Centro de Estudios
de Seguridad
Internacional

CESI

Centro de Estudios
de Seguridad Internacional

CESI

EL COMPLIANCE PENAL EN EL ECOSISTEMA DE LOS CRIPTOACTIVOS

DELANO CERQUEIRA BUNN[1]

MADRID
03 DE OCTUBRE DE 2023

[1] Director de TFM (UCIII/CUGC). Máster en Derecho Penal Económico (UNIR)

Centro de Estudios
de Seguridad Internacional

CESI

La Sociedad Española de Investigación en Seguridad Global (SEISG) se dedica a estudios académicos en seguridad internacional y actúa como portavoz para el intercambio de resultados de investigación, promoviendo la cultura de seguridad y comprometiéndose con el estado de derecho, la justicia y los derechos humanos.

Como instituto académico de referencia de la SEISG, el Centro de Estudios de Seguridad Internacional (CESI) tiene como principal objetivo dirigir y coordinar todas las actividades educativas de la SEISG, incluyendo cursos, seminarios, conferencias, publicaciones y demás eventos que tienen como finalidad promover el avance científico y profesional en el campo de la seguridad internacional.

Para más informaciones sobre la SEISG y el CESI, visite https://seisg.es/

Referencia de la citación:

CERQUEIRA BUNN, D., (2023). El Compliance Penal en el Ecosistema de los Criptoactivos, en Cuadernos Anuales de Seguridad Global, Ed. 2023, SEISG/CESI, Madrid, España, Disponible en https://seisg.es/
DOI: 0000
CUADERNOS ANUALES DE SEGURIDAD GLOGAL, Ed. 2023, eISSN 0000

1. INTRODUCCIÓN. 2. EL ECOSISTEMA DE LOS CRIPTOACTIVOS. 3. EL COMPLIANCE PENAL COMO HERRAMIENTA DE PREVENCIÓN DE DELITOS. 4. REFERENCIAS

SUMARIO

Las nuevas tecnologías, incluidas las criptomonedas, han influido en el comportamiento social y el ámbito criminológico, extendiendo delitos tradicionales al entorno digital. Estos cambios tecnológicos requieren de una adaptación legislativa para proteger bienes jurídicos. El aumento de delitos informáticos, junto con el crecimiento del mercado mundial y el anonimato digital, exige respuestas y cooperación internacional. En 2020, el GAFI destacó medidas preventivas contra el blanqueo de capitales relacionado con activos virtuales. Finalmente, las empresas deben adoptar programas de compliance conforme a diversos estándares y directrices internacionales, enfocándose en una gestión proactiva de riesgos relacionados con criptoactivos.

PALABRAS-CLAVE

Tecnologías, Criptomonedas, Delitos, Compliance

ABSTRACT

New technologies, including cryptocurrencies, have influenced social behavior and the criminological field, extending traditional crimes to the digital environment. These technological changes require legislative adaptation to protect legal goods. The increase in computer crimes, together with the growth of the global market and digital anonymity, demands responses and international cooperation. In 2020, the FATF highlighted preventive measures against money laundering related to virtual assets. Finally, companies must adopt compliance programs in accordance with various international standards and guidelines, focusing on proactive risk management related to cryptocurrencies.

KEY WORDS

Technologies, Cryptocurrencies, Crimes, Compliance

RECIBIDO: 14/09/2023

ACEPTADO: 03/10/2023

1. Introducción

El presente artículo es un resumen del Trabajo de Fin de Máster del autor, con el mismo título, dirigido por D.ª Rocío Leal Ruiz, en la Facultad de Derecho de la Universidad Internacional de la Rioja – UNIR, en el Máster Universitario en Derecho Penal Económico, Coordinado por el Doctor Alfredo Abadías Selma.

El mercado de criptoactivos lleva más de una década en desarrollo, pese a la volatilidad y la incertidumbre de las posturas de los países en la regulación. Las plataformas de negociación han mejorado su infraestructura, aunque persisten ciberataques que sustraen criptomonedas de inversores. La consolidación del entorno cripto y la percepción del valor intrínseco de estos activos, así como el empleo de la tecnología *blockchain* en otras ramas de negocios[2], han fortalecido el mercado y se reveló una herramienta imprescindible en momentos de crisis, como hiperinflación en países o en la guerra de Rusia contra Ucrania, cuando las criptomonedas fueron instrumentos de recaudaciones del ejército de Ucrania y de alternativas cambiarias los ciudadanos rusos ante las sanciones internacionales del bloqueo.

