La actuación normativa del Grupo de Acción Financiera Internacional frente al criptoblanqueo

Regulatory action by the Financial Action Task Force on crypto laundering

YAGO GONZÁLEZ QUINZÁN
Investigador Predoctoral (FPU de Derecho Penal)
Universidad de Santiago de Compostela (España)

yagogonzalez.quinzan@usc.es

https://orcid.org/0000-0002-2500-4839

Resumen: La disrupción financiera positiva que suponen los criptoactivos, mediante el logro de ventajas como la desintermediación y la seguridad criptográfica de las transacciones, se minimiza en atención a los riesgos de blanqueo de capitales que se asocian ampliamente con aquellos. El Grupo de Acción Financiera Internacional (en adelante, GAFI) ha reaccionado a ello mediante la adopción de nuevas medidas para las actividades con activos virtuales (en adelante, AV), categoría más amplia en donde se agrupan los criptoactivos y, dentro de estos, las criptomonedas. En el presente trabajo se analizan las políticas antiblanqueo más recientes aprobadas por el GAFI para conseguir, de un lado, la armonización de los enfoques jurídicos nacionales y, de otro, la configuración de un régimen preventivo eficaz contra el criptoblanqueo.

Abstract: *The positive financial disruption brought about by crypto assets, through the achievement of benefits such as disintermediation and cryptographic security of transactions, is minimised in view of the money laundering risks that are widely associated with them. The Financial Action Task Force (hereinafter, FATF) has reacted to this by adopting new measures for activities involving virtual assets (hereinafter, VA), a broad category that*

Recepción: 10/09/2024 Aceptación: 07/11/2024

Cómo citar este trabajo: GONZÁLEZ QUINZÁN, Yago, "La actuación normativa del Grupo de Acción Financiera Internacional frente al criptoblanqueo", *Revista de Estudios Jurídicos y Criminológicos*, n.º 10, Universidad de Cádiz, 2024, pp. 217-264, DOI: https://doi.org/10.25267/REJUCRIM.2024.i10.07

includes crypto assets and, within these, cryptocurrencies. This paper analyses the most recent anti-money laundering policies adopted by the FATF to achieve, on the one hand, the harmonisation of national legal approaches and, on the other hand, the configuration of an effective preventive regime against crypto laundering.

Palabras clave: activos virtuales, criptomonedas, blanqueo de capitales, nota interpretativa, regla de viaje.

***Keywords**: virtual assets, cryptocurrencies, money laundering, interpretative note, travel rule.*

1. INTRODUCCIÓN

El desarrollo que ha experimentado el ecosistema de los criptoactivos con la aparición de nuevos productos y servicios se traduce en una nueva economía basada en activos criptográficos que, a su vez, altera por completo el tradicional sistema financiero y comercial[1]. Acerca de las cotas de uso alcanzadas por los criptoactivos resultan sumamente representativos los siguientes datos[2]. Alrededor de 300 millones de personas emplean criptoactivos para realizar operaciones financieras y comerciales, pudiéndose apreciar en un tipo de criptomoneda particular como

1 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", en *Cyber Laundering: International Policies and Practices*, (ed. Rébé, N.), Singapur, World Scientific Publishing, 2023, 1.ª ed., p. 197.

2 Vid. WANG, H. M. y HSIEH, M. L., "Cryptocurrency is new vogue: a reflection on money laundering prevention", *Security Journal*, 37, 2024, p. 26 y ss.

Ethereum hasta más de un millón de transacciones al día. Asimismo, más de 83 millones de personas disponen de billeteras de *Bitcoin* destinadas a su uso comercial en más de 200 países.

Los criptoactivos han adquirido un papel protagonista en el sistema financiero mundial hasta el punto de considerarse como la alternativa perfecta para recuperar la confianza tras la crisis financiera global iniciada en 2008[3], pretensión a la que responde mismamente el lanzamiento inicial de *Bitcoin*[4]. Los usuarios apuestan cada vez más por un sistema alternativo que se fundamente en la prueba criptográfica y no participe de la centralización en que se basa el sector bancario tradicional[5]. A este respecto ABEL SOUTO[6] indica que los criptoactivos representan una respuesta a la necesidad de disponer de cauces financieros alternativos que no excluyan a nadie del sistema por mala calificación crediticia y que aporten facilidades de acceso sin importar determinados factores como, por ejemplo, el lugar de residencia y la oferta bancaria disponible en aquel.

El aumento significativo en la emisión de *tokens* criptográficos, que se denominan ICO (por sus siglas en inglés, *Initial Coin Offering*), permite señalar, acogiendo las palabras de WRONKA[7], la amplia demanda existente de criptoactivos y su traslado "desde los márgenes del nicho tecnológico y el territorio marginal a la agenda reguladora internacional"[8]. Mediante las ICO los inversores reciben *tokens* criptográficos que habilitan el acceso a bienes, servicios o instrumentos financieros a cambio de moneda fiduciaria u otros criptoactivos[9], mientras que el emisor recibe financiación para su proyecto[10]. La recaudación a

3 Cfr. KOUTSOUPIA, V., "Challenges of the Use of Virtual Assets in Money Laundering", *Nordic Journal of European Law*, 6(4), 2023, p. 54.

4 Cfr. COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *European Journal of Crime, Criminal Law and Criminal Justice*, 28(3), 2020, p. 219.

5 Cfr. WRONKA, C., "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight", *Journal of Banking Regulation*, 25(1), 2024, p. 86.

6 Cfr. ABEL SOUTO, M., "La comisión del delito de blanqueo de dinero mediante las nuevas tecnologías y la internacionalización del Derecho penal", en *VIII Congreso Internacional sobre prevención y represión del blanqueo de dinero*, (coords. Abel Souto, M.; Lorenzo Salgado, J. M.; y Sánchez Stewart, N.), Valencia, Tirant lo Blanch, 2022, 1.ª ed., p. 507.

7 Cfr. WRONKA, C., "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight", *Op. cit.*, p. 85.

8 *Ibidem*.

9 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 202.

10 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", en *Organised Crime, Financial Crime and Criminal Justice*, (eds. Jasinski, D.; Phillips, A.; y Johnston E.), Londres, Routledge, 2023, 1.ª ed., p. 122; NAVARRO CARDOSO, F., "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", *Revista electrónica de ciencia penal y criminología*, 21(14), 2019, p. 33.

través de las ICO no se frena ni en atención a los riesgos inherentes a la inversión (*v. gr.* manipulación del mercado, ciberataques o blanqueo de capitales), siendo el objeto de mayor inversión las plataformas basadas en la tecnología *blockchain* (en adelante, BCT)[11].

El ecosistema de los criptoactivos no se restringe únicamente a los propios activos y a los emisores y usuarios, sino que en ellos se incluyen una amplia gama de participantes que extienden todavía más la industria cripto[12]. En la actualidad han adquirido un papel protagonista, por ejemplo, los *mixing services* (*tumblers*), las empresas de minería, los proveedores de servicios de cambio de criptoactivos por otros criptoactivos o por moneda fiduciaria, así como los proveedores de servicios de custodia de monederos electrónicos[13]. La actividad desarrollada por todos esos participantes en el ámbito de los criptoactivos también debe ser objeto de urgente regulación en aras de conseguir un marco normativo que reduzca los riesgos existentes en torno al ecosistema cripto[14].

2. POSIBLES FORMAS DE REACCIÓN ANTE LA INCIDENCIA DE LOS CRIPTOACTIVOS: LA APUESTA PARTICULAR DEL GAFI

La consolidación de los criptoactivos demanda la confección de una amplia regulación a nivel internacional que proteja a los inversores frente a los peligros inherentes al ecosistema (v. gr. riesgo de impago o de liquidez de los emisores y de los proveedores de servicios, riesgo de mercado o fraude), el correcto desarrollo del sistema financiero y comercial y, sobre todo, evite la consolidación de los criptoactivos como un campo propicio para la criminalidad[15]. A dicha reclamación responden los últimos esfuerzos normativos por parte del G20, el GAFI o el Fondo Monetario Internacional, que luego se acogen por la Comisión Europea y el Banco Central Europeo[16]. Todas estas instituciones y organizaciones centran sus esfuerzos en la

11 Cfr. PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Journal of Investment Compliance*, 21(1), 2020, p. 2.

12 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 197.

13 Cfr. DESMOND, D. B., LACEY, D. y SALMON, P., "Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review", *Journal of Money Laundering Control*, 22(3), 2019, p. 482.

14 Cfr. WRONKA, C., "Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures", *Journal of Money Laundering Control*, 25(1), 2022, p. 83.

15 Cfr. WRONKA, C., "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight", *Op. cit.*, p. 89.

16 Cfr. PONAMORENKO, V. E., "International Organizations' Approaches to Digital Assets Legalization (Monetary Policy and AML/CFT)", en *Engineering Economics: Decisions and Solutions from Eurasian Perspective. Lecture Notes in Networks and Systems*, (eds. Ashmarina, S.; Mantulenko, V.; y Vochozka, M.), Cham, Springer, 2021, 1.ª ed., p. 112.

aprobación de regulaciones exhaustivas sobre la aplicación de las nuevas tecnologías en el sector financiero[17].

Al igual que ha sucedido con otras innovaciones como las tarjetas de prepago, la banca online o el sistema de pagos por Internet, las principales instancias internacionales han ido aprobando diferentes normativas para hacer frente a los retos planteados por la industria de los criptoactivos, especialmente en relación con ciertos delitos como el blanqueo de capitales y la financiación del terrorismo[18]. La regulación de los diferentes organismos supranacionales, con especial mención del GAFI, trata de no frenar el amplio abanico de oportunidades que los criptoactivos representan para la innovación financiera, si bien contrarrestando los riesgos inherentes a aquellos. Esta postura constituye una de las tres reacciones posibles a la hora de regular las actividades con criptoactivos:

1) Oposición a la introducción de aquellos en el sector financiero (enfoque cerrado), considerándose como "una moda pasajera o una burbuja"[19].

El GAFI pone de manifiesto en sus diversos informes anuales relativos al seguimiento de sus medidas sobre AV que un número creciente de jurisdicciones opta por la adopción de este enfoque de prohibición. Ello se debe a que tal postura supone un ahorro de recursos o simplemente es más fácil de implementar que la adopción de un régimen de control y supervisión de las operaciones, especialmente en punto a los sistemas de licencia y registro requeridos para los proveedores de servicios de AV (en adelante, PSAV). Con todo, el GAFI se opone a este enfoque cerrado[20], ya que puede tener por consecuencia un aumento del uso sumergido de los AV, traduciéndose ello en actividades no sujetas al régimen de prevención del blanqueo de capitales y la financiación del terrorismo (en adelante, PBC/FT)[21].

2) Una apuesta total e irreflexiva por la innovación financiera (enfoque liberal).

3) La adopción de medidas legales coetáneas al desarrollo tecnológico en aras de promocionar la innovación financiera, pero al mismo tiempo combatir los riesgos propios del ecosistema (enfoque abierto, pero estricto)[22].

---

17 *Ibidem.*

18 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 198.

19 PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Op. cit.*, p. 2.

20 Cfr. NAVARRO CARDOSO, F., "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", *Op. cit.*, p. 25.

21 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 205.

22 Cfr. COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *Op. cit.*, p. 220.

En el plano mundial se apuesta por esta última solución y ello determina que se erija como un reto mayúsculo para las instancias reguladoras la promoción de la tecnología financiera (*FinTech*), con ejemplos como las finanzas descentralizadas (en adelante, *DeFi*), la BCT, los *tokens* no fungibles (NFT) o la revolución *Play to Earn*, y la prevención de determinadas actividades delictivas, como el blanqueo de capitales[23]. El GAFI ha adoptado un papel proactivo y ha venido sometiendo sus estándares a una constante evolución en paralelo al desarrollo de los AV. La iniciativa adoptada obedece a la desigual integración de tales avances en los sistemas jurídicos nacionales y a la deficiente regulación de las actividades prestadas por los PSAV. Estas circunstancias han propiciado una intervención sin pausa por el GAFI en aras de colmar las lagunas existentes y combatir el abanico de oportunidades delictivas que se relacionan con los AV.

La presente investigación se destina al estudio del marco normativo aprobado por el GAFI para combatir el blanqueo de capitales mediante AV. Para ello se realiza una aproximación preliminar a los conceptos de "AV", *criptoactivos* y *criptomonedas*. Posteriormente se analiza la reformulación del delito de blanqueo de capitales mediante el empleo de las monedas virtuales descentralizadas. Estas últimas poseen una serie de características que contribuyen a su utilización como herramientas para el delito. Una vez lo anterior, se examina el régimen preventivo instaurado por el GAFI para reaccionar frente al criptoblanqueo. Se identifican las principales tendencias seguidas en la política diseñada por la citada organización, así como algunas discordancias de la regulación aprobada. Con la aprobación de las novedades en las Recomendaciones del GAFI se ha iniciado por los distintos estados una aplicación de tales directrices, especialmente relevante en la Unión Europea (en adelante, UE) con la Directiva 2018/843, de 30 de mayo[24], por lo que se incluyen referencias al respecto. Finalmente, se realiza una valoración global acerca de la actividad del GAFI y su contribución a la prevención del criptoblanqueo.

3. PRECISIONES TERMINOLÓGICAS: ¿QUÉ SE ENTIENDE POR "AV", "CRIPTOACTIVOS" Y "CRIPTOMONEDAS"?

La confusión terminológica es una de las primeras cuestiones que conviene aclarar para poder analizar posteriormente el régimen de prevención del criptoblanqueo instaurado por el GAFI. La consolidación en nuestra sociedad de un vocabulario nuevo requiere de la aclaración de diversos términos, sobre todo ante

23 Cfr. WRONKA, C., "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight", *Op. cit.*, p. 85.

24 Vid. Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE, DOUE, 156, 19 de junio de 2018, pp. 43-74.

un uso indistinto de conceptos diversos como *AV*, *criptoactivos* y *criptomonedas*[25]. Esta situación constituye un claro obstáculo para la elaboración de una normativa precisa para la prevención del criptoblanqueo[26]. Con todo, las imprecisiones conceptuales entre la población en general resultan más que comprensibles debido a las mismas divergencias existentes en la definición de cada categoría en los sistemas jurídicos nacionales. El GAFI ha ayudado con sus disposiciones, sujetas a un proceso constante de aclaración, a comprender el contenido al que se refiere cada concepto, por lo que se estima positiva su aportación.

El primero de los términos por clarificar es el de *AV*. Este ha sido utilizado por el GAFI para hacer referencia a todas aquellas representaciones digitales de valor que se pueden comercializar o transferir digitalmente, o también se pueden emplear con fines de pago o de inversión. Esta aproximación se complementa con la exclusión de las representaciones digitales de monedas fiduciarias emitidas por los bancos centrales (en adelante, CBDC, por sus siglas en inglés *Central Bank Digital Currency*), por más que el GAFI defienda reiteradamente en las actualizaciones de su normativa la necesidad de interpretar el concepto de AV de la forma más amplia posible. Esta primera precisión terminológica permite poner de manifiesto pues que los criptoactivos se engloban dentro del concepto de AV, si bien constituyen una subcategoría en atención al empleo de técnicas criptográficas y al sistema de la cadena de bloques en que basan su funcionamiento[27].

Los criptoactivos se definen por su origen en el sector privado y su dependencia de la tecnología de registro distribuido (en adelante, TRD)[28]. Así se recoge por la Autoridad Bancaria Europea (en adelante, ABE) y el Consejo de Estabilidad Financiera en la medida en que indican que por criptoactivo debe entenderse aquel tipo de activo privado que depende de la criptografía y la TRD como parte de su valor percibido o intrínseco[29], no es emitido ni garantizado por bancos centrales y puede utilizarse como medio de cambio y/o con fines de inversión y/o para acceder a un producto o servicio. Esta posición se corrobora en el Reglamento 2023/1114, de 31 de mayo[30], conocido

25 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 200.

