UNIVERSIDAD DE SALAMANCA

FACULTAD DE DERECHO

DOCTORADO EN ESTADO DE DERECHO Y GOBERNANZA GLOBAL

TESIS DOCTORAL

LAVADO DE ACTIVOS MEDIANTE LA UTILIZACIÓN DE CRIPTOACTIVOS

AUTOR: GERARDO LUIS LAMAS SUAREZ

TUTORA: PRO. DRA. LAURA ZUÑIGA RODRIGUEZ

SALAMANCA, 2023

AGRADECIMIENTOS

La presente tesis doctoral ha sido lograda gracias al apoyo que recibido por parte de valiosas personas. En primer término, de mi tutora de tesis doctoral, la Dra. Laura Zúñiga Rodríguez, por haber asumido la dirección de este proyecto de tesis doctoral y haberme dado todo el soporte académico y motivacional para llevar adelante una investigación que han significado tres años de arduo esfuerzo. Asimismo, agradezco a mi familia y en especial a mi padre Luis Lamas Puccio, el mayor referente que me pudo dar la vida para seguir el camino de la abogacía y la investigación jurídica. Por último, agradezco a la Universidad de Salamanca por permitirme seguir mis estudios doctorales en su institución y de esa forma lograr el máximo anhelo académico al que puede aspirar un abogado en la carrera de derecho.

ÍNDICE

AGRADECIMIENTOS.....8

INTRODUCCIÓN.....9

CAPÍTULO I

LAVADO DE ACTIVOS A PARTIR DE LA UTILIZACIÓN DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

I. CONSIDERACIONES GENERALES POLÍTICO-CRIMINALES CON RELACIÓN CON EL FACTOR TECNOLÓGICO.....18

II. EL FENÓMENO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC).....25

III. LAS CARACTERÍSTICAS DE LAS TIC.....28

1. Inmaterialidad.....28

2. Interactividad.....29

3. Interconexión.....29

4. Instantaneidad.....29

5. Digitalización.....30

6. Penetración en todos los sectores.....30

7. Innovación.....30

IV. EL CIBERESPACIO, UN *GLOBAL COMMON*.....30

1. La transnacionalidad.....35

2. La neutralidad de la red.....36

3. La virtualidad.....38

4. La falta de territorialidad.....40

V. DERECHO PENAL Y TIC.....41

V. CIBERCRIMINALIDAD.....44

VI. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS SEGÚN TEMPERINI.....49

1. Los delitos de cuello blanco.....49

2. Transnacionales.....49

3. Instantáneos.....50

4. Masivos.....50

5. Anonimato.....50

6. Pluriofensivos.....51

7. Investigación compleja.....51

VII. CLASIFICACIÓN DE LOS CIBERCRÍMENES SEGÚN MIRÓ LLINARES.....51

1. Los cibercrímenes económicos.....51

2. Los cibercrímenes sociales **52**
3. Los cibercrímenes políticos **53**
VIII. LAVADO DE ACTIVOS Y EL CIBERESPACIO **53**
IX. GRUPO DE ACCIÓN FINANCIERA Y LAS NUEVAS TECNOLOGÍAS **59**
1. La recomendación n.º 13: Banca corresponsal **59**
2. La recomendación n.º 15: Nuevas tecnologías **60**
3. *Report of New Payment Methods* **62**
4. *Money Laundering Using New Payment Methods* **62**
5. *Guidance for a risk-based approach prepaid cards, mobile payments and Internet-Based Payment Services* **63**
X. CRIMINALIDAD ORGANIZADA Y TIC **64**

CAPÍTULO II

CONSIDERACIONES GENERALES RELATIVAS A LOS CRIPTOACTIVOS Y AL *BITCOIN*

I. DEFINICIONES TERMINOLÓGICAS EN RELACIÓN CON EL DINERO Y LOS CRIPTOACTIVOS **67**
1. Dinero **68**
2. Criptoactivos **68**
3. Monedas virtuales centralizadas **70**
4. Monedas virtuales descentralizadas **71**
5. Esquemas cerrados de moneda virtual **71**
6. Esquemas de moneda virtual con flujo unidireccionaL **72**
7. *Altacoins* **73**
8. *Stablecoins* **73**
9. *Tokens* de pago **73**
10. *Tokens* de activos **74**
11. *Tokens* de utilidad **74**
12. *Tokens* no fungibles (NFT) **74**
II. OTROS CONCEPTOS RELEVANTES EN EL ENTORNO DE LOS CRIPTOACTIVOS **75**
1. intercambio de moneda virtual (IMV) o Intercambiador (*exchanger*) **75**
2. Administrador **75**
3. Minero **75**
4. Criptografía **76**
5. Billeteras o monederos virtuales **76**
6. Monederos *online* **76**
7. Monederos instalados en dispositivos móviles **77**
8. Monederos físicos **77**
9. Monederos fríos **77**

10. Monederos calientes **78**
11. Monederos de papel (*paper wallets*) **78**
12. Monederos de firma múltiple (*multi-signature wallets*) **78**
13. Monederas controladas por el Estado **79**
14. Árboles de Merkle **79**
15. Contratos inteligentes (*smart contracts*) **79**
16. DeFi (finanzas descentralizadas) **80**
17. Agentes centralizados (CEX) **80**
18. Agentes descentralizados (DEX) **81**
19. Dirección de criptoactivos **81**
20. Oferta inicial de moneda (ICO) **81**
III. EL *BITCOIN*, SUS ELEMENTOS Y FUNCIONAMIENTO **82**
1. Concepto de *bitcoin* **87**
2. Protocolo *bitcoin* **88**
3. *Bitcoin core* **88**
4. Nodos **89**
5. Las transacciones **89**
6. Funcionamiento de la cadena de bloques en *bitcoin* **91**
7. Función de *hash* **92**
8. Firma digital **94**
9. La prueba de trabajo *proof of work* **95**
10. La red **96**
11. La minería *bitcoin* **96**
12. P2P o punto a punto **98**
13. Privacidad **99**
12. Volatilidad **100**
14. La falta de territorialidad **102**
15. La falta de intermediarios **103**
16. Criptografía **103**
17. La falta de regulación del *bitcoin* en el sistema financiero **104**
18. El *bitcoin* en El Salvador **105**
19. El *bitcoin* en República Centroafricana (RCA) **110**
20. BitLicence **110**
21. Cajero automático de *bitcoin* **111**
22. Algunas reflexiones entorno a los conceptos señalados **112**
IV. OTROS CRIPTOACTIVOS DE RELEVANCIA **112**
1. *Ethereum* **113**
2. *Solana* **115**
3. *Cardano* **116**
4. *Polkadot* **118**

5. *Decentraland* **119**

V. PROPUESTA DEL REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVO A LOS MERCADOS DE CRIPTOACTIVOS Y POR EL QUE SE MODIFICA LA DIRECTIVA (UE) 2019/1937 (MICA) **120**

1. Ficha de servicio (*utility tokens*) **123**

2. Ficha referenciada a activos (*asset-referenced tokens*) **125**

3. Ficha de dinero electrónico (*electronic money tokens*) **126**

4. Proveedores de servicios de criptoactivos según la propuesta MICA **127**

5. Otros puntos relevantes a tener en cuenta en la propuesta MICA **127**

VI. COMITÉ DE BASILEA: "UN TRATAMIENTO PRUDENCIAL DE LA EXPOSICIÓN DE CRIPTOACTIVOS" **128**

1. Mismo riesgo, misma actividad, mismo tratamiento **129**

2. Sencillez **129**

3. Estándares mínimos **129**

VII. ALGUNAS REGULACIONES DE LOS CRIPTOACTIVOS EN AMÉRICA **132**

1. Estados Unidos **132**

2. Perú **134**

3. Colombia **137**

4. Argentina **138**

CAPÍTULO III

LAVADO DE ACTIVOS Y CRIPTOACTIVOS

I. LAVADO DE ACTIVOS MEDIANTE CRIPTOACTIVOS **140**

II. EL DELITO PREVIO EN EL LAVADO DE ACTIVOS MEDIANTE CRIPTOACTIVOS **141**

III. DELITOS FUENTE GENERADORES DE GANANCIAS ILÍCITAS EN CRIPTOACTIVOS **144**

1. *Hacking* **145**

2. Ciberexotorsion **145**

3. Estafa **145**

4. *Cryptojacking* **146**

5. *Illegal Cryptomarkets* **147**

IV. POLÍTICA CRIMINAL PREVENTIVA EN RELACIÓN CON LOS CRIPTOACTIVOS **149**

V. LA DIRECTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO Y DEL CONSEJO **150**

VI. LOS CRIPTOACTIVOS COMO OBJETO DEL DELITO DE LAVADO DE ACTIVOS **157**

VII. CARACTERÍSTICAS QUE HACEN A LOS CRIPTOACTIVOS ÚTILES PARA EL LAVADO DE ACTIVOS **162**

1. Fácil acceso **162**

2. Descentralización **164**

3. Red entre pares (*peer-to-peer*) **165**

4. Coste cero en las transacciones **165**

5. Transnacionalidad en las transacciones **165**

6. Anonimato **166**

7. Falta de regulación **166**

8. *Tokens* no fungibles (NTF) **167**

9. Irreversibilidad de las operaciones **168**

VIII. FASES DEL LAVADO Y CRIPTOACTIVOS 169

1. Colocación de criptoactivos **169**

a) Plataforma de cambio **169**
b) Vendedores locales **170**
c) Cajeros automáticos BTC **170**
d) Tarjetas *bitcoin* **170**
e) Minería **170**

2. Ensombrecimiento de criptoactivos **171**

3. Integración de criptoactivos **171**

IX. EL DECRETO LEGISLATIVO N.° 1106 Y LOS CRIPTOACTIVOS 172

1. Los actos de conversión y transferencia **173**

2. Actos de ocultamiento y tenencia **174**

3. Actos de transporte, traslado, ingreso o salida por territorio nacional de dinero o títulos valores de origen ilícito **175**

X. DECOMISO E INCAUTACIÓN DE CRIPTOACTIVOS 176

1. Fase de localización **177**

2. La clave pública **178**

3. La clave privada **180**

XI. CASOS INTERNACIONALES RELEVANTES EN MATERIA PENAL SOBRE CRIPTOACTIVOS 181

1. *United States of America v. Ross William Ulbricht,* No. 15-1815-cr (2D Cir. May 31, 2017) **181**

2. STS 326/2019 - Tribunal Supremo en lo Penal **185**

CAPÍTULO IV

PREVENCIÓN DE LAVADO DE ACTIVOS Y CRIPTOACTIVOS

I. SISTEMA DE GESTIÓN DE PREVENCIÓN DE LAVADO DE ACTIVOS PARA PLATAFORMAS DE INTERCAMBIO DE CRIPTOACTIVOS 187

II. RECOMENDACIONES DEL GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE PREVENCIÓN DE LAVADO DE ACTIVOS PARA INTERCAMBIADORES DE CRIPTOACTIVOS 189

1. *Monedas virtuales: Definiciones claves y riesgos potenciales de LA/FT* **190**

2. *Directrices para un Enfoque Basado en Riesgo. Monedas Virtuales* **191**

3. *Ejercicio Bienal de Tipologías Regionales: Casos y tipologías regionales 2017-2018* **193**

4. Nota interpretativa de la recomendación N.º 15 ..... **195**

5. Indicadores de bandera roja de activos virtuales de lavado de dinero y financiamiento del terrorismo. **197**

6. Guía de activos virtuales y proveedores de servicios de activos virtuales **.....201**

7. Actualización dirigida en implementación de estándares del GAFI sobre virtual activos y activo virtual proveedores de servicio *(travel rule*) **.....207**

III. IMPLEMENTACIÓN DE UN SISTEMA DE TRAZABILIDAD DE OPERACIONES EN CRIPTOACTIVOS PARA LA PREVENCIÓN DE LAVADO DE ACTIVOS.....210

IV. LOS SUJETOS OBLIGADOS EN LAS OPERACIONES CON CRIPTOACTIVOS.....211

CAPÍTULO V

PROPUESTA DE *LEGE FERENDA*

I. Decreto Legislativo N.° 1106.....215

CONCLUSIONES **.....218**

BIBLIOGRAFÍA**.....222**

INTRODUCCIÓN

Con la irrupción en el mundo global de las nuevas tecnologías de la información y de la comunicación, más conocidas por sus siglas como (TIC), se viene propiciando un intenso proceso de digitalización en la sociedad, que va teniendo grandes proyecciones en distintos estamentos y ámbitos de la vida humana cotidiana, tanto en términos individuales como colectivos, sociales, societarios, mercantiles y de distinta índole, como es el aspecto legal o jurídico[1]. Además, está la reciente aparición de las *fintech,* que son empresas innovadoras que están emergiendo de a pocos en el sector financiero y ofrecen nuevas soluciones utilizando como soporte las nuevas tecnologías, que afectan todos los métodos tradicionales de pago mediante la banca, como es el caso concreto de los criptoactivos.

