Desafíos del cumplimiento normativo y la estandarización del reporte digital en los ecosistemas DeFi: la *travel rule* ante el paradigma de la transparencia algorítmica

Challenges of regulatory compliance and digital reporting standardization in DeFi ecosystems: The travel rule facing the algorithmic transparency paradigm

Juan Ignacio Leo-Castela*
Universidad de Salamanca, Salamanca, España
leocastela@usal.es | https://orcid.org/0000-0003-2936-6017

◆

Recibido: 07/04/2026 | Aceptado: 07/07/2026 | Publicado: 09/09/2026

Resumen. Este artículo aborda la configuración de la auditoría de cumplimiento con ocasión de la implementación de los nuevos estándares sobre reporte digital iXBRL e ISO 20022. En concreto, la investigación se centra en la problemática asociada a la aplicación de la *travel rule* en ecosistemas de finanzas descentralizadas (DeFi) al amparo del marco legal vigente en la Unión Europea. La metodología empleada combina el análisis descriptivo y analítico de estos estándares con la revisión de las políticas de organismos internacionales (FATF, ESMA y FinCEN). La investigación revela que en los ecosistemas DeFi existen brechas de implementación en los protocolos previstos y que, si bien la estandarización facilita la auditoría, existe un vacío estructural derivado de la ausencia de un sujeto obligado (VASP) que impide el intercambio de los datos exigido por la norma. Se identifican riesgos de privacidad y se advierte una tendencia creciente hacia la exclusión financiera institucional. Como posible alternativa, este artículo propone un modelo de cumplimiento desde el diseño (*compliance by design*) basado en el recurso hacia *soulbound tokens* (SBT) y *zero-knowledge proofs* (ZKP) para monitorear el cumplimiento normativo manteniendo a salvo la privacidad de los usuarios.

* Licenciado en Derecho, Licenciado en Administración y Dirección de Empresas, Doctor internacional y Premio Extraordinario de Doctorado (2019) por la Universidad de Salamanca, España. Profesor Permanente Laboral (acreditado a Profesor Titular) en el Departamento de Economía Aplicada de la Universidad de Salamanca. Investigador en el Centro de Investigación para la Gobernanza Global de la Universidad de Salamanca (CIGG-Usal).

Palabras clave. DeFi, *travel rule*, MiCA, XBRL, auditoría digital, *blockchain analytics*, *compliance-by-design*

Abstract. This paper addresses the compliance auditing configuration in light of the new digital reporting standards implementation iXBRL and ISO 20022. Specifically, this research focuses on the challenges associated with applying the travel rule in decentralized finance (DeFi) ecosystems under the current legal framework in the European Union. The methodology employed combines descriptive and analytical analysis of these standards with a review of the international bodies policies (FATF, ESMA, and FinCEN). The research reveals implementation gaps in the intended protocols within DeFi ecosystems and that, while standardization facilitates auditing, a structural gap exists due to the absence of a reporting entity (VASP), which prevents the exchange of data required by the standard. Privacy risks are identified, and a growing trend toward institutional de-risking is noted. As a possible alternative, this paper proposes a compliance-by-design model based on the use of soulbound tokens (SBT) and zero-knowledge proofs (ZKP) to monitor regulatory compliance while safeguarding user privacy.

Keywords. DeFi, Travel Rule, MiCA, XBRL, digital audit, blockchain analytics, compliance-by-design

1. Introducción

A lo largo de la última década, la digitalización de la información financiera y de los mecanismos previstos para su reporte ha transformado la arquitectura tradicional del *compliance* corporativo en el sector financiero (Alonge et al., 2024, pp. 28 y ss.). La transición hacia estándares de lectura mecánica (iXBRL[1]/ISO 20022[2]) no solo ha optimizado el intercambio de datos facilitando la interoperabilidad y fomentando un contexto de mayor transparencia, sino que ha permitido la implementación de una semántica común alcanzando nuevas cotas de comparabilidad y trazabilidad entre

[1] Algunas evidencias destacadas sobre el impacto global que representa el uso del *eXtensible Business Reporting Language* (XBRL) han sido puestas de manifiesto por Bartolacci et al. (2021) y por Tawiah y Borgi (2022) pp. 518 y ss.

[2] ISO 20022 sobre servicios financieros, esquema universal de mensajería. Si bien la arquitectura técnica de esta norma internacional data del año 2004, alcanza su plena eficacia técnica y operativa a partir de marzo de 2023 cuando el tradicional esquema SWIFT de la red global de pagos comenzó a migrar hacia ISO 20022. Ambos sistemas convivieron hasta el pasado mes de noviembre de 2025 marcando este hito el inicio de una nueva era en la mensajería financiera a partir de la "transparencia por defecto". Por su parte, el sistema Target2 (T2) de la Unión Europea obliga a todos los bancos centrales y comerciales a utilizar exclusivamente ISO 20022 para pagos de alto valor.

entidades[3]; lo cual favorece la toma de decisiones informada y contribuye a mejorar la eficiencia de los mercados[4]. Este hecho representa una oportunidad para el diseño de nuevos mecanismos de vigilancia y control orientados hacia una prevención más eficaz de la delincuencia económica en el sector financiero tanto a nivel doméstico como en el espacio transnacional[5]. De manera particular, para una mejor protección de los datos personales que figuran en los registros distribuidos.

En este artículo se pretende posicionar el *compliance* financiero como una infraestructura esencial que garantice la integridad y la estabilidad del sistema económico global en la era digital. En un mundo caracterizado por la hiperconectividad y la desintermediación, el *compliance* deja de ser una función meramente reactiva en las organizaciones y empresas del sector financiero para convertirse en una herramienta estratégica en la prevención de la delincuencia económica. La digitalización acelera (y a veces incluso precipita) los flujos de capital (Górka, 2025) trayendo consigo nuevas formas de delincuencia económica, cada vez más sofisticadas. En este contexto, la estandarización del reporte digital mediante iXBRL e ISO 20022 surge como una respuesta técnica necesaria para dotar de un lenguaje común a los datos, permitiendo que la supervisión sea dinámica y ágil[6]. Si bien esta estandarización no es perfecta se defiende la idea de que permite transformar la auditoría en un proceso de monitorización continua, capaz de detectar desviaciones en tiempo real y de prevenir más eficazmente el uso de las infraestructuras financieras para fines ilícitos.

En este contexto el papel que desempeñan los organismos internacionales es crucial. La ESMA en la Unión Europea o la FinCEN[7] norteamericana han subrayado que el control sobre los proveedores de servicios de activos virtuales (*Virtual Asset Service Providers*, en adelante, VASP) resulta fundamental para evitar que los criptoactivos se conviertan en un "activo refugio" para la evasión fiscal o el fraude (D'avino, 2023, pp. 208 y ss.)[8].

La expansión del marco regulatorio europeo hacia otras latitudes (efecto Bruselas) aspira a consolidar un estándar técnico que, de manera particular, los ordenamientos

[3] En profundidad, Dixon et al. (2020) pp. 519 y ss. De manera particular, estos autores ofrecen un enfoque basado en el estudio de los principales usos, aplicaciones, y limitaciones del *machine learning* en el sector financiero.

[4] La investigación sobre la vinculación entre la eficiencia económica de los mercados financieros y la simetría en la información viene arrojando resultados significativos desde hace más de una década. Robb et al. (2014, pp. 522 y ss.) analizaron estas ventajas precisamente a partir del uso de XBRL.

[5] La innovación financiera y la aplicación del estándar ISO 20022 en el marco de la prevención de la delincuencia económica han permitido también impulsar la actividad institucional de las agencias de inteligencia financiera en la Unión Europea (Europol). En tal sentido, Moncalvo y Díaz (2025) pp. 638 y ss.

[6] En detalle, Borgi (2022) p. 226.

[7] La *Financial Crimes Enforcement Network* (FinCEN) o Red de Control de Delitos Financieros es una oficina estatal adscrita al Departamento del Tesoro de los Estados Unidos. Su misión principal consiste en la salvaguardia del sistema financiero y en la prevención de la delincuencia económica. En detalle: https://www.fincen.gov

[8] Sobre los problemas de agencia comúnmente asociados a la regulación para la prevención del lavado de activos, véase Naheem (2020).

latinoamericanos tienden a asimilar de forma refleja. Este fenómeno se proyecta de manera paradigmática en el ecosistema chileno a partir de la Ley 21.521 por la que se promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros (Ley Fintec). A partir de esta norma el ordenamiento jurídico chileno se consolida como un claro referente en Iberoamérica al establecer por primera vez un marco de supervisión para los proveedores de servicios de tecnologías financieras, incorporando la regulación expresa de intermediarios y custodios de criptoactivos al estilo europeo. Sin embargo, mientras que el regulador europeo impone una serie de prerrogativas directas sobre los activos digitales, el chileno se decanta por una mayor flexibilidad en su arquitectura regulatoria al delegar en la Comisión para el Mercado Financiero. Esta técnica legislativa destaca positivamente en el panorama internacional al optar por un enfoque basado en el riesgo frente al desafío de implementar mandatos equivalentes a los propuestos por el legislador europeo (tales como la *travel rule*). A mayores, conviene tener en cuenta que la estrategia del legislador chileno puede resultar particularmente útil en un mercado caracterizado por una escasa profundidad institucional sobre la que se añade, además, el objetivo fundamental de evitar la asfixia del sector tecnológico-financiero local.

A propósito de este efecto Bruselas, la estandarización del reporte de la información financiera se presenta como una solución que permite aplicar modelos de aprendizaje automático y calificación de riesgo sobre grandes volúmenes de datos, identificando señales de fraude que antes eran invisibles para el ojo humano. Esto nos permite reducir las ambigüedades que históricamente han aprovechado las organizaciones criminales y supone claramente un cambio de paradigma para la auditoría de cumplimiento tradicional. Nos encontramos por tanto ante una redefinición del *compliance* financiero que está propiciando su evolución desde una validación manual y fragmentada hacia un proceso cada vez más automatizado, continuo y basado en la trazabilidad íntegra de los datos. Desde este enfoque en las páginas que siguen se exponen algunas reflexiones y argumentos con la finalidad de contribuir al debate sobre las posibilidades de mejorar la transparencia algorítmica[9] en estos procesos.