26 Cfr. BENSON, V. et al., "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions", *European Journal of Law and Economics,* 57, 2024, p. 40.

27 Cfr. MPF (Ministerio Público Fiscal de la Nación), *Guía práctica para la identificación, trazabilidad e incautación de criptoactivos. Consideraciones teórico-prácticas sobre activos virtuales basados en la tecnología de cadena de bloques y su investigación penal*, Buenos, Aires, 2023, pp. 11 y 12.

28 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 127.

29 Cfr. WRONKA, C., "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight", *Op. cit.*, p. 87.

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

como Reglamento MiCA, que incluye la siguiente definición de criptoactivo: "representación digital de un valor o de un derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro distribuido o una tecnología similar"[31].

La referencia al origen en el sector privado en la propia categorización de los criptoactivos propicia nuevamente la exclusión de las CBDC, al igual que se puso de manifiesto en relación con el concepto de AV formulado por el GAFI. Las CBDC responden a la pretensión de aplicar la BCT para la emisión, transferencia y control monetarios[32]. Los proyectos de investigación sobre CBDC realizados por los bancos centrales obedecen asimismo a un intento inequívoco de mejorar el sistema de pagos, al igual que tratan de dar respuesta a la creciente demanda en el mercado de un equivalente digital al dinero fiat. A las razones expuestas se añaden por los bancos centrales nacionales las siguientes ventajas relacionadas con las CBDC[33]: 1. Reducción de costes respecto a la emisión de efectivo; 2. Progreso en la estabilidad de pagos; 3. Mejor inclusión financiera; 4. Fomento de la TRD; y 5. Eliminación de la privacidad del dinero fiat.

El término criptoactivos se emplea ampliamente para hacer referencia a las monedas virtuales descentralizadas (criptomonedas), entre las que destaca *Bitcoin, Ethereum, Cardano o Polkadot*[34]. No obstante, estas últimas se tratan únicamente de una modalidad de *tokens* de tipo pago/intercambio como primera subclasificación en la categoría de los criptoactivos, en donde se diferencian a su vez los *tokens* de inversión/seguridad y de utilidad para acceder a aplicaciones o servicios[35]. Los *tokens* de tipo pago/intercambio tienen como función principal su uso como medio de pago[36] y, aunque pueden ser emitidos por una entidad centralizada, normalmente se fundamentan en su propia cadena de

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, DOUE, 150, 9 de junio de 2023, pp. 40-205.

31 Art. 3.1 numeral 5) del Reglamento 2023/1114, de 31 de mayo.

32 Cfr. PONAMORENKO, V. E., "International Organizations' Approaches to Digital Assets Legalization (Monetary Policy and AML/CFT)", *Op. cit.*, p. 116.

33 *Ibidem.*

34 Cfr. WANG, H. M. y HSIEH, M-L., "Cryptocurrency is new vogue: a reflection on money laundering prevention", *Op. cit.*, p. 32.

35 Cfr. PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Op. cit.*, p. 1; COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *Op. cit.*, p. 231.

36 Cfr. HAFFKE, L., FROMBERGER, M. y ZIMMERMANN, P., "Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them", *Journal Bank Regulation*, 21, 2020, p. 126.

bloques descentralizada[37]. Este tipo de *tokens* no tienen un valor inherente[38] y dependen del valor que otros participantes en el mercado reconozcan al *token*[39].

Las criptomonedas tienen su origen en 2008, con la publicación del documento "Bitcoin: un sistema de efectivo electrónico usuario-a-usuario"[40], firmado bajo el seudónimo de Satoshi Nakamoto. Hoy en día aún no se sabe si detrás de tal seudónimo hay una o varias personas[41], por más que a veces se asocie con el desarrollador de *software* estadounidense *Hal Finnley* (primer destinatario de una transacción en la cadena de bloques)[42]. El lanzamiento de *Bitcoin* ha supuesto el inicio de un nuevo paradigma financiero en cuanto permite la eliminación de intermediarios centralizados[43]. Y la fuerte irrupción de las criptomonedas en general se relaciona con los métodos criptográficos en que se basan, ya que garantizan la seguridad e integridad de las transacciones, el control en la creación de unidades adicionales y la verificación de las transferencias de activos[44].

La primera clasificación de las monedas virtuales se introdujo por el GAFI en junio de 2014. En el documento "Definiciones clave y riesgos potenciales para la lucha contra el blanqueo de capitales y la financiación del terrorismo"[45] se dividen las monedas virtuales en dos grupos: convertibles y no convertibles. A su vez, las monedas virtuales convertibles pueden ser centralizadas (respaldadas por autoridades que ejercen una labor de supervisión y control) o descentralizadas (también denominadas criptomonedas). Esta aproximación resulta transcendente en cuanto permite afirmar que las criptomonedas son un tipo de moneda virtual convertible que se caracterizan por la ausencia de una autoridad central que supervise el funcionamiento de aquellas.

---

37 Cfr. FROMBERGER, M. y ZIMMERMANN, P., "Technische und wirtschaftliche Grundlagen", en *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings*, (eds. Maume, P., Maute, L. y Fromberger, M.), Munich, Verlag C.H. Beck, 2020, 1.ª ed., p. 20.

38 Cfr. HAFFKE, L., FROMBERGER, M. y ZIMMERMANN, P., "Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them", *Op. cit.*, p. 127.

39 Cfr. FROMBERGER, M. y ZIMMERMANN, P., "Technische und wirtschaftliche Grundlagen", *Op. cit.*, p. 20.

40 Vid. NAKAMOTO, S., Bitcoin: *A Peer-to-Peer Electronic Cash System*, 2008, pp. 1-9. Disponible en https://bitcoin.org/en/bitcoin-paper.

41 Cfr. BRAMESHUMMER, G. y EDELMANN, B., "Einführung, Krypto 1x1 für Strafrechtler", en *Finanzstrafrecht 2022: Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht,* (eds. Leitner, R. y Brandl, R.), Viena, Linde Verlag, 2023, 1.ª ed., p. 3.

42 Cfr. WRONKA, C., *"*Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures*"*, *Op. cit.*, p. 81.

43 Cfr. BENSON, V. et al., "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions", *Op. cit.*, p. 38.

44 *Ibidem.*

45 Vid. FATF, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, Paris, 2014, pp. 1-17.

Los esfuerzos del GAFI no se han limitado a realizar una clasificación de las monedas virtuales, sino que define cada una de las tipologías de forma más o menos precisa. En relación con las criptomonedas especifica que son representaciones digitales de valor no emitidas por un banco o autoridad central, sin vinculación a monedas legalmente establecidas, carentes de curso legal, que resultan aceptadas por personas físicas y jurídicas como medio de pago, al tiempo que pueden transferirse, almacenarse o negociarse electrónicamente. Esta aproximación permite subrayar, en primer lugar, el necesario acuerdo de aceptación por parte de una determinada comunidad. Y, en segundo lugar, la ausencia de reconocimiento como moneda de curso legal, si bien ello resulta en cierto punto superado en la medida en que países como El Salvador o la República Centroafricana han admitido el *Bitcoin* como moneda de curso legal[46].

4. LA BCT COMO FUNDAMENTO OPERATIVO DE LAS CRIPTOMONEDAS: NOTAS SOBRE SU FUNCIONAMIENTO

Las criptomonedas han eliminado el papel protagonista que poseía el sistema financiero tradicional en favor de un régimen semianónimo y descentralizado. El desarrollo tan rápido experimentado por el ecosistema ha dado lugar a una modificación de "la valoración, el intercambio y la contabilidad de los activos económicos y las transacciones comerciales, eliminando a los intermediarios institucionales de las transacciones"[47]. Ello se posibilita mediante la BCT que, esencialmente, se trata de una las aplicaciones básicas de la TRD[48]. Esta última tecnología se considera un avance fundamental en la medida en que permite conseguir una mejora de la comerciabilidad, una mayor transparencia y liquidez de los activos, así como una reducción de costes[49].

Las criptomonedas permiten el almacenamiento de valor con sencillez, así como una rápida transferibilidad sin límites fronterizos[50]. No obstante, el principal aspecto que se destaca en todas las aproximaciones a las criptomonedas es su fundamento operativo en la BCT. Esta última se define como un gran libro de contabilidad público y descentralizado, asegurado mediante criptografía, en el que se registran todas

46 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *ZEuS Zeitschrift für Europarechtliche Studien*, 24(2), 2023, p. 193.

47 GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 197.

48 Cfr. WRONKA, C., "Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures", *Op. cit.*, p. 81.

49 Cfr. WRONKA, C., "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight", *Op. cit.*, p. 85.

50 Cfr. WANG, H. M. y HSIEH, M. L., "Cryptocurrency is new vogue: a reflection on money laundering prevention", *Op. cit.*, p. 26.

las transacciones tras el consenso alcanzado por la red de nodos intervinientes[51]. La transcendencia de la cadena de bloques radica principalmente en que permite la eliminación de intermediarios centralizados[52]. Por ello se afirma que la BCT ha revolucionado el sector financiero, si bien la falta de regulación "ha obstaculizado considerablemente la innovación[53]" basada en dicha tecnología.

Las ventajas que ampliamente se asocian con la BCT son la transparencia, una fuerte protección frente a posibles manipulaciones y la eliminación de riesgos en cuanto a su integridad en caso de que alguno de los participantes de la red actúe incorrectamente[54]. Así se destaca por MEIER[55], que añade que la operatividad de la BCT se concentra en torno a un código fuente que se puede utilizar para determinar el número de transacciones que se insertan en los distintos bloques, así como la frecuencia en la creación de estos últimos. Como su nombre indica, la BCT se compone de una serie de bloques en el que cada uno se define por un *hash* propio, al que se suma el *hash* del bloque anterior[56], lo que impide la modificación posterior de transacciones, pues de ser el caso deberían modificarse todos los bloques anteriores de la cadena[57].

El sistema de la cadena de bloques posee como notas básicas las siguientes: carácter público, distribuido e inalterable. Estas características se traducen en que la red no se gestiona por una entidad central, sino que múltiples nodos mantienen idénticas copias del registro. La descentralización garantiza precisamente la transparencia y la seguridad del registro. En cada uno de los bloques se contiene la información relativa a una serie de transacciones que, en todo caso, son objeto de validación mediante un *hash* alfanumérico que se aporta tras la solución de una ecuación criptográfica por los nodos. Este proceso algorítmico permite la consecución de una amplia privacidad, seguridad y validez de las transacciones, por lo que apenas existe manipulación en el envío o almacenamiento[58].

---

51 Cfr. KOUTSOUPIA, V., "Challenges of the Use of Virtual Assets in Money Laundering", *Op. cit.*, p. 55.

52 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 190.

53 BENSON, V. et al., "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions", *Op. cit.*, p. 38.

54 Cfr. MEIER, M., *Geldwäsche-Compliance für Kryptowerte, Jenaer Wissenschaftliche Verlagsgesellschaft*, Jena, 1.ª ed., 2022, p. 31.

55 *Ibidem.*

56 Cfr. NAVARRO CARDOSO, F., "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", *Op. cit.*, p. 4.

57 Cfr. MEIER, M., *Geldwäsche-Compliance…*, *Op. cit.*, p. 31.

58 Cfr. WANG, H. M. y HSIEH, M-L., "Cryptocurrency is new vogue: a reflection on money laundering prevention", *Op. cit.*, p. 33.

La criptografía asimétrica constituye pues el pilar sobre el que se fundamenta la BCT[59]. Esta garantiza la seguridad de las transacciones y el anonimato del emisor y receptor mediante la puesta a disposición para cada usuario de dos claves: una pública y otra privada[60]. La primera se identifica con el número de una cuenta bancaria en cuanto constituye la dirección del monedero. Se utiliza para verificar las transacciones y resulta la dirección en la BCT a la que se pueden asignar *tokens* a favor de un participante, por lo que puede llegar a considerarse como pseudónimo de aquel[61]. La clave privada se define por su parte como una contraseña secreta que puede gestionarse por el propio usuario o dejar bajo custodia virtual de un proveedor externo[62]. En esta dualidad de claves puede comprobarse la falta de revelación de información personal, si bien la premisa del anonimato debe calificarse más bien como "desidentificación"[63], ya que resulta posible el análisis de la cadena de bloques y, con ello, el rastreo de las transacciones[64].

Las criptomonedas, con el ejemplo particular de *Bitcoin* por ser la que ostenta una mayor capitalización de mercado, se tratan de una de las aplicaciones de la BCT. Como señalan BRAMESHUMMER y EDELMANN[65], la confianza en *Bitcoin* deriva de la base de datos descentralizada, publica e inmutable que a nivel mundial se gestiona por una multiplicidad de ordenadores que funcionan en una red *peer-to-peer*. Cada nodo de la red posee una copia del registro de las transacciones y su función elemental es la validación o no de cada operación. De esta forma se garantiza la imposibilidad de acceso a la red de transacciones fraudulentas. Y todo ello en su conjunto se traduce pues en la posibilidad de que dos usuarios realicen transacciones con la máxima seguridad en cuanto a que no resultarán posibles manipulaciones al respecto[66].

---

59 Cfr. NAVARRO CARDOSO, F., "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", *Op. cit.*, p. 12.

60 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 195.

61 Cfr. MEIER, M., *Geldwäsche-Compliance…*, *Op. cit.*, p. 36.

62 Cfr. BRAMESHUMMER, G. y EDELMANN, B., "Einführung, Krypto 1x1 für Strafrechtler", *Op. cit.*, p. 8.

63 PALPACUER, J. y AOUIZERAT, B., "Anti-Cyber Laundering: The Inclusion of Virtual Asset Service Providers", *en Cyber Laundering: International Policies and Practices*, (ed. Rébé, N.), Singapur, World Scientific Publishing, 2023, 1.ª ed., p. 261.

64 *Ibidem.*

65 Cfr. BRAMESHUMMER, G. y EDELMANN, B., "Einführung, Krypto 1x1 für Strafrechtler", *Op. cit.*, p. 2.

66 *Ibidem.*

5. CARACTERÍSTICAS DE LAS CRIPTOMONEDAS QUE FAVORECEN LA COMISIÓN DEL BLANQUEO DE CAPITALES

La razón de ser del presente apartado dedicado al examen de las notas técnicas de las monedas virtuales descentralizadas y su relación con el blanqueo de capitales se debe a que en diversas investigaciones se ha constatado que las criptomonedas son las que presentan mayores estadísticas de uso criminal. Asimismo, debe precisarse que, si bien en el ámbito de las criptomonedas se hace referencia a *Bitcoin* como la más empleada para operaciones de blanqueo de capitales, en realidad la mayoría de las billeteras asociadas a tales hechos ilícitos se compone de otras *altcoins*[67].

El blanqueo de capitales cometido mediante criptomonedas consiste en una técnica de mayor complejidad que los métodos tradicionales de legitimación de fondos ilícitos[68], si bien facilita a los delincuentes sus pretensiones de ocultación del origen del dinero y su movimiento a través de las fronteras sin posibilidad de detección[69]. Las criptomonedas llevan asociadas un pseudoanonimato y una descentralización que generan evidentes riesgos de blanqueo de capitales, en cuanto su funcionamiento dificulta el rastreo del historial de las transacciones y se aleja del sistema financiero tradicional[70]. Precisamente, en atención a estas características se afirma que la determinación de las cifras de criminalidad asociada a las criptomonedas resulta verdaderamente compleja[71].