Bajo estos alcances de orden tecnológico, el derecho como ciencia eminentemente reguladora del comportamiento humano, no se mantiene al margen de este proceso de evolución y transformaciones, los cuales han permitido entablar relaciones jurídicas de distinta índole entre las personas y estos a su vez con el Estado, que hasta hace años eran menos que impensables.

El fenómeno de la globalización ha supuesto innumerables cambios en la vida social, económica y política de los pueblos, se han acortado distancias, por lo que el mundo entero vive en un mercado denominado *la sociedad de la información*[2]. De igual forma, en el ámbito criminal organizativo local y transnacional, la delincuencia tradicional ha tenido que reinventarse y adaptarse a esta transformación digital de la sociedad moderna[3]. Muy acertada es la

---

[1] LAMAS SUÁREZ, Gerardo, "El Derecho Penal y Procesal Penal en la nueva sociedad digital en el Perú", en *Peruweek.pe*, Lima: 2020. Disponible en: <https://www.peruweek.pe/tag/gerardo-luis-lamas-suarez/>.

[2] ZÚÑIGA RODRÍGUEZ, Laura, *Criminalidad de empresa y criminalidad organizada*, Lima: Jurista Editores, 2013, p. 566.

[3] GRANADOS ROMERO, Sonia, "La influencia de las nuevas tecnologías en el crimen organizado", en *Propuestas Penales Nuevos Retos y Modernas Tecnologías. Memorias del IV Congreso de Jóvenes Investigadores de Ciencias Penales*, Salamanca: Ed. Universidad de Salamanca, 2016, pp. 67 y 68.

opinión de ROMERO GRANADO cuando refiere que, en tiempos de perturbación política y económica, la criminalidad organizada se fortalece y expande, disminuyéndose los controles que permiten el rastreo de los beneficios de origen delictivo[4].

El socialismo tradicional ha sido desplazado por el modelo libre mercado, sumado al desarrollo de la tecnología, con mayor énfasis en las telecomunicaciones, lo cual ha facilitado el movimiento de capitales, bienes y servicios a través del comercio virtual internacional; sin embargo, estas innovaciones tecnológicas también han permitido y han potenciado el blanqueo de capitales[5].

Los tipos penales clásicos contra el patrimonio se han modernizado en cuanto al *modus operandi* para su perpetración y consumación, ya que en la actualidad el patrimonio dinerario se encuentra almacenado en su gran mayoría en soportes electrónicos. Similar situación ocurre con la información de carácter sensible; es decir, han aparecido nuevas conductas delictivas asociadas estrechamente al uso de las nuevas tecnologías.

Este nuevo fenómeno criminógeno se ha visto enmarcado dentro de lo que se denomina *cibercriminalidad*, que, a diferencia de la delincuencia tradicional, es un tipo de criminalidad especial, que se configura a través de medios informáticos y telemáticos[6]. Esta denominación, que cada vez viene siendo utilizada con mayor afluencia por las legislaciones penales en el mundo, se trata, pues, de una forma de criminalidad desarrollada a partir del elevado uso de tecnología informática[7].

---

[4] *Ibid.*, p. 68

[5] *Idem*.

[6] FERNÁNDEZ BERMEJO, Daniel y MARTÍNEZ ATIENZA, Gorgonio, *Ciberseguridad, ciberespacio y ciberdelincuencia*, Pamplona: Editorial Aranzandi, 2018, p. 116.

[7] VILLAVICENCIO, Felipe, "Delitos Informáticos", en *IUS ET VERITAS,* vol. 24, n.º 49, 2014, pp. 284-304. Disponible en: <https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630>.

Concretamente, hablo del ciberlavado de activos mediante la utilización de criptoactivos, construcción dogmática penal poco desarrollada por la doctrina y la jurisprudencia en el mundo.

El fenómeno delictivo del lavado de activos ofrece a las organizaciones criminales un abanico de posibilidades para poder camuflar las ganancias ilícitas obtenidas en actividades criminales. Esta compleja forma de criminalidad se caracteriza por tratarse de operaciones encubiertas, que cada vez son más sofisticadas, y le permiten al agente del delito poder disfrazar sus ganancias ilícitas para legitimarlas en el sistema económico tradicional. Es bajo este escenario de operaciones con fines de blanqueo que los Estados han venido consolidando de forma bastante satisfactoria la represión criminal contra el blanqueo. Básicamente se han manejado dos líneas de acción en materia de control y prevención de actos vinculados al blanqueo: la primera, de índole administrativa, vinculada a las operaciones o movimiento de dinero, a través del sistema financiero tradicional; y la segunda, vinculada al transporte o movilización de activos sucios de origen ilícito de forma física.

En ese contexto, la moneda tradicional, conocida como un activo financiero que sirve como medio de pago, reserva de valor y unidad de cuenta, está empezando a ser reemplazada por representaciones digitales que se crean y operan al margen del sistema financiero y monetario tradicional, sin ningún organismo central que funja de emisor y supervisor frente a este tipo de transacciones. Lo curioso radica en que esta creación tecnológica está siendo respaldada por un sector de la población mundial de pensamiento liberatorio conformado en su mayoría por ciberactivistas, donde el objetivo primordial estaría enfocado en salir de ese control liderado por los intermediarios financieros tradicionales conocidos como los bancos. Se trata de un *software* libre basado en distintos mecanismos tecnológicos para la emisión de activos virtuales y un sistema de protección de las transacciones entre los usuarios del mismo sistema.

A esta nueva fenomenología digital se le conoce como los criptoactivos o monedas virtuales. Como toda innovación tecnológica, los criptoactivos también han generado un impacto en lo económico, en algunos casos positivos y en otros

negativos, dependiendo del valor que le atribuyan los actores sociales implicados, como son las personas naturales, las entidades financieras y gubernamentales. Una de las mayores críticas que recibe este medio de pago sustituto del dinero tradicional es la falta de un aval estatal que garantice su valor, así como la ausencia de una entidad que controle su producción y distribución y comercialización. Al tratarse de un modo de pago bastante dinámico, es que ha generado gran aceptación por un grupo importante de la comunidad mundial, y por esa razón es que los criptoactivos ya hace algunos años vienen llamando la atención por parte de algunos organismos internacionales, como es el caso del Grupo de Acción Financiera Internacional (GAFI), el U.S Securities and Exchange Comisión, el Department of the Treasury Financial Crimes Enforcement Networt, la United Office on Drugs and Crime, el Banco Central Europeo, el Parlamento Europeo y el Consejo de la Unión Europea, el European Banking Authority, entre otros.

Recientemente, en el año 2019, el Grupo de Acción Financiera Internacional ha emitido un documento-guía denominado *Guidance for a risk-based approach to virtual assets and virtual asset service providers*, en el que se describe la necesidad de que los países en los que operan proveedores de monedas virtuales tomen las medidas preventivas suficientes, para poder hacerle frente a su uso potencial e instrumentalización para el blanqueo de capitales y otras actividades criminales.

1. Importancia y motivos de la elección del tema

Constituye razón suficiente para llevar a cabo la presente investigación, la entrada en vigor de la Directiva (UE) 2018/843, la cual modifica la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, regulación que es considerada como el principal instrumento jurídico en prevención de la utilización del sistema financiero de la Unión Europea para el blanqueo de capitales y la financiación del terrorismo. La problemática principal que aborda la Directiva se enfoca en los proveedores de servicios de cambios de monedas virtuales por monedas fiduciarias, ya que estos no estaban siendo obligados por la Unión Europea a reportar operaciones sospechosas, como producto del intercambio de

criptoactivos por dinero fíat, situación que puede ser capitalizada para la realización de actos constitutivos del blanqueo de capitales y otras formas de criminalidad.

Además, está lo referido al anonimato del que se revisten los adquirentes de los criptoactivos, que también es un elemento esencial en el funcionamiento y operatividad de estos, ya que los usuarios pueden realizar infinidad de transacciones dentro del mismo sistema, sin que estas operaciones puedan ser supervisadas o vigiladas por un organismo central. En el caso de España, ya se están dando algunos avances significativos, a través de las consultas vinculantes emitidas por la Secretaría de Estado de Hacienda, con respecto a la regulación de las monedas virtuales. En el ámbito penal jurisdiccional, se han emitido autos y sentencias judiciales, además de los distintos informes efectuados por entidades europeas, donde se empieza a vislumbrar este nuevo escenario delictivo particularmente complejo. Además de lo señalado, en España ya está en trámite la transposición de la Quinta Directiva, mediante el Anteproyecto de Ley propuesto por el Ministerio de asunto Económicos y Transformación Digital.

2. Objetivos

Nuestro objetivo es realizar un análisis del fenómeno de las criptomonedas, y su potencial uso para el blanqueo de capitales. Para un mejor entendimiento de este fenómeno, analizaremos el ciberespacio y sus elementos, para luego adentrarnos en el fenómeno de las criptomonedas desde una perspectiva del derecho y las ciencias criminológicas. Actualmente, existen en el cibermercado una gran variedad de criptomonedas, por lo que hemos decidido centrar nuestros objetivos principales a partir del análisis de la criptomoneda denominada como *bitcoin*, ya que en la actualidad es la moneda virtual que tienen mayor repercusión social, por lo que, para un mejor entendimiento de esta problemática, explicaré sus antecedentes, estructura, funcionamiento, elementos y naturaleza jurídica. A nivel político criminal, buscaré establecer cuáles deberían ser los lineamientos de control estatal que se deberían asumir frente a la utilización de criptomonedas con una finalidad delictiva, a partir de las directivas emitidas por la Unión Europea y los distintos informes y pronunciamientos. Sumado a ello,

haré un análisis jurisprudencial de las resoluciones en materia penal, que se han venido emitiendo en España en relación con las criptomonedas. Por último, analizaremos desde el ámbito dogmático penal los elementos del tipo penal delito de blanqueo de capitales, con el objetivo de establecer el objeto material del delito a partir de los actos de blanqueo con criptomonedas.

3. Metodología

La presente investigación doctoral emplea el método descriptivo, analítico, dogmático-interpretativo y sistemático, mediante la utilización de recursos de las nuevas tecnologías, el derecho comparado y la metodología deductiva-inductiva. Es descriptivo, porque parte de la constatación empírica acerca de la frecuencia y problemática social-jurídica de la comisión del delito de blanqueo de capitales a través del uso de criptomonedas, que están siendo empleadas por la criminalidad organizada y delincuencia común. Para tal efecto, se describirá el estado actual de la discusión en la cual se sitúa la normativa vigente y jurisprudencial en materia de criptomonedas, que constituye la fuente principal de la decisión global por implementar medidas represivas al fenómeno del blanqueo de capitales. Es analítico, porque cada elemento de la realidad, como lo son los múltiples casos de blanqueo de capitales a través del uso de criptomonedas, que serán evaluados en la presente investigación, así como la diversa normativa aplicable a los Estados español y americano, acerca de la tipicidad de este fenómeno criminal, tendrán como punto de partida una desmembración particular que permitirá su estudio intensivo. Es dogmático penal, porque analizaremos los distintos elementos del tipo penal del delito de lavado de activos regulado mediante el Decreto Legislativo N° 1106 Decreto Legislativo de Lucha Eficaz contra el Lavado de Activos y otros Delitos Relacionados a la Minería Ilegal y cómo se subsumen bajo la modalidad del lavado mediante criptoactivos.