Este artículo parte de un conflicto central y es que mientras la estandarización internacional (iXBRL/ISO 20022) busca crear datos de lectura mecánica para reducir errores humanos, lo cierto es que la arquitectura DeFi (sin intermediarios centralizados) hace que algunas obligaciones legalmente establecidas en el derecho comunitario como la *travel rule*[10] choquen con un vacío estructural adentrándonos en un callejón sin salida. En este

[9] El concepto de transparencia algorítmica que se utiliza en este trabajo surge a partir de la combinación de tres dimensiones que, por las razones que se exponen en las páginas que siguen, resultan fundamentales: la auditoría del flujo de datos, el cumplimiento desde el diseño y la supervisión automatizada.

[10] Véase, el artículo 4 del Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849.

trabajo se sostiene la tesis de que el éxito en la nueva auditoría de cumplimiento depende de la capacidad de los supervisores para avanzar desde un control de formatos hacia un control de flujos e infraestructuras de datos y declaraciones electrónicas de atributos[11]. La eficacia de este enfoque se pone a prueba con la emergencia de protocolos DeFi[12] y con el auge de los activos digitales donde, como se verá, no siempre resulta sencilla la implementación de la *travel rule*.

La metodología que se sigue en esta investigación combina la revisión analítica-narrativa de la literatura reciente, el análisis del marco regulatorio europeo y de las políticas internacionales más relevantes, y el análisis de los estándares iXBRL e ISO 20022. En segunda instancia, se apuesta por un análisis basado en las ventajas del cumplimiento desde el diseño (*compliance by design*) y en la recopilación de evidencias digitales como ejes vertebradores de un control más riguroso y acorde con las exigencias que impone la realidad actual del sector financiero.

Con el propósito de articular formalmente el alcance de esta investigación, el análisis se divide en los siguientes objetivos específicos: i) descomponer la naturaleza jurídica y técnica del principio de neutralidad tecnológica y examinar las fricciones operativas de la *travel rule* en arquitecturas desintermediadas; ii) diagnosticar el riesgo de exclusión financiera (*de-risking*) que introduce la asincronía regulatoria internacional en los mercados europeos e iberoamericanos; y iii) proponer una matriz de controles automatizados fundamentada en el principio de saturación en el riesgo y la transparencia algorítmica, mediante el recurso de *Soulbound Tokens* (SBT) y pruebas de conocimiento cero (*Zero-Knowledge Proofs*), capaces de superar el vacío estructural de fiscalización en los protocolos DeFi.

2. Reglamento (UE) 2023/1114 (*Markets in Crypto-Assets*, MiCA) y el desafío de la *travel rule*

La revolución tecnológica del sector financiero arroja nuevas realidades virtuales. Entre ellas, los llamados criptoactivos que a su vez confluyen con la expansión de los ecosistemas DeFi. En la Unión Europea, el reglamento MiCA (*Markets in Crypto-Assets*[13]) y la reciente regulación sobre la transferencia de fondos (en adelante, TFR[14]) buscan extender los

[11] Declaración en formato electrónico que permite la autenticación de atributos en el sentido indicado por el art. 1. j) 44) del Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) N.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital.

[12] En detalle, Jensen et al. (2021) p. 47; Ozili (2022) pp. 178 y ss.

[13] Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, 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.

[14] Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849.

principios fundamentales que apuntalan la transparencia del sistema financiero tradicional a estas nuevas realidades virtuales (Desai, 2025).

El pilar fundamental sobre el que se asienta esta nueva arquitectura jurídica europea para un control más eficaz de las transacciones financieras (y para una mejor trazabilidad del reporte de la información asociada a ellas) consiste en la aplicación de llamada regla del viaje o *travel rule*. La aplicación de esta regla en la práctica representa un desafío de primer orden para los operadores jurídicos, de manera particular en el contexto de la prevención del blanqueo de capitales y la financiación del terrorismo (sobre todo en presencia de activos digitales). En pocas palabras, esta regla constituye una nueva obligación para las instituciones financieras (y ahora también para los proveedores de criptoactivos) consistente en recopilar y transmitir la información personal del emisor (ordenante) y del receptor (beneficiario) de una transferencia de fondos; de manera tal que esta información exigida por la norma[15] "viaje adherida a la transacción". Las primeras referencias a esta obligación se remontan a finales de los años 90[16] y, desde entonces, su importancia ha crecido en paralelo a la expansión de la digitalización en el sector financiero.

Durante años, el anonimato en los criptoactivos representó un punto ciego para la ciberseguridad global y comportó riesgos que afectaban gravemente a la prevención de la financiación del terrorismo y de otros delitos económicos[17]. Algunos de estos riesgos persisten incluso hoy en día a pesar de los ingentes esfuerzos del legislador europeo por contribuir a la seguridad jurídica y la confiabilidad de su uso en el territorio común. Tradicionalmente, el regulador buscaba evitar que los fondos vinculados con activos cripto pudieran viajar sin dejar rastro. Incluso, favoreciendo que las autoridades judiciales

[15] Nombre del ordenante y del beneficiario, número de cuenta o dirección del monedero, dirección física, número de documento de identidad o fecha y lugar de nacimiento del ordenante; entre otros datos relevantes. Véase, el artículo 4 del Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849.

[16] En 1996 la FinCEN norteamericana introdujo la regla original bajo la *Bank Secrecy Act* (BSA, 31 CFR § 1010.410 (f)). Su objetivo era que los bancos dejaran de procesar transferencias anónimas para que las autoridades norteamericanas pudieran rastrear mejor el flujo de dinero ilícito. Años después, en 2012, el Grupo de Acción Financiera Internacional (GAFI/FATF) incorporó este principio en sus recomendaciones internacionales para transferencias electrónicas tradicionales. Sin embargo, en este trabajo se sostiene la idea de que el verdadero punto de inflexión llega a partir del año 2019 cuando el GAFI actualizó sus estándares ante el auge de los activos virtuales para incluir a los VASP (*Virtual Asset Service Providers*). Esto obligó a que las transferencias de Bitcoin, Ethereum y otros activos dejaran de ser pseudo-anónimas cuando sus flujos transitan por plataformas reguladas. Sobre esta última actualización, González (2024).

[17] El GAFI fue pionero en identificar este problema. El marco regulatorio internacional para los criptoactivos se vertebra sobre la nota interpretativa de la Recomendación 15 del GAFI, la cual realiza una remisión funcional a la Recomendación 16 (*travel rule*). Este encaje normativo obliga a la industria hacia una interoperabilidad técnica sin precedentes, donde la eficacia del cumplimiento ya no depende de la voluntad del sujeto obligado, sino de la implementación de protocolos técnicos capaces de transmitir datos financieros a tiempo real conforme a la Guía del GAFI para Activos Virtuales (2021/2024). Disponible en: https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/Recommendations/FATF-40-Rec-2012-Spanish.pdf.coredownload.inline.pdf La implementación técnica de estas recomendaciones suele seguir los estándares de mensajería financiera iXBRL e ISO 20022.

pudieran congelar dichos fondos e identificar a los responsables en caso de delito. Sin embargo, las políticas internacionales basadas en la imposición de sanciones se han topado en este punto con el llamado problema del amanecer (o *sunrise issue*). Es decir, que dado que existen jurisdicciones sin obligación de *travel rule* (e incluso otras donde su aplicación puede tener lugar de manera extemporánea) el cumplimiento normativo de esta regla en el sector financiero (y el reporte de la información asociada a cada transacción) puede verse gravemente comprometido. Así, por ejemplo, si un proveedor de servicios de criptoactivos (*Crypto-Asset Service Provider*, en adelante CASP) en un país "A" de la Unión Europea (con obligación de *travel rule)* desea enviar fondos a otro CASP en un país "B" (sin obligación de *travel rule*), el CASP europeo podría verse obligado a bloquear la transacción sencillamente porque no tiene a quién enviarle los datos exigidos por la norma.

La asincronía entre los calendarios de los distintos legisladores dificulta ostensiblemente la resolución del fenómeno crítico del *sunrise issue* en el panorama internacional. Las externalidades negativas de este fenómeno impactan con severa disparidad en el Sur Global. Mientras que las jurisdicciones periféricas avanzan progresivamente hacia el diseño formal de sus marcos locales (Ley Fintec chilena), la rigidez en las exigencias de cumplimiento normativo impuestas por la Unión Europea y el GAFI operan, de facto, como una barrera técnica al comercio financiero transfronterizo. Ante la imposibilidad material de intercambiar datos de identidad homólogos con contrapartes ubicadas en regiones donde la norma aún no es ejecutable, los CASP/VASP latinoamericanos se ven abocados a un escenario de exclusión preventiva (*de-risking* institucional). El *sunrise issue* transforma así una loable aspiración de integridad financiera en una fuerza centrífuga que amenaza con aislar (al menos operativamente) a los actores del Sur Global, dividiendo el ecosistema financiero digital entre nodos centrales plenamente conformes y mercados periféricos desconectados. A la postre, esto incentiva el desplazamiento de la actividad financiera hacia infraestructuras opacas y radicalmente desreguladas como se verá a continuación.

En las páginas que siguen se ofrecen algunas propuestas formales frente a este problema y se sostiene la tesis de que el éxito en la implementación de la *travel rule* tal y como aparece redactada en la reglamentación europea podría depender en gran medida de la creación de procesos híbridos de extracción, transformación y armonización de datos[18] capaces de fusionar la transparencia del dato registrado en la cadena con

[18] Ogunsola et al. (2022, pp. 794 y ss.) sugieren que la automatización de los modelos de extracción, transformación y carga o armonización de datos (*extract-transform-load*; ETL) pueden contribuir significativamente a mejorar su gobernanza en el seno interno de una organización.

la privacidad exigida por el Reglamento General de Protección de Datos (en adelante, RGPD) en la Unión Europea[19].

En resumidas cuentas, una de las motivaciones clave de esta investigación es precisamente esta tensión entre la rigidez regulatoria y la descentralización del sector financiero. Mientras que la estandarización del reporte digital presupone la existencia de intermediarios que actúan como garantes de la protección de datos, la realidad es que los protocolos DeFi puros operan mediante *smart contracts* autónomos y carecen de un sujeto obligado definido (Zetzsche et al., 2020, p. 187). De esta forma, la aplicación de la *travel rule* en entornos de acceso abierto (*permissionless*)[20] choca frontalmente con la arquitectura de las cadenas de bloques, donde el "pseudo anonimato" y las interacciones contrato a contrato impiden el cumplimiento normativo respecto de la identificación previa exigida por la Unión Europea.

