2021 sobre la propuesta de un Reglamento relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937. https://edps.europa.eu/system/files/2021-06/21-06-24_edps_opinion_mica_en.pdf

Tejerina Rodríguez, O. (2021). Criptoactivos y ciberseguridad, en Barrio Andrés, M. (Ed.), *Criptoactivos. Retos y desafíos normativos*. Wolters Kluwer España S.A.

Ulrich, P. y Kratt, M. (9-10 de septiembre, 2021). *Garantía combinada vs. Tres líneas de defensa: una comparación empírica*. **7ª** Conferencia Internacional CARF en línea -Lucerna-. https://www.hslu.ch/-/media/campus/common/files/dokumente/w/ifz/seminare-konferenzen/carf/konferenzbeitraege-2021/risiko/combined-assurance-vs-three-lines-of-defenseulrichkratt.pdf?la=de-ch

Von Mises, L. (2018). *Acción humana: tratado de economía.* Unión Editorial.

Westhausen, H.-U. (2021). Acerca del cálculo del valor de compliance y su relevancia práctica. *Ekonomika*, vol. 100, nº 2, 171-189. https://doi.org/10.15388/Ekon.2021.100.2.8