4. Sistemática

La investigación propuesta tiene un contenido sistemático. Si bien en los dos primeros capítulos se pondrá de relieve el problema criminológico y político criminal del lavado de activos a la luz de la normativa internacional, a partir del tercer capítulo iniciaremos un desarrollo del ciberespacio, valiéndonos de la problemática de falta de territorialidad y transnacionalidad de este fenómeno criminal. Lo que propone esta tesis es que la problemática expuesta no solo tenga como contenido un estudio de la legislación penal española, con referencia a la normativa internacional sobre la incriminación del blanqueo de capitales, sino realizar un estudio de derecho comparado de esta nueva fenomenología delictiva, así como un análisis crítico de las legislaciones, doctrina y jurisprudencia penales de represión del blanqueo de capitales en materia de criptomonedas. Esto permitirá darle a la investigación, además de un contenido teórico, relevancia práctica totalmente ceñida al actual quehacer judicial y fiscal de nuestras regiones hispana y peruana, siempre en el marco del análisis de los procesos o investigaciones por el tipo comisivo doloso del blanqueo de capitales.

El capítulo I "Lavado de activos a partir de la utilización de las nuevas tecnologías de la información y la comunicación" contiene un análisis pormenorizado de las tecnologías de la información y la comunicación, el ciberespacio, así como sus distintos componentes como son la virtualidad, transnacionalidad, neutralidad de la red, para posteriormente adentrarnos en el desarrollo conceptual del ciberlavado. Además, desarrollaremos lo referente al lavado de activos y nuevas tecnologías.

El capítulo II "Consideraciones generales relativas a los criptoactivos y de forma pormenorizada al *bitcoin*". Así mismo, en relación al lavado todo lo referido al concepto de criptoactivos y sus clases. También se explica todo lo referente al *bitcoin*, sus antecedentes, funcionamiento, tecnología de forma pormenorizada, y legislaciones comparadas en las que se ha adoptado como una moneda virtual de curso legal, ya que es el criptoactivo con mayor poder de valor en el mercado, y el más usado para fines delictivos. Por último, desarrollamos otros criptoactivos, así como la tendencia regulatoria en algunos países de Latinoamérica y Europa.

El capítulo III “Lavado de activos y criptoactivos” es, sin duda, el capítulo más importante de este trabajo de investigación, ya que consolidamos todos los objetivos planteados a fin de establecer si efectivamente los criptoactivos pueden ser instrumentalizados para el blanqueo de capitales. Acá explicamos de forma rigurosa toda la problemática vigente en relación con la política criminal mundial en relación con la peligrosidad y falta de regulación en materia preventiva de criptoactivos, haciendo un mayor énfasis en la legislación del Perú para el blanqueo. De igual forma, establecemos cómo los criptoactivos, por su propia naturaleza jurídica, pueden ser considerados como un objeto material del delito blanqueo y subsumirse en las tipologías clásicas contempladas en el Decreto Legislativo N.º 1106. Por último, desarrollamos en materia jurisprudencial dos casos emblemáticos a nivel mundial, que están marcando la ruta en materia de regulación de criptoactivos para fines delictivos, para luego abordar las conclusiones de la investigación.

El capítulo IV “Prevención de lavado de activos y criptoactivos” está enfocado en investigar cuáles son los parámetros que se deben seguir para elaborar un sistema de prevención de lavado de activos para todas aquellas personas jurídicas que se dedican a intercambio, custodia o comercialización de criptoactivos; es decir, con qué herramientas tecnológicas adicionales debemos contar para elaborar de forma eficaz un programa de prevención de lavado, por lo que en dicho capítulo hacemos mayor énfasis en la trazabilidad de las operaciones con criptoactivos.

El capítulo V “Propuesta de *lege ferenda*” está encaminado a realizar una propuesta legislativa en la que se modifique e incorpore, en la normativa actual contra el lavado de activo regulada en la ley especial del Decreto legislativo N.° 1106, a los criptoactivos como objetos del delito de lavado de activos.

CAPÍTULO I
LAVADO DE ACTIVOS A PARTIR DE LA UTILIZACIÓN DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

I. CONSIDERACIONES GENERALES POLÍTICO-CRIMINALES CON RELACIÓN CON EL FACTOR TECNOLÓGICO

La función esencial de la política criminal es fundamentar cada determinación legal en la que se regulan nuevas conductas prohibidas o que modifican la regulación de conductas ya contempladas, con argumentos estadísticos, en coordinación con la criminología y la dogmática penal[8]. Sin embargo, en los últimos años se ha venido dando a nivel mundial una expansión del factor tecnológico de niveles inimaginables, convirtiéndose este fenómeno en un instrumento imprescindible para que la sociedad pueda avanzar. El ámbito referido a la comunicación e información es el que viene alcanzando un mayor protagonismo[9]; es decir, se acortan las brechas de comunicación entre las personas, generándose un traslado inmediato de la información.

En el plano económico, las transacciones se multiplican y se perfeccionan en tiempo real, pues el teléfono, el correo electrónico y otras tecnologías, mediante el principio transnacional, como veremos más adelante, acercan en tiempo real a las partes intervinientes del acto jurídico por muy alejadas que estas se encuentren[10]. En el sector financiero, hemos pasado de realizar operaciones en cajeros automáticos sin la intervención de un operador bancario a realizar transacciones financieras a través del teléfono móvil, mediante la utilización del

---

[8] LAMAS SUÁREZ Gerardo, *El delito previo en el tipo penal de lavado de activos*, Lima: Instituto Pacifico, 2017, p. 92.

[9] En ese sentido, refiere Zúñiga que los avances tecnológicos más espectaculares de la última década han hecho dentro del ámbito de la comunicación, lo cual va a dar lugar a importantes consecuencias en la esfera del saber general y especialmente en las funciones sociales que han ido adquiriendo los instrumentos de control, en particular en el derecho penal. ZÚÑIGA RODRÍGUEZ, Laura, *Política criminal*, Madrid: Colex, 2001, p. 252.

[10] BORJA JIMÉNEZ, Emiliano, *Curso de política criminal*, Valencia: Tirant lo Blanch, 2003, p. 301.

Internet y la virtualidad. Si bien algunos delitos clásicos como es el caso de la apropiación ilícita, el robo y el hurto siguen cometiéndose contra los cajeros y bancos, la mayor dificultad se da cuando los actos criminales se hacen a través del Internet, recurriendo al ciberespacio para delinquir mediante los denominados ciberdelitos económicos[11], como son el *hacking,* el *phishing,* el *cracking,* etc., a los cuales simplemente los tomamos de forma referencial, ya que no son parte del objeto de investigación de esta tesis doctoral.

En los últimos años han aparecido en el mundo financiero las denominadas nuevas tecnologías, que se basan en la creación de empresas plasmadas en plataformas con un alto contenido tecnológico, además de otras tecnologías como es el caso de los criptoactivos, fenómeno que será abordado con mayor profundidad en el capítulo específico como unos de los objetivos principales de esta tesis doctoral.

La misma globalización dinámica de la económica ha generado la necesidad de contar con nuevos instrumentos financieros, que han generado que el medio de pago metálico sea relegado a un segundo plano y sea reemplazado por medios de pago más ágiles y seguros[12], ya que el enorme desarrollo de los intercambios económicos que viene experimentado nuestra sociedad ha demostrado las limitaciones a las que se encuentra sujeto el dinero tradicional como medio de pago[13].

En este nuevo escenario la política criminal debe plantearse varios cambios en la concepción de conductas punibles en relación con la configuración de delitos

---

[11] Los cibercrímenes económicos "tienen como objetivo la obtención de un beneficio económico patrimonial, por parte de sus autores, por lo que todos los ataques están dirigidos y afectan el patrimonio individual de un individuo o al sistema económico en relación con las transacciones comerciales en Internet". MIRÓ LLINARES, Fernando, *Cibercrimen, cibercriminales y cibervíctimas,* Universitat Oberta de Catalunya, 2013, p. 9. Disponible en: <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/70006/4/Delincuencia%20y%20TICs_M%C3%B3dulo%202_Cibercrimen%2C%20cibercriminales%20y%20ciberv%C3%ADctimas.pdf>.

[12] *Ibid.,* p. 9.

[13] FABIÁN CAPARRÓS, Eduardo, *El delito de blanqueo de capitales*, Madrid: Editorial Colex, 1998. p. 111.

con contenido tecnológico. Estas nuevas tecnologías no han sido ajenas al reforzamiento del delito de lavado de activos, ya que, como se ha pronunciado de forma muy acertada FABIÁN CAPARRÓS, "el reciclaje de dinero sucio es una actividad que se apoya en la multiplicidad de interrelaciones sostenidas en diversos agentes económicos, ya que su propia operatividad se encuentra condicionada a diversos instrumentos jurídicos económicos y tecnológicos"[14]. Así pues, las tipologías delictivas clásicas del lavado han quedado relegadas, por no decir obsoletas, por nuevas formas de macular activos sucios, con un alto componente tecnológico, como es el caso de los activos virtuales.

Bajo el pensamiento de ZUÑIGA RODRIGUEZ, nos encontramos frente a lo que se conoce como una "criminalidad de riesgo", en la que los bienes jurídicos que provienen del desarrollo tecnológico[15] son merecedores de nuevas valoraciones jurídicas para poder establecer su ámbito de protección. No cabe duda alguna que el surgimiento de estas nuevas tecnologías son una respuesta a los conflictos sociales que se muestran en las sociedades posindustriales caracterizadas por una crisis del modelo económico de cada Estado. Actualmente, las transacciones se multiplican y se perfeccionan en tiempo real[16]. Como consecuencia de esa inmediatez en la obtención de la información, se van borrando las barreras de las fronteras nacionales, propiciándose un fenómeno que cada vez más tiende a la homogeneización del mundo y que se le conoce ahora bajo el nombre de globalización[17].

El marco jurídico, que ha servido como base de la técnica legislativa aplicable para reprimir el lavado de activos a nivel mundial, se ha basado principalmente en la normativa elaborada por organismos internacionales con un suficiente grado de cooperación entre sus intervinientes[18], lo que ha permitido cierta

---

[14] FABIÁN CAPARRÓS, Eduardo, *Combate del Lavado de Activos desde el Sistema Judicial*, Fimart, Washington DC, 2006, p. 4.

[15] ZÚÑIGA RODRÍGUEZ, *Política criminal*, *op. cit.,* p. 270.

[16] BORJA JIMÉNEZ, *Curso de política criminal*, *op. cit*., p. 301.

[17] *Ibid.,* p. 301.

homogeneidad al momento de tipificar las modalidades delictivas del blanqueo de capitales, el cual surge criminológicamente como un acto de encubrimiento realizado para evitar la detección de bienes de procedencia delictiva[19]. Nos referimos a un conjunto de operaciones minuciosas y sofisticadas destinadas a ocultar o encubrir activos con una procedencia criminal.