Durante la última década la doctrina especializada ha estudiado ampliamente la eficiencia del iXBRL (Kumar et al., 2019, p. 42; Birt et al., 2017, p. 121), incluso en relación con los retos legales del Reglamento MiCA. Sin embargo, en este trabajo se identifica una brecha fundamental en el análisis de cómo la estandarización del reporte de la información financiera puede (o no) integrarse en protocolos sin un nodo central de control. A lo largo de este artículo se mantiene la idea de que la imposición de controles tradicionales en DeFi está provocando un fenómeno creciente de exclusión financiera por riesgo (también llamado *de-risking* institucional) (Joo y Seo, 2024, p. 720) por parte de las instituciones financieras; lo que reduce significativamente la interoperabilidad y la transparencia global. Como posible solución, en este trabajo se propone un modelo de cumplimiento desde el diseño y se sugiere que, en lugar de forzar la centralización, la auditoría debería evolucionar, al menos, en dos sentidos. En primer lugar, hacia el uso de capas de acceso basadas en declaraciones electrónicas de atributos conformes a la reglamentación europea (a menudo el recurso hacia estas declaraciones se asocia con los llamados tokens intransferibles o *Soulbound Tokens*; SBT) (Joo y Seo, 2024, p. 720). Y, en segundo lugar, hacia un mejor aprovechamiento de las pruebas de conocimiento cero (o ZKP (Hasan, 2019, p. 436)), favoreciendo un cumplimiento normativo respetuoso con la naturaleza descentralizada.

[19] 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.

[20] Por entorno *permissionless* (sin permisos) se entenderá en este trabajo cualquier sistema o red donde no exista una autoridad central con capacidad para controlar el acceso y la participación. Es decir, que cualquier usuario podría acceder, utilizar y contribuir al sistema en cualquier momento y desde cualquier lugar sin necesidad de autorización previa, sin documentos de identidad (ausencia de protocolos KYC) y sin la obligación de cumplir criterios de elegibilidad. Dado que la *travel rule* exige identificar al emisor y al receptor, se estaría intentando imponer una capa de permisos e identidad sobre una tecnología diseñada para funcionar sin ellos. Sobre esta fricción se hablará en detalle a lo largo de las páginas que siguen.

3. Auditoría del flujo de datos: cumplimiento desde el diseño y supervisión automatizada

La expresión "transparencia algorítmica" se refiere en este trabajo a la capacidad de supervisar, auditar y comprender los procesos automatizados que ejecutan tanto los protocolos DeFi como los sistemas de *compliance* y de gestión de riesgos. Hablar de transparencia en este contexto significa también que las reglas de cumplimiento normativo están integradas eficazmente y que son técnicamente verificables. A continuación, se desglosa con más detalle este concepto de transparencia a partir de tres dimensiones fundamentales: la auditoría del flujo de datos, el cumplimiento desde el diseño, y la supervisión automatizada.

3.1. La auditoría del flujo de datos

En el contexto del *compliance* digital el flujo de datos se presenta como un elemento estratégico para cualquier proceso de auditoría. Podría definirse como un conjunto de procesos e infraestructuras que permiten que los datos fluyan desde su origen (fuente) hasta su destino final; ya sea este un reporte interno, un canal de denuncias o una base de datos sometida a supervisión[21]. A lo largo de estos flujos es muy posible que los datos puedan sufrir diversas transformaciones; a menudo orientadas a asegurar su utilidad. Para un análisis más detallado de los procesos de auditoría del flujo de datos se propone un esquema basado en cuatro fases fundamentales.

3.1.1. Fase 1: el origen del dato

La primera fase se identifica con la fuente o el origen del dato. En esta fase se capturan los datos primarios ya sean datos registrados en la cadena (transacciones capturadas directamente de la *blockchain*) o ya sean datos fuera de registro u *off-chain* (por ejemplo, bases de datos KYC o mensajería de pagos conforme al estándar ISO 20022; entre otros). Una de las dificultades que caracterizan a esta primera fase es que la extracción de los datos desde fuentes heterogéneas (registradas en la cadena y no registradas) aporta una complejidad importante para cualquier proceso de auditoría.

3.1.2. Fase 2: transformación y procesamiento de los datos

Una vez identificado el origen del dato comienza la fase de transformación y procesamiento. En esta segunda fase, los datos se limpian, se normalizan y se estructuran bajo un lenguaje común (iXBRL/ISO 20022). Cualquier transformación de los datos mal gobernada en esta fase podría generar inconsistencias en todo el sistema. En este contexto, se propone reforzar la seguridad del flujo de datos en esta segunda fase a partir de dos tareas fundamentales y complementarias: a) el mapeo de todos los datos registrados y b) la verificación de los requisitos previstos por la *travel rule*. A partir del

[21] Esta aproximación al concepto permite la normalización conforme al estándar ISO 20022.

concepto de transparencia definido anteriormente, la supervisión de la transformación del dato se configura como una palanca de cambio que permite traccionar todo un engranaje de cumplimiento legal. Un error en la supervisión de esta fase podría ser letal para una gestión eficaz de los riesgos legales asociados al blanqueo de capitales o a cualquier otra figura similar. La necesidad de expandir el radar del auditor a todas las reglas de transformación y a todos los flujos e infraestructuras de datos viene impuesta por la realidad actual de los ecosistemas DeFi.

Pensemos, por ejemplo, en un proceso de transformación donde se pretende convertir una dirección de registro pseudónima en un registro que cumpla escrupulosamente con los criterios de la *travel rule*. En un momento posterior los datos procesados se cargarán en su destino final (ya sea este un repositorio o almacén de datos[22] o cualquier registro para reportes regulatorios) con la finalidad de analizarlos y de enviarlos a la autoridad competente.

En el caso del repositorio de datos[23] se identifican al menos tres ventajas fundamentales relacionadas con el objeto de estudio en este trabajo. La primera es que permite la consolidación de fuentes heterogéneas al unificar los datos registrados (provenientes de la cadena) con los datos no registrados (provenientes de cualquier otra fuente). Esta visión holística permite que el auditor pueda detectar discrepancias con más facilidad. En segundo lugar, toda vez que el dato entra en el repositorio institucional es inmutable y, por lo tanto, se genera una mayor seguridad jurídica facilitando también la eficacia probatoria. Y, por último, el repositorio institucional estructura los datos optimizando los procesos de lectura automatizada; lo cual facilita también la identificación de posibles patrones de blanqueo de capitales.

En términos prácticos, la implementación de un repositorio de datos robusto tiende a presentarse como una condición *sine qua non* para la auditoría continua; ya que sin él, la transparencia podría quedar relegada a un mero ejercicio de monitorización superficial (en el que, posiblemente, podrían presentarse problemas a la hora de acreditar la carga de la prueba en un proceso de supervisión bajo el Reglamento MiCA)[24].

En conclusión, esta fase de transformación se presenta como la última oportunidad del supervisor de cumplimiento para detectar posibles fraudes antes del reporte final. Como sugerencia, quizás podría ser interesante automatizar la asignación de calificaciones de riesgo durante el procesamiento de datos. Por ejemplo, mediante la implementación de alguna inteligencia artificial regulatoria con supervisión humana. De esta forma es

[22] También conocido internacionalmente como *data warehouse*. Se concibe en este trabajo como un sistema de almacenamiento centralizado diseñado para el análisis de datos, la generación de informes y la toma de decisiones estratégicas. A diferencia de una base de datos tradicional, no registra operaciones individuales a tiempo real, sino que procesa grandes volúmenes de datos provenientes de múltiples fuentes.

[23] Rentería y Font (2026, p. 41) defienden la idea de que los repositorios institucionales pueden servir como una herramienta de transparencia algorítmica en el ámbito del sector público.

[24] No en vano, en los ecosistemas DeFi se está avanzando hacia el concepto de *data lakehouse* o DLH, que combina la flexibilidad del almacenaje de datos encadenados con la estructura rigurosa de un repositorio de datos para el reporte regulatorio en armonía con los nuevos formatos exigidos por la *European Banking Authority*, (EBA).

posible contribuir a la buena gobernanza del proceso de transformación y evitar riesgos que pudieran comprometer el reporte de cumplimiento e incluso dar lugar a sanciones derivadas de la normativa comunitaria (MiCA, TFR y RGPD, entre otros).

Dado el carácter estratégico de esta segunda fase, a continuación se propone un esquema formal basado en un conjunto de doce controles. Con esta propuesta se aspira a dar cobertura a la totalidad del ciclo de vida del dato para un reporte estandarizado y acorde con las exigencias de *compliance* en cualquier ecosistema DeFi. La selección de estos controles es consistente con la normativa vigente y con los principios clásicos de confidencialidad, integridad y disponibilidad de la información. El esquema propuesto consta de cuatro dimensiones fundamentales cada una de las cuales comprende a su vez tres controles distintos que se dirigen hacia un aseguramiento holístico y riguroso; de conformidad con lo previsto por el regulador europeo.

La justificación de estos doce controles parte en primer lugar del principio de saturación en el riesgo (Arner et al., 2022, p. 17) y de la necesidad de garantizar la eficiencia operativa en cualquier entidad financiera. Tomando como referencia la curva de utilidad marginal del control, en la auditoría de sistemas complejos existe un punto de equilibrio donde el coste de implementar un control adicional supera al beneficio de la mitigación del riesgo que este aporta. Un número menor de controles dejaría ángulos muertos en la trazabilidad del dato (especialmente en la fase de transformación); mientras que una cifra superior podría generar una hipertrofia en la operativa diaria y un exceso de costes. En una infraestructura financiera digital, el exceso de controles manuales o redundantes introduce cierta latencia en la toma de decisiones y aumenta la probabilidad de incurrir en errores humanos.

Con esta propuesta, en segundo lugar, se persigue también el equilibrio entre la necesidad de regular la realidad actual de los mercados financieros digitales y la complejidad inherente a los ecosistemas DeFi. En otras palabras, se pretende cubrir la complejidad técnica de los registros sin perder de vista la rigidez del sistema financiero tradicional. Esta justificación comprende, entre otros aspectos, el reto de la interoperabilidad normativa.