El ámbito de las criptomonedas se erige como un campo propicio para las actividades de blanqueo de capitales ya que permiten transferir, recaudar y estratificar los beneficios ilícitos[72]. La descentralización, el pseudoanonimato y la facilidad para realizar rápidamente operaciones a nivel global son notas técnicas que atraen no solo a usuarios legítimos, sino también a criminales en búsqueda de *modus operandi* más sofisticados para perpetrar con éxito sus acciones delictivas[73]. Las características enunciadas de las criptomonedas dificultan la prevención y la persecución de las

67 Cfr. WANG, H. M. y HSIEH, M. L., "Cryptocurrency is new vogue: a reflection on money laundering prevention", *Op. cit.*, p. 34.

68 Cfr. WRONKA, C., "Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures", *Op. cit.*, p. 84.

69 Cfr. WRONKA, C., «"Cyber-laundering": the change of money laundering in the digital age», *Journal of Money Laundering Control*, 25(2), 2022, p. 341.

70 Cfr. BENSON, V. et al., "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions", *Op. cit.*, p. 39.

71 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 126.

72 Cfr. HAFFKE, L., FROMBERGER, M. y ZIMMERMANN, P., "Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them", *Op. cit.*, p. 130.

73 Cfr. TROZZE, A., "Cryptocurrency Crime", en *Cryptocurrency Concepts, Technology, and Applications*,(ed. Liebowitz, J.), Londres, CRC Press, 2023, p. 94.

actividades de blanqueo de capitales[74], sobre todo mediante el uso de herramientas de investigación convencionales[75].

A continuación, se esbozan las ideas básicas en torno a cada uno de los rasgos operativos que las criptomonedas presentan para el blanqueo de capitales.

5.1. Descentralización

La descentralización implica la imposibilidad de adopción de las medidas antiblanqueo que habitualmente aplican las entidades financieras[76]. La ausencia de intermediarios elimina un primer eslabón para la detección e información de operaciones sospechosas de blanqueo de capitales a las autoridades competentes. Las monedas virtuales descentralizadas carecen de un control ejercido por un banco u otra autoridad central que vigile las transacciones realizadas en la red. Esto es, el sistema *peer-to-peer* en que se fundamentan permite operar libremente a cada ordenador de la red con otros nodos sin riesgo alguno para la transacción de la que se trate.

Más en concreto, como pone de manifiesto WRONKA[77], la naturaleza descentralizada de las criptomonedas implica que las transacciones no pueden ser bloqueadas por las entidades bancarias, como ocurre en el caso de las transacciones electrónicas con moneda fiduciaria, al no existir una autoridad central con capacidad de detección, bloqueo y denuncia de transacciones sospechosas. Ello supone que los usuarios pueden operar libremente sin la intermediación de un tercero, por lo que esta característica resulta decisiva para el blanqueo de capitales y un claro desafío para las instancias reguladoras por la falta de ayuda que los intermediarios aportan en las investigaciones[78].

5.2. Anonimato vs. pseudoanonimato

La idea de partida es que las criptodirecciones de los usuarios son anónimas y no existen elementos que permitan vincular aquellas con identidades personales concretas. Los protocolos operativos de las criptomonedas no requieren la identificación de los usuarios[79]. Esta naturaleza se trata de uno de los puntos de máxima atención

---

74 Cfr. BRANDL, R. y BÜLTE, J., "Kryptowährungen/-assets-Geldwäsche und Terrorismusbekämpfung-Perspektive Sorgfaltsverpflichtete", en *Finanzstrafrecht 2022: Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht*,(eds. Leitner, R. y Brandl, R.), Viena, Linde Verlag, 2023, 1.ª ed., p. 107.

75 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 198.

76 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 197.

77 Cfr. WRONKA, C., *"*Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures*"*, *Op. cit.*, p. 84.

78 *Ibidem.*

79 Cfr. KOUTSOUPIA, V., "Challenges of the Use of Virtual Assets in Money Laundering", *Op.*

por los reguladores, ya que las políticas antiblanqueo se basan en la verificación de las identidades personales, por lo que aun pudiéndose detectar ciertos patrones de transacciones, la incapacidad para vincular aquellas a un usuario impide conocer a las personas específicas que se hallas detrás de las transacciones. A ello se añade que cada persona puede disponer de varias cuentas[80] o, incluso, crear una nueva dirección para realizar una determinada transacción[81].

El anonimato deriva de la tecnología de cifrado en que se fundamentan las criptomonedas, ya que aquella garantiza la protección de las identidades personales, al mismo tiempo que sirve para hacer frente a posibles acciones provenientes de la cibercriminalidad, al fraude y a revelaciones no autorizadas[82]. Si bien hasta aquí pudiera pensarse que el cifrado únicamente reporta ventajas significativas, debe ponerse de manifiesto que también ostenta una dimensión negativa en cuanto facilita actos de blanqueo de capitales sin posibilidad de detección de las identidades personales por parte de las fuerzas de seguridad[83]. De ahí que se subraye ampliamente como una de las características elementales de las criptomonedas que facilitan la comisión del blanqueo de capitales.

A pesar de que el anonimato de las criptomonedas se estipule como una de las aptitudes para el delito, esta premisa no constituye una máxima absoluta. El anonimato de los usuarios se puede ver reducido a través del examen de direcciones IP únicas, la geolocalización y, especialmente, mediante el historial de las transacciones[84]. Las monedas virtuales descentralizadas no proporcionan un anonimato pleno, sino que son pseudónimas[85], ya que las transacciones se registran en la cadena de bloques pública[86], por lo que, aun reconociéndose su complejidad, esta última puede ser objeto de "desanonimización futura"[87]. La identificación de los usuarios que se hallan detrás de las criptodirecciones resulta posible mediante el empleo de herramientas

cit., p. 59.

80 Cfr. CHASIN VELKES, G., "International Anti-Money Laundering Regulation of Virtual Currencies and Assets", *New York University Journal of International Law and Politics*, 52, 2020, p. 877.

81 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 196.

82 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 130.

83 *Ibidem*.

84 Cfr. DESMOND, D. B., LACEY, D. y SALMON, P., "Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review", *Op. cit.*, p. 482.

85 Cfr. RAYMAEKERS, W., "Cryptocurrency Bitcoin: Disruption, challenges and opportunities", *Journal of Payments Strategy & Systems*, 9(1), 2015, p. 38.

86 Cfr. HOSSAIN, M. B., "Acquiring an awareness of the latest regulatory developments concerning digital assets and anti-money laundering", *Journal of Money Laundering Control*, 26(6), 2023, p. 1262.

87 PAESANO, F., "Following the Virtual Money: Investigating Crypto-Based Money Laundering and Confiscating Virtual Assets", en *Cryptocurrency Concepts, Technology, and Applications*, (ed. Liebowitz, J.), Londres, CRC Press, 2023, 1.ª ed., p. 123.

de análisis de la cadena de bloques que se articulan en base a técnicas de agrupación a partir de los patrones de las transacciones[88]. Algunas empresas de análisis de la cadena de bloques han adquirido especial transcendencia, como *Chainalysis*, *Elliptic* o *Scorechain*[89].

5.3. Facilidad de acceso, negociabilidad global y rápida disponibilidad

La facilidad de acceso y la rapidez de las transacciones mediante las criptomonedas son dos extremos relacionados que también se estipulan como claras aptitudes para el blanqueo de capitales. Únicamente resulta necesario para el uso de las criptomonedas acceso a Internet[90], por lo que existe una escasa dificultad para realizar transacciones seguras, irreversibles y de bajo coste[91]. La infraestructura de las criptomonedas ha alcanzado una dimensión mundial mediante las plataformas *online* y los cajeros automáticos, por lo que la compra e intercambio de monedas virtuales carece de límites temporales y espaciales[92]. A lo anterior se añade a la ausencia de trabas burocráticas que supongan algún tipo de intermediación en los envíos de fondos[93].

6. EL CRIPTOBLANQUEO: APROXIMACIÓN Y PRINCIPALES ESTRATEGIAS PARA EL DELITO

6.1. La reformulación del blanqueo de capitales a través de las criptomonedas

El blanqueo de capitales se define como el proceso por el que se dota de apariencia de legalidad a bienes ilícitos. La esencia del delito radica en el diseño de diferentes estrategias para disfrazar el origen de los bienes y otorgarles plena legitimidad para su disfrute. Concebido el blanqueo como proceso, en él se distinguen las fases de colocación, estratificación e integración. La primera consiste en la introducción del dinero fiat ilícito en el sistema financiero; los métodos para tal fin son múltiples, si bien el más frecuente es la fragmentación del dinero ilícito en pequeñas cantidades y su ingreso en cuentas bancarias (*smurfing*). La estratificación se realiza mediante una multiplicidad de transferencias electrónicas transfronterizas destinadas a mover indiscriminadamente los fondos en aras de dificultar el rastreo del origen

88 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 196.

89 Cfr. DUPUIS, D. y GLEASON, K., "Money laundering with cryptocurrency: open doors and the regulatory dialectic", *Journal of Financial Crime*, 28(1), 2020, p. 65.

90 Cfr. MEIER, M., *Geldwäsche-Compliance…*, *Op. cit.*, p. 73.

91 Cfr. TROZZE, A., "Cryptocurrency Crime", *Op. cit.*, p. 94.

92 Cfr. KOUTSOUPIA, V., "Challenges of the Use of Virtual Assets in Money Laundering", *Op. cit.*, p. 59.

93 *Ibidem.*

de aquellos. Y en la integración se reintroduce el dinero en la economía legal para adquirir bienes o servicios.

En la era tecnológica que nos hallamos podía presumirse que los delincuentes acudirían a los nuevos avances digitales, y en especial a las criptomonedas, para perpetrar sus acciones criminales sin límites temporales o espaciales[94]. El recurso a las nuevas tecnologías permite el aprovechamiento de la "doble ventaja"[95] inherente a la aparición de una nueva aplicación digital. Por un lado, la falta de regulación y la necesidad de tiempo por parte de los legisladores internacionales y nacionales para el diseño y la adopción de un marco legal óptimo. Y, por otro, la falta de protocolos de detección y reacción por las autoridades encargadas de la investigación que, apresuradamente, se ven obligadas al desarrollo de estrategias para reaccionar a nuevos *modus operandi* delictivos.

El avance que representan las criptomonedas se sitúa comúnmente en segundo plano en atención a múltiples factores negativos como, por ejemplo, la falta de respaldo de su valor, la volatilidad imperante en torno a ellas y el excesivo coste energético que requiere el proceso de minería en que basan su emisión y funcionamiento[96]. Entre las derivadas negativas que ponen en jaque la valoración positiva que merecen las criptomonedas sobresale su instrumentalización para fines criminales[97]. A través de las monedas virtuales se facilita la comisión de delitos en el ciberespacio debido a la rapidez y a la seguridad de las transacciones, así como a la dificultad para rastrear las operaciones[98].

El catálogo de actividades delictivas potenciadas por el empleo de las criptomonedas resulta amplio, pero entre ellas destacan el *ransomware* y el blanqueo de capitales. El primer fenómeno consiste en el robo de datos personales en equipos informáticos mediante la introducción de un *malware* que bloquea la computadora de la víctima hasta el pago de un rescate a través de criptomonedas[99]. Las principales investigaciones ponen de manifiesto que *Bitcoin* se trata de la moneda más utilizada, si bien proliferan también solicitudes de pago mediante monedas de privacidad (*privacy coins*)[100], entre las que destacan *Monero*, *ZCash*, *Dash*, *NAVCoin*, *Verge* o *PIVX*[101].

---

94 Cfr. DUPUIS, D. y GLEASON, K., "Money laundering with cryptocurrency: open doors and the regulatory dialectic", *Op. cit.*, p. 71.

95 PAESANO, F., "Following the Virtual Money: Investigating Crypto-Based Money Laundering and Confiscating Virtual Assets", *Op. cit.*, p. 134.

96 *Ibidem.*

97 Cfr. BENSON, V. et al., "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions", *Op. cit.*, p. 38.

98 Cfr. KOUTSOUPIA, V., "Challenges of the Use of Virtual Assets in Money Laundering", *Op. cit.*, p. 56.

99 Cfr. TROZZE, A., "Cryptocurrency Crime", *Op. cit.*, p. 99.

100 *Ibidem.*

101 Cfr. DUPUIS, D. y GLEASON, K., "Money laundering with cryptocurrency: open doors and the regulatory dialectic", *Op. cit.*, p. 68; NAVARRO CARDOSO, F., "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", *Op. cit.*, p. 33.

En punto al blanqueo de capitales, las criptomonedas representan un canal idóneo para transmitir, limpiar y almacenar activos ilícitos en cuanto ofrecen factores clave como la descentralización o el anonimato[102].

6.2. El proceso de criptoblanqueo

El blanqueo de capitales se caracteriza actualmente por ser un fenómeno globalizado y sofisticado mediante los nuevos métodos de pago que requiere de la máxima cooperación internacional para su prevención y represión[103]. La mención a las criptomonedas resulta ineludible al hablar de la reformulación del blanqueo de capitales, ya que posibilitan la ocultación del origen del dinero y un movimiento ilimitado de los fondos, al mismo tiempo que generan excesivas dificultades para la detección de actividades ilícitas por las fuerzas de seguridad[104]. Las transacciones mediante criptomonedas se caracterizan por su dimensión transfronteriza y por resultar instantáneas y de bajo coste, lo cual convierte a aquellas en instrumentos idóneos para el blanqueo de capitales[105].

Antes de la exposición de las tres fases del proceso de criptoblanqueo puede adelantarse el papel fundamental que ostentan las plataformas de intercambio (*exchanges*) en cada una de ellas. En la fase de colocación, tales entidades constituyen una vía de entrada elemental en la medida en que permiten el intercambio de dinero fiat ilícito por criptomonedas. Asimismo, tales plataformas pueden verse involucradas en la fase de estratificación, ya que una de las técnicas más seguidas es el *chain hopping*, esto es, "el intercambio de cripto derivado del delito por monedas limpias"[106]. Y, finalmente, en la integración los *exchanges* desarrollan un papel esencial en cuanto permiten la conversión de criptomonedas en dinero fiat. Por ello, la inclusión de estas plataformas en la lista de sujetos obligados se erige como una de las principales medidas del GAFI[107], si bien con relativa eficacia para una prevención eficaz del criptoblanqueo.

---

102 Cfr. KOUTSOUPIA, V., "Challenges of the Use of Virtual Assets in Money Laundering", *Op. cit.*, p. 54.

103 Cfr. ABEL SOUTO, M., "La comisión del delito de blanqueo de dinero mediante las nuevas tecnologías y la internacionalización del Derecho penal", *Op. cit.*, p. 505.

104 Cfr. WRONKA, C., «"Cyber-laundering": the change of money laundering in the digital age», *Op. cit.*, p. 334.

105 Cfr. CALAFOS, M. W. y DIMITOGLOU, G., "Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency", en *Principles and Practice of Blockchains*, (eds. Daimi, K.; Dionysiou, I. y El Madhoun, N.), Cham, Springer, 2023, 1.ª ed., p. 286.

106 RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 205.

107 *Ibidem.*

El proceso de criptoblanqueo participa igualmente de las fases de colocación, estratificación e integración[108], si bien con algunas particularidades. En cada una de ellas se utilizan diferentes métodos que varían desde una relativa simplicidad hasta una complejidad que requiere de conocimientos técnicos[109]. A ello todavía cabe añadir la constante innovación predominante en relación con las criptomonedas, lo que puede suponer el abandono de dichos procedimientos y la aparición de otros cauces o estrategias eficientes para actividades de blanqueo de capitales[110].