Dentro de la estrategia político-criminal en la lucha contra el lavado, podemos encontrar dos objetivos claramente establecidos. El primero se basa en una finalidad preventiva, que consiste en la persecución de las ganancias que se obtienen a través de la comisión de hechos delictivos, que constituyen el centro neurálgico de las organizaciones criminales[20]. Este objetivo tiene como finalidad la disuasión frente a la convicción del potencial lavador, que piensa únicamente en la ganancia economía del acto criminal, por lo que sí sabe que no obtendrá ningún beneficio económico, se desistirá de la comisión del hecho delictivo[21]. El segundo objetivo, respecto a las transacciones electrónicas por medio de sistema financiero bancario, razón por la que en los últimos años se han venido desarrollando nuevos mecanismos preventivos entre las distintas entidades públicas y privadas, con la finalidad de identificar clientes y reportar aquellas operaciones sospechosas que pudieran configurar el lavado[22]. De otro lado, tenemos la persecución penal tradicional, que busca la represión punitiva de aquellos autores y partícipes en el blanqueo de capitales, que han sido obtenidos en actividades criminales[23].

---

[18] JORGE, Guillermo, "Políticas de Control del Lavado de Dinero", en *Tratado de lavado de activos y financiación al terrorismo*, t. I, Buenos Aires: La Ley, 2012, p. 46.

[19] GARCÍA CAVERO, Percy, *El delito de lavado de activos*, Lima: Jurista Editores, 2015, p. 21.

[20] MANSO PORTO, Teresa, "El blanqueo de capitales entre la dogmática y la política criminal internacional: resultados desde una perspectiva de derecho comparado", en *El delito de lavado de activos,* t. I., Lima: Editorial Grijley, 2017, p. 222.

[21] CÓRDOBA, Fernando J, *Delito de lavado de dinero*, Buenos Aires: Hammurabi, p. 20.

[22] MANSO PORTO, *op. cit.*, p. 223. De igual parecer, CÓRDOBA refiere que "la idea que está detrás del medio más eficaz para obtener resultados en la prevención y la represión de la criminalidad organizada es concentrar los esfuerzos en el decomiso de los bienes que son beneficio de su actividad ilícita". CÓRDOBA, *op. cit.*, p. 19.

[23] MANSO PORTO, *op. cit.*, p. 223.

Sin embargo, en los últimos tiempos, como explicamos anteriormente, la irrupción de las tecnologías aplicadas[24] en el sector financiero, han generado mucha atención por parte de la economía mundial, especialmente por la banca mundial, ya que, a través de estas nuevas empresas innovadoras basadas en la aplicación de la tecnología a las finanzas, las operaciones de dinero podrían ya no requerir de intermediarios financieros, situación que ha generado gran preocupación por parte comunidad bancaria[25].

Dentro de esta expansión tecnológica, ha surgido el fenómeno de los denominados criptoactivos, criptomonedas, monedas virtuales o *criptocurrecny*. Existen a la fecha más de mil tipos de criptoactivos en el mercado virtual, dentro de los más populares están el *bitcoin* (BTC), *etherium* (ETH), *cardano* (ADA), *tether* (USDT), *polkadot* (DOT) *ripple* (XRP), *uniswap* (UNI), *solana* (SOL), *decentrland* (MANA), *dogecoin* (DOGE), *sushiSwap* (SUSHI). El fenómeno tecnológico de los criptoactivos no ha sido ajeno a las entidades reguladoras que buscan velar por la estabilidad de los mercados y activos financieros, para darles protección a los inversores minoristas. Dentro de las más conocidas están la Comisión de Bolsa y Valores de Estados Unidos (Sec- Securities and Exchanges Comisión), que, en el año 2014, emitió un documento en su página web alertando a los inversores de *bitcoin* y señalando que el auge de *bitcoin* y otras monedas virtuales y digitales crea nuevas preocupaciones para los inversores[26], ya que por sus propias características se vuelven muy tentativas para los inversores.

---

[24] "La FinTech es una industria naciente en la que las empresas usan la tecnología para brindar servicios financieros de manera eficiente, ágil, cómoda y confiable. La palabra se forma a partir de la contracción de los términos finance y technology en inglés. Las empresas FinTech ofrecen diversos tipos de servicios financieros y operan dentro de mercados variados. Algunas prestan sus servicios directamente a los usuarios del sistema financiero y otras diseñan soluciones para otras empresas". FINTECH MÉXICO, "¿Qué es FinTech?". Disponible en: <https://www.fintechmexico.org/qu-es-fintech>.

[25] David IGUAL refiere que "las fintech (finance + tecnology) son empresas innovadoras que están emergiendo en estos últimos años y que ofrecieron nuevas soluciones financieras con el soporte de las nuevas tecnologías. Las primeras fintech, aún sin denominación, tienen su origen en el año 2008, aunque su impulso y desarrollo notable no se produce hasta el año 2010, principalmente en Estados Unidos y Reino Unido". IGUAL, David, *Fintech: Lo que la tecnología hace por las finanzas*, Barcelona: Profit Editorial, 2016, p. 21.

[26] U.S. SECURITE AND EXHCHANGE COMMISSION, "Investor Alert: Bitcoin and other virtual currency - releated investments", mayo del 2014. Disponible en: <https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html>.

España, mediante la Comisión Nacional de Mercados de Valores (CNMV) y el Banco de España, ha emitido un comunicado sobre los riesgos de inversión en criptomonedas por una falta de regulación normativa, refiriéndose a que aún no existe en la Unión Europea un marco que regule los criptoactivos como el *bitcoin* y que se debe proporcionar garantías y protección similares a las aplicables a los productos financieros[27]. En el Perú, la Superintendencia de Mercados y Valores refiere que no existe una regulación específica que ampare la oferta y/o promoción de criptomonedas o monedas virtuales o de *tokens*, ya que estas no cuentan con el respaldo de una entidad gubernamental o supervisor financiero alguno; y, por tanto, las empresas que realizan tales ofertas y/o promociones no están bajo supervisión[28].

En Alemania está la Autoridad Alemana Federal de Supervisión (Bundesanstalt für Finanzdienstleistungsaufsicht [BaFin]), que ha señalado que, debido al anonimato parcial de las transacciones, el *bitcoin* también corre el riesgo de ser mal utilizado para el blanqueo de dinero y otras actividades ilegales. Esto puede llevar a la realización de investigaciones policiales empleando el análisis de la tecnología *blockchain*[29]. En Reino Unido, La Autorización de Conducta Financiera (Financial Conduct Authority [FCA]), con relación a la protección del consumidor, señaló que algunas inversiones que anuncian altos rendimientos basados en criptoactivos pueden no estar sujetas a regulaciones más allá de los requisitos contra el lavado de dinero[30].

---

[27] BANCO DE ESPAÑA y CNMV, "Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión", 9 de febrero del 2021. Disponible en: <https://www.cnmv.es/Portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D>.

[28] SUPERINTENDENCIA DEL MERCADO DE VALORES, "Advertencia sobre la adquisición de monedas virtuales o criptomonedas y la participación en esquemas de financiamiento mediante el uso de unidades de valor denominadas tokens", Lima, 2020. Disponible en: <https://www.smv.gob.pe/Uploads/COMUNICADO_Criptomoneda_ICO_Logo.pdf>.

[29] BUNDESANSTALT FÜR FINANZDIENSTLEISTUNGSAUFSICHT, "Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer", 19 de diciembre del 2013. Disponible en: <https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html>.

[30] FINANCIAL CONDUCT AUTORITY, "FCA warns consumers of the risks of investments advertising high returns based on cryptoassets", enero del 2021. Disponible en: <https://www.fca.org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets>.

En Suiza, la Autoridad de Supervisión del Mercado Financiero de Suiza (Swiss Financial Market Supervisory Authority [FINMA]) recientemente ha emitido un pronunciamiento desfavorable con relación a la presentación de licencia bancaria solicitada por Bitcoin Suisse AG, bajo el argumento de que ya que existen varios elementos relevantes bajo la ley de otorgamiento de licencias que hacen poco probable que se otorgue una licencia. Entre otras cosas, hay indicios de debilidades en los mecanismos de defensa contra el blanqueo de capitales[31].

El Grupo de Acción Financiera Internacional, en sus informes denominados *Monedas virtuales. Definiciones claves y riesgos potenciales de LA/FT,* de julio del 2014, y las *Directrices para un Enfoque Basado en Riesgo. Monedas Virtuales*, de junio del 2015, resalta los riesgos potenciales que se presentan en el uso de monedas virtuales como es el caso del *bitcoin*, ya que se encuentran protegidas por un anonimato que es parte del funcionamiento operativo de la criptomoneda. En esa misma línea preventiva, el 30 de mayo del 2018, el Parlamento Europeo y del Consejo ha emitido la Directiva (UE) 2018/243, la cual modifica la Directiva 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, en la que se hace referencia a la utilización indebida de las monedas virtuales producto del anonimato asociados a las transacciones de las mismas[32].

---

[31] SWISS FINANCIAL MARKET SUPERVISORY AUTHORITY, "FINMA makes an unfavorable prognosis for Bitcoin Suisse AG licensing produce", marzo del 2021. Disponible en: <https://www.finma.ch/en/news/2021/03/20210317-mm-btcs/>.

[32] La Directiva (UE) 2018/843 establece lo siguiente: "El anonimato de las monedas virtuales permite su posible uso indebido con fines delictivos. La inclusión de los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias y de los proveedores de servicios de custodia de monederos electrónicos no resolverá totalmente la cuestión del anonimato asociado a las transacciones con monedas virtuales, al mantenerse el anonimato en gran parte del entorno de la moneda virtual, puesto que los usuarios pueden llevar a cabo transacciones al margen de tales proveedores de servicios. Para combatir los riesgos relacionados con ese anonimato, las Unidades de Inteligencia Financiera (UIF) nacionales deben poder obtener informaciones que les permitan asociar las direcciones de las monedas virtuales a la identidad del propietario de la moneda virtual. Además, debe analizarse más a fondo la posibilidad de que los usuarios efectúen, con carácter voluntario, una autodeclaración a las autoridades designadas". Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, en *Diario Oficial de la Unión Europea*, 30 de mayo del 2018. Disponible en: <https://blanqueo.icaib.org/wp-content/uploads/2018/06/CELEX3A32018L08433AES3ATXT.pdf>.

El intercambio de criptoactivos es un fenómeno de la era digital que día a día va ganando más adeptos e interesados en su adquisición, ya sea por medio de plataformas virtuales de intercambio, o de forma directa entre los mismos usuarios, por lo que urge establecer nuevos lineamientos en materia de una política criminal que se adecue a los nuevos estándares de prevención del lavado de activos en relación con la adquisición y utilización de criptodivisas como es el caso del *bitcoin*.

II. EL FENÓMENO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)

Un nuevo paradigma tecnológico surgió durante los años 70 en Estados Unidos, dando lugar a un nuevo modelo de desarrollo basado en el uso de las tecnologías de la información y comunicación, desterrando de esta manera al modelo industrial vigente del siglo XIX. Para SAIN, la revolución de las tecnologías de la información produce a nivel global un nuevo modo de producir, comunicar, gestionar y vivir[33] los quehaceres de la vida cotidiana.

Hoy por hoy, el siglo XXI se ha convertido en una sociedad definida[34] y caracterizada por el avance[35] de las tecnologías de la información y la comunicación[36] y la influencia que estas vienen generando en distintos

---

[33] SAIN, Gustavo, *La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal en cibercriminal y delitos informáticos*, Buenos Aires: Erreius, 2018, p. 11.

[34] En ese sentido, "la sociedad de la información se nutre necesariamente con el uso permanente de las Tecnologías de la Información y la Comunicación, que en su aplicación al ciberespacio han revolucionado por completo la de relacionrase del hombre y han contribuido enormemente a la globalización e internacionalización". FERNÁNDEZ BERMEJO y MARTÍNEZ ATIENZA, *op. cit.,* p. 116.

[35] En ese sentido las nuevas tecnologías tienen una fuerte influencia en el ambito cultural de las sociedades modernas y, a menudo, son modeladas por los ambientes culturales que las adoptan. Sirviera Martins, Amaury, El Derecho y las Nuevas Tecnologías en Ciberdelitos, Nuevas Tecnologías y Derecho Penal, Ciudad de México: Flores Editor, 2022, p. 266.