Los ecosistemas DeFi operan bajo una lógica de transparencia algorítmica inmutable a partir del registro (Pastor, 2026, p. 82), mientras que el sistema financiero tradicional se rige por la responsabilidad legal del intermediario (ya sea éste una persona física o jurídica) y por la rigidez del reporte estático (a menudo fuera del registro). En este sentido, el esquema que se propone puede ser también una oportunidad para la convergencia entre ambos mundos puesto que combina elementos más propios de los registros descentralizados con otros aspectos más tradicionales. De esta forma se posibilita que los protocolos DeFi hablen en el mismo "idioma" que el regulador europeo (MiCA/TFR) sin perder su esencia. Como se verá enseguida, con esta propuesta se persigue también evitar la exclusión financiera basada en el riesgo, proponiendo que el cumplimiento normativo sea un elemento estratégico para este fin.

Por último, se aspira a que esta estructura aporte una cierta escalabilidad. Para ello, es necesario que pueda ser aplicable tanto a un pequeño VASP/CASP como

a una infraestructura más amplia y estandarizada conforme a la norma ISO 20022. Esta justificación se basa en el principio de neutralidad tecnológica y proporcionalidad (exigido por organismos como la *European Securities and Markets Authority* (ESMA)[25], o el FATF[26]) y está alineada con las preocupaciones actuales de los supervisores internacionales.

La estructura modular de estos controles parte de la premisa de que un modelo solvente de cumplimiento debe ser capaz de funcionar en diferentes escalas de volumen y complejidad sin perder su integridad semántica. Para un pequeño VASP/CASP, los doce controles ofrecen una hoja de ruta clara para su gobernanza de datos desde el inicio. Y, para una infraestructura que procese millones de transacciones bajo el estándar ISO 20022, estos controles proporcionan la utilidad necesaria para automatizar la auditoría mediante una interfaz de programación de aplicaciones[27]. Al estar alineada con estándares internacionales de mensajería financiera, la propuesta garantiza que la información sea de lectura mecánica y comparable a nivel global, permitiendo que la arquitectura de cumplimiento pueda adaptarse a la realidad de cada entidad financiera.

Tabla 1

Matriz de controles para la mitigación del riesgo de incumplimiento en la auditoría del flujo de datos.

PROPUESTA PARA LA AUDITORÍA DEL FLUJO DE DATOS
Dimensión I (E): Integridad y validación del origen del dato (extracción).
Control 1. Conciliación entre los datos procedentes de distintas fuentes. Verificar que los datos extraídos del registro coincidan con el resto de los registros internos.
Control 2. Autenticación del origen del dato. Controlar que las aplicaciones de los proveedores de datos cuenten con mecanismos de ciberseguridad suficientes para evitar alteraciones no deseadas.
Control 3. Control de completitud. Verificar que no existan saltos entre los bloques de la cadena ni transacciones perdidas en los procesos de extracción masiva de datos.
Dimensión II (T): Vigilancia en la transformación semántica (transformación).
Control 4. Revisión de la esencia de la transacción. Validar que la conversión de datos a estándares iXBRL (o a los requisitos de la *travel rule*) sea coherente y no afecte al significado de la transacción.

[25] Véanse, entre otros referentes, las directrices ESMA sobre las condiciones y los criterios para la calificación de los criptoactivos como instrumentos financieros. Disponible en: https://www.esma.europa.eu/sites/default/files/2025-03/ESMA75453128700-1323_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs_ES.pdf

[26] Véase el *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, publicado por el GAFI en 2021 y disponible en: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

[27] Una API (*Application Programming Interface* o Interfaz de Programación de Aplicaciones) es un conjunto de reglas y protocolos que permite que dos aplicaciones de *software* se comuniquen entre sí.

Dimensión II (T): Vigilancia en la transformación semántica (transformación).
Control 5. Verificación de la lógica del *smart contract.* Verificar que las reglas de cumplimiento estén correctamente codificadas en los procesos autoejecutables de transformación de datos.
Control 6. Normalización y armonización. Controlar que las direcciones de los repositorios y almacenes de datos pertenecientes a un mismo sujeto se identifiquen correctamente (ausencia de contradicciones).
Dimensión III: Seguridad y privacidad de los datos (confidencialidad y RGPD).
Control 7. Encriptación de PII[28] estática y dinámica. Verificar que los datos personales requeridos por la *travel rule* viajan y se almacenan cifrados, cumpliendo con el RGPD.
Control 8. Control de acceso. Verificar que solo los roles autorizados pueden acceder a la información sensible del originador/beneficiario de la transacción.
Control 9. Pruebas de conocimiento cero. Validar la implementación de pruebas de conocimiento cero para acreditar el cumplimiento normativo sin exponer datos sensibles.
Dimensión IV (L): Gobernanza y monitoreo (normalización).
Control 10. Auditoría de proveedores. Evaluar periódicamente los sesgos y tasas de falsos positivos de los diferentes proveedores integrados en los flujos de datos.
Control 11. Registro de evidencias. Garantizar que cada transformación del dato genera una evidencia inmutable que asegure su trazabilidad.
Control 12. Alertas de discrepancias. Implementar un monitoreo continuo que notifique automáticamente cualquier fallo o discrepancia.

Elaboración propia.

3.1.3. Discusión: el impacto de la matriz de controles en la mitigación del riesgo de incumplimiento y la prevención de delitos

Con la implementación de esta matriz de controles se pretende redefinir el nexo causal entre la elevada exigencia que a menudo acompaña a los procesos de auditoría de datos en el sector financiero con una prevención más eficaz de los delitos que típicamente atenazan a este sector; básicamente, el blanqueo de capitales y la financiación del terrorismo. Desde una perspectiva jurídica, un flujo de datos gobernado por estos controles permite que los sujetos obligados puedan construir una defensa robusta de cumplimiento legal.

Frente a cualquier posible investigación, la capacidad de presentar una evidencia inmutable (control 11) y registros de reconciliación (control 1) podría trasladar la carga

[28] En este trabajo el término PII (*Personally Identifiable Information* o información de identificación personal) se refiere en sentido amplio a cualquier dato que permita identificar a una persona de manera directa o indirecta.

de la prueba hacia la demostración de una debida diligencia. Esto acercaría a cualquier entidad financiera a la eximente de responsabilidad penal prevista en la mayor parte de los ordenamientos jurídicos de los Estados miembro de la Unión Europea, al demostrar que el modelo de prevención era idóneo y capaz de detectar patrones de fraude proactivamente.

La pérdida y la fragmentación de información relevante constituye uno de los mayores riesgos en cualquier ecosistema DeFi. En este sentido, la ausencia de contradicciones entre diferentes registros (control 6) combate directamente el riesgo de fragmentación de transacciones que tanto preocupa a las autoridades europeas. Al unificar direcciones de diferentes almacenes de datos bajo un mismo esquema, el sistema de cumplimiento puede aplicar de forma efectiva los umbrales de reporte exigidos por la *travel rule* y por el Reglamento MiCA. Por su parte, el conocimiento del cliente (KYC) también contribuye significativamente a mejorar la transparencia.

Otro de los puntos más controvertidos jurídicamente es la colisión entre el deber de informar (*travel rule*) y el derecho a la protección de datos de carácter personal. La discusión sobre las pruebas de conocimiento cero o ZKP (control 9) ofrece bajo el esquema propuesto una solución novedosa: permite el cumplimiento de la normativa vigente sin vulnerar el principio de minimización de datos[29]. Jurídicamente, esto supone un cambio de paradigma donde el regulador no recibe el dato privado, sino una declaración del cumplimiento, protegiendo la privacidad del usuario y reduciendo la responsabilidad de la entidad financiera ante posibles brechas de seguridad de información sensible. Sin perjuicio de ello, si bien el SBT salvaguarda la privacidad *on-chain*, la entidad de confianza o el proveedor que emitió la certificación de identidad *off-chain* debe retener la capacidad técnica y la obligación legal de revelar la identidad subyacente en caso de orden judicial o de iniciarse una investigación criminal.

Por último, la estandarización bajo estos controles actúa como un mecanismo de seguridad jurídica. El fenómeno de exclusión de sectores de riesgo por parte de la banca tradicional[30] a menudo deriva de la incapacidad de auditar los procesos internos de los VASP/CASP. Al adoptar una estructura escalable y compatible con la norma ISO 20022, los proveedores de servicios pueden ofrecer un nivel de transparencia equivalente al de una entidad de crédito tradicional, facilitando la interoperabilidad y reduciendo el riesgo de exclusión financiera. En relación con todo ello, los controles 4, 5 y 10 elevan el concepto de diligencia reforzada de manera coherente con la gravedad del riesgo que se desea prevenir. Y, particularmente, el control 10 (auditoría de proveedores).

3.1.4. Fase 3: almacenamiento y gobernanza de datos

Para alcanzar niveles satisfactorios de transparencia los datos procesados deben guardarse ordenadamente de forma que sean trazables y, a ser posible, facilitando una lectura mecánica. En esta etapa los datos pueden aparecer encriptados o con algún

[29] En este sentido, Gupta (2025) p. 5757.
[30] En detalle, Toso Milos (2020) p. 3.

control de privacidad con la finalidad de ejecutar un proceso adecuado de auditoría sin dejar de cumplir con los requisitos exigidos por el RGPD. De esta forma, la entidad puede ejercer una gobernanza más eficiente de todos sus datos.

3.1.5. Fase 4: reporte final de datos

Esta fase consiste en la entrega final del dato a la autoridad competente y permite una auditoría continua, donde a menudo se utilizan interfaces de programación de aplicaciones para monitorizar los flujos de datos en tiempo real. El recurso a estas herramientas representa un avance significativo desde el modelo tradicional (basado en el reporte de informes periódicos) hacia un reporte más inmediato y continuo.

En este momento, la estandarización del reporte exige que el auditor supervise cada flujo de datos completo realizando una revisión general de todo su ciclo de vida. Entre las cuestiones con mayor trascendencia jurídica deberá comprobar si la transformación del dato fue correcta, si se ha mantenido su integridad, o si los controles automatizados funcionaron correctamente. De esta forma, se dota de mayor transparencia al proceso. Gracias a la estandarización del reporte de la información financiera es posible identificar la fuente del dato y sus posibles relaciones con otros datos.

3.2. Cumplimiento desde el diseño y gobernanza del dato

En el contexto de este trabajo y a la luz de la matriz de controles propuesta en el apartado anterior, el cumplimiento desde el diseño aflora como el resultado natural de una evolución de la doctrina de la responsabilidad proactiva (Santamaría, 2020, p. 144). En tal sentido, está alineado con el principio de privacidad desde el diseño del RGPD (trasladado ahora a la integridad del mercado financiero).