6.2.1. Colocación

La colocación consiste en la conversión del dinero sucio a criptomoneda. Preferentemente se lleva a cabo mediante *exchanges* disponibles en la *Darknet* que no aplican medidas *know your customer* (en adelante, KYC)[111] o, en menor medida, a través de la compra de criptomonedas en cajeros ATM conectados a Internet. Estos últimos terminales posibilitan la compraventa de monedas virtuales, operan como si de un cajero automático normal se tratase y promueven el anonimato en los casos en los que no se requiere identificación[112]. El funcionamiento de tales cajeros es sencillo, ya que puede depositarse el dinero ilícito en efectivo y, tras una comisión, recibirse en un monedero una cantidad de criptomoneda (por ejemplo, *Bitcoin*) equivalente al valor depositado[113].

La fase inicial de colocación se elimina en los supuestos en los que el dinero proviene de actividades como el *ransomware* al resultar el beneficio ilícito una cantidad de criptomoneda[114]. A ello se añade que se pueden obtener criptomonedas como pago por entrega de estupefacientes, armas, pasaportes, falsos y otros documentos en la *Darknet*[115].

---

108 Cfr. DESMOND, D. B., LACEY, D. y SALMON, P., "Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review", *Op. cit.*, p. 482.

109 Cfr. ALMEIDA, H.; PINTO, P. y VILAS, A., "A review on cryptocurrency transaction methods for money laundering", en *Proceedings of the 5th International Conference on Finance, Economics, Management and IT Business*, (eds. Arami, M.; Baudier, P. y Chang, V.), Setúbal, Science and Technology Publications, 2023, 1.ª ed., p.120.

110 *Ibidem.*

111 Cfr. WRONKA, C., "Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures", *Op. cit.*, p. 85.

112 Cfr. ALMEIDA, H.; PINTO, P. y VILAS, A., "A review on cryptocurrency transaction methods for money laundering", *Op. cit.*, p. 119.

113 Cfr. WRONKA, C., "Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures", *Op. cit.*, p. 85.

114 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 198.

115 Cfr. MEIER, M., *Geldwäsche-Compliance…*, *Op. cit.*, p. 76.

6.2.2. Estratificación

El esquema delictivo en el criptoblanqueo transcurre seguidamente por la creación de diversas capas o movimientos de las criptomonedas en aras de conseguir el máximo anonimato posible. En esta fase de estratificación se establecen como técnicas principales el *chain hopping*, el recurso a *mixing services* (*tumblers*) o el uso de monedas con protocolos especiales para la privacidad de los intervinientes y de los datos de la operación. El predominio en la práctica de estos recursos mencionados provoca que en este trabajo se atienda especialmente a ellos, si bien deben añadirse también los criptocasinos y los intercambios descentralizados (DEX) como mercados basados en la BCT y que permiten transacciones entre pares[116].

El *chain hopping* consiste en el intercambio de un tipo de criptomoneda, como por ejemplo *Bitcoin*, por otras *altcoins* con la finalidad de lograr mayor privacidad[117]. Los transvases de fondos entre las distintas cadenas de bloques dificultan el rastreo de las transacciones[118]. Esta técnica suele realizarse mediante la conversión de una criptomoneda tipo *Bitcoin* en *privacy coins*, en cuanto estas últimas facilitan el anonimato de las partes y la ofuscación del importe de la transacción[119]. El objetivo fundamental de esta técnica consiste en realizar una serie rápida de transacciones e involucrar diferentes cadenas de bloques para dificultar el rastreo del origen y destino de las criptomonedas objeto del intercambio; a ello se añade que los intercambios se realizan normalmente en *exchanges* poco exigidos desde un punto de vista legal[120].

Los *mixing services* (*v. gr. Bitcoin Mixer*, *Blender.io*, *Chip-Mixer*, *FoxMixer*, *SmartMixer* o *CryptoMixer*) constituyen otra técnica para impedir la trazabilidad de las transacciones en la BC[121]. Tales servicios están disponibles en la *Dark Web*, a la cual se puede acceder mediante el empleo de navegadores tipo TOR (por sus siglas en inglés, T*he Onion Router*)[122]. La transcendencia de tales servicios radica en que permiten oscurecer la cadena de bloques mediante la unión de múltiples operaciones de distintos usuarios que se registran en las cadenas de bloques como una única transacción. Ello imposibilita conocer qué salidas provienen de cada usuario[123]. Una vez realiza-

---

116 Cfr. ALMEIDA, H.; PINTO, P. y VILAS, A., "A review on cryptocurrency transaction methods for money laundering", *Op. cit.*, p. 119.

117 Cfr. PAESANO, F., "Following the Virtual Money: Investigating Crypto-Based Money Laundering and Confiscating Virtual Assets", *Op. cit.*, p. 135.

118 *Ibidem.*

119 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 199.

120 Cfr. ALMEIDA, H.; PINTO, P. y VILAS, A., "A review on cryptocurrency transaction methods for money laundering", *Op. cit.*, p. 119.

121 Cfr. WANG, H-M. y HSIEH, M-L., "Cryptocurrency is new vogue: a reflection on money laundering prevention", *Op. cit.*, p. 35.

122 Cfr. TROZZE, A., "Cryptocurrency Crime", *Op. cit.*, p. 105.

123 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering

das numerosas operaciones simuladas, el *mixing service* transfiere a la clave pública del cliente u a otra especificada por aquel una cantidad equivalente a la inicial[124]. A cambio el mezclador deduce una tasa por la prestación del servicio que oscila desde el 0,5% hasta el 5%[125].

La operatividad de los *tumblers* radica en la ofuscación de las transacciones en las distintas cadenas de bloques. Siguiendo a FROMBERGER y ZIMMERMANN[126], tales servicios permiten oscurecer la cadena de bloques mediante un ciclo económico que imposibilita que terceros puedan rastrear el origen de los *tokens*. Como indican los autores citados, los *tumblers* disponen de múltiples claves públicas para la transferencia aleatoria y automática de los *tokens* procedentes de sus clientes y en el proceso se divide la cantidad ingresada en menores cuantías para completar el ciclo económico. El proceso termina con una transferencia de *tokens* equivalente a la cuantía original a una clave pública del cliente, previa comisión porcentual que puede ser una tarifa variable aleatoria[127].

Debido al pseudoanonimato que ofrecen criptomonedas como el *Bitcoin*, las personas implicadas en acciones delictivas recurren también a las *privacy coins* en cuanto ofrecen soluciones tecnológicas para la ocultación de las identidades del remitente y receptor, así como del importe de la transacción[128]. Acerca de estas monedas conviene señalar, como pone de relieve WRONKA[129], que, si bien su capitalización en el mercado resulta menor, cada vez están ganando más presencia, especialmente en la *Darknet*, ya que facilitan la ocultación de las transacciones y, por tanto, ostentan mayor operatividad para la perpetración de actividades delictivas.

Entre las *privacy coins* destaca *Monero* (XMR) que, para el aseguramiento de un mayor anonimato, incluye como característica complementaria las firmas de anillo[130]. Esta técnica supone que un grupo de usuarios puede generar la firma de la transacción, lo que impide conocer totalmente al remitente, esto es, la clave utilizada[131]. Más en

---

and terrorism financing", *Op. cit.*, p. 128.

124 Cfr. MEIER, M., *Geldwäsche-Compliance…*, *Op. cit.*, p. 53.

125 Cfr. WANG, H-M. y HSIEH, M-L., "Cryptocurrency is new vogue: a reflection on money laundering prevention", *Op. cit.*, p. 35.

126 Cfr. FROMBERGER, M. y ZIMMERMANN, P., "Technische und wirtschaftliche Grundlagen", *Op. cit.*, p. 31.

127 *Ibidem*.

128 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti- Money Laundering Framework", *Op. cit.*, p. 196.

129 Cfr. WRONKA, C., *"*Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures*"*, *Op. cit.*, p. 84.

130 Cfr. COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *Op. cit.*, p. 241.

131 Cfr. PAESANO, F., "Following the Virtual Money: Investigating Crypto-Based Money Laundering and Confiscating Virtual Assets", *Op. cit.*, p. 136.

concreto, MEIER[132] apunta que las firmas de anillo implican el uso no solo de la firma del remitente, sino también de otros participantes aleatorios que establecen una firma válida y equivalente para la transacción. Ello supone diversas salidas para una transacción en un anillo, al mismo tiempo que cada remitente configura la salida de la transacción de los restantes. Las firmas de anillo imposibilitan un rastreo de las transacciones mediante una combinación de claves públicas y privadas que se utilizan una sola vez[133].

El recurso a las *privacy coins* determina la imposibilidad de aplicar los protocolos de conocimiento del cliente, por lo que se advierte de la necesidad de que, desde el plano internacional, especialmente la UE siguiendo los parámetros establecidos por el GAFI, se tome partido contra este tipo de monedas virtuales. No obstante, el GAFI no prohíbe directamente su uso siempre y cuando se acompañen de medidas que permitan conocer la identidad de los participantes. Esto es, el enfoque adoptado responde al principio de neutralidad tecnológica, que supone que no se prohíben las *privacy coins* en cuanto se apliquen eficazmente obligaciones de diligencia debida con el cliente (en adelante, DDC), con independencia de la tecnología en cuestión[134]. En caso de no poder cumplirse lo anterior, el GAFI propone que los PSAV no participen en transferencias mediante monedas con protocolos de mejora del anonimato.

6.2.3. Integración

La última fase del proceso de criptoblanqueo es la integración. Tras el movimiento de los fondos ilícitos se pretende la reintroducción de aquellos en el sistema económico legal. Para ello existen desde algunos recursos simples hasta otros de mayor sofisticación. En el primer sentido, los *exchanges* permiten el intercambio de criptomonedas por moneda fiduciaria; también los cajeros ATM (*v. gr.* terminales electrónicos de *Bitcoin*)[135], que posibilitan esquivar los controles máximos de retirada mediante el uso de distintos cajeros[136]. Otra técnica sencilla consiste en la conversión de las criptomonedas en alguna de las aceptadas en el sector comercial para el pago de bienes o servicios. Otros métodos más cualificados son, en primer lugar, la creación de una empresa que admita el pago en criptomonedas para convertir las monedas virtuales contaminadas en limpias en cuanto pasa a constituir el resultado económico de la actividad empresarial[137]. Y, en segundo lugar, la compra

132 Cfr. MEIER, M., *Geldwäsche-Compliance…*, *Op. cit.*, p. 56.

133 *Ibidem.*

134 Cfr. COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *Op. cit.*, p. 241

135 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 199.

136 Cfr. ALMEIDA, H.; PINTO, P. y VILAS, A., "A review on cryptocurrency transaction methods for money laundering", *Op. cit.*, p. 118.

137 Cfr. WRONKA, C., «"Cyber-laundering": the change of money laundering in the digital age»,

de *hardware* de minería para minar nuevas criptomonedas e intercambiarlas luego por monedas fiduciarias[138].

7. LOS ESTÁNDARES DEL GAFI EN RELACIÓN CON EL CRIPTOBLANQUEO

7.1. Evolución de las políticas aprobadas

La ausencia de una amplia regulación para la prevención de operaciones de blanqueo de capitales mediante el uso de criptoactivos en general constituye el principal motivo que explica la intensa atención prestada por el GAFI. Esta organización intergubernamental trata de instaurar un régimen de prevención del criptoblanqueo lo más uniforme posible a nivel mundial, por lo que desarrolla una función de auxilio elemental a las jurisdicciones nacionales para combatir los riesgos delictivos asociados a los criptoactivos. Las medidas adoptadas por el GAFI son además un fiel reflejo del desarrollo alcanzado por el ecosistema cripto, pues cada nuevo avance ha tenido como respuesta la elaboración de nuevas disposiciones para combatir los riesgos de blanqueo de capitales[139].

La consolidación de los AV demanda una actuación reglamentaria permanente, tal y como viene realizando el GAFI, al mismo tiempo que las medidas adoptadas deben acompañarse de trabajos de evaluación y actualización para solventar las nuevas problemáticas que se generan. Así ocurre, por ejemplo, con la cuestión relativa a la jurisdicción. El GAFI ha instaurado un sistema de licencias o registro en relación con los PSAV que, a su vez, requiere determinar en qué país reside la entidad o si se trata de supuestos de aplicación extraterritorial de normativa nacional. Siguiendo a DE KOKER et al.[140], el sistema previsto por el GAFI involucra en un buen número de ocasiones a diferentes países que deben autorizar la actividad de un PSAV, por lo que determinar dónde se encuentra la entidad resulta fundamental en el marco de una economía digital que posibilita la búsqueda de espacios de actuación ajenos a regulación.

La primera de las iniciativas del GAFI, más allá de la pionera clasificación de las monedas virtuales en 2014, fue la publicación en 2015 de la "Guía para un enfoque basado en el riesgo en relación con las monedas virtuales"[141]. La aportación principal

---

Op. cit., p. 334.

138 Cfr. WRONKA, C., *"*Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures*"*, *Op. cit.*, p. 87.

139 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 203.

140 Cfr. DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", en *Financial Technology and the Law*, (eds. Goldbarsht, D. y de Koker, L.), Cham, Springer, 2022, p. 152.

141 Vid. FATF, *Guidance for a risk-based approach virtual currencies*, Paris, 2015, pp. 1-48.

del texto consiste en la sujeción de las monedas virtuales y los proveedores de servicios de moneda virtual a los estándares normativos. En el documento se expone la idea de que resulta transcendental la adopción de una diligencia reforzada en punto a las monedas virtuales convertibles y descentralizadas de mayor riesgo[142]. No obstante, este documento presenta serias limitaciones para una prevención eficaz del criptoblanqueo pues, como advierte CHASIN VELKES[143], únicamente se centra en los puntos de intersección (entrada y salida) de las monedas virtuales con el sistema financiero, sin atender a "las transferencias internas del mercado, dejando así un gran número de transacciones sin regular"[144].

En la Cumbre del G20 celebrada en Buenos Aires en junio de 2018 se analizó la incidencia de las criptomonedas en la estabilidad financiera global. Los ministros de finanzas y gobernadores de los bancos centrales del G20 solicitaron al GAFI que aclarase la aplicación de sus recomendaciones contra el blanqueo de capitales en relación con tales innovaciones[145]. Ello se justificó particularmente en un crecimiento notable en el número de delitos, generando una preocupación mundial sin precedentes ante la falta de una respuesta jurídica[146]. La solicitud derivó en la revisión de la Recomendación n.º 15 en octubre del 2018, en la que el GAFI realizó una ampliación del ámbito de aplicación de sus estándares para abarcar todas las actividades con AV, al igual que introdujo el régimen de licencias y registro nacionales para los PSAV[147].

La Recomendación n.º 15, tras su modificación en 2018, también demanda expresamente que las autoridades nacionales supervisen el cumplimiento por parte de los PSAV de los estándares antiblanqueo. Los estados miembros del GAFI deben designar a una autoridad nacional con capacidad suficiente para realizar inspecciones, requerir informes e imponer sanciones disciplinarias y/o financieras, entre las que se halla la suspensión, restricción o retirada de la licencia para operar como PSAV[148]. La supervisión no puede ser realizada por un organismo de autorregulación, sino que debe tratarse de una autoridad nacional que tenga incluso potestad para imponer sanciones[149]. Estas últimas, conforme a lo estipulado en la Recomendación n.º 35

142 Cfr. NAVARRO CARDOSO, F., "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", *Op. cit.*, p. 24.

143 Cfr. CHASIN VELKES, G., "International Anti-Money Laundering Regulation of Virtual Currencies and Assets", *Op. cit.*, p. 880.

144 *Ibidem.*

145 Cfr. PAESANO, F., "Following the Virtual Money: Investigating Crypto-Based Money Laundering and Confiscating Virtual Assets", *Op. cit.*, p. 126.

146 Cfr. DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", *Op. cit.*, p. 158.

147 *Ibidem.*

148 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 204.