[36] SUEIRO, CARLOS, *El derecho penal en la era digital*, Lima: A&C Ediciones, 2018, p. 29.

estamentos de la vida cotidiana como la medicina, genética, educación, comunicación, informática, transporte y el derecho. Como refiere SUEIRO, este impacto, generado por la influencia informática a finales del siglo XX y la primera década del siglo XXI, se le conoce como la *sociedad de la información*[37], que es un fenómeno basado en transformación y adaptación por parte de los individuos que conforman una sociedad, en el uso de medios tecnológicos, que facilitan la creación, manipulación y distribución de la información. Este nuevo modelo social se suele confundir con la *sociedad del conocimiento*[38], a pesar de que son topologías distintas, ya que la información funciona como un instrumento del conocimiento.

Para entender esta fenomenología de las TIC, debemos desarrollar conceptualmente tres fenómenos que se encuentran estrechamente conectados entre sí. El primero tiene que ver con la *cibernética* (*cybernetics*), que es "aquella ciencia teórica que estudia las leyes generales de los sistemas de tratamiento de la información"[39]. La segunda, en relación con la *informática* (*computing*), entendida como una disciplina integrada que se encarga del tratamiento automático y racional de la información[40]. Y, por último, está la *telemática* (*telematics*), que es una técnica de comunicación a distancia para intercambiar información mediante equipos informáticos con un ordenador o computador[41].

Como refiere PALOMINO MARTÍN, "en la sociedad actual todos estos conceptos quedan integrados en los términos Tecnologías de la Información y la

---

[37] SUEIRO, Carlos, *op. cit.,* p. 29

[38] La Organización de Estados Americanos señala lo siguiente: "Una sociedad del conocimiento se refiere al tipo de sociedad que se necesita para competir y tener éxito frente a los cambios económicos y políticos del mundo moderno. Asimismo, se refiere a la sociedad que está bien educada, y que se basa en el conocimiento de sus ciudadanos para impulsar la innovación, el espíritu empresarial y el dinamismo de su economía". Disponible en: <https://www.oas.org/es/temas/sociedad_conocimiento.asp>.

[39] PALOMINO MARTÍN, José María, *Derecho penal y nuevas tecnologías*, Valencia: Editorial Tirant lo Blanch, 2016, pp. 37 y 38.

[40] *Ibid*., p. 38.

[41] *Idem.*

Comunicación (TIC) o Nuevas Tecnologías (NN. TT.)"[42]. Las TIC hace referencia a todas las formas de producción, almacenamiento, procesamiento y reproducción de la información; y las NN. TT., a las tecnologías de la comunicación a toda forma de transmisión e información[43].

En la actualidad, las tecnologías de la información y la comunicación han pasado a constituir una parte esencial en el desarrollo de la sociedad contemporánea. Hablamos de un tipo de tecnología que está compuesta de tres elementos: 1) la tecnología de la información a partir del uso de las computadoras, que permiten a la sociedad moderna el procesamiento de datos con ahorro de tiempo y esfuerzo[44], 2) la tecnología de las telecomunicaciones, basada en teléfonos fijos y móviles, radio, televisión mediante el uso de satélites, y 3) la tecnología de redes, con Internet, con ciertas extensiones a móviles, etc. Una de las características a resaltar de las TIC es que estas no pueden operar de forma aislada. Bajo ese precepto, como veremos más adelante, el Internet constituye un medio eficiente de bajo costo que facilita la interrelación con otras tecnologías[45].

Respecto a las políticas vinculadas a las TIC, básicamente se componen de cuatro campos: tecnología, industria, telecomunicaciones y medios de comunicación, las mismas que vienen siendo implementadas por los distintos

---

[42] *Idem.*

[43] SIRVIERA MARTINS, Amaury, *El derecho y las nuevas tecnologías en ciberdelitos*, Ciudad de México: Nuevas Tecnologías y Derecho Penal, 2022, p. 265.

[44] ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES, *Políticas TIC: Manual para principiantes,* Chris NICOL (ed.), Montevideo, 2005. Disponible en: <https://www.apc.org/sites/default/files/ICT_Policy_Handbook_ES.pdf>.

[45] En ese sentido, "las nuevas tecnologías no solo tienden a la convergencia; también sus ámbitos de aplicación se interrelacionan cada vez más. Las telecomunicaciones están firmemente basadas en la tecnología informática y dependen principalmente de Internet". ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES, *Políticas TIC: Manual para principiantes,* Chris NICOL (ed.), Montevideo, 2005, p. 10. Disponible en: <https://www.apc.org/sites/default/files/ICT_Policy_Handbook_ES.pdf>. Por su parte, TEMPERINI refiere sobre las características de las TIC, las cuales podemos concentrar en tres: 1) la inmediatez de la comunicación a la distancia, 2) la posibilidad de la realización de las acciones masivas (automatizadas o no) y 3) la posibilidad de realizar acciones con un determinado nivel de anonimato. TEMPERINI, Marcelo, "Delitos Informáticos y Cibercrimen: Alcances, conceptos y características", en *Cibercriminal y delitos informáticos*, Buenos Aires: Erreius, 2018, p. 52.

Gobiernos. Dentro de este proceso, el sector particular privado también aporta en determinados procesos como es el caso de la Unión Internacional de las Telecomunicaciones (UIT), que es un organismo intergubernamental que coordina la normativa y regulaciones y las telecomunicaciones[46]. En términos prácticos, las TIC sirven para distribuir información de manera novedosa para que este llegue a millones de personas sin las barreras burocráticas tradicionales, impuestas por las barreras de la distancia[47].

En el plano bancario, también se ha dado un fenómeno de globalización del sistema financiero[48], ya que en la actualidad podemos operar cuentas bancarias desde un dispositivo celular o móvil, desde cualquier parte del mundo, contando con altos niveles de seguridad. Además, debemos hacer énfasis en el dinero electrónico y de las criptomonedas, que, como refiere PICÓN GONZÁLES, hacen aún más sencillo tener riqueza exenta de controles de distinto tipo como es el caso de las criptomonedas[49].

III. LAS CARACTERÍSTICAS DE LAS TIC

1. Inmaterialidad

La inmaterialidad es el proceso virtual remoto mediante el cual las TIC realizan la creación y la comunicación de la información, la cual a su vez es inmaterial y puede ser llevada de forma transparente e instantánea a lugares lejanos[50].

---

[46] *Ibid*., p. 11.

[47] *Ibid*., p. 14.

[48] Actualmente, se podría decir que el sector financiero se encuentra a la vanguardia en el uso de las TIC en España. La inversión realizada por la banca española ascendió a la suma de 3.800 millones de euros en el 2009, lo que sitúa al sector como el primero en esfuerzo en tecnología. Dentro de este presupuesto, un 29,3 % está destinado a desarrollo y mantenimiento evolutivo. MARTÍN ENRÍQUEZ, Álvaro, NAVARRO GIMENO, M.ª Ángeles, RODRÍGUEZ FERNÁNDEZ, Esther y ONTIVEROS BAEZA, Emilio, *Las TIC y el sector financiero del futuro*, Madrid: Editorial Ariel, 2011, p. 52.

[49] PICÓN GONZÁLES, Jorge, *Paraísos fiscales: Rompiendo mitos: Evolución, uso y medidas antiparaísos,* Lima: Dogma Ediciones, 2020, p. 19.

2. Interactividad

Mediante la interactividad se logra un intercambio de información entre el usuario y el ordenador, lo cual permite adaptar los recursos utilizados a las necesidades y características de los sujetos, en función de la interacción concreta[51].

3. Interconexión

Se puede definir como el proceso que posibilita el intercambio de datos a partir de la conexión entre dos usuarios de distintas tecnologías.

4. Instantaneidad

Mediante las TIC se han posibilitado el uso de servicios que permiten la comunicación y transmisión de la información a través de la red, entre lugares alejados físicamente, de una forma rápida e instantánea[52].

---

[50] BELLOCH ORTÍ, Consuelo. *Las tecnologías de la información y la comunicación (TIC),* Unidad Tecnología Educativa, Universidad de Valencia, p. 1. Disponible en: <https://www.uv.es/~bellochc/pdf/pwtic1.pdf>.

[51] *Ibid*., p. 2. En ese sentido, ADELL refiere otra característica de la comunicación mediada por ordenador: su capacidad para soportar complejos procesos de interacción entre los participantes. Platón, en el *Fedro*, abjuraba del texto escrito frente a la comunicación oral, porque no respondía a las dudas que pudiera provocar en los lectores. "La interactividad en la comunicación está ligada a un factor clave: que emisor y receptor intercambien sus papeles. Los ordenadores imitan la auténtica interactividad. Por ejemplo, en los sistemas de enseñanza asistida por ordenador, los mensajes de respuesta a la ejecución del sujeto son estereotipados porque están previamente programados. En cambio, en la comunicación mediada por ordenador las posibilidades de retroalimentación entre los participantes son infinitas: a fin de cuentas, lo que hay al otro lado de la red son otras personas. Un debate realizado mediante el correo electrónico es interactivo, aunque no se produzca en tiempo real (lo que también tiene algunas ventajas: es más flexible, reflexivo y elaborado)". ADELL, Jordi, "Redes y Educación", en J. DE PABLOS, J. y J. JIMÉNEZ (eds.), *Nuevas tecnologías, comunicación audiovisual y educación,* Barcelona: Ed. Cedecs, 1998, pp. 10 y 11. Disponible en: <https://elbonia.cent.uji.es/jordi/wp-content/uploads/docs/Adell_redesyeducacion.pdf>.

[52] *Ibid.,* p. 2

5. Digitalización

Es un proceso por el cual se buscan transformar objetos físicos en digitales, su objetivo es que la información de distinto tipo pueda ser transmitida por los mismos medios digitales al estar representada en un formato único universal[53].

6. Penetración en todos los sectores

Las TIC están impactando en todos los estamentos de la sociedad, es decir, no se reflejan únicamente en un individuo, grupo, sector o país, sino que se extiende al conjunto de las sociedades del planeta.

7. Innovación

Las TIC de forma permanente están en un proceso de cambio constante en todos los ámbitos sociales. Sin embargo, estos cambios no siempre indican un rechazo a las tecnologías o medios anteriores, sino que en algunos casos se produce una especie de simbiosis con otros medios[54].

IV. El CIBERESPACIO, UN *GLOBAL COMMON*

La tierra, mar, aire y espacio exterior, todos ellos explotados y explorados por el ser humano, se caracterizan en que en todos ellos imperan leyes de la naturaleza reguladas por el derecho positivo[55]. Bajo esta premisa, el ciberespacio se ha vuelto el último dominio en el que el hombre se ha aventurado a ejercer un control

---

[53] *Idem.*

[54] *Ibid.,* p. 3.

[55] ENRIQUE GONZÁLES, Carlos, "Estrategias internacionales para el ciberespacio" en MINISTERIO DE DEFENSA E INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (eds.), *El ciberespacio. Nuevo escenario de confrontación*, España, 2012, p. 73.

normativo; a diferencia de los espacios mencionados anteriormente, este se rige por un conjunto de protocolos lógicos[56].

Se puede considerar al ciberespacio como un *global common*[57], que es una figura recogida del derecho británico medieval en el que todos los terrenos son considerados bienes comunes globales; es decir, estos no se encuentran sujetos a la soberanía de ningún país y son utilizados por las distintas naciones para transportar personas bienes o servicios y transmitir datos[58]. La diferencia más notoria entre el espacio virtual y los otros espacios o *commons* persistentes es su naturaleza artificial.