El cumplimiento desde el diseño trasciende del enfoque tradicional que lo concebía como una función de supervisión. En el marco de los servicios financieros descentralizados, el cumplimiento desde el diseño propone, en primer lugar, la integración de las normas de prevención de delitos (tales como la *travel rule* o los límites transaccionales de MiCA) directamente en la lógica de los contratos autoejecutables.

Desde una perspectiva basada en la técnica legislativa reguladora de la responsabilidad penal corporativa, esto supone transitar desde una capa de cumplimiento externa (y más bien reactiva) hacia una arquitectura de “normatividad conductual intrínseca” (y con frecuencia estandarizada). Bajo este enfoque, la infracción de la norma no es solo una conducta sancionable, sino un defecto técnico del sistema. Este nivel de exigencia debería contribuir a la reducción significativa de los niveles de riesgo y de los costes de monitorización.

En segundo lugar, se propone un modelo de cumplimiento desde el diseño que incorpora como herramientas fundamentales en el entorno digital la declaración electrónica de atributos para datos encadenados en el registro, los tokens intransferibles (SBT), y las pruebas de conocimiento cero o ZKP.

Uno de los mayores retos jurídicos de la *travel rule* en los entornos de acceso abierto o *permissionless* es precisamente la identificación de los sujetos intervinientes. En este contexto parece razonable reflexionar sobre el uso de SBT como vehículos de credenciales verificables aprovechando su carácter intransferible. Jurídicamente, podrían funcionar como declaraciones de idoneidad ya que permiten, por ejemplo, que un usuario pueda demostrar fehacientemente que ha superado un proceso de debida diligencia (KYC) realizado por un tercero de confianza sin necesidad de que el protocolo DeFi o la contraparte tengan acceso a la identidad subyacente. De esta forma, el mecanismo del SBT armoniza el deber de identificación que exige la normativa europea con la naturaleza descentralizada. Para una mejor transparencia y trazabilidad se podrían incluso generar "listas blancas" dinámicas y auditables.

Por otro lado, dado que la aplicación de la *travel rule* exige el intercambio de información personal (y que esta exigencia entra en colisión directa con el principio de minimización de datos del RGPD), las ZKP se presentan como una herramienta bastante útil a la hora de resolver este conflicto jurídico. Mediante una ZKP, un sujeto cualquiera puede demostrar criptográficamente que una transacción cumple con requisitos legales específicos (por ejemplo, que el sujeto ordenante no reside en una jurisdicción de alto riesgo o que el importe a transferir no supera el umbral de reporte) sin revelar los datos crudos de la transacción ni la identidad de las partes. Frente a cualquier supervisor esto garantiza un nivel satisfactorio de transparencia puesto que el cumplimiento es verificable y, al mismo tiempo, el derecho a la privacidad y al secreto financiero del usuario permanecerían indemnes.

Esta propuesta persigue también el objetivo de configurar la verificación de los atributos de legalidad como una condición previa a la ejecución de cualquier transferencia de activos. Así, conforme a la normativa europea que rige en los ecosistemas DeFi, este objetivo representa un nuevo estándar de transparencia que va más allá de la mera declaración del sujeto obligado. Este estándar de *lex cryptographica* aspira a proteger la integridad del sistema financiero y, al mismo tiempo, los derechos fundamentales de los ciudadanos de la Unión Europea en entornos digitales.

3.3. Supervisión automatizada y herramientas para el análisis de registros distribuidos

La transición hacia este paradigma de cumplimiento desde el diseño y basado en datos parte de la interoperabilidad semántica (iXBRL/ISO 20022) y de una vigilancia que debe ser ágil y proactiva. En este punto, la supervisión automatizada contribuye a mejorar la transparencia y, sobre todo, a reducir los costes comúnmente asociados a la vigilancia humana en los ecosistemas DeFi (Toledo-Castillo et al., 2026, pp. 47 y ss.).

En los últimos tiempos, la migración de los mercados financieros hacia infraestructuras de registros distribuidos (DLT) en la Unión Europea ha modificado sustancialmente la ontología de los activos y ha redefinido la actividad supervisora de los organismos y autoridades de vigilancia. En esta línea, a continuación, se ofrece una reflexión sobre la conveniencia de

transitar desde una vigilancia tradicionalmente reactiva hacia un modelo de transparencia y cumplimiento efectivo. Como se anticipó anteriormente, la transparencia se encuentra íntimamente relacionada con la capacidad real del regulador para verificar la trazabilidad de los datos en entornos estandarizados. La implementación de estándares como la norma ISO 20022 y la arquitectura de una interfaz de programación de aplicaciones permiten la interoperabilidad de los datos en el sector financiero. Si bien es cierto que esto faculta a los organismos de control (como la ESMA en el contexto europeo) para la implementación de nodos de observación que realicen una auditoría continua, no es menos cierto que el paso de la "vigilancia basada en reportes" a una "vigilancia basada en datos" permite mitigar el riesgo sistémico mediante la detección temprana de anomalías y reduce la asimetría de información entre el sujeto obligado y el supervisor. En este contexto, los procesos de auditoría se convierten en concurrentes y ponen de manifiesto la obsolescencia del modelo tradicional basado en los reportes periódicos o de "foto fija". En segundo lugar, no puede olvidarse el debate sobre la validación de las herramientas de análisis de registros distribuidos, pilar crítico en la supervisión automatizada.

En el sistema financiero actual se identifican al menos tres utilidades en la validación de estas herramientas. En primer lugar, la banca privada y los CASP a menudo utilizan el análisis de registros distribuidos en sus protocolos AML/KYC (Wronka, 2022, pp. 84 y ss.) y en sus sistemas internos de *compliance* y gestión de riesgos legales, esencialmente, con la finalidad de verificar que las entradas de fondos no tienen su origen en un acto ilícito.

En segundo lugar, la herramienta es útil para la investigación criminal ya que permite que la autoridad policial o instructora pueda identificar mejor el rastro digital de los delitos cometidos en línea o después de un ataque malicioso.

Por último, aporta seguridad y confianza al mercado financiero y a los inversores que concurren en él. Sin ir más lejos, permite verificar, por ejemplo, si una plataforma digital descentralizada se encuentra realmente respaldada por los fondos que dice tener. El aspecto clave es, por tanto, la validación de cualquier herramienta de análisis de registros distribuidos; pues de ello dependerá en buena medida su utilidad desde esta triple hélice.

Sin embargo, esta validación por parte de las autoridades externas introduce un nuevo riesgo jurídico en la ecuación: la opacidad del criterio de riesgo. Una gobernanza adecuada de cualquier modelo basado en el dato exige que el auditor no solo valide el resultado sino, lo que es más importante aún, la metodología empleada para la calificación del riesgo. Para evitar falsos positivos que vulneren derechos fundamentales (como el bloqueo indebido de fondos), resulta fundamental la aplicación de auditorías de sesgo. A propósito de este debate no sobra referir aquí que, en el marco del Reglamento MiCA, las exigencias de idoneidad de los administradores y los requisitos de gobernanza interna de los CASP encuentran en los SBT una solución disruptiva.

Como se refirió anteriormente, los SBT permiten contrastar atributos de idoneidad de forma inmutable y vinculada de manera unívoca a la dirección del CASP. Frente a los requerimientos de información bajo MiCA (véanse los artículos 59 y 60), el sujeto

obligado no se limita a una mera declaración de cumplimiento, sino que presenta una declaración electrónica de atributos que puede contrastarse de manera inmediata. Esto permite alcanzar un cierto estándar de verificabilidad. Por otro lado, la arquitectura de los SBT permite condicionar la operatividad del protocolo a la posesión de credenciales específicas (por ejemplo, una certificación de inversor cualificado o de cumplimiento de KYC). De esta forma, podemos concebir de nuevo el cumplimiento normativo como una especie de condición previa a la ejecución de cualquier operación financiera aportando seguridad jurídica a los intervinientes. Aspecto particularmente relevante cuando se trata de servicios financieros complejos.

En conclusión, podría decirse que el concepto de transparencia algorítmica defendido en este trabajo representa la evolución del cumplimiento normativo hacia un modelo donde la confianza no reside exclusivamente en la declaración del sujeto obligado, sino que además incorpora la verificabilidad del dato. Desde este enfoque, los SBT se posicionan como credenciales de un cumplimiento normativo *sui generis* con una utilidad clara: permitir una supervisión automatizada, confiable y segura.

Llegados a este punto es muy posible que el lector se esté preguntando si el recurso hacia las herramientas de análisis de registros distribuidos y las nuevas formas de supervisión automatizada vulneran el principio fundamental de neutralidad tecnológica o si, por el contrario, nos encontramos más bien ante una evolución necesaria. Desde una perspectiva purista, la obligación de adoptar estándares específicos (como ISO 20022 o iXBRL) podría interpretarse como una quiebra del principio de neutralidad, al forzar a los sujetos obligados a adaptar sus sistemas internos a una infraestructura técnica predefinida por el supervisor. La "imposición" de lenguajes de lectura mecánica específicos podría desincentivar la innovación en protocolos alternativos que, siendo igualmente eficaces para el *compliance*, sin embargo, podrían no ser compatibles con el nodo de observación del regulador.

Para los VASP/CASP de menor escala, esta exigencia podría suponer una barrera de entrada, contraviniendo el principio de proporcionalidad y agregando una carga operativa elevada. No obstante, la doctrina más reciente sugiere que la neutralidad tecnológica no debe entenderse como una pasividad técnica del regulador[31]. En los ecosistemas DeFi, la supervisión efectiva es técnicamente imposible sin un mínimo de interoperabilidad semántica. Por otro lado, si atendemos a la eficacia del bien jurídico protegido, la neutralidad no puede ser una "patente de corso" para la opacidad de los datos. Si una tecnología impide de facto la supervisión (pongamos por caso, protocolos puros sin puntos de control para la *travel rule*), el supervisor estará legitimado para exigir estándares que garanticen la transparencia y la acreditación de que el operador está cumpliendo normativamente con la regulación europea.

[31] Bertolini (2025) defiende por ejemplo que debe entenderse, más bien, como una exigencia necesaria para la interoperabilidad.