Sucede que la regulación sigue siendo un tema en debate y los sistemas criptográficos, al operar sin una autoridad central, pueden ser propensos a los delitos financieros. Así, fue elegido problema de investigación del TFM el uso de los criptoactivos para la comisión de delitos y como pregunta ¿cuáles son las medidas necesarias para un efectivo sistema de prevención de delitos orientado a las empresas que actúan en el ecosistema de los criptoactivos?.

2. El ecosistema de los criptoactivos

Inicialmente, la investigación buscó definir los criptoactivos, así como delimitar lo que estaría fuera del escopo de este concepto. El estudio propuso la definición de que las criptomonedas son activos privados, representaciones digitales de valor o derecho (GAFI 2014), no emitidas por una autoridad estatal (*European Banking Authority* 2014) que, para tramitar electrónicamente, dependen de la criptografía y de la tecnología de registros distribuidos o

[2] Como en el entorno notarial, por ejemplo.

similar (*International Organization of Securities Commissions* 2020; *Financial Stability Board* 2019), con la finalidad de pago, comercialización, almacenamiento o inversión entre personas físicas o jurídicas (Comisión Europea 2020c), denominadas en una unidad de cuenta distinta de las monedas emitidas por gobiernos soberanos, cuyo precio puede expresarse en otras monedas (Banco Central do Brasil 2014).

Como sujetos de derechos en este ecosistema, merecen destaque las plataformas de negociación, proveedores de servicios de activos virtuales, *digital currency exchange* (*DCE*) o *virtual asset service provider* (*VASP*), que son las personas físicas o jurídicas, aunque non financiera, que realizan, para o en nombre de otra persona física o jurídica, al menos una de las siguientes actividades: (a) operaciones de intercambio entre activos virtuales y monedas fiduciarias, (b) intercambio entre una o más formas de activos virtuales, (c) transferencia de activos virtuales, custodia o administración de activos virtuales o instrumentos que permitan el control sobre activos virtuales y (d) participación y prestación de servicios financieros relacionados con la oferta o venta de un activo virtual por parte de un emisor (FATF 2019).

En octubre de 2018, por medio de la Recomendación 15, el GAFI se extendió las políticas *anti-money laundering* (*AML*) y *countering the financing terrorism* (CFT) para que los proveedores de servicios de activos virtuales, como las plataformas de negociación de criptoactivos, orientando los países a obligar las correctoras a identificar, evaluar y adoptar medidas eficaces para mitigar sus riesgos del blanqueo de capitales y de la financiación del terrorismo. La referida recomendación extendió la orientación a los países de los proveedores de servicios con activos virtuales que realizan operaciones desde su jurisdicción, a los que se deben imponer la obligación de comunicar las transacciones financieras ocasionales, en el umbral designado de € 1.000,00 (mil euros) (GAFI 2018).

Conforme el Real-decreto Ley 7/2021, de 27 de abril, deben registrarse y someterse al control del Banco de España las personas físicas o jurídicas que ofrezcan servicios de cambio de criptomonedas. Las personas físicas «cuando la base, la dirección o la gestión de estas actividades radique en España, con independencia de la ubicación de los destinatarios del servicio». Las

personas jurídicas establecidas en España, cuando «presten estos servicios, con independencia de la ubicación de los destinatarios» (Boletín Oficial del Estado 2021).

Como un artículo resumido, otros sujetos de derechos del ecosistema de los criptoactivos que fueron objeto de estudio del TFM fueron suprimidos, como los emisores de criptomonedas, los mineros, los proveedores de servicios de monederos electrónicos, los fondos de inversión institucional en criptoactivos, los proveedores de mercancías y servicios y las personas naturales usuarias de los criptoactivos.

3. El compliance penal como herramienta de prevención de delitos

El capítulo se dedica a detallar el problema de investigación del estudio: el uso de los criptoactivos para la comisión de delitos.

Las nuevas tecnologías, en que las criptomonedas están inseridas, han provocado cambios en el comportamiento social e influido directamente en el universo criminológico. Conductas delictivas que en otros tiempos tenían sus estándares clásicos solo en la realidad física de la vida social, también comenzaron a practicarse en el entorno de la internet y de las redes sociales manteniendo, en algunos casos, la misma identidad del bien jurídico violado. Asimismo, las nuevas tecnologías también han impuesto al legislador penal la necesidad de ampliar el espectro de protección de los bienes jurídicos, individuales o colectivos, mientras presupuestos de autorrealización y desarrollo de la personalidad (Muñoz Conde y García Arán 2019), en estricta observancia al carácter fragmentario del Derecho Penal al considerar otras ramas del ordenamiento jurídico con sus antijuridicidades para tipificar como crimen y defender al bien jurídico solamente las lesiones de especial gravedad (Muñoz Conde y García Arán 2019).