En los espacios precedentes, su entorno existe y es palpable por el ser humano, es decir, este tiene que adaptar medios artificiales para su utilización[59]. Sin embargo, en el ciberespacio ocurren dos fenómenos, el continente y el contenido, que son creados por el ser humano y, por ende, su diseño e imperfecciones responden a circunstancias específicas que se dieron al momento de la creación de este[60]. No debemos soslayar que el resto de los espacios tienen una creación basada en las leyes de la naturaleza y estas solo pueden ser modificadas por cambios de índole meteorológico; situación contraria

---

[56] En ese sentido, "cuando los sistemas se comunican entre sí, existen ciertas normas o *protocolos*, que les permiten transmitir y recibir datos de una forma ordenada. En todo el mundo, uno de los conjuntos de protocolos utilizados más habitualmente es TCP/IP (Transmission Control Protocol / Internet Protocol - Protocolo de control de transmisiones / Protocolo Internet)". Disponible en: <https://www.ibm.com/docs/es/aix/7.2?topic=management-transmission-control-protocolinternet-protocol>.

[57] En ese sentido, "el ciberespacio se diferencia de los demás bienes comunes porque no es un dominio físico y por el papel preponderante del sector privado tanto en la infraestructura como en la gestión del dominio. Todos los nodos físicos de Internet también existen dentro de los estados y están sujetos a la legislación nacional, en lugar de existir físicamente fuera del control nacional como ocurre con los demás bienes comunes". STANG, Gerald, "Bienes comunes globales: Entre la cooperación y la competencia", *Issue Brief,* n.º 17, Instituto de Estudios de Seguridad de la Unión Europea, 2013, p. 3.

[58] GÓMEZ DE ÁGREDA, Ángel, "El Ciberespacio como Escenario de Conflictos, Identificación de las Amenazas", en MINISTERIO DE DEFENSA e INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (eds.), *El ciberespacio. Nuevo escenario de confrontación*, España, 2012, p. 171.

[59] *Ibid.,* p. 3.

[60] *Idem*.

ocurre en el ciberespacio, ya que su evolución y desarrollo depende únicamente de la manufactura humana[61].

Dentro de su composición, el ciberespacio está estructurado en tres capas, cada cual con sus propias características y vulnerabilidades[62]. La primera es la *capa semántica,* conformada por toda la data, programas que son introducidos para su gestión; todo este conocimiento acumulado en los servidores y disco duro constituye dicha capa[63]. La segunda es la *capa sintáctica,* conformada por los protocolos, sistemas operativos y demás lenguajes que sirven para el funcionamiento de los distintos programas[64]. La tercera es la *capa física*, compuesta por aquellos que podemos ver y tocar que sea parte de nuestro ordenador, discos duros, teclados, CPU, ratones; debemos tener en cuenta que la capa física muchas veces se encuentra muy alejada y eso que sea de difícil acceso para el común denominador, hablamos de servidores ubicados en otros países, cableado submarino y satélites[65].

Desde un punto de vista técnico científico, el ciberespacio es un entorno generado a partir de la interacción de distintos actores, basados en tecnologías digitales que generan, transmiten, almacenan y procesan datos[66]. El National Institute of Standards and Technology lo define como "un dominio global dentro de la información que consiste en una red interdependiente de infraestructura de sistemas de información que incluyen el Internet, las redes de telecomunicaciones, los sistemas informáticos, procesadores y controladores integrados"[67]. Una concepción más técnica considera al ciberespacio como

---

[61] *Ibid.,* p. 72.

[62] GÓMEZ DE ÁGREDA, *op. cit.*, p. 172.

[63] *Ibid.,* p. 172

[64] *Idem.*

[65] *Ibid.,* p. 173.

[66] BARRIA HUIDOBRO, Cristian, "La dimensión del ciberespacio: Una propuesta de ciberseguridad", en *Cuaderno de Trabajo,* n.° 01-2019, Chile: CIEE, 2019, p. 6.

aquellas infraestructuras técnicas de un conjunto interconectado de redes de información, tanto públicas como privadas, incluyendo el Internet[68].

Pero lo concreto es que el ciberespacio no se encuentra situado en ningún sitio concreto; en un sentido funcional está en todos los lugares, pero físicamente lo encuentras en ningún lado en concreto[69]. Es muy común utilizar como sinónimo del ciberespacio al "espacio virtual", y como antítesis de este al "espacio real". Físicamente, el espacio virtual no existe, pero en la mente de los seres humanos se da un proceso a través de los sentidos que nos permite transformar parte de esta realidad virtual en real. El ciberespacio se ha convertido en una metáfora de la sociedad digital hecha posible mediante computadoras y redes de computadoras[70].

Para que el espacio de vivencia virtual pueda funcionar y desarrollarse requiere de un elemento trascendental conocido como el Internet, que se define como un sistema de intercomunicación global, cuya tecnología permite vincular millones de computadoras entre sí y acceder desde cualquier sitio del planeta a la información o servicios que se ofrezcan en él[71]. Este sistema se ha vuelto de vital importancia[72] para el desarrollo de la humanidad, ya que, a raíz del aparecimiento de las denominadas tecnologías de la información y la

---

[67] NIST - COMPUTER SECURITY RESOURCE CENTER, "Cyberspace". Disponible en: <https://csrc.nist.gov/glossary/term/cyberspace#:~:text=Definition(s)%3A,and%20embedded%20processors%20and%20controllers>.

[68] PÉREZ CORTÉS, Manuel, "Tecnologías para la defensa en el ciberespacio", en MINISTERIO DE DEFENSA e INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (eds.), *El ciberespacio. Nuevo escenario de confrontación*, España, 2012, p. 257.

[69] MIRÓ LLINARES, Fernando, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid: Marcial Pons, 2012, p. 153.

[70] MARTÍNEZ HERNÁNDEZ, Luis Manuel, CECEÑAS TORRERO, Paula Elvira, ONTIVEROS HERNÁNDEZ, Verónica Clementina, "Qué es el ciberespacio", en Luis MARTÍNEZ, PAULA CECEÑAS, Verónica ONTIVEROS (coords.), *Virtualidad, ciberespacio y comunidades virtuales,* México: Red Durango de Investigaciones Educativas, 2014, p. 48. Disponible en: <http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf>.

[71] ABOSO, Gustavo y ZAPATA, Florencia. *Cibercriminalidad y derecho penal*, Buenos Aires: B de F, 2006, p. 6.

[72] En el mismo sentido, MARTÍNEZ HERNÁNDEZ, *op. cit,* p. 51, refiere el Internet es parte fundamental del ciberespacio, ya que el ciberespacio está dentro del Internet y el este se construye con la interconexión de las redes.

comunicación (TIC), cada vez es mayor la tendencia hacia la digitalización de los servicios comerciales convencionales, que antes no eran parte del ciberespacio[73].

A diferencia del espacio físico real en el que se relacionan las personas, el mismo que va a seguir existiendo antes y después de un punto de encuentro, el ciberespacio agota su existencia en cuanto cumple con su finalidad de comunicación[74]. No obstante, el ciberespacio requiere necesariamente de puntos de encuentro con el espacio terrestre, si no sería materialmente imposible que los usuarios pudieran acceder a la red; es ahí donde las terminales de acceso a Internet cumplen un rol de suma importancia, dependiendo de la regulación que tenga cada Estado[75]. Aunado a ello, tenemos la red Wi-Fi, que es una red de comunicaciones de datos y, por lo tanto, permite conectar servidores, computadoras, impresoras, etc., con la particularidad de alcanzarlo sin necesidad de cableado[76]. Dentro de sus componentes básicos tiene un punto de acceso (AP)[77] y una antena[78], con lo cual la condición para ingresar al ciberespacio ha sido superada por la tecnología Wi-Fi[79].

---

[73] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *El ciberdelito: Guía para los países en desarrollo,* abril del 2012, p. 12. Disponible en: <https://www.itu.int/dms_pub/itu-d/oth/01/0b/d010b0000073301pdfs.pdf>.

[74] MIRÓ LLINARES, *El cibercrimen…, op. cit.*, p. 146.

[75] El ciberespacio, en todo caso, convive con el espacio físico y terrestre, y también tiene en algunos aspectos, una relación directa con el que debe ser obviada: las redes telemáticas que conforman el ciberespacio vienen a unir, de forma virtual pero también física, terminales o sistemas informáticos que están ubicados en espacios terrestres concretos en países nacionales determinados con contextos sociales de facilitación del acceso a Internet específicos. MIRÓ LLINARES, *El cibercrimen*…, *op. cit.*, p. 147.

[76] MARTÍNEZ HERNÁNDEZ *et al.*, *op. cit.*, p. 48.

[77] Es el dispositivo que gestiona la información transmitida y la hace llegar a destino. Asimismo, proporciona la unión entre la red Wi-Fi y la red fija. *Las tecnologías wifi y wimax*, p. 15. Disponible en: <http://www.dip badajoz.es/agenda/tablon/jornadawifi/doc/tecnologias_wifi_wmax.pdf>.

[78] Las antenas son los elementos que envían al aire señales en forma de ondas electromagnéticas que contienen la información dirigida en el dispositivo de destino y, a la vez, captan del aire las señales de las cuales se extraerá la información que llega de otro dispositivo. *Las tecnologías wifi y wimax*, *op. cit.*, p. 15.

[79] *Idem.* Además, también va cambiando la relación entre espacio físico fijo y el virtual: hace unas décadas era necesario un lugar físico fijo para entrar en el ciberespacio. MIRÓ LLINARES, *El cibercrimen…, op. cit.*, p. 147.

1. La transnacionalidad

En el ciberespacio, la transnacionalidad[80] se manifiesta en la posibilidad que la red permite a sus usuarios de poder acceder, desde cualquier parte del mundo, a cualquier sitio web que se encuentre localizado en un servidor concreto. Ese mundo virtual, siguiendo lo dicho por LINS RIBEIRO, es un concepto clave para entender el tipo de cultura de la comunidad transnacional[81], ya que la virtualidad es característica general de los seres humanos porque somos capaces de ser simbólicamente transportados a otros lugares, imaginar lo que no está aquí y, aún más, crear realidades de estructuras que son puras abstracciones antes de volverse hechos empíricos[82].

La transnacionalidad del ciberespacio se traduce, a los efectos que nos interesan, en la total ausencia, para la comunicación e interacción entre individuos, de barreras que no sean impuestas o configuradas por el propio sujeto[83]. Existe una libertad absoluta por parte de los usuarios para acceder de forma virtual a cualquier Estado desde el Internet.

Con precisión describe, LINS RIBEIRO que "el transnacionalismo atraviesa diferentes niveles de integración de tal forma que es muy difícil circunscribirlo a algún territorio"[84]. Una de las grandes dificultades que se suscitan en el elemento de la transnacionalidad se da a consecuencia del principio fundamental de la soberanía nacional, "sin el cual no se pueden realizar investigaciones en jurisdicciones extranjeras"[85], sin el permiso de las autoridades locales. Es ahí

---

[80] El término transnacionalidad aparece en diferentes contextos: por un lado, en el de las ciencias y, por otro, en el del mundo social. Se ha escrito mucho sobre los fenómenos de la transnacionalidad, partiendo desde diferentes enfoques científicos y desde disciplinas distintas. KNIFFKI, Johannes, "Transnacionalidad y Comunidad: un enfoque construccionista y discursivo", en *Espacios transnacionales: revista latinoamericana-europea de pensamiento y acción social,* año 1, n.º 1, 2013, p. 27.

[81] LINS RIBEIRO, "La condición de la transnacionalidad", en *Maguaré,* n.º 14, 1999, p. 87.

[82] *Ibid.,* p. 87.

[83] MIRÓ LLINARES, *El cibercrimen…, op. cit.*, p. 154.

[84] LINS RIBEIRO, *op. cit.*, p. 86.

donde la cooperación judicial internacional entre los Estados cumple un rol de suma importancia para le persecución penal de los cibercrímenes.

Como apunta de forma acertada BALLESTEROS, el Internet es un entorno de gran particularidad para la seguridad, ya que no cuenta con fronteras geográficas generando un problema de supraterritorialidad y confrontación de legislaciones[86], lo cual le permite al crimen organizado transnacional.