En este trabajo se sostiene la tesis de que, en un entorno de auditoría continua, el principio de neutralidad tecnológica debe reinterpretarse bajo el paradigma de la interoperabilidad. La supervisión automatizada no obliga a los operadores que intervienen en el tráfico jurídico y económico a adoptar una tecnología concreta, sino a participar en un lenguaje común de reporte que eleve los estándares básicos de seguridad y confianza en el sistema financiero. Este enfoque contribuye a la mitigación significativa del riesgo sistémico y a reducir las asimetrías de información. En última instancia, la estandarización no contraviene la neutralidad, sino que facilita que la autoridad supervisora pueda ejercerse eficazmente en un entorno descentralizado sin la necesidad de forzar una centralización contraria a la naturaleza de la propia tecnología DLT. A continuación, se ofrece una tabla resumen con las características esenciales de ambos modelos:

Tabla 2
Evolución del modelo de supervisión financiera.
Propuesta frente al vacío estructural de ecosistemas DeFi.

A la izquierda, el flujo lineal y asincrónico del modelo tradicional de reporte; a la derecha, el ecosistema circular y concurrente basado en contratos inteligentes y cumplimiento normativo desde el diseño propuesto en este trabajo.

	Flujo de datos en la auditoría tradicional (basada en reportes periódicos)	**Flujo de datos en la auditoría continua** (basada en el modelo propuesto)
Descripción del modelo	Reactivo y dependiente de la declaración del sujeto obligado.	Basado en la auditoría concurrente y el cumplimiento desde el diseño.
Generación del dato	La transacción financiera ocurre en los sistemas internos de la entidad sin medidas de cumplimiento normativo automatizadas.	La transacción financiera está programada para ejecutarse (incluso automáticamente) solo si se cumplen las reglas de cumplimiento previamente embebidas.
Registro interno	El dato se almacena en bases de datos privadas o silos de información.	Validación de identidad (SBT/ZKP). Antes de la ejecución, se verifica el SBT de las partes sin revelar datos sensibles.
Extracción y consolidación	Proceso manual o semiautomático para la elaboración de informes periódicos.	Un organismo o autoridad actúa como puente asegurando que los metadatos de la travel rule se transmiten de forma cifrada.
Envío del reporte (iXBRL/ ISO 20022)	El sujeto obligado envía la información al regulador con un desfase temporal considerable.	Registro inmutable en cadena. La transacción y su declaración de cumplimiento se graban en el registro de forma permanente.
Revisión del supervisor o exégesis	La autoridad competente (ESMA/ EBA) analiza el reporte ex-post.	El regulador no espera un reporte, tiene un “nodo de observación” que audita los datos en tiempo real (ISO 20022).

	Flujo de datos en la auditoría tradicional (basada en reportes periódicos)	**Flujo de datos en la auditoría continua** (basada en el modelo propuesto)
Acción regulatoria	Si se detecta una anomalía o desviación de la norma, la respuesta suele ocurrir meses después del evento.	Monitorización continua. Los sistemas de lectura mecánica analizan flujos de datos y detectan anomalías en tiempo real.
Resultado	Alta asimetría informativa y riesgo de manipulación de datos previos al envío.	Transparencia, eliminación del desfase temporal y reducción del riesgo de exclusión financiera.

Elaboración propia.

4. La nueva auditoría de cumplimiento en los ecosistemas DeFi

La utilidad real del *compliance* en el siglo XXI pasa necesariamente por su capacidad de adaptación a la realidad actual de los entornos digitales. Desde hace años se venía advirtiendo que la auditoría tradicional de "foto fija" era insuficiente para detectar cualquier irregularidad, sobre todo, dada la velocidad con la que circulan los flujos en los ecosistemas DeFi (De la Hoz et al., 2025, pp. 64 y ss.); y que, además, esto generaba una brecha temporal que las organizaciones criminales solían aprovechar para el blanqueo de capitales.

Cualquier posible solución frente a este problema exige la implementación de protocolos de auditoría continua capaces de detectar desviaciones de forma concurrente a la transacción. Pues solo así podrá combatirse este tipo de delincuencia económica de una manera real y efectiva. Neutralizando este incentivo se reduce también la asimetría de información entre el sujeto obligado y el supervisor.

Por su parte, la estandarización de los datos facilita la identificación de señales de fraude y la detección de patrones de delincuencia económica que bajo el esquema tradicional a menudo solían quedarse "fuera del radar". Una auditoría digital robusta protege a los inversores y aporta seguridad jurídica a todo el sector financiero. Más allá del potencial efecto disuasorio de una sanción, esta transformación de los procesos de auditoría persigue un impacto social positivo (externalidad positiva) como lo es la mitigación del riesgo sistémico y la lucha contra la exclusión financiera; fenómeno que se aborda en detalle en el apartado siguiente.

En este nuevo escenario, es posible ofrecer niveles de transparencia en ecosistemas DeFi "equivalentes" a los de la banca tradicional y también es posible fomentar la inclusión financiera de los activos digitales dentro del marco regulatorio europeo. En definitiva, se hace más fácil contribuir a la configuración de un ecosistema más resistente y robusto frente al crimen organizado.

5. La exclusión financiera institucional: implicaciones jurídicas y propuestas de mitigación

El riesgo de exclusión financiera institucional representa la consecuencia no deseada más severa de la asimetría entre la presión del regulador europeo y la realidad tecnológica que impera hoy en día en el sector financiero. En un contexto marcado por el auge de los activos digitales (y por la complejidad de los retos jurídico-sociales comúnmente asociados a su uso), este fenómeno no solo amenaza la viabilidad operativa de los VASP/CASP, sino que pone en peligro la propia integridad y la transparencia del sistema financiero global.

Para una mejor explicación del problema, se exponen en primer lugar la naturaleza y el alcance de la exclusión financiera en los ecosistemas DeFi. En este contexto, la exclusión financiera consiste, dicho muy básicamente, en la práctica de las instituciones financieras tradicionales (principalmente la banca comercial) de rescindir o restringir de manera masiva sus relaciones de negocio con determinadas categorías de clientes o sectores, con el fin de evitar (en lugar de gestionar y gobernar), los riesgos de blanqueo de capitales y financiación del terrorismo.

Este comportamiento, a menudo impulsado por la presión regulatoria de organismos internacionales (como la FinCEN norteamericana, la ESMA, o las exigencias derivadas del Reglamento MiCA en la Unión Europea) genera efectos contraproducentes desde una perspectiva de política pública. A menudo esta decisión responde a una lógica empresarial de coste-beneficio que puede estar basada, a mi juicio, en tres razones principales.

La primera de ellas es el miedo a sufrir una sanción. Los escándalos que han salpicado al sector financiero en los últimos años han reforzado la idea de que quizás sea mejor "no arriesgarse" cuando la entidad no ha alcanzado un nivel de seguridad suficiente sobre la adecuada gestión y gobernanza de según qué riesgos.

La segunda son los costes del cumplimiento. Mantener una vigilancia constante sobre activos complejos (por ejemplo, cripto o remesas) puede elevar considerablemente la factura del cumplimiento normativo. Dicho en pocas palabras, si el beneficio que da el cliente es menor que el coste de vigilarlo, el banco no tendrá incentivos para evitar su exclusión financiera.

Por último, no podemos olvidar la presión del regulador. A veces, los supervisores nacionales e internacionales dan instrucciones explícitas o implícitas de que ciertos sectores representan un riesgo alto. Estas señales pueden activar implícitamente el riesgo de exclusión financiera. El GAFI ya ha advertido que este fenómeno masivo realmente resulta contraproducente. Si un banco expulsa del sistema financiero formal a un sector por considerarlo excesivamente complejo (costoso de gestionar), lo cierto es que el sector no desaparece, sino que simplemente se desplaza al terreno de la economía informal donde, por cierto, será más difícil de rastrear. Esto crea una paradoja y es que, en el intento de evitar el blanqueo, las entidades financieras terminan haciendo que los flujos sean más opacos y difíciles de investigar para las autoridades.

A propósito de todo ello, la *travel rule* y el TFR imponen obligaciones técnicas tan complejas y costosas que en ocasiones conducen a esta paradoja, sobre todo cuando se trata de entidades financieras y/o intermediarios más modestos o con menos recursos para una adecuada gobernanza de este tipo de riesgos. No en vano, el GAFI insiste en que las instituciones financieras deben aplicar un enfoque basado en el riesgo (gestionar y gobernar el riesgo) en lugar de un enfoque de exclusión (eliminar al cliente). Sin embargo, en la práctica se identifican otros aspectos de relevancia que se exponen a continuación.

En primer lugar, sobre el problema de opacidad en las transacciones es cierto que desde el momento en el que se impide que determinados usuarios puedan acceder al sistema financiero regulado se les está desplazando implícitamente hacia interfaces y canales no supervisados. También es cierto que esto reduce claramente la visibilidad de los supervisores y su capacidad para controlar, monitorear y regular los riesgos sobre estos flujos. Sin embargo, el compromiso del regulador a menudo se limita a la aprobación de la norma y, en este contexto, resulta imprescindible su adaptación conforme a criterios objetivos que permitan clasificar al sujeto obligado atendiendo, por ejemplo, a su capacidad real para gobernar estos riesgos. En este segundo nivel resulta fundamental el compromiso de las autoridades e instituciones públicas y de los *policy makers* para una mejor aplicación (y, por ende, para un mejor cumplimiento) de la regulación europea.

En segundo lugar, esta práctica genera nuevas barreras a la interoperabilidad. La incapacidad de auditar los procesos internos de los VASP/CASP por parte de la banca tradicional fragmenta el mercado y limita la adopción de estándares de reporte. En otras palabras, este resultado puede resultar contrario a la estandarización del reporte digital en el sentido que se viene defendiendo a lo largo de estas páginas y, por lo tanto, impediría que las entidades de supervisión pudieran beneficiarse de las ventajas que comporta la transparencia en los ecosistemas DeFi.

Por último, en tercer lugar, se identifica implícitamente un riesgo sistémico de exclusión. Pues con esta práctica se están creando “silos financieros” que impiden la convergencia entre la economía tradicional y la digital, desincentivando el cumplimiento normativo proactivo. Lo cual, genera a su vez nuevos riesgos en el sistema financiero.

Con la finalidad de atajar estos problemas y de poner sobre la mesa las implicaciones jurídicas y económicas reales de este fenómeno se ofrece a continuación una propuesta de mitigación basada en el cumplimiento normativo como herramienta fundamental para garantizar la seguridad jurídica de los operadores e inversores. En primer lugar, la solución no debe residir en la centralización forzada, sino en el fomento de una transparencia acorde con el modelo propuesto en la matriz de controles y, al mismo tiempo, con la adopción de una infraestructura de cumplimiento robusta. A partir de este enfoque la prevención del riesgo de exclusión financiera es posible si consideramos, al menos, tres elementos fundamentales.