Como consecuencia del fenómeno de la globalización, del avance tecnológico, del crecimiento del mercado mundial y del diminuto riesgo de detección, mediante nuevas formas de anonimato, los delitos informáticos avanzaron y exigieron respuestas estatales de persecución por medio de herramientas de cooperación internacional en materia penal, con el objetivo de hacer frente al fenómeno de la globalización de la delincuencia informática (VIVÓ CABO 2018). A

su vez, los criptoactivos incrementaron el riesgo de la ciberseguridad como instrumento para la práctica de delitos informáticos con su posibilidad de realización de transacciones de manera anónima, con sucesivas operaciones con el uso de recursos tecnológicos, ingeniería social y el empleo de cuentas intermediarias para dificultar el seguimiento y su persecución criminal (Tejerina Rodríguez 2021). El TFM detalló el estudio de las medidas de prevención de blanqueo de capitales bajo la perspectiva del Grupo de Acción Financiera Internacional, terceros países (Estados Unidos y Brasil), Unión Europea y España.

En septiembre de 2020, por ejemplo, el GAFI publicó un informe con respecto a los *Activos Virtuales, Señales de Alerta de AML/CFT* con el objetivo de contribuir con los sujetos obligados para identificar y reportar movimientos posibles de blanqueo de capitales o financiación del terrorismo, reforzando el enfoque basado en riesgos para el cumplimiento de las reglas de las medidas preventivas de debida diligencia del cliente, identificando sus clientes, beneficiarios finales, tratando de entender la particularidad financiera de la relación comercial e identificar la fuente de los recursos. Los indicadores de alerta apuntados por el GAFI fueron resultados de más de cien estudios de casos recopilados entre 2017 y 2020 (GAFI 2020b).

Al analizar una transacción financiera que involucre criptoactivos, es deber de los sujetos obligados identificar su contexto, nunca considerándolas aisladamente, buscando encontrar una justificación mercantil lógica cuyas características apuntan a una mayor necesidad de seguimiento, análisis y elaboración de informes, cuando pertinente. Algunos de los indicadores apuntados relacionados con el volumen y recurrencia de las operaciones fueron: (a) cantidades de cambios o transferencias abajo de los umbrales de mantenimiento de registro o informes; (b) transferencia de criptoactivos inmediatamente a múltiples *exchanges*, principalmente registradas o con operaciones en otras jurisdicciones donde no hay relación con sus negocios o en países de baja regulación; (c) depósitos de criptoactivos en una *exchange* y, enseguida, retiros frecuentes de los criptoactivos sin actividad o convertirlos en otros activos virtuales, mediante el pago de tarifas de servicios, para diversificar una cartera de inversión sin una explicación lógica o, todavía, retiros de los criptoactivos de una *exchange* y envío para un monedero electrónico;

así como, (d) almacenamiento de criptoactivos de direcciones que han sido vinculadas como tenedoras de fondos robados (GAFI 2020b).

La investigación contempló el estudio cualitativo y cuantitativo de todas las resoluciones de enjuiciamiento criminal del Poder Judicial que utilizó la palabra *bitcoin*, y después de depurar los datos para evitar, por ejemplo, duplicidad en función del doble grado de jurisdicción, se clasificaron en función del tipo penal subyacente, momento del empleo en el *iter criminis*, del titular de la pose originaria del criptoactivo *ex ante* el delito, de la utilidad de la criptomoneda (producto del crimen, medio de pago, medio de ocultación o medio de engaño, entre otros. Para ilustrar, se presenta es ultimo criterio de clasificación:

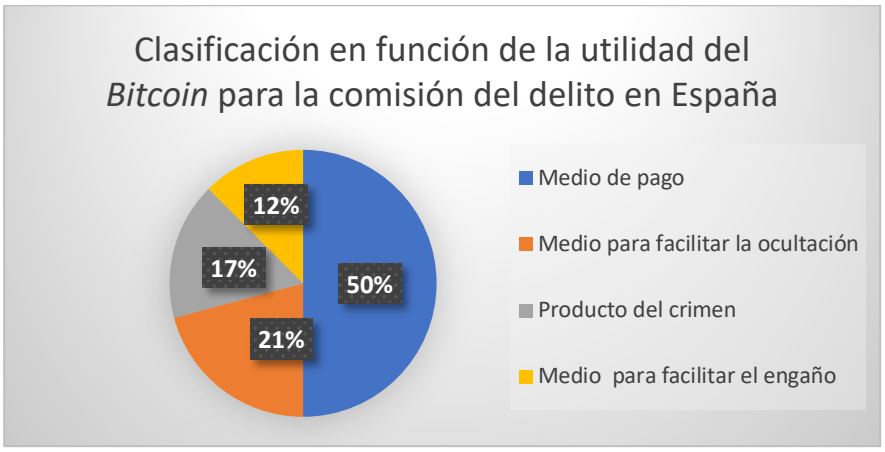

Gráfico 1: Clasificación de los delitos en función de la utilidad del *bitcoin* para la comisión delictiva en España entre 2016 y 2021.

Después de estudiar los estandartes del GAFI y los modelos propuestos por la Comisión Europea, el estudio concluyó la necesidad de la definición de principios regulatorios que deben ser comunes a todos los países: (I) Protección de consumidores e inversores, (II) construcción de infraestructuras de plena trazabilidad de las transacciones, (III) obligación de estricta cooperación institucional por parte de las empresas que actúan con los criptoactivos.

Por último, para contestar la pregunta de investigación, las empresas deben adoptar un efectivo programa de *compliance* penal, conforme los estándares del sistema de gestión de compliance ISO 37301:2021, del sistema de gestión de compliance penal UNE 19601:2017 y de la norma ISO 31000:2014 para la gestión de riesgos; (b) cumplir con las directivas y resoluciones

de la UE, bien así con las normas vigentes en España; (c) observar y actuar, de manera proactiva, en conformidad con las orientaciones del GAFI, así como los estudios, propuestas y dictámenes de la UE; (d) seguir los informes de los cuerpos de seguridad responsables por la investigación criminal, del Ministerio Fiscal y de la jurisprudencia penal con el fin de conocer y actuar en las más distintas tipologías penales que tengan relación con los criptoactivos, analizando los escenarios prospectivos para proyectarlos en medidas efectivas de organización y gestión para prevenir los riesgos penales, formando una cultura de cumplimiento, en conformidad con los estándares vigentes, bien así con una actuación preventiva de identificación, análisis y control de riesgos, mediante el empleo de las herramientas, entre otras, del mapas de riesgo, canal de denuncias, investigaciones internas y la debida diligencia.

Referencias

Brasil. BACEN: COMUNICADO Nº 25.306, DE 19 DE FEVEREIRO DE 2014, 2 (2014).

Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daño (2021).

Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO n. 2020/0265, relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937, Pub. L. No. 265/2020, 185 (2020).

European Banking Authority. (2014). EBA Opinion on virtual currencies. In *European Banking Authority* (Issue EBA/Op/2014/08). Disponible en https://bit.ly/3GuJvVd, [fecha de la última consulta: 20 de octubre de 2021]

FATF. (2019). *GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS* (Issue June).

Financial Stability Board. (2019). *Crypto-assets Work underway, regulatory approaches and potential gaps* (Issue May).

GAFI. (2014). *Virtual currencies – Key Definitions and Potential* AML/CFT Risks. In *FATF Report* (Issue June). Disponible en: https://bit.ly/32ydTj2, [fecha de la última consulta: 20 de diciembre de 2021].

GAFI. (2018). RECOMENDACIÓN 15/2018. Nuevas Tecnologías, 7 (2018).

GAFI. (2020). *Informe del GAFI Activos Virtuales Señales de alerta de LD / FT Activos Virtuales Señales de alerta de LD / FT*.

International Organization of Securities Commissions. (2020). *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (Consultation Report)*.

Muñoz Conde, F., & García Arán, M. (2019). *Derecho Penal Parte General* (10ª). Tirant lo Blanch.

Tejerina Rodríguez, O. (2021). Criptoactivos y Ciberseguridad. In *Criptoactivos. Retos y desafíos normativos* (pp. 295–309). Wolters Kluwer.

VIVÓ CABO, S. (2018). La globalización del delito : ciberdelincuencia. *La Ley Penal*, 1–8.