2. La neutralidad de la Red

Otra característica que presenta el ciberespacio radica en la libertad que otorga a sus usuarios el poder navegar sin ningún tipo de restricción[87], en un mundo virtual en el que no existen límites físicos, ni territoriales[88]. Por estas consideraciones es que el ciberespacio se ha convertido en el quinto espacio estratégico dentro del mundo, conformado por mar tierra, aire y espacio[89]. Esta libertad ha sido objeto de innumerables críticas por parte de un sector. Los Estados Unidos ha sido el país en el que se ha generado mayor controversia respecto a esta discusión. Durante el Gobierno del presidente Barak Obama en el año 2015, se promulgaron regulaciones que impedían que las empresas proveedoras, que ofrecían el servicio de acceso a la red, pudieran incrementar sus tarifas. Sin embargo, en el año 2017, estos dispositivos legales fueron derogados por la Comisión Federal de las Comunicaciones (FCC)[90]. A pesar de

[85] ORGANIZACIÓN DE LAS NACIONES UNIDAS, "Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético", 12.° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador (Brasil), 12 a 19 abril del 2010, p. 4. Disponible en: <https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf>.

[86] BALLESTEROS SÁNCHEZ, Julio, *Exigencias político criminales y operativas en la lucha contra la criminalidad organizada transnacional en instrumentos jurídicos y operativos en la lucha contra el tráfico internacional de drogas*, Pamplona: Thomson Reuters Aranzandi, 2015, p. 175

[87] MIRÓ LLINARES, *El cibercrimen…, op. cit.*, p.155.

[88] ÉCIJA BERNAL, Álvaro. *El ciberespacio un mundo sin ley*, Madrid: Editorial Wolters Luwer, 2017, p. 9.

[89] *Ibid.,* p. 9.

ello, el en el 2018 el Estado de Washington ha promulgado la ley estatal que preserva la Internet abierta[91], con lo cual el debate aún sigue abierto.

En el caso del Perú, la neutralidad de la red se encuentra regulada en el artículo 6 de la Ley Nº 29904[92] y su reglamento, denominada Ley de promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fibra Óptica. El referido artículo 6, sobre la libertad de uso de aplicaciones o protocolos de banda ancha, establece: "Los proveedores de acceso a Internet respetarán la neutralidad de red por la cual no pueden de manera arbitraria bloquear, interferir, discriminar ni restringir el derecho de cualquier usuario a utilizar una aplicación o protocolo, independientemente de su origen, destino, naturaleza o propiedad".

El Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) lo define como a la neutralidad de la red, como un principio regulatorio, adoptado por el Perú mediante la Ley N.º 29904 y su reglamento (Decreto Supremo N.° 014-2013-MTC), por el cual se busca proteger el derecho a la libre elección de los usuarios del servicio de acceso a Internet, es decir, el derecho de acceder, de manera legal, a cualquier aplicación, protocolo, servicio o tráfico disponible en su servicio de acceso a Internet[93]. Además, la norma hace especial referencia a que el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) es el encargado de determinar las conductas que no serán consideradas arbitrarias, relativas a la neutralidad de red.

---

[90] LA CAPITAL, "EE. UU. deroga la ley de Obama que aseguraba la neutralidad de la red", 15 de diciembre del 2017. Disponible en: <https://www.lacapital.com.ar/el-mundo/eeuu-deroga-la-ley-obama-que-aseguraba-la-neutralidad-la-red-n1524319.html>.

[91] CNN, "Washington es el primer estado en aprobar una ley para proteger la neutralidad de la red", 6 de marzo del 2018. Disponible en: <https://cnnespanol.cnn.com/2018/03/06/neutralidad-red-estados-unidos-washington-ley-hb2282/>.

[92] El artículo 1 de la Ley N.º 29904 establece: "Artículo 1.- *Objeto de la Ley*. El propósito de la Ley es impulsar el desarrollo, utilización y masificación de la Banda Ancha en todo el territorio nacional, tanto en la oferta como en la demanda por este servicio, promoviendo el despliegue de infraestructura, servicios, contenidos, aplicaciones y habilidades digitales, como medio que favorece y facilita la inclusión social, el desarrollo socioeconómico, la competitividad, la seguridad del país y la transformación organizacional hacia una sociedad de la información y el conocimiento".

[93] OPSITEL, "Neutralidad de red". Disponible en: <https://www.osiptel.gob.pe/portal-de-operadoras/regulacion/neutralidad-de-red/>.

En el caso de España, su normativa en materia de regulación de neutralidad de la red se rige por el Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, del 25 de noviembre de 2015, por el que se establecen las medidas referentes al acceso a la Internet abierta y esta su vez se modificó por la Directiva 2002/22/CE, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones.

3. La virtualidad

En la actualidad el derecho virtual del siglo XXI, está pasando por un proceso de transformación en cuanto a sus características y estructuras como son el ser desterritorializado y fractalizado[94]. Bajo esa premisa, refiere CARREÑO DÍAZ que el derecho comprende la cibercultura emergente que está reconstruyendo y reconfigurando un nuevo mundo, el cibermundo[95]. Este derecho de la era posindustrial, cubierto de un alto contenido tecnológico, requiere de nuevas bases para su desarrollo, ya que sus cambios y rápidos avances plantean la necesidad de un derecho amplio y participativo, y esto se da en razón de que "los ciberciudadanos, gracias a la interconexión, en redes se constituyen en intérpretes y participantes activos en la vida del Estado y de la Constitución, es una sociedad abierta, transparente y ante todo participativa[96].

Desde hace muchos años, el término virtualidad se ha utilizado como algo que existe, gracias a nuestra parte sensorial, basada en los sentidos y en cómo estas sensaciones llegan al cerebro[97]. En la actualidad el concepto de virtualidad se emplea en espacios económicos, financieros, laborales, académicos, judiciales, el mercado, el arte, la inteligencia colectiva, administrativos, científicos y educativos[98]; es decir, los seres humanos tienen la capacidad de imaginar esa

---

[94] CARREÑO DUEÑAS, Dalia, "El Derecho en la era de la Virtualidad. Nuevas Realidad Nuevo Derecho Virtual", en *Ars Boni et Aequi*, vol. 8, n.º 2, 2012, p. 265.

[95] *Ibid.,* p. 266.

[96] *Idem*.

[97] MARTÍNEZ HERNÁNDEZ *et al., op. cit.*, p. 6.

realidad que se da en el ciberespacio. Bajo las palabras de MARTÍNEZ HERNÁNDEZ *et al.*, "el concepto de virtualidad se utiliza no solo en algo inexistente o videojuegos, sino que se utiliza en espacios económicos, financieros, el trabajo, el mercado, el arte, la inteligencia colectiva, administrativos, científicos y educativos como lo son la lectura, escritura, el ciberespacio y las aulas virtuales, entre otros muchos"[99].

En ese sentido, siguiendo lo dicho por MARTÍNEZ HERNÁNDEZ *et al.*, la palabra virtualidad significa que, por medio del proceso imaginario, permite al hombre entrar en otro proceso que es el de aprendizaje; por medio de él podemos transformar la realidad y a su vez entenderla[100]. Para LEVY, el concepto de lo virtual lleva tres sentidos: la acepción del sentido común, el sentido filosófico y la noción técnica de mundo virtual[101].

Con el auge de los avances de la tecnología y la información de la comunicación, se han podido crear determinados entornos de comunicación, que no están sujetos a un medio físico y en los que la información se sitúa en un espacio no real, ciberespacio o espacio virtual, de modo que se puede transmitir la información de modo instantáneo y a escala mundial[102]. Es en este entorno de la modernidad que la palabra virtual adquiere un significado de vital importancia, en lo que se refiere a espacio virtual, moneda virtual, educación virtual, economía virtual, banca virtual, etc. En la virtualidad, los seres humanos nos comunicamos, interactuamos e intercambiamos diverso tipo de información, que puede variar desde lo muy personal a aspectos eminentemente financieros. A través de la virtualidad, podemos escuchar, leer y ver imágenes digitales; por lo tanto, el sistema binario permite la traducción y codificación de las palabras, números y

---

[98] *Ibid.,* p. 6.

[99] *Idem*.

[100] *Idem*.

[101] CARREÑO DUEÑAS, *op. cit.*, p. 255.

[102] GONZÁLES SÁNCHEZ, Margarita y HERNÁNDEZ SERRANO, María José, "Interpretación de la virtualidad. El conocimiento mediado por espacio de interacción social", en *Apertura,* vol. 8, n.º 9, diciembre del 2008, p. 10. Disponible en: <http://www.redalyc.org/articulo.oa?id=68811230001>.

otras variables en series de ceros y unos, para procesarlos por medio de microprocesadores; esto explica las características básicas de la tecnología y su dimensión revolucionaria[103].

4. La falta de territorialidad

El territorio es un espacio de tierra que le pertenece a un Estado o jurisdicción determinado. En el caso del Perú, el artículo 54 de la Constitución Política establece, en lo que se refiere al territorio, soberanía y jurisdicción, que "el territorio del Estado es inalienable e inviolable, comprende el suelo, subsuelo, el dominio marítimo, y el espacio aéreo que los cubre"[104]. De manera general, el principio de territorialidad puede definirse como aquel criterio que establece con carácter exclusivo la aplicación de una ley a todos los hechos que se cometan dentro de ese territorio[105]. En buena cuenta, el estado solo tiene poder para legislar y ejercer su *ius imperium*, con la limitación de no exceder sus fronteras físicas[106].

En materia estrictamente punitiva, en lo que se refiere a la aplicación espacial de la ley penal, el principio de territorialidad plasmado en el artículo 1[107] del Decreto Legislativo N.º 635, Código Penal peruano, de forma taxativa, determina que la ley penal peruana se aplica a todo el que comete un hecho punible en el territorio de la República, salvo determinadas excepciones contenidas en el derecho internacional. Está claro entonces que los territorios en el mundo se rigen bajo determinadas regulaciones que permiten ejercer un determinado tipo de control, respecto a los sucesos que pudieran ocurrir en sus espacios o jurisdicciones.

---

[103] MARTÍNEZ HERNÁNDEZ *et al., op. cit.*, p. 14.

[104] Artículo 24 de Constitución Política del Perú de 1993.

[105] ÉCIJA BERNAL, *op. cit.,* p. 14.

[106] *Ibid.,* p. 14.

[107] Artículo 1 del Decreto Legislativo N.º 635 - Código Penal.

Sin embargo, en el ciberespacio pasa todo lo opuesto. Si bien este nos transmite la sensación de que se encontraría en todos lados, lo cierto y concreto es que físicamente no se encuentra en ningún sitio como para poder establecer una ubicación en relación con un suceso específico acontecido dentro de este espacio virtual, que permita ejercer algún tipo reacción por parte del Estado. Como bien explica ÉCIJA BERNAL, este no está limitado por fronteras físicas, ni por ciberfronteras[108]. "Cualquier persona, puede acceder desde cualquier dispositivo a una Web, si se cuenta con una dirección URL"[109].

V. DERECHO PENAL Y TIC

El derecho penal, a lo largo de su concepción, ha variado sus formas y ámbito de intervención, siempre teniendo como premisa que este es de *ultima ratio* y se ampara en el principio de mínima intervención y fragmentariedad[110]. Sin embargo, con la aparición de la informática, el derecho penal tradicional ha tenido que sufrir un proceso de adaptación teórica en lo que se refiere a la protección de datos y a la información digital como bienes jurídicos protegidos[111].

En el ámbito del derecho penal, se están planteando nuevas bases jurídicas y normativas relacionadas con el control del espacio digital, que permitan contrarrestar la aparición de nuevas actividades criminales de particulares proyecciones en un mundo cada vez más digitalizado. Hablo de una nueva sociedad digitalizada que supera el sentido de la territorialidad nacional, que plantea nuevos desafíos éticos y morales, que violenta la intimidad de la sociedad en términos masivos, que utiliza un metalenguaje distinto al formal sobre el que opera las normas legales tradicionales, que manipula el Internet a

---

[108] ÉCIJA BERNAL, *op. cit.,* p. 14.