El primer elemento es la transparencia. El nuevo modelo de auditoría propuesto incluye garantías de transparencia a partir de elementos tales como el control de los flujos de datos y la posibilidad de verificar el dato como criterio fundamental (en lugar de fiarlo todo a la mera declaración subjetiva del sujeto obligado). De esta forma las entidades financieras pueden ofrecer a cualquier contraparte una seguridad razonable.

El segundo elemento consiste en la incorporación de nuevas evidencias de idoneidad para eliminar la opacidad tradicional que justificaba este fenómeno. Estas evidencias de idoneidad parten del uso de SBT y ZKP como herramientas claves para permitir que un VASP/CASP cualquiera pueda demostrar aspectos tan relevantes como el cumplimiento de la *travel rule* o la integridad de los derechos de sus usuarios de conformidad con lo establecido en el RGPD.

En tercer lugar, la adopción de una semántica común para el reporte digital permite que el cumplimiento sea una propiedad intrínseca del sistema. Cuando la información es de lectura mecánica y comparable globalmente, el riesgo de cumplimiento se vuelve más predecible y gestionable, incentivando a las instituciones financieras a mantener y a abrir canales de servicios (en lugar de cerrarlos).

Sin embargo, existen algunas limitaciones que podrían dificultar la implementación en la práctica del modelo propuesto. En primer lugar, la evolución del cumplimiento normativo como una herramienta útil para la prevención de riesgos en el sector financiero está alcanzando cotas desconocidas hasta la fecha. Sin embargo, el nivel de compromiso de los agentes que participan en este sector y su implicación en el uso de esta herramienta (desde esta perspectiva) presenta una evolución desigual y poco uniforme (Paredes et al., 2026, pp. 1082 y ss.).

En segundo lugar, el éxito en la implementación de esta propuesta depende también del diseño de nuevas políticas públicas (no solo legislativas) que coadyuven en aspectos tan relevantes como la concienciación, el fomento de la cultura de cumplimiento, la auditoría concurrente y el reconocimiento de las mejores prácticas corporativas en el sector financiero.

Por último, en tercer lugar, no debemos olvidar la importancia de la capacitación y de la formación para altos directivos y cargos intermedios. Solo desde un conocimiento cualificado de estas herramientas será posible su correcta implementación en la práctica. En este punto las grandes corporaciones financieras que operan en el mercado internacional han tomado consciencia y han comenzado a apostar por la formación periódica para altos directivos buscando que la aplicación del *compliance* se perciba cada vez más como una herramienta estratégica para los objetivos de la compañía.

6. Problemas de extemporalidad y falta de reciprocidad en la aplicación de la *travel rule*: propuestas desde un enfoque basado en el riesgo

El éxito de la arquitectura jurídica impuesta por el legislador europeo se enfrenta al desafío geopolítico y temporal del problema del amanecer anteriormente expuesto. Si un CASP en una jurisdicción con plena vigencia normativa pretende celebrar una transacción con una contraparte en una región donde la obligación de la *travel rule* no es ejecutable, el sistema se ve abocado a un bloqueo preventivo o a una exclusión financiera claramente contraria a la eficiencia de los mercados. Con la finalidad de mitigar este riesgo, se plantean a continuación algunas propuestas basadas en el enfoque defendido a lo largo de este trabajo.

La primera de ellas consiste en la implementación de un enfoque basado en el riesgo dinámico y automatizado (FATF, 2024, p. 33)[32]. Frente a la rigidez de la *travel rule* (y el consecuente bloqueo), quizás una alternativa a considerar pueda ser que los sujetos obligados adopten un enfoque proactivo que no dependa exclusivamente de la recepción de metadatos de identidad de la contraparte, sino de la declaración electrónica del riesgo. Siguiendo con el esquema propuesto anteriormente, esta propuesta pasaría por la integración del flujo de datos (Fase 2: Transformación) con algoritmos de lectura mecánica que realicen una calificación del riesgo asociado a cada transacción en tiempo real. De esta forma, si la contraparte se encuentra en una jurisdicción bajo el *sunrise issue*, el CASP puede autorizar la transacción si el análisis en la cadena no revela patrones de riesgo (por ejemplo, vinculación con protocolos de mezcla[33] o direcciones sancionadas).

En segundo lugar, cabe considerar la creación de pasarelas de interoperabilidad mediante SBT y ZKP. Conectando con la tesis del cumplimiento desde el diseño expuesta anteriormente, el problema del amanecer podría mitigarse mediante el uso de infraestructuras de identidad descentralizada. Aquí la propuesta consistiría en el uso de SBT como declaraciones electrónicas de cumplimiento para permitir que un usuario demuestre que su identidad

[32] Conforme a las recomendaciones del FATF, si un VASP no puede cumplir la regla por el *sunrise issue*, debería aplicar un Enfoque Basado en el Riesgo (EFB). Así, por ejemplo, si el *exchange* A no puede enviar los datos al B porque el B no tiene sistema, el *exchange* A debe investigar más a fondo quién es el beneficiario antes de autorizar el envío (debida diligencia reforzada). Como segunda recomendación, en lugar de bloquear el 100% de las transacciones, el regulador puede permitir envíos de bajo importe hacia jurisdicciones "sin amanecer", siempre que no haya alertas de sanciones o riesgo de blanqueo de capitales (límites provisionales). Por último, los *exchanges* pueden crear directorios de contrapartes que, aunque estén en países sin reciprocidad, hayan aceptado voluntariamente usar estándares que faciliten la interoperabilidad (listas blancas de VASP).

[33] En el contexto de este artículo, los protocolos de mezcla (también llamados *mixers*) representan un desafío jurídico diametralmente opuesto a la trazabilidad. Un protocolo de mezcla se concibe aquí como cualquier servicio de mejora de la privacidad que rompa el vínculo de la cadena entre el origen (la dirección del remitente) y el destino de los fondos. Estos sistemas agrupan las transacciones de múltiples usuarios en un fondo común y las redistribuyen a las direcciones de destino de forma aleatoria y fragmentada desvirtuando la lógica de la cadena de bloques.

ha sido verificada por un tercero de confianza (por ejemplo, un VASP/CASP regulado en la Unión Europea) sin necesidad de que el receptor de la transacción en zona "*sunrise*" tenga que procesar datos de identidad sensibles. La principal ventaja es que, mediante las ZKP, se genera una evidencia electrónica del cumplimiento verificable de manera universal. La consecuencia inmediata es que el flujo de capital no quedaría bloqueado (y, al mismo tiempo, el cumplimiento normativo viajaría "adherido" a la transacción, con independencia de la normativa vigente en la jurisdicción de destino).

Por último, conviene recordar que la desconexión informativa entre VASP/CASP a menudo se ve agravada por la falta de un lenguaje común de reporte. Frente a este problema, la adopción del estándar ISO 20022 para la mensajería de la *travel rule* actúa como un mecanismo de neutralización del problema del amanecer. Al utilizar una semántica de lectura mecánica y comparable globalmente, se facilita que incluso las entidades en jurisdicciones menos avanzadas tecnológicamente puedan integrar módulos de recepción de datos.

En resumidas cuentas, con este paquete de propuestas se persigue enfatizar la idea de que las soluciones frente al *sunrise issue* no deben buscar la uniformidad legislativa global (a mi juicio, un objetivo inalcanzable a corto y medio plazo), sino la convergencia técnica.

7. Conclusiones

La investigación desarrollada permite concluir que la transición hacia un modelo de reporte digital estandarizado responde a la necesidad de reconfigurar la gobernanza financiera en la era digital. El concepto de transparencia algorítmica que se propone en este trabajo constituye el vector fundamental para superar las tensiones entre la descentralización de los protocolos DeFi y la presión supervisora del legislador europeo. En tal sentido, la sustitución de la declaración subjetiva del sujeto obligado por la verificabilidad inmutable del dato eleva el estándar de *compliance* y lo posiciona como una herramienta particularmente útil en la realidad financiera actual.

El modelo de cumplimiento desde el diseño que se propone, basado en la integración de SBT y ZKP, ofrece una respuesta frente al conflicto entre la *travel rule* y el RGPD. Esta arquitectura permite que la identificación de los intervinientes sea verificable sin necesidad de una exposición masiva de datos personales registrados, preservando la naturaleza *permissionless* de la tecnología a la vez que se satisface el interés público de la prevención del blanqueo de capitales.

El fenómeno de la exclusión financiera institucional representa una externalidad negativa de la incertidumbre regulatoria. La estandarización semántica (iXBRL/ISO 20022) y la validación de herramientas de análisis de registros distribuidos son condiciones necesarias para restaurar la confianza interbancaria. Solo mediante la creación de un lenguaje común de riesgo será posible evitar la exclusión de los VASP/CASP del sistema financiero formal, impidiendo el desplazamiento de la actividad hacia interfaces opacas y no reguladas.

Como resultado de esta investigación, se proponen las siguientes líneas de acción para futuras regulaciones jurídicas. En primer lugar, una apuesta clara por el reconocimiento de la declaración electrónica de atributos como prueba efectiva de cumplimiento. En este sentido, la promoción de marcos legales que reconozcan las credenciales verificables (SBT) como pruebas de cumplimiento válidas contribuiría a mejorar los procesos de diligencia debida. En segundo lugar, el fomento de la supervisión automatizada cooperativa. Si se incentiva la creación de diferentes "nodos supervisores" operados por autoridades competentes que cooperan entre sí resultaría más sencilla la auditoría concurrente de protocolos sin comprometer la descentralización. En tercer lugar, el establecimiento de auditorías de sesgo algorítmico. El hecho de establecer requisitos de transparencia contribuye al aseguramiento de que la calificación del riesgo pueda ser auditable, explicable y libre de sesgos que vulneren derechos fundamentales. Finalmente, en cuarto lugar, la armonización del *sunrise issue.* Desde la Unión Europea se aspira a liderar una coordinación internacional para que la asimetría tecnológica entre jurisdicciones no se convierta en una barrera para el flujo lícito de activos digitales. Sin embargo, para alcanzar el éxito en esta tarea se requiere de una colaboración interinstitucional que en ocasiones choca frontalmente con la soberanía nacional de cada Estado. Para ello, se propone la configuración de marcos regulatorios multilaterales que, al menos en lo básico, permitan el aseguramiento de un mínimo común denominador suficiente para la prevención de los riesgos globales más significativos en el contexto de la seguridad de los mercados financieros globales. Pues si la amenaza es global, las herramientas para combatirla también deben serlo. Un sistema financiero más transparente y seguro es, en última instancia, un sistema más justo y resistente frente al fraude.