149 Cfr. PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Op. cit.*, p. 4.

y la Nota Interpretativa de la Recomendación n.º 15 (en adelante, NIR n.º 15), deben ser "efectivas, proporcionadas y disuasorias"[150] y aplicables tanto a PSAV como a sus altos directivos[151].

Los países son los encargados de identificar a las personas físicas o jurídicas que prestan servicios relacionados con AV sin licencia o registro, todo ello con el fin de imponer las sanciones oportunas. La necesidad de que los estados impidan operar a las entidades que carezcan de autorización o registro supone una llamada de atención por parte del GAFI acerca de la proactividad que los estados deben adoptar en la identificación de servicios irregulares. Para la consecución de este último extremo, el GAFI dispone que los estados miembros deben emplear el máximo número de medios posibles, entre los que sugiere la aplicación de herramientas de rastreo para las webs, el uso de mecanismos de retroalimentación pública, así como el aprovechamiento del apoyo que ofrecen las informaciones de las Unidades de Inteligencia Financiera (en adelante, UIF)[152].

El GAFI determina que los PSAV deben cumplir con las obligaciones en materia de PBC/FT en idénticos términos que cualquier otro sujeto obligado. Como manifiestan DE KOKER et al.[153], los PSAV deben adoptar medidas de DDC para verificar la identidad de aquellos, crear perfiles de riesgo, controlar las transacciones y notificar operaciones sospechosas a las UIF. El GAFI no introduce disposiciones que difieran en lo sustancial de lo exigido a los demás sujetos obligados, por más que existan particularidades derivadas del funcionamiento técnico de los AV. Por ello, gran parte del régimen de prevención del criptoblanqueo instaurado por el GAFI remite esencialmente al contenido de las Recomendaciones n.º 10 a 21[154].

El GAFI introdujo también en 2018 dos nuevas definiciones en el Glosario de sus Recomendaciones. La primera se refiere a AV, entendiéndose por tales las representaciones digitales de valor que pueden comercializarse o transferirse digitalmente y pueden ser utilizadas con fines de pago o inversión, así como las representaciones digitales de valor que cumplen las funciones como medio de cambio, unidad de cuenta y/o depósito de valor. Esta definición se incluyó con la pretensión de que fuese lo suficientemente amplia como para permitir la inclusión de futuras innovaciones. La trascendencia del concepto radica en que no se limita a los *tokens* de tipo pago/intercambio, sino que también abarca los *tokens* de inversión/seguridad y de

150 PALPACUER, J. y AOUIZERAT, B., "Anti-Cyber Laundering: The Inclusion of Virtual Asset Service Providers", *Op. cit.*, p. 265.

151 Cfr. PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Op. cit.*, p. 5.

152 *Ibidem*.

153 Cfr. DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", *Op. cit.*, p. 162.

154 Cfr. PALPACUER, J. y AOUIZERAT, B., "Anti-Cyber Laundering: The Inclusion of Virtual Asset Service Providers", *Op. cit.*, p. 266.

utilidad[155]. Todos ellos poseen como notas en común su origen en el sector privado y su dependencia de la TRD. El concepto de AV va más allá pues de las criptomonedas, si bien no es ilimitado al excluirse expresamente las CBDC[156].

La segunda adición conceptual es la relativa a los PSAV que, según el GAFI, debe interpretarse con vocación de máxima amplitud, en igual forma que el concepto de AV, en aras de incluir a todas aquellas entidades que no se hallen sujetas previamente a los estándares normativos[157]. La definición de PSAV hace referencia a cualquier persona física o jurídica no incluida en otra parte de las Recomendaciones que, siempre como negocio, lleve a cabo alguna de las siguientes actividades para o en nombre de otra persona física o jurídica: 1. Intercambio entre AV y monedas fiduciarias; 2. Intercambio entre una o más formas de AV; 3. Transferencia de AV; 4. Custodia y/o administración de AV; y 5. Prestación de servicios financieros relacionados con la oferta y/o venta de un AV por parte de un emisor. Con esta definición el GAFI va más allá de lo estipulado en 2015 y amplía su atención a las actividades de cambio de AV por AV, a los cajeros ATM de criptomonedas y a los *mixing services*[158].

Apenas un año más tarde, en julio de 2019, el GAFI publicó la NIR n.º 15 para aclarar todavía más su aplicación respecto a las actividades prestadas por los PSAV. El origen de esta disposición se halla en la Cumbre del G20 celebrada en Osaka los días 28 y 29 de junio de 2019, en la que también se acogieron enmiendas a la Recomendación n.º 15 y al Glosario del GAFI[159]. La NIR n.º 15 resulta especialmente trascendente en cuanto establece los siguientes puntos: 1. La extensión del enfoque basado en el riesgo (en adelante, EBR) a las actividades con AV; 2. La supervisión de las actividades de los PSAV para lograr un régimen eficaz de PBC/FT; 3. Las medidas de DDC exigibles; 4. El deber de conservación de documentos; 5. El sistema para reportar operaciones sospechosas a las autoridades competentes; y 6. Los extremos relativos a la cooperación internacional[160].

La NIR n.º 15 incide nuevamente en el régimen que debe seguirse para la concesión de licencias o registros para los PSAV. Una de las novedades fundamentales aportadas reside en la necesidad de que el registro de los PSAV tenga lugar como mínimo

155 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti- Money Laundering Framework", *Op. cit.*, p. 207.

156 Cfr. DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", *Op. cit.*, p. 159.

157 Cfr. COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", p. 239.

158 Cfr. CHASIN VELKES, G., "International Anti-Money Laundering Regulation of Virtual Currencies and Assets", *Op. cit.*, p. 881.

159 Cfr. PONAMORENKO, V. E., "International Organizations' Approaches to Digital Assets Legalization (Monetary Policy and AML/CFT)", *Op. cit.*, p. 113.

160 *Ibidem.*

en la jurisdicción en la que se crean[161]. Esta declaración supone que un PSAV determinado, para ofrecer productos o desarrollar su actividad en otros países distintos al de creación, puede quedar sometido nuevamente a otro requisito de licencia o registro[162]. Con este modelo, como señala PAVLIDIS[163], el GAFI no hace otra cosa que involucrar a múltiples países en el control y supervisión de las actividades prestadas por los PSAV, si bien tal apuesta demanda como correlativa el establecimiento de canales de cooperación eficaces entre los distintos supervisores nacionales.

La NIR n.º 15 contempla el deber para las autoridades nacionales de garantizar que los delincuentes o cómplices no posean una participación significativa de control o gestión en las entidades que prestan servicios de AV[164]. Por ello se estipula que cualquier cambio en la estructura de aquellas debe ser objeto de aprobación por las autoridades competentes[165]. Esta medida se halla en íntima relación con la concesión de licencias o el registro necesario al que se ven sometidos los PSAV, pues ambas persiguen que los delincuentes no desempeñen un papel activo en tales entidades. Como indican DE KOKER et al.[166], uno de los extremos básicos en el proceso de concesión de licencias o registro de los PSAV es la identificación de las personas que ofrecen los servicios, asumiendo tal función la autoridad que se encarga de la concesión de licencias o registro o quien cumpla con dicha tarea por delegación.

La NIR n.º 15 extiende la regla de viaje (*travel rule*) a las transacciones criptográficas. Los PSAV están obligados a recopilar y compartir datos de los usuarios en transacciones superiores a 1.000 USD/€; por encima de tal cuantía, los PSAV deben aplicar medidas de DDC y realizar un manejo cuidadoso de los datos. Para las operaciones con AV que no superen el umbral de los 1.000 USD/€ también se contempla el deber de recopilar los nombres y números de cuenta del ordenante y del beneficiario, al igual que la dirección de la billetera de cada uno o la identificación numérica de la transacción[167]. Estas transacciones no serán objeto de comprobación, salvo sospechas de blanqueo de capitales. La extensión de la *travel rule* a las operaciones con

161 Cfr. PALPACUER, J. y AOUIZERAT, B., "Anti-Cyber Laundering: The Inclusion of Virtual Asset Service Providers", *Op. cit.*, p. 264.

162 Cfr. PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Op. cit.*, p. 4.

163 *Ibidem.*

164 Cfr. DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", *Op. cit.*, p. 162.

165 Cfr. PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Op. cit.*, p. 4.

166 Cfr. DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", *Op. cit.*, p. 162.

167 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 207; PAESANO, F., "Following the Virtual Money: Investigating Crypto-Based Money Laundering and Confiscating Virtual Assets", *Op. cit.*, p. 127.

AV permite afirmar que el GAFI involucra al máximo a los PSAV en la PBC/FT, al mismo tiempo que destaca la diferencia entre la cantidad fijada para las transacciones mediante AV y el umbral establecido para las transacciones financieras (15.000 USD/€). La distinción se fundamenta inequívocamente en la consideración de que las actividades con AV entrañan mayor riesgo de blanqueo de capitales[168].

La *travel rule* supone, a tenor de lo dispuesto en la Nota Interpretativa de la Recomendación n.º 16, que tanto el PSAV ordenante como el PSAV beneficiario deben recabar y conservar la siguiente información en las transferencias de AV: a) el nombre del ordenante; b) el número de cuenta del ordenante cuando dicha cuenta se utilice para procesar la transacción; c) la dirección del ordenante, o su número nacional de identidad, o su número de identificación de cliente, o su fecha y lugar de nacimiento; d) el nombre del beneficiario; e) y el número de cuenta del beneficiario cuando se utilice dicha cuenta para procesar la transacción. Si no hay cuenta, debe incluirse un número de referencia de transacción único que permita la trazabilidad de la transacción. Tales entidades deben mantener durante cinco años la información sobre el ordenante y el beneficiario[169], así como poner aquella a disposición de las UIF o de las autoridades policiales y/o judiciales cuando sea requerida[170].

La exigencia de que los PSAV cumplan con las tradicionales medidas antiblanqueo impuestas a los demás sujetos obligados, incluyéndose la *travel rule*, conforman un "enfoque basado en intermediarios"[171], a los que se les otorga cierta flexibilidad[172] para cumplir con los requisitos impuestos en aras de no frenar la innovación financiera[173]. Con todo, algunos autores muestran un claro escepticismo a la traslación de los deberes de PBC/FT a las entidades que prestan servicios en el ecosistema cripto por las siguientes razones. En primer lugar, tal extensión puede traducirse en una necesaria reorganización de la BCT[174], dado que los protocolos en que se fundamenta no requieren de tales datos para completar una transacción. En segundo lugar, esta política también puede aumentar el coste de las criptomonedas[175], en la medida en que la *travel rule* supone una carga más costosa para los PSAV que para

168 Cfr. PALPACUER, J. y AOUIZERAT, B., "Anti-Cyber Laundering: The Inclusion of Virtual Asset Service Providers", *Op. cit.*, p. 267.

169 Vid. Recomendación n.º 11 del GAFI.

170 Vid. Nota Interpretativa a la Recomendación n.º 17 apartado 7 letra b).

171 RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 210.

172 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 137.

173 Cfr. PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Op. cit.*, p. 5.

174 Cfr. ABEL SOUTO, M., "La comisión del delito de blanqueo de dinero mediante las nuevas tecnologías y la internacionalización del Derecho penal", *Op. cit.*, p. 517.

175 *Ibidem.*

las instituciones financieras tradicionales[176]. Y, en tercer lugar, se añade el riesgo de remisión de información a entidades no reguladas ante transferencias de AV al margen de los PSAV[177].

La *travel rule* resulta aplicable a las transferencias electrónicas, en donde se incluyen también las transacciones realizadas con AV. El concepto de "transferencias electrónicas" establecido por el GAFI se ha visto sometido a una constante reforma para incluir en él las transferencias mediante criptoactivos en general, en la medida en que estas últimas se equiparan a las transacciones financieras tradicionales[178]. En ambas formas se identifica pues a un ordenante que pone a disposición de un beneficiario una cantidad determinada de fondos por medios electrónicos, por más que las operaciones utilicen una tecnología diferente y se caractericen ampliamente por la desintermediación.

El GAFI adoptó en octubre de 2019 una nueva versión de la "Guía sobre la aplicación de un enfoque basado en el riesgo a los AV y a los PSAV"[179]. El objetivo era auxiliar a las jurisdicciones en la configuración de un marco de control y supervisión óptimo en relación con las actividades de AV. Entre las principales novedades destaca, en primer lugar, el énfasis en la definición de AV como representación digital de valor que puede comercializarse o transferirse digitalmente y puede usarse con fines de pago o inversión. Ello supone reafirmar la inclusión de los *tokens* de utilidad y de inversión/seguridad. El GAFI subraya la necesidad de flexibilizar la definición de AV por tratarse de una gama de productos y servicios en evolución; por ello, a efectos de aplicación de los estándares antiblanqueo considera a los AV "bienes", "productos", "fondos", "fondos u otros activos" o un "valor correspondiente"; esta matización se considera positiva ya que difumina toda duda respecto a la naturaleza jurídica de los criptoactivos y su sujeción a los estándares antiblanqueo[180].

En el documento de 2019 se señala que las *stablecoins* y los proveedores de servicios de monedas estables deben someterse igualmente a los estándares del GAFI, bien como AV y PSAV, bien como activos financieros y proveedores de servicios financieros tradicionales[181]. Las *stablecoins* vinculan su valor mayoritariamente a monedas fiduciarias como activo estable con la finalidad de reducir la alta volati-

176 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 138.

177 *Ibidem.*

178 Cfr. PALPACUER, J. y AOUIZERAT, B., "Anti-Cyber Laundering: The Inclusion of Virtual Asset Service Providers", *Op. cit.*, p. 268.

179 Vid. FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* Paris, 2019, pp. 1-59.

180 Cfr. PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Op. cit.*, p. 3.

181 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 131.

lidad predominante en cuanto al precio de mercado. *Tether* es el principal ejemplo en la medida en que el valor de sus *tokens* USDT se condicionan al valor del dólar estadounidense; no obstante, es solo un único ejemplo de *stablecoin* que se respalda a través de dinero fiat, al mismo tiempo que existen otras que se apoyan en otros activos o instrumentos financieros para reducir la volatilidad y aumentar su empleo en el sector comercial[182].

Entre los proyectos de *stablecoins* destacó especialmente en 2019 la denominada por aquel entonces Libra, promovida por Facebook, hasta tal punto que el GAFI centró su atención en las *stablecoins* por los riesgos de blanqueos de capitales que llevaban asociadas[183]. El GAFI identificó dos preocupaciones principales relacionadas con las *stablecoins*: la adopción masiva en el mercado y la proliferación de transferencias peer-to-peer sin sujetarse a la regulación sobre PBC/FT[184]. Estas preocupaciones dieron lugar a que el GAFI publicase en junio de 2020 un nuevo dictamen adicional sobre las *stablecoins* para aclarar su sujeción a las recomendaciones[185]. Este informe resulta transcendental en cuanto sirve como una actualización para los reguladores nacionales sobre el desarrollo alcanzado por las *stablecoins* y la necesidad de garantizar que estas se sujeten a controles de PBC/FT adecuados[186].

La Guía aprobada en 2019 también matiza la noción de PSAV con las siguientes restricciones. El GAFI subraya la sujeción a sus estándares de aquellas entidades que prestan en calidad de negocios diversos servicios relacionados con AV, siempre en nombre de otra persona física o jurídica. Esta previsión determina a *sensu* contrario que los usuarios individuales de AV no se incluyen entre los PSAV, así como tampoco aquellas personas que desarrollen un *software* destinado a servir como nueva plataforma de funcionamiento para los AV y se dedican exclusivamente a la venta de la aplicación[187].

Uno de los éxitos del GAFI es el examen periódico de la implementación de todos sus estándares en los estados miembros. Las disposiciones normativas sobre AV son también objeto de revisión en aras de analizar el grado de seguimiento del régimen en las distintas jurisdicciones nacionales. Esta evaluación se realiza en un marco temporal periódico (12 meses) en el que cada uno de los miembros del GAFI y los

182 Cfr. WRONKA, C., "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight", *Op. cit.*, p. 85.

183 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 134.

184 *Ibidem.*

185 Vid. FATF, FATF *Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, Paris, 2020, pp. 1-32.

186 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 131.

187 Cfr. DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", *Op. cit.*, p. 160.

órganos regionales asimilados a este (que agrupan a más de 200 jurisdicciones nacionales) cubren un cuestionario al respecto[188]. La transcendencia de esta metodología de evaluación seguida por el GAFI no solo radica en el conocimiento del *statu quo* normativo existente en cada jurisdicción, sino que permite revisiones regulares de la guía sobre AV y PSAV[189].

El GAFI publicó en junio de 2020 la primera revisión de 12 meses acerca de la implementación de las disposiciones contenidas en la Guía de 2019[190]. En esta evaluación se pusieron de manifiesto las principales problemáticas a la hora de aplicarse los estándares normativos, destacando el *sunrise problem*. Este es un aspecto recurrente tras la aparición de una nueva normativa en cuanto su implementación en el plano nacional difiere en función de los esfuerzos adoptados por cada estado. En relación con los AV y el desigual cumplimiento de las normas, el problema radica en que la *travel rule* no podrá aplicarse con éxito en aquellos casos en los que un cliente de un *exchange* que opera en una jurisdicción vinculada a las obligaciones de identificación envía dinero a una persona que utiliza un *exchange* sito en un país que no incorporó la regulación de la *travel rule*[191]. Este supuesto determina la falta de respuesta por el PSAV beneficiario en la medida en que carece de la información solicitada por no aplicarse en su país la *travel rule*[192].

La rapidez de las transacciones que permiten los AV se acompaña de un grado de anonimato, desde parcial a absoluto[193], que potencia el blanqueo de bienes procedentes de delitos como el tráfico de drogas, la ciberdelincuencia o la trata de personas. Con el objetivo de auxiliar a los estados en la detección de tales actividades ilícitas, el GAFI publicó en septiembre de 2020 el documento "Indicadores de alerta de blanqueo de capitales y financiación del terrorismo asociados con activos virtuales"[194] en el que, sobre la base de más de 100 estudios de caso, expone una serie de indicadores que los PSAV deben tener en cuenta para detectar posibles operaciones de blanqueo de capitales[195]. Entre ellos destacan: 1. El uso de *privacy coins* o el recurso a *mixing services* para aumentar el anonimato de las transacciones; 2. El hecho de que las operaciones involucren jurisdicciones muy laxas en cuanto a la adopción de medidas

188 Cfr. PALPACUER, J. y AOUIZERAT, B., "Anti-Cyber Laundering: The Inclusion of Virtual Asset Service Providers", *Op. cit.*, p. 263.

189 *Ibidem.*

190 Vid. FATF, *12-month Review Virtual Assets and VASPs*, Paris, 2020, pp. 1-26.

191 Cfr. PAESANO, F., "Following the Virtual Money: Investigating Crypto-Based Money Laundering and Confiscating Virtual Assets", *Op. cit.*, p. 129.

192 *Ibidem.*

193 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti- Money Laundering Framework", *Op. cit.*, p. 197.

194 Vid. FATF, *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*, Paris, 2020, pp. 1-24.

195 Cfr. PALPACUER, J. y AOUIZERAT, B., "Anti-Cyber Laundering: The Inclusion of Virtual Asset Service Providers", *Op. cit.*, p. 266.

de PBC/FT; 3. Que el patrón de transacciones resulte irregular o inhabitual; 4. La regularidad anormal de las transacciones sin responder a un modelo de negocio concreto; y 5. Que la cantidad de las transacciones resulte excesivamente elevada.

En julio de 2021 el GAFI publicó la segunda evaluación de 12 meses sobre la implementación de sus estándares sobre AV y PSAV[196]. En ella se confirman las principales tendencias en la comisión del blanqueo de capitales detectadas en el primer informe de 2020, reconociéndose que la instrumentalización delictiva de los AV todavía no supera a los productos financieros más tradicionales. No obstante, el GAFI alerta de la proliferación de casos en los que los *mixing services* desarrollan un papel esencial en la fase de estratificación del blanqueo de capitales. El incremento de AV recaudados a partir de actividades de *ransomware* se vio motivado por el confinamiento a causa de la COVID-19. El GAFI indica que las ganancias obtenidas por actos de *ransomware*, estafas en los mercados de la *Dark Web* y hackeos son objeto de criptoblanqueo posterior, ya que los fondos ilícitos se mueven a través de *unhosted wallets* o se intercambian por *privacy coins*, hasta convertirse en otros AV o dinero fiat.

Tras la segunda revisión de 12 meses el GAFI publicó en octubre de 2021 la "Guía actualizada para un enfoque basado en el riesgo de los AV y PSAV"[197], con el fin de auxiliar a los países en la aplicación de los requisitos demandados por la NIR n.º 15. En esta segunda versión de la guía publicada en 2019 se incluyó como una de las principales novedades la ampliación de las definiciones de AV y PSAV a efectos de incluir las *stablecoins* y sus órganos de gobierno. En particular, el GAFI señala que las personas físicas o jurídicas que establecen las normas de funcionamiento de las *stablecoins* o que poseen las funciones de estabilización pueden ser considerados como PSAV debido a la transcendencia de sus funciones en el funcionamiento de las *stablecoins*[198].

Otro de los puntos objeto de actualización en 2021 fue la sección relativa a la autorización y registro de los PSAV. La principal novedad consiste en exigir tales condicionantes a las personas físicas en las jurisdicciones en que tengan situado su centro de actividad[199]. No obstante, aquí se genera una cierta indeterminación ya que cada estado puede tener en cuenta un criterio concreto para determinar el centro de actividad de un PSAV persona física[200]. El centro de actividad puede venir dado por la

196 Vid. FATF, *Second 12-month Review Virtual Assets and VASPs*, Paris, 2021, pp. 1-46.

197 Vid. FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Paris, 2021, p. 1-111.

198 Cfr. DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", *Op. cit.*, p. 161.

199 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 206.

200 Cfr. DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", *Op. cit.*, p. 163.

ubicación principal en la que se desarrolla la actividad[201]. También puede fijarse a partir del lugar en el que se realiza la llevanza de los libros y registros[202]; sin embargo, esta pauta resulta discutible en la era digital actual, pues los libros y registros pueden permanecer en un servidor de la nube y trasladarse rápidamente a otra jurisdicción, imposibilitándose así un control idóneo por las autoridades nacionales[203]. Y el tercer criterio es el lugar de residencia de la persona física, que puede tomarse en cuenta ante la falta de un lugar de actividad[204].

En esta nueva actualización se hace especial mención de la aplicación de las medidas de DDC en relación con operaciones basadas en AV, al igual que se ahonda en la necesidad de que los PSAV cumplan con los requisitos en materia de notificación de transacciones sospechosas[205]. Respecto al primer punto se establece que los PSAV deben instaurar procedimientos eficaces para verificar la identidad del cliente en el momento de establecerse relaciones comerciales, con independencia de la cuantía, así como en todos los casos en los que haya dudas acerca de la veracidad de los datos obtenidos. Y, en punto a la notificación de operaciones sospechosas a las UIF, el GAFI indica que cualquier PSAV, al margen de la jurisdicción en la que opere, resulta obligada a notificar transacciones sospechosas, ya bien se traten de operaciones fiat a fiat, virtual a virtual, fiat a virtual o virtual a fiat[206].

La nueva Guía de 2021 destaca asimismo por dar entrada a una nueva sección en la que se contemplan los principios de intercambio de información y cooperación entre los supervisores de PSAV. Tales disposiciones abordan aspectos concretos de la cooperación entre los supervisores de PSAV: 1. Acuse de recibo de la información solicitada, 2. Mantenimiento de una base de datos segura, 3. Respuesta a peticiones de información y 4. Facilitación de redes de cooperación multilaterales. El elemento que caracteriza a estos principios consiste en la proactividad sobre la que se configura el intercambio de información y cooperación entre supervisores nacionales.

En junio de 2022 el GAFI ha publicado una nueva actualización acerca de la implementación de sus normas sobre AV y PSAV en cada jurisdicción nacional[207]. Como principal novedad del documento destaca la advertencia que el GAFI realiza a los

---

201 Cfr. COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *Op. cit.*, p. 249.

202 *Ibidem.*

203 Cfr. DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", *Op. cit.*, p. 163.

204 Cfr. COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *Op. cit.*, p. 249.

205 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 207.

206 *Ibidem.*

207 Vid. FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*, Paris, 2022, pp. 1-22.

estados miembros acerca de la necesidad de controlar el desarrollo del ecosistema de las *DeFi*. Como señala BENSON et al.[208], se trata de un régimen cerrado alejado del campo de las finanzas tradicionales con intermediarios, que se caracteriza por el hecho de que los participantes interactúan directamente entre sí. A ello se une un claro anonimato de las transacciones que impide el bloqueo de cuentas en cuanto se desconoce quién es el receptor de los fondos sospechosos[209].

El GAFI volvió a publicar en junio de 2023 una nueva evaluación relativa a la aplicación de sus estándares normativos sobre AV y PSAV en cada una de las jurisdicciones nacionales[210]. En este texto subraya, entre otros aspectos, la irregular y escasa aplicación de las medidas de registro y autorización para los PSAV en los distintos países y advierte de los negativos efectos de tal déficit en cuanto se acrecienta con ello el riesgo de blanqueo de capitales. En particular, se indica que casi un tercio (45 de 151) de las jurisdicciones aún no se pronunciaron respecto a la admisión o no de las operaciones con AV y cómo debe desarrollarse el ejercicio de las actividades por parte de los PSAV. Asimismo, como dato complementario se pone de relieve que, entre el número de jurisdicciones que sí regulan las actividades de los PSAV, únicamente 24 estados satisfacen plenamente los requisitos de la Recomendación n.º 15 y la NIR.15.

El GAFI advierte que la actividad de entidades sin licencia o no registradas en países que carecen de sistemas de autorización implica un mayor riesgo de blanqueo de capitales por no hallarse sujetas tales personas físicas o jurídicas a medidas de supervisión. En tales circunstancias, los PSAV son potencialmente idóneos para el delito, al mismo tiempo que la falta de adopción de medidas de PBC/FT por aquellos dificulta la posterior labor de las fuerzas de seguridad[211]. Además, la cooperación entre PSAV se resquebraja ante la existencia de entidades no autorizadas, ya que las que sí cumplan con el requisito del registro tendrán mayores dificultades para obtener y verificar información. Todo ello se traduce pues, a juicio del GAFI, en una clara reducción del éxito de las políticas de prevención configuradas a partir de un EBR.

El documento de 2023 también recoge el *sunrise problem* como uno de los principales retos para conseguir una política eficaz contra el criptoblanqueo. La desigual implementación de la *travel rule* aplicable a las transacciones mediante AV, sobre todo en lo que se refiere a la información que los PSAV deben recopilar sobre los datos del beneficiario, dificulta un seguimiento pleno de las normas del GAFI, por más que estas sean flexibles y susceptibles de aproximaciones en la práctica. El propio GAFI reconoce que no es realista una armonización plena de las normativas nacionales al

208 Cfr. BENSON, V. et al., "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions", *Op. cit.*, p. 52.

209 *Ibidem.*

210 Vid. FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*, Paris, 2023, pp. 1-42.

211 Cfr. NAZZARI, M., "From payday to payoff: Exploring the money laundering strategies of cybercriminals", *Trends in Organized Crim*e, 1, 2023, p. 13.

respecto, pues cada una se articula a partir de un EBR. Por ello, se limita a pedir a los estados miembros el cumplimiento del marco de mínimos aprobado y, cuando resulte posible, una armonización legislativa de los regímenes de PBC/FT.

El GAFI indica que únicamente la mitad de las jurisdicciones que han adoptado las medidas necesarias para la aplicación de la *travel rule* establece que los PSAV nacionales operarán únicamente con contrapartes sujetas a regulación y a la aplicación de la *travel rule*. Ello supone que una gran parte de jurisdicciones nacionales permiten a sus PSAV realizar transacciones con cualquier otra entidad extranjera, por más que no se hallen sujetas a un sistema de registro, así como tampoco deban cumplir con la *travel rule*. Todo ello deriva en una situación en la que el GAFI destina últimamente gran parte de sus esfuerzos a promocionar la acogida de la Recomendación n.º 15 por las jurisdicciones nacionales, en cuanto estima que solo un seguimiento pleno de la *travel rule* mitigará los riesgos efectivos de blanqueo de capitales.

Otro de los aspectos recogidos por el GAFI en el 2023 se refiere a la escasa regulación de los *unhosted wallets* y las transacciones P2P. El déficit se extiende también a la evaluación de riesgos, pues la mayoría de los países encuestados no llevaron a cabo dicho extremo que, a su vez, se convierte en una tarea compleja ante la falta de datos sobre el tamaño del ecosistema P2P y el volumen global de transacciones ilícitas. A pesar de que las transacciones entre pares quedan fuera del ámbito de aplicación de los estándares normativos del GAFI, este último remite a la guía de 2021 que contempla distintos enfoques que las jurisdicciones nacionales pueden adoptar en relación con tales plataformas: 1. Mejora de las métricas del mercado de transacciones P2P; 2. Empleo de herramientas de análisis de la cadena de bloques; o 3. Exigencia de políticas adicionales a los PSAV que permiten transacciones hacia o desde entidades no obligadas.

Finalmente, en julio de 2024 se ha publicado la última evaluación sobre la aplicación de la Recomendación n.º 15 y la NIR n.º 15[212]. Uno de los aspectos destacados es la comprobación de un avance por parte de las jurisdicciones nacionales en la concesión de licencias o números de registro de PSAV. A este respecto se indica que 82 de 94 países, sin contar a las jurisdicciones que prohíben o se hallan próximas a la prohibición de los PSAV, han incorporado la exigencia de licencia o registro para operar como entidad proveedora de servicios relacionados con AV. En concreto, se pone de relieve que hasta 69 de esas 82 jurisdicciones han comunicado la autorización o registro previo de PSAV. El GAFI valora estas cifras como un avance respecto a la situación de 2023, en el que solo 60 de 135 jurisdicciones comunicaron la emisión de licencia o registro para PSAV.

El GAFI recoge como contrapartida a los datos anteriores la insuficiente adaptación de las legislaciones nacionales para garantizar una aplicación efectiva de la *travel rule*. Se indica que casi un tercio de los países todavía no adaptaron sus marcos jurídicos a

212 Vid. FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*, Paris, 2024, pp. 1-36.

lo estipulado en las Recomendaciones, a lo que se añade que hasta 58 jurisdicciones no completaron la encuesta del GAFI. Esta falta de colaboración se interpreta por la propia organización como un presumible incumplimiento por los estados de la adopción de las medidas para una aplicación efectiva de la *travel rule*. Además, el GAFI subraya que a pesar de que una parte de las legislaciones nacionales hayan dado entrada a la *travel rule* en operaciones con AV, existe un déficit de control sobre la aplicación de aquella, ya que solo 17 de 65 jurisdicciones nacionales supervisan la adopción por parte de los PSAV.

La última de las secciones de la evaluación publicada en 2024 hace referencia a los riesgos de blanqueo de capitales y financiación del terrorismo relacionados con las *stablecoins*, las *DeFi*, los *unhosted wallets* y las transacciones P2P. Respecto a cada una de ellas el GAFI pone de manifiesto lo siguiente.