Acerca del artículo

Notas de conflicto de interés. El autor declara no tener ningún conflicto de interés en relación con la publicación de este artículo.

Contribución en el trabajo. El autor asumió todos los roles establecidos en *Contributor Roles Taxonomy* (CRediT).

Financiación. Este trabajo forma parte del proyecto de I+D+I Cumplimiento normativo y protección penal de la Administración Pública, financiado por el Ministerio de Ciencia e Innovación del Gobierno de España, referencia PID2022-138775NB-I00.

Referencias

Alonge, E., Dudu, O. y Alao, O. (2024). The impact of digital transformation on financial reporting and accountability in emerging markets. *International Journal of Science and Technology Research Archive, 7*(2), 025-049. https://doi.org/10.53771/ijstra.2024.7.2.0061

Arner, D., Buckley, R. y Zetzsche, D. (2022). FinTech and the four horsemen of the apocalypse: building financial ecosystems for resilience, innovation and sustainable development. *Banking & Finance Law Review, 39*(1), 5-31.

Bartolacci, F., Caputo, A., Fradeani, A. y Soverchia, M. (2021). Twenty years of XBRL: What we know and where we are going. *Meditari Accountancy Research, 29*(5), 1113-1145. https://doi.org/10.1108/medar-04-2020-0846

Bertolini, A. (2025). ¡La inteligencia artificial no existe! Desafiando la narrativa de la neutralidad tecnológica en la regulación de la responsabilidad civil de las tecnologías avanzadas. *Revista de Derecho Privado*, (49), 31-82. https://doi.org/10.18601/01234366.49.02

Birt, J., Muthusamy, K. y Bir, P. (2017). XBRL and the qualitative characteristics of useful financial information. *Accounting Research Journal, 30*(01), 107-126. https://doi.org/10.1108/arj-11-2014-0105

Borgi, H. (2022). XBRL technology adoption and consequences: A synthesis of theories and suggestions of future research. *Journal of Accounting and Management Information Systems, 21*(2), 220-235. https://doi.org/10.24818/jamis.2022.02004

D'avino, C. (2023). Money laundering and AML regulatory and judicial system regimes: investigation of FinCEN files. *European Journal of Law and Economics, 55*(2), 195-223. https://doi.org/10.1007/s10657-022-09756-3

De la Hoz, B., Morán, I., Tete, A. y de la Hoz, A. (2024). Inteligencia artificial como estrategia para gestionar los procesos de auditoría financiera. *Revista Estrategia Organizacional, 13*(1), 57-72. https://doi.org/10.22490/25392786.7818

Desai, H. (2025). Cryptocurrency regulation as a strategic game: modeling market reactions and capital flight. *Journal of Financial Regulation and Compliance.* https://doi.org/10.1108/JFRC-03-2025-0069

Dixon, M. F., Halperin, I. y Bilokon, P. (2020). Frontiers of machine learning and finance. In *Machine learning in finance: From theory to practice* (pp. 519-541). https://doi.org/10.1007/978-3-030-41068-1_12

ESMA. (2025). Directrices ESMA sobre las condiciones y los criterios para la calificación de los criptoactivos como instrumentos financieros. https://www.esma.europa.eu/sites/default/files/2025-03/ESMA75453128700-1323_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs_ES.pdf

European Central Bank (2022). *ISO 20022 strategy for the Eurosystem.* ECB.

FATF. (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF, Paris. www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html

FATF. (2024). Estándares internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo, y el financiamiento de la proliferación de armas de destrucción masiva. https://biblioteca.gafilat.org/wp-content/uploads/2025/05/RecomendacionesMetodologia-para-la-Quinta-Ronda-de-Evaluaciones-Mutuas-1.pdf

FATF. (2025). Best Practices on Travel Rule Supervision. FATF, Paris. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf

González, Y. (2024). La actuación normativa del Grupo de Acción Financiera Internacional frente al criptoblanqueo. *Revista de Estudios Jurídicos y Criminológicos,* (10), 217-264. https://doi.org/10.25267/rejucrim.2024.i10.07

Górka, J. (2025). The rise of instant payments: a cross-country comparison. *Central European Management Journal*, *33*(4), 575-589. https://doi.org/10.1108/CEMJ-10-2024-0297

Gupta, S. (2025). Zero-Knowledge Proofs For Privacy-Preserving Systems: A Survey Across Blockchain, Identity, And Beyond. *Engineering And Technology Journal, 10*(7), 5755-5761. https://doi.org/10.47191/etj/v10i07.23

Hasan, J. (2019). Overview and applications of zero knowledge proof (ZKP). *International Journal of Computer Science and Network, 8*(5), 2277-5420.

ISO (2023). *ISO 20022: Financial services. Universal financial industry message scheme.* International Organization for Standardization.

Jensen, J., von Wachter, V. y Ross, O. (2021). An introduction to decentralized finance (defi). *Complex Systems Informatics and Modeling Quarterly,* (26), 46-54. https://doi.org/10.7250/csimq.2021-26.03

Joo, Y. y Seo, J. (2024). User authentication techniques using a dynamic soulbound token. *Journal of Web Engineering, 23*(5), 717-733. https://doi.org/10.13052/jwe1540-9589.2356

Kumar, P., Kumar, S. y Dilip, A. (2019). Effectiveness of the adoption of the XBRL standard in the Indian banking sector. *Journal of Central Banking Theory and Practice, 8*(1), 39-52. https://doi.org/10.2478/jcbtp-2019-0002

Moncalvo, D., Oliva M. y Díaz, A. (2025). Innovation practices and priorities in AML/CFT financial intelligence. *Journal of Money Laundering Control*, *28*(4-5), 626-644. https://doi.org/10.1108/JMLC-05-2025-0063

Naheem, M. A. (2020). The agency dilemma in anti-money laundering regulation. *Journal of Money Laundering Control, 23*(1), 26-37. https://doi.org/10.1108/jmlc-01-2016-0007

Ogunsola, K., Balogun, E. y Ogunmokun, A. (2022). Developing an automated ETL pipeline model for enhanced data quality and governance in analytics. *International Journal of Multidisciplinary Research and Growth Evaluation, 3*(1), 791-796. https://doi.org/10.54660/.ijmrge.2022.3.1.791-796

Ozili, P. (2022). Decentralized finance research and developments around the world. *Journal of Banking and Financial Technology, 6*(2), 117-133. https://doi.org/10.1007/s42786-022-00044-x

Paredes, J., Arias, B., Plua, K. y Paredes, J. (2026). Gestión Compliance en el ámbito de Gobernanza Financiera y Transparencia como Factores Determinantes de la Sostenibilidad Empresarial. *Polo del Conocimiento, 11*(3), 1075-1094. https://doi.org/10.23857/pc.v11i3.11269

Pastor, C. (2026). Inteligencia artificial y finanzas descentralizadas: nuevos retos en el régimen europeo de protección de usuarios. En *Criptoactivos, inteligencia artificial y sistema financiero europeo* (pp. 77-103). Colex.

Rentería, C. y Font, J. L. O. (2026). *Inteligencia artificial en el ámbito público mexicano: Dónde estamos y hacia dónde vamos.* FLACSO-México. https://doi.org/10.2307/jj.40271704

Robb, D., Rohde, F. y Green, P. (2014). Standard Business Reporting in Australia: Efficiency, effectiveness, or both? *Accounting and Finance, 56*(2), 509-544. https://doi.org/10.1111/acfi.12094

Santamaría, F. (2020). El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano. *Derecho PUCP*, (85), 139-174. https://doi.org/10.18800/derechopucp.202002.005

Tawiah, V. y Borgi, H. (2022). Impact of XBRL adoption on financial reporting quality: a global evidence. *Accounting Research Journal, 35*(6), 815-833. https://doi.org/10.1108/arj-01-2022-0002

Toledo-Castillo, N. del R., Huera-Paltán, B. P., Lemache-Noriega, D. G. y Oñate-Bastidas, B. A. (2026). Riesgos de responsabilidad legal en el uso de chatbots e IA para asesoría financiera y tributaria en Ecuador. *Journal of Economic and Social Science Research, 6*(1), 46-58. https://doi.org/10.55813/gaea/jessr/v6/n1/229

Toso Milos, Á. (2020). De-risking: Una consecuencia indeseada del enfoque basado en el riesgo aplicado por los bancos en materia de prevención del lavado de activos y financiamiento del terrorismo. *Revista chilena de derecho, 47*(1), 3-24. http://dx.doi.org/10.4067/S0718-34372020000100003

Wronka, C. (2022). Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control, 25*(1), 79-94. https://doi.org/10.1108/jmlc-02-2021-0017

XBRL International (2021). *XBRL Data Stack: From Taxonomy to Data Point Model.*

Zetzsche, D., Arner, D. y Buckley, R. (2020). Decentralized finance. *Journal of Financial Regulation, 6*(2), 172-203. https://doi.org/10.1093/jfr/fjaa010

Normativa citada

Ley 21.521. (4 de enero de 2023). Promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros [Ley Fintec]. https://bcn.cl/3b2f5

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.

Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849.

Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, 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.

Siglas y abreviaturas

API	Application Programming Interface
ASP	Crypto-Asset Service Provider
DeFi	Finanzas descentralizadas
DLH	Data lakehouse
DLT	Distributed Ledger Technology
EBA	European Banking Authority
EFB	Enfoque basado en el riesgo
ESMA	European Securities and Markets Authority
ETL	extract-transform-load
FATF/GAFI	Grupo de Acción Financiera Internacional
FinCEN	Financial Crimes Enforcement Network
KYC	Know Your Client
MiCA	Markets in Crypto-Assets
PII	Personally Identifiable Information
RGPD	Reglamento General de Protección de Datos
SBT	Soulbound tokens
TFR	Transferencia de fondos
VASP	Virtual Asset Service Providers
XBRL	eXtensible Business Reporting Language
ZKP	Zero-knowledge proofs