En punto a las *stablecoins* configura a *Tether* como la opción preeminente para la comisión de actividades ilícitas. No obstante, el GAFI indica que la aparición de otras *stablecoins* supone una amplificación de los riesgos de blanqueo de capitales ya que aquellas, almacenadas en *unhosted wallets*, pueden destinarse al pago de bienes o servicios sin conversión a moneda fiduciaria.

Los intercambios *DeFi*, si bien resultan de menor atención por parte de las investigaciones científicas, constituyen otro método criminal de especial transcendencia práctica en cuanto eliminan a todo tipo de intermediarios. Las transferencias de dinero se realizan entre pares mediante contratos inteligentes autoejecutables. Estas notas atribuyen a las *DeFi* las características de anonimato, automatización y ausencia de intermediarios, en base a lo cual se afirma la dificultad para su regulación[213]. El GAFI señala que entre las 80 jurisdicciones que han aprobado legislación para aplicar la *travel rule* a los PSAV, hasta 41 de ellas no aplican su marco a las *DeFi*; a su vez, únicamente 18 de las 41 jurisdicciones adoptan medidas para combatir los riesgos en dicho ámbito.

Al igual que en 2023, el GAFI señala una falta de evaluación de los riesgos de blanqueo de capitales relacionados con *unhosted wallets* y transacciones P2P. Entre las 80 jurisdicciones que han aprobado medidas legales para la aplicación de la *travel rule* a los PSAV, únicamente 12 de ellas desarrollan una serie de trabajos para la recopilación y la evaluación de métricas del mercado P2P con la finalidad de evaluar los riesgos de BC/FT. A estos efectos el GAFI recoge algunas medidas que ciertas jurisdicciones exigen a los PSAV para mitigar los riesgos de BC/FT: 1. Exigencia de herramientas de análisis de la cadena de bloques; 2. Permiso exclusivo para emitir transferencias a unhosted wallets controlados por el originador; 3. Aplicación similar de la *travel rule* a las transacciones PSAV-unhosted wallets; y 4. Adopción de una diligencia debida mejorada.

213 Cfr. BENSON, V. et al., "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions", *Op. cit.*, p. 52.

7.2. Valoración de la actividad del GAFI: balance positivo, pero con deficiencias

La interconexión entre los criptoactivos y el sector financiero tradicional requiere de soluciones normativas que eviten la consolidación de los primeros como instrumentos óptimos para la comisión de delitos como el blanqueo de capitales. La existencia de riesgos no justifica *per se* una política de represión contra los criptoactivos, por lo que el GAFI trata acertadamente de promover la innovación financiera, diseñar un marco de evaluación de riesgos ante ciertas notas técnicas de los criptoactivos como la descentralización o el pseudoanonimato, así como instaurar un régimen legal armonizado que dote a las jurisdicciones de las herramientas básicas frente al criptoblanqueo. Como punto de partida se atribuye pues un balance positivo a la actividad del GAFI, en cuanto da respuesta a los nuevos métodos utilizados para actos de criptoblanqueo como, por ejemplo, el *chain hopping*, el uso de *privacy coins* y el recurso a *mixing services* disponibles en la *Dark Web* que permiten una anonimización plena de las transacciones[214].

Las sucesivas reformas de las directrices del GAFI se estiman positivas por el hecho de que han permitido alcanzar las siguientes dos metas. De un lado, la determinación clara de la naturaleza de los criptoactivos, con la finalidad de aportar una seguridad jurídica que fomente el desarrollo del criptomercado y elimine actitudes cautelosas por parte de los inversores[215]. Y, de otro lado, una convergencia normativa en la regulación del ecosistema cripto que impida el *forum shopping* por parte de los delincuentes[216]. A la consecución de ambos extremos obedece tanto la reforma de la Recomendación n.º 15 en octubre de 2018 como la publicación de la NIR n.º 15 en junio de 2019, que constituyen las dos principales novedades a través de las que se instaura un enfoque global tendente a mitigar los riesgos de criptoblanqueo.

El establecimiento de medidas de registro y licencia para los PSAV es otro de los puntos fuertes de la política preventiva diseñada por el GAFI frente al criptoblanqueo y que, en términos generales, ha dado lugar a un resultado satisfactorio. Con la introducción de esta medida corresponde a los estados conceder licencias o requerir el registro de los PSAV, por lo que se consigue que las jurisdicciones nacionales desarrollen en todo caso un papel proactivo en la PBC/FT. La ausencia del cumplimiento de tales condiciones previas a la actividad debe suponer en todo caso, como reclama el GAFI, la exclusión del mercado de servicios de todas las personas o entidades que operen sin una identificación y aprobación de su estructura por las autoridades nacionales. Ello además deberá acompañarse de sanciones eficaces, proporcionadas y disuasorias.

---

214 Cfr. PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Op. cit.*, p. 6.

215 Cfr. BENSON, V. et al., "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions", *Op. cit.*, p. 46.

216 Cfr. KOUTSOUPIA, V., "Challenges of the Use of Virtual Assets in Money Laundering", *Op. cit.*, p. 73.

La extensión de la *travel rule* a las transacciones criptográficas se considera como otro de los aciertos en la evolución de la normativa contra el criptoblanqueo elaborada por el GAFI. Esta valoración se sustenta en que la aplicación de dicha medida permite combatir el anonimato y la falta de transparencia que se asocian con el ecosistema cripto[217]. No obstante, la virtualidad de esta política carece de eficacia por los frecuentes retrasos en su adopción y cumplimiento. Esta situación negativa, conocida como *sunrise problem*, no resulta desconocida por el GAFI, pues se traduce en un freno a la colaboración en la prevención del criptoblanqueo que deben realizar los PSAV ordenantes y beneficiarios. La *travel rule* supone que las entidades que prestan servicios con criptoactivos deben recopilar información sobre sus clientes, así como conservar y compartir aquella con las autoridades. Sin embargo, estos extremos son difíciles de conseguir por la deficitaria implementación de la travel rule en las jurisdicciones nacionales.

A pesar del balance positivo que se ha realizado sobre la actuación desarrollada por el GAFI contra el criptoblanqueo, el régimen establecido por la citada organización internacional presenta dos grandes deficiencias que lastran el alcance de sus pretensiones.

La primera es la falta de atención a la tecnología operativa en que se fundamentan los criptoactivos. Los esfuerzos normativos del GAFI se concentran en torno a las personas físicas o jurídicas que, en calidad de negocios, utilizan las tecnologías emergentes para prestar servicios relacionados con los criptoactivos. Sin embargo, una plena equiparación de estos últimos con las instituciones financieras tradicionales y la imposición de las mismas obligaciones preventivas en punto al blanqueo de capitales supone no tener en cuenta las particularidades tecnológicas en que se basan los productos criptográficos, especialmente en punto a la TRD. De acuerdo pues con RISTIC[218], el enfoque basado en intermediarios tendría que complementarse con la promoción de un sistema tendente al análisis de la cadena de bloques, ya que con ello se lograría salvar las limitaciones del tratamiento y permitiría disponer de una herramienta preventiva frente al criptoblanqueo.

El segundo de los déficits en la normativa del GAFI es el insuficiente tratamiento de los riesgos de blanqueo de capitales relacionados con las transacciones P2P. El enfoque adoptado en la lucha contra el criptoblanqueo tiene como punto débil la falta de previsión de que, por ejemplo, los usuarios de criptomonedas pueden realizar transacciones P2P u operaciones OTC, "eludiendo así todo el alcance de las medidas KYC"[219] que se imponen a los PSAV. Este extremo diluye la eficacia de la política de prevención de criptoblanqueo instaurada por el GAFI que, si bien reconoce

217 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 135.

218 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 135.

219 *Ibidem*.

mismamente el crecimiento de las operaciones sobre bases desintermediadas, se limita sin embargo a sugerir a las jurisdicciones nacionales que traten de supervisar este ámbito y recopilen el mayor conjunto de datos a efectos de mitigar los riesgos existentes.

8. LA IMPLEMENTACIÓN DE LAS MEDIDAS DEL GAFI EN ESTADOS UNIDOS Y LA UE

La normativa del GAFI frente al criptoblanqueo ha tenido una repercusión relevante en primer lugar en los Estados Unidos. La Oficina de Control de Delitos Financieros (en adelante, FinCEN, como acrónimo de *Financial Crimes Enforcement Network*), publicó el 9 de mayo de 2019 el documento "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies", complementado con el texto "Advisory on Illicit Activity Involving Convertible Virtual Currency". En ambos se enuncia que las monedas virtuales convertibles constituyen alternativas a los sistemas tradicionales de pago y transmisión de dinero, al igual que están siendo explotadas para un uso criminal. Ello se debe a la naturaleza global, transparencia limitada y velocidad de las transacciones, a lo que se une el desarrollo de nuevos tipos de monedas virtuales con protocolos de anonimato mejorado. Por estas razones, FinCEN puso el foco en la necesidad de las entidades que prestan servicios de monedas virtuales mantengan registros actualizados y cumplan con la obligación de presentar regularmente informes.

A las anteriores declaraciones contenidas en los textos *supra* se añade, como señala GIBBS[220], la propuesta de 27 de octubre de 2020 realizada por FinCEN para el establecimiento de nuevos requisitos en punto al mantenimiento de registros y a la aplicación de normas de viaje. El cambio principal consiste en la reducción del umbral desde los 3.000 USD fijados por la *Bank Secrecy Act* (en adelante, BSA) hasta los 250 USD para las transacciones internacionales, aplicándose ello también a monedas virtuales convertibles y otros activos digitales con estatus de moneda de curso legal (en adelante, LTDA). Otra nueva propuesta de 23 de diciembre de 2020 impone nuevos requisitos para bancos y empresas de servicios monetarios con el fin de que recopilen información sobre los intervinientes en las transacciones con monedas virtuales convertibles o LTDA superiores a 10.000 USD, o que entre ambas superen esta cuantía, e impliquen *unhosted wallets* o monederos alojados en jurisdicciones previamente identificadas por FinCEN.

Los anteriores cambios propuestos se acompañaron de dos nuevas leyes a partir del 1 de enero de 2021[221]. En primer lugar, una nueva Ley de Transparencia Corporativa,

220 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 218.

221 Cfr. HOSSAIN, M. B., "Acquiring an awareness of the latest regulatory developments

que responde a las declaraciones constantes formuladas por el GAFI en punto a que la creación de estructuras corporativas sin identificación de los beneficiarios reales se trata de un vehículo claro para la comisión de actos de blanqueo de capitales. Y, en segundo lugar, una nueva Ley contra el Blanqueo de Capitales (en adelante, AMLA), que forma parte de la Ley de Autorización de Defensa Nacional. Esta novedad formaliza diversas cuestiones que FinCEN venía poniendo de manifiesto anteriormente y refuerza el poder de este organismo sobre los activos digitales, al igual que impone el registro de intercambios y la aplicación de requisitos de información. La nueva AMLA modifica la BSA e incluye la expresión *"*valor que sustituye a la moneda*"*, en aras de incluir en el concepto de instituciones financieras y transmisores de dinero a los negocios relacionados con moneda virtual y activos digitales.

En el ámbito comunitario europeo el criptoblanqueo se aborda especialmente en la Directiva 2018/843, de 30 de mayo, cuyas disposiciones sobre monedas virtuales pretenden obtener la máxima información con el fin de vincular las claves públicas de los participantes en la red con las concretas identidades personales que se esconden tras ellas[222]. La aprobación de la citada directiva obedece a la actividad desarrollada por el GAFI, que ha coadyuvado a que la UE reaccionase normativamente frente a la realidad del criptoblanqueo. Ello se estima pues como un aspecto positivo, por más que la actuación de la UE se haya retrasado en el tiempo[223]; en este sentido, la ABE[224] venía alertando desde años atrás de los riesgos de blanqueo de capitales que se derivaban de la falta de regulación de las monedas virtuales.

A través de la Directiva 2018/843, de 30 de mayo, se incorporaron diversas novedades entre las que destaca, en primer lugar, la determinación como sujetos obligados de los proveedores de servicios de cambio de moneda fiduciaria por moneda virtual y los proveedores de servicios de custodia de monederos electrónicos[225], de modo que deban cumplir con normas de DDC y una serie de obligaciones de información[226]. En el Considerando 8 del Preámbulo de la norma se indica que la no inclusión de los *exchanges* entre los sujetos obligados permite a los grupos terroristas utilizar las monedas virtuales para ingresar dinero ilícito en los cauces financieros de la UE. Esta tesitura sirvió pues para justificar la adición de las plataformas de intercambio como nuevos sujetos obligados, a lo que se añade la concepción de los *exchanges* como método elemental para la conversión de dinero ilícito en criptomonedas.

---

concerning digital assets and anti-money laundering*"*, *Op. cit.*, p. 1264.

222 Cfr. WRONKA, C., *"*Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures*"*, *Op. cit.*, p. 88.

223 Cfr. GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", *Op. cit.*, p. 213.

224 Vid. ABE, *Opinion on Virtual Currencies*, Londres, 2014, pp. 1-46.

225 Cfr. NAVARRO CARDOSO, F., "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", *Op. cit.*, p. 14

226 Cfr. COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *Op. cit.*, p. 235.

Junto a las plataformas de intercambio, otros nuevos sujetos obligados conforme a la Directiva 2018/843, de 30 de mayo, han sido los proveedores de servicios de custodia de monederos electrónicos. Las entidades que prestan tales servicios salvaguardan las claves privadas de sus clientes para mantener, almacenar y transferir criptomonedas. El recurso a estas entidades se trata de una de las opciones que los usuarios de criptomonedas pueden utilizar para almacenar su clave privada. Al igual pues que a los *exchanges*, la directiva asegura la imposición de obligaciones de identificación y verificación de la identidad del cliente y del beneficiario, la naturaleza y propósito de la relación comercial, así como un deber general de cooperación con las autoridades, en aras de que las UIF puedan controlar las operaciones con monedas virtuales e identificar a los titulares de las criptocarteras[227].

Las novedades expuestas se acompañan de la inclusión de la obligación de que los estados miembros impongan un sistema de registro para los nuevos sujetos obligados. La finalidad de esta medida radica en que las autoridades nacionales puedan evaluar las actividades de los sujetos obligados, los mecanismos incorporados por estos para hacer frente a los riesgos a los que se hallan expuestos y la forma de reacción ante ellos[228]. En línea con las directrices de GAFI, la información proporcionada en el registro permite evaluar que las funciones de dirección de las entidades se llevan a cabo por personas idóneas, lo cual debe entenderse con el intento de evitar que un delincuente financiero asuma funciones de control en las entidades.

De lo he expuesto hasta aquí se puede ver que en la Directiva 2018/843, de 30 de mayo, se adoptó la terminología de monedas virtuales, definidas como representaciones digitales de valor, no emitidas ni garantizadas por bancos centrales autoridades, no vinculadas necesariamente a monedas legalmente establecidas, sin estatus de moneda o dinero legal, pero aceptadas por personas físicas o jurídicas como medio de intercambio y que pueden ser transferida, almacenada y negociada electrónicamente[229]. Esta definición supone la exclusión de las CBDC del concepto de monedas virtuales, así como también de los *tokens* de utilidad y de inversión/seguridad en la medida en que el requisito de aceptación por personas físicas o jurídicas como medio de intercambio alude, inequívocamente, a los *tokens* de tipo pago.

La regulación ofrecida en la Directiva 2018/843, de 30 de mayo, se estima en todo caso insuficiente y poco exhaustiva para combatir el fenómeno del criptoblanqueo. La relativa eficacia de las medidas adoptadas se reconoce mismamente en el Considerando 9 de la norma comunitaria, en el que se señala que los usuarios podrán realizar transacciones al margen de los nuevos sujetos obligados[230]. A ello se

227 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti- Money Laundering Framework", *Op. cit.*, p. 205.

228 *Ibidem*.

229 Cfr, art. 1.2 letra d) de la Directiva 2018/843, de 30 de mayo.

230 Cfr. NAVARRO CARDOSO, F., "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", *Op. cit.*, p. 28.

añade que la UE centra su atención en las plataformas de intercambio entre monedas fiduciaria y monedas virtuales por concebirse estas como el paso final en los esquemas de criptoblanqueo. No obstante, ello genera lagunas al dejar fuera a los servicios de intercambio de cripto a cripto[231] que, como anteriormente se expuso, ostentan una clara relevancia en la técnica del *chain hopping* predominante en la fase de estratificación del criptoblanqueo.

La Directiva 2018/843, de 30 de mayo, tampoco centra su atención en los *mixing services* (*tumblers*), que también ocupan un papel fundamental en la segunda fase del criproblanqueo[232]. En la misma medida, la norma comunitaria no hace referencia alguna a las plataformas P2P, que permiten la interacción entre usuarios de criptomonedas y el establecimiento de relaciones comerciales directamente entre sí. Las plataformas P2P se pueden dividir en centralizadas o descentralizadas y, en el caso de las primeras, si debiera haberse exigido la aplicación de los requisitos antiblanqueo mediante su inclusión en la lista de sujetos obligados, ya que el administrador de las plataformas P2P centralizadas ostenta la dirección de la plataforma, supervisa los procesos en curso, ofrece servicios de custodia y desarrolla la función de contacto y responsabilidad en la plataforma[233].

Finalmente, la Directiva 2018/843, de 30 de mayo, propone en el Considerando 9 la introducción de un sistema de registro para que los usuarios de criptomonedas realicen una autodeclaración voluntaria. Esta medida se estima poco efectiva en la medida en que una de las virtualidades de las criptomonedas radica precisamente en el pseudoanonimato que ofrecen a los usuarios. Tamaña característica resulta pues una de las principales atracciones, por lo que se estima que la medida propuesta carece de utilidad[234]. Únicamente podría servir de alternativa un registro obligatorio de usuarios en la medida en que ello permitiría, siguiendo a RISTIC[235], que las autoridades nacionales pudiesen recopilar e intercambiar información acerca de las personas usuarias de criptomonedas, combatiendo así en cierta medida el pseudoanonimato asociado a aquellas.

---

231 Cfr. COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *Op. cit.*, p. 236.

232 Cfr. WRONKA, C., "Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures", *Op. cit.*, p. 86.

233 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework", *Op. cit.*, p. 206.

234 Cfr. COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *Op. cit.*, p. 238.

235 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti- Money Laundering Framework", *Op. cit.*, p. 201.

9. CONCLUSIONES

La proliferación de criptoactivos supone un "cambio de paradigma"[236] en el sector financiero y comercial en la medida en que aquellos permiten la realización de transacciones rápidas, seguras, sin límites fronterizos ni tampoco barreras de entrada, todo ello en un marco operativo y técnico común[237]. Por ello resulta necesario disipar la etiqueta delictiva que ampliamente se atribuye a los criptoactivos[238], aumentar la credibilidad de la población en aquellos y no "obstaculizar innecesariamente la diversidad y el cambio tecnológicos"[239]. La forma de alcanzar tales metas se vincula con el diseño de una regulación a conciencia del ecosistema cripto, ya que un tratamiento uniforme determinará el éxito de una nueva economía basada en productos criptográficos, al igual que contribuirá a que "el sector se convierta en una industria financiera madura"[240].

El diseño de un régimen de PBC/FT en relación con los criptoactivos se presenta como un reto complejo para las instancias internacionales, pero también como una tarea elemental ante el carácter transfronterizo de aquellos. Esta dimensión determina pues que la respuesta legal deba ser de carácter global. De acuerdo con PAVLIDIS[241], consideramos que corresponde al GAFI, como principal organización intergubernamental para la lucha contra el blanqueo de capitales, el diseño de las políticas que permitan vigilar los riesgos asociados a los criptoactivos, sin menoscabar el avance financiero que representan. La actuación del GAFI se estima crucial en la pretensión de dotar de legitimidad al ecosistema cripto e incrementar la confianza en él[242], si bien la eficacia de su respuesta se condiciona a una efectiva aplicación de las medidas publicadas a nivel nacional.

Para la consecución de los anteriores objetivos, el GAFI participa en los últimos años en los foros mundiales de máxima transcendencia política y económica, como los realizados en el seno del G20[243]. En las últimas cumbres se manifiesta como una

---

236 WRONKA, C., "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight", *Op. cit.*, p. 85.

237 *Ibidem*.

238 Cfr. RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti- Money Laundering Framework", *Op. cit.*, p. 215.

239 WRONKA, C., "Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures", *Op. cit.*, p. 90.

240 WRONKA, C., "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight", *Op. cit.*, p. 86.

241 Cfr. PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Op. cit.*, p. 3.

242 Cfr. KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", *Op. cit.*, p. 135.

243 Cfr. KOUTSOUPIA, V., "Challenges of the Use of Virtual Assets in Money Laundering", *Op. cit.*, p. 71.

constante que la aplicación de la innovación en el sector financiero reporta ventajas indiscutibles para la economía en general, si bien ello debe acompañarse de una atención a los riesgos que presentan los AV para la estabilidad financiera mundial[244]. A estos extremos responden las principales iniciativas adoptadas por el GAFI, debiéndose mencionar especialmente la modificación de la Recomendación n.º 15, la publicación de la NIR n.º 15 y la incorporación de los conceptos de AV y PSAV en el Glosario del GAFI. El G20 ha declarado expresamente su compromiso de acoger las novedades normativas realizadas por el GAFI, hasta el punto de calificarlas como avance transcendental[245].

La principal virtualidad de las disposiciones sobre AV y PSAV elaboradas por el GAFI radica en que son objeto de continuo examen en las rondas de evaluaciones mutuas. Este extremo determina, al igual que sucede en general con el conjunto de estándares normativos confeccionados por la citada organización intergubernamental, una amplia acogida por los estados en términos generales, a pesar de constituir normas pertenecientes a la categoría de *soft law*. El éxito del GAFI en el cumplimiento de sus directrices a través de la inclusión de los países no cooperantes en las listas negras/grises refuerza la definición de dicha organización como la mejor instancia para la elaboración de un marco jurídico base para la prevención del criptoblanqueo, pues aquel resulta luego seguido ampliamente por las iniciativas nacionales en la materia

10. BIBLIOGRAFÍA

ABE, *Opinion on Virtual Currencies, Londres*, 2014.

ABEL SOUTO, M., "La comisión del delito de blanqueo de dinero mediante las nuevas tecnologías y la internacionalización del Derecho penal", en *VIII Congreso Internacional sobre prevención y represión del blanqueo de dinero*, (coords. Abel Souto, M.; Lorenzo Salgado, J. M.; y Sánchez Stewart, N.), Valencia, Tirant lo Blanch, 2022, 1.ª ed., pp. 501-528.

ALMEIDA, H.; PINTO, P. y VILAS, A., "A review on cryptocurrency transaction methods for money laundering", en *Proceedings of the 5th International Conference on Finance, Economics, Management and IT Business*, (eds. Arami, M.; Baudier, P. y Chang, V.), Setúbal, Science and Technology Publications, 2023, 1.ª ed., pp. 114-121. https://doi.org/10.5220/0011993300003494

BENSON, V. et al., "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions", *European Journal of Law and Economics*, 57, 2024, pp. 37–61. https://doi.org/10.1007/s10657-024-09797-w

244 Cfr. PONAMORENKO, V. E., "International Organizations' Approaches to Digital Assets Legalization (Monetary Policy and AML/CFT)", *Op. cit.*, p. 120.

245 *Ibidem.*

BRAMESHUMMER, G. y EDELMANN, B., "Einführung, Krypto 1x1 für Strafrechtler", en *Finanzstrafrecht 2022: Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht*, (eds. Leitner, R. y Brandl, R.), Viena, Linde Verlag, 2023, 1.ª ed., pp. 1-12

BRANDL, R. y BÜLTE, J., "Kryptowährungen/-assets-Geldwäsche und Terrorismusbekämpfung-Perspektive Sorgfaltsverpflichtete", en *Finanzstrafrecht 2022: Virtuelle Währungen und Kryptoassets im Steuer(straf) recht und Strafrecht*, (eds. Leitner, R. y Brandl, R.), Viena, Linde Verlag, 2023, 1.ª ed., pp. 105-123.

CALAFOS, M. W. y DIMITOGLOU, G., "Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency", en *Principles and Practice of Blockchains*, (eds. Daimi, K.; Dionysiou, I. y El Madhoun, N.), Cham, Springer, 2023, 1.ª ed., pp. 271-294. https://doi.org/10.1007/978-3-031-10507-4_12

CHASIN VELKES, G., "International Anti-Money Laundering Regulation of Virtual Currencies and Assets", *New York University Journal of International Law and Politics*, 52, 2020, pp. 875-905.

COVOLO, V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", *European Journal of Crime, Criminal Law and Criminal Justice*, 28(3), 2020, pp. 217-251. https://doi.org/10.1163/15718174-bja10003

DE KOKER, L. et al., "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", en *Financial Technology and the Law*, (eds. Goldbarsht, D. y de Koker, L.), Cham, Springer, 2022, pp. 151-183. https://doi.org/10.1007/978-3-030-88036-1_7

DESMOND, D. B., LACEY, D. y SALMON, P., "Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review", *Journal of Money Laundering Control*, 22(3), 2019, pp. 480-497. https://doi.org/10.1108/JMLC-10-2018-0063.

Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE, DOUE, 156, 19 de junio de 2018.

DUPUIS, D. y GLEASON, K., "Money laundering with cryptocurrency: open doors and the regulatory dialectic", *Journal of Financial Crime*, 28(1), 2020, pp. 60-74. https://doi.org/10.1108/JFC-06-2020-0113

FATF, *12-month Review Virtual Assets and VASPs*, Paris, 2020. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html

FATF, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, Paris, 2020. https://www.fatf-gafi.org/en/publications/Virtualassets/Report-g20-so-called-stablecoins-june-2020.html

FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Paris, 2019. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html

FATF, *Guidance for a risk-based approach virtual currencies*, Paris, 2015. https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-rba-virtual-currencies.html

FATF, *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*, Paris, 2020. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

FATF, *Second 12-month Review Virtual Assets and VASPs*, Paris, 2021. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Second-12-month-review-virtual-assets-vasps.html

FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*, Paris, 2022. https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html

FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*, Paris, 2023. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html

FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*, Paris, 2024. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Paris, 2021. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

FATF, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, Paris, 2014. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html

FROMBERGER, M. y ZIMMERMANN, P., "Technische und wirtschaftliche Grundlagen", en *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings*, (eds. Maume, P., Maute, L. y Fromberger, M.), Munich, Verlag C.H. Beck, 2020, 1.ª ed., pp. 1-64.

GIBBS, T., "Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US", en *Cyber Laundering: International Policies and Practices*, (ed. Rébé, N.), Singapur, World Scientific Publishing, 2023, 1.ª ed., pp. 197-233. https://doi.org/10.1142/9781800612839_0008

HAFFKE, L., FROMBERGER, M. y ZIMMERMANN, P., "Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them", *Journal Bank Regulation*, 21, 2020, pp. 125–138. https://doi.org/10.1057/s41261-019-00101-4

HOSSAIN, M. B., "Acquiring an awareness of the latest regulatory developments concerning digital assets and anti-money laundering", *Journal of Money Laundering Control*, 26(6), 2023, pp. 1261-1268. https://doi.org/10.1108/JMLC-10-2022-0147

KAPSIS, I., "Crypto-assets and criminality. A critical review focusing on money laundering and terrorism financing", en *Organised Crime, Financial Crime and Criminal Justice*, (eds. Jasinski, D.; Phillips, A.; y Johnston E.), Londres, Routledge, 2023, 1.ª ed., pp. 122-141. https://doi.org/10.4324/9781003020813-8

KOUTSOUPIA, V., "Challenges of the Use of Virtual Assets in Money Laundering", *Nordic Journal of European Law*, 6(4), 2023, pp. 53-78. https://doi.org/10.36969/njel.v6i4.25919

MEIER, M., *Geldwäsche-Compliance für Kryptowerte, Jenaer Wissenschaftliche Verlagsgesellschaft*, Jena, 1.ª ed., 2022.

MPF (Ministerio Público Fiscal de la Nación), *Guía práctica para la identificación, trazabilidad e incautación de criptoactivos. Consideraciones teórico-prácticas sobre activos virtuales basados en la tecnología de cadena de bloques y su investigación penal*, Buenos, Aires, 2023.

NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. https://bitcoin.org/en/bitcoin-paper

NAVARRO CARDOSO, F., "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", *Revista electrónica de ciencia penal y criminología*, 21(14), 2019, pp. 1-45. http://criminet.ugr.es/recpc/21/recpc21-14.pdf

NAZZARI, M., "From payday to payoff: Exploring the money laundering strategies of cybercriminals", *Trends in Organized Crime*, 1, 2023, pp. 1-18. https://doi.org/10.1007/s12117-023-09505-1

PAESANO, F., "Following the Virtual Money: Investigating Crypto-Based Money Laundering and Confiscating Virtual Assets", en *Cryptocurrency Concepts, Technology, and Applications*, (ed. Liebowitz, J.), Londres, CRC Press, 2023, 1.ª ed., pp. 119-139.

PALPACUER, J. y AOUIZERAT, B., "Anti-Cyber Laundering: The Inclusion of Virtual Asset Service Providers", en *Cyber Laundering: International Policies and Practices*, (ed. Rébé, N.), Singapur, World Scientific Publishing, 2023, 1.ª ed., pp. 261-280. https://doi.org/10.1142/9781800612839_0010

PAVLIDIS, G., "International regulation of virtual assets under FATF's new standards", *Journal of Investment Compliance*, 21(1), 2020, pp. 1-8. https://doi.

org/10.1108/JOIC-08-2019-0051

PONAMORENKO, V. E., "International Organizations' Approaches to Digital Assets Legalization (Monetary Policy and AML/CFT)", en *Engineering Economics: Decisions and Solutions from Eurasian Perspective. Lecture Notes in Networks and Systems,* (eds. Ashmarina, S.; Mantulenko, V.; y Vochozka, M.), Cham, Springer, 2021, 1.ª ed., pp. 112-121. https://doi.org/10.1007/978-3-030-53277-2_13

RAYMAEKERS, W., "Cryptocurrency Bitcoin: Disruption, challenges and opportunities", *Journal of Payments Strategy & Systems*, 9(1), 2015, pp. 30-46.

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, DOUE, 150, 9 de junio de 2023.

RISTIC, P., "Cryptocurrency Money Laundering: A New Challenge for the European Anti- Money Laundering Framework", *ZEuS Zeitschrift für Europarechtliche Studien*, 24(2), 2023, pp. 189-218. https://doi.org/10.5771/1435-439X-2023-2-189

TROZZE, A., "Cryptocurrency Crime", en *Cryptocurrency Concepts, Technology, and Applications*, (ed. Liebowitz, J.), Londres, CRC Press, 2023, pp. 93-118

WANG, H-M. y HSIEH, M-L., "Cryptocurrency is new vogue: a reflection on money laundering prevention", *Security Journal*, 37, 2024, pp. 25–46. https://doi.org/10.1057/s41284-023-00366-5

WRONKA, C., "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight", *Journal of Banking Regulation*, 25(1), 2024, pp. 84–93. https://doi.org/10.1057/s41261-023-00217-8

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

WRONKA, C., «"Cyber-laundering": the change of money laundering in the digital age», *Journal of Money Laundering Control*, 25(2), 2022, pp. 330-344. https://doi.org/10.1108/JMLC-04-2021-0035