[109] *Ibid.,* p. 14.

[110] JIMÉNEZ HERRERA, Juan Carlos, *Manual de derecho penal informático*, Lima: Jurista Editores, 2017, p. 90.

[111] SAIN, Gustavo, *La estrategia gubernamental…*, *op. cit*., p. 12.

su antojo y propia conveniencia, y que hace uso de una robótica cada vez más sofisticada como medio de operatividad para lograr sus fines.

Con el uso de las nuevas tecnologías para cometer ataques cibernéticos contra gobiernos, negocios e individuos, palabras y frases que hace una década apenas existían hoy forman ahora parte de nuestro vocabulario diario. Estos delitos no conocen fronteras, ni físicas ni virtuales, causan importantes daños y suponen un peligro muy real para las víctimas de todo el mundo. Las formas tradicionales de delincuencia también han evolucionado. Igual acontece con las organizaciones delictivas que utilizan cada vez más Internet, con el fin de facilitar sus actividades y maximizar los beneficios en el menor tiempo posible. Estos delitos facilitados por medios electrónicos no son necesariamente nuevos —robo, fraude, estafa, juegos de azar ilícitos, lavado de activos, venta de medicamentos falsificados—, pero han adquirido una nueva dimensión en línea.

La ciberdelincuencia viene creciendo a un ritmo cada vez más acelerado, con nuevas tendencias impredecibles emergiendo continuamente con nuevas modalidades que superan la legislación penal vigente. La policía y los órganos de control penal deben por lo tanto mantenerse al día en las nuevas tecnologías, con el fin de comprender las posibilidades que crean los delincuentes digitalizados, como una herramienta eficaz para prevenir y controlar la ciberdelincuencia. En nuestro medio, desde algún tiempo relativamente reciente, se vienen planteando algunas medidas sustantivas y adjetivas reformadoras para prevenir, procesar y enfrentar el fenómeno de la delincuencia cibernética o digitalizada en sus distintas y cada vez más variadas y complejas modalidades.

En el ámbito delictivo, como refiere TEMPERINI, a lo largo de la historia el delito ha encontrado en la tecnología a una poderosa aliada, toda vez que los delincuentes, como parte de su evolución en la ejecución delictiva, siempre han buscado estar a la vanguardia con la innovación tecnológica[112] para lograr sus objetivos. El progreso tecnológico que se está produciendo en esta nueva era de la sociedad de la información permite que se genere un nuevo espacio de

[112] TEMPERINI, *op. cit.*, p. 52.

reflexión jurídica, productos de los problemas que puedan ir dándose con la implementación de estas nuevas TIC[113].

En la búsqueda de soluciones normativas, de orden doctrinario y jurisprudencial que plantean la telemática e informática, es que el derecho se ha visto en la necesidad de crear una nueva rama en la que se puedan discutir y plantear soluciones dogmáticas a una nueva especialidad a la que se le conoce como *derecho informático*, que es una vertiente que se caracteriza por regular las relaciones jurídicas con alto componente y telemático[114]. En esa misma el *derecho penal informático* tiene como finalidad la protección de bienes jurídicos que nacen del derecho sobre la información[115].

El derecho penal que se pretende para la sociedad de la información estaría regido por premisas similares a las que han inspirado el derecho penal de la sociedad del riesgo; se debe comprender como una expansión en forma de respuesta a dicha sociedad del riesgo, que se vincula básicamente a su utilización para defender a la sociedad moderna de esos nuevos peligros tecnológicos[116].

En el pensamiento de SILVA SÁNCHEZ, la sociedad actual en la que vivimos es una sociedad de riesgos, que aparece caracterizada por un entorno económico de permanente evolución y la incorporación de los avances tecnológicos. Si bien estos avances en la economía y tecnología han tenido una gran incidencia positiva en el desarrolla de la humanidad; sin embargo, estos nuevos estándares modernos también dan lugar a que en el ámbito de la delincuencia tradicional aparezcan nuevas modalidades delictivas que se consuman en espacios de un alto contenido tecnológico[117].

---

[113] PALOMINO MARTÍN, *op. cit.* pp. 48-49.

[114] *Ibid.,* p. 50.

[115] *Ibid.,* p. 51.

[116] NARRALO BOLARTE, Enrique, "Incidencia de las nuevas tecnologías en el sistema penal: Aproximación al derecho penal en la sociedad de la información", en *Derecho y Conocimiento,* vol. 1, Universidad de Huelva: 2001, pp. 191-257.

Con toda esta evolución e innovación tecnológica urge la necesidad de que el derecho penal intervenga, ya que los delitos convencionales, como es el caso del delito de hurto y estafa, por mencionar algunos, vienen siendo potenciados por estas nuevas tecnologías, que no hacen otra cosa que elevar a un nivel de desarrollo del *iter criminis*[118]. Además de lo señalado, el delito informático no hace diferencia entre los sujetos pasivos, es decir, basta que el usuario acceda a la red o Internet, para poder ser una potencial víctima de esta nueva era delictiva digital.

En el ámbito de protección jurídica de los delitos contra el honor, la masividad de la difusión del contenido, mediante el uso de las nuevas tecnologías (difamación, injuria y calumnia), hace que la producción del daño al darse de forma masiva e instantánea se vea enormemente potenciada[119]. A partir de lo señalado, podemos decir que es necesaria la intervención del derecho penal en esta nueva era social moderna enmarcada en la utilización de las nuevas tecnologías de la información y la comunicación (TIC), en la que los delitos tradicionales se ven altamente potenciados por la tecnología. Además de los delitos informáticos clásicos que ya son parte de los ordenamientos jurídicos en todo el mundo, siguen apareciendo nuevas formas delictivas que requieren de una tipificación específica.

VI. CIBERCRIMINALIDAD

El cibercrimen se encuentra estrechamente vinculada con la evolución y utilización de las tecnologías de la información y la comunicación (TIC), fenómeno el cual sigue siendo algo totalmente novedoso y poco entendido por otros, como veremos más adelante[120]. En la década del 70 surge un nuevo

---

[117] SILVA SÁNCHEZ, Jesús María, *La expansión del derecho penal: Aspectos de la política criminal y las sociedades postindustriales*, Buenos Aires: Edisofer, 2011, p. 13.

[118] TEMPERINI, *op. cit.*, p. 53.

[119] *Ibid.,* p. 53.

[120] MIRÓ LLINARES, *El cibercrimen…, op. cit.*, p. 25.

paradigma que da lugar a un nuevo modelo de desarrollo social, basado en el uso de las nuevas tecnologías de la información y la comunicación; mediante ellas se desplaza al modelo adoptado por la revolución industrial vigente desde el siglo XIX[121]. En los años 80 se caracteriza por ser un modelo de desarrollo social basado en la *información*, lo que hoy en día se conoce como la *sociedad de la información,* en la cual el procesamiento de la información es fundamental para el desarrollo organizativo y productivo de la sociedad[122].

Este nuevo paradigma de las tecnologías de la información y la comunicación, dotado de una permanente evolución, ha generado una nueva forma de poder, denominado *poder informático*, el cual no ha sido indiferente al derecho. Como explica MARTÍNEZ, "este se debe adoptar, por un lado, la nueva postura de legitimarlos en virtud de los magníficos beneficios que proporciona a los individuos; por otro lado, debe adoptar una postura contenedora, debido a los peligros que puede ocasionar a las personas"[123]; es decir, se van creando nuevas herramientas jurídicas con la finalidad de resguardar y proteger los derechos frente a esta nueva forma de abuso de poder tecnológico en desmedro de la sociedad.

Tradicionalmente, se ha pensado que la informática abarca la ciencia de la computación compuesta del *hardware* y *software;* sin embargo, esa apreciación es muy limitada, ya que hoy por hoy la informática proporciona una serie beneficios en distintos estamentos del desarrollo de la sociedad, como los negocios, medicina, inteligencia artificial, medios de pago, etc. Sin embargo, así como las nuevas tecnologías han significado una gran contribución para el

---

[121] ÉCIJA BERNAL, *op. cit.,* p. 11. En ese sentido, MARTÍNEZ refiere que "con el advenimiento del fenómeno informático se ha originado una revolución en todo el mundo, lo que nos permite afirmar que estamos siendo protagonistas de una nueva era: la Era Informática. Así, se ha sostenido que "en la sociedad del siglo XXI se ha producido el tránsito de la era industrial a la de la información". MARTÍNEZ, Matilde S., "Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil", en *Cibercrimen y delitos informáticos Los nuevos tipos penales en la era del internet,* Buenos Aires: Erreius, 2018, p. 33.

[122] *Ibid.,* p. 11.

[123] *Ibid.,* p. 33.

desarrollo económico y social, no es menos cierto que también se han abiertos nuevos espacios para que lo individuos puedan cometer conductas delictivas, las cuales se les conocen como *cibercrimen, cybercrime, cyberdelinquency, cibercriminalidad, ciberdelincuencia, delitos informáticos.* Las dos últimas acepciones son las de mayor uso en países de habla hispana.

El *Manual de Recursos de Justicia Criminal del Departamento de Justicia* de los Estados Unidos del año 1979 lo define como "cualquier acto ilegal donde el conocimiento de la tecnología computacional es esencial para el éxito de su prosecución"[124]. La Organización de Cooperación y Desarrollo Económico en 1983 definía al delito informático como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y transmisiones de datos"[125].

El Consejo de Europa los define como "cualquier delito penal donde las autoridades de investigación deben obtener acceso a información que ha sido procesada o transmitida por sistemas de computacionales o sistemas de procesamiento electrónico de datos"[126]. La vinculación entre la tecnología y el delito se da a partir del surgimiento del telégrafo durante el siglo XIX; en aquel entonces se interceptaban comunicaciones con la finalidad de falsear el contenido de las mismas con fines económicos[127]. En los años 70, también se dieron antecedentes de cibercrímenes vinculados al sabotaje del financiamiento gubernamental a la guerra de Vietnam[128], realizado por los *phreakers*[129].

---

[124] *Idem.*

[125] *Idem*.

[126] *Idem*.

[127] SAIN, Gustavo, *La estrategia gubernamental…*, *op. cit*., p. 7.

[128] *Ibid*., p. 7.

[129] Término que se refiere a un grupo de adolescentes, varios de ellos ciegos, que en los años 60 y 70 estaban fascinados con el sistema telefónico, que pasaban sus días buscando y encontrando ingeniosas formas de lograr que la red hiciera cosas que ni las compañías telefónicas se habían llegado a imaginar. GRANGE, Jeremy, "Quiénes eran los *phreakers*, los extraordinarios personajes que hackeaban las redes telefónicas cuando no había computadores", en *BBC,* 1 de abril del 2017. Disponible en: <https://www.bbc.com/mundo/noticias-39433955>. "El activismo político hippie de la época tuvo

Asimismo, en estos años se empiezan a consolidar las primeras consumaciones de delitos informáticos de contenido económico, dentro de los cuales destacaban el espionaje informático en la modalidad de extracción de discos rígidos de las computadoras o hurto de *diskettes*, la piratería de *software*[130] o programas[131]. A comienzos de la década de los 80, se dan los primeros fraudes informáticos financieros; estos se basaban en la alteración de bases de datos de empresas y entidades financieras[132].

En los años 90, con la expansión global del Internet en el mundo y el ingreso de las distintas empresas y financieras en el comercio electrónico, empezaron a darse un cúmulo de ciberataques vinculados al sector discográfico, cinematográfico, afectándose primordialmente derechos de autor, mediante las descargas ilícitas en línea de material digital, además de la distribución de material pornográfico infantil, con lo cual las nuevas tecnologías comenzaron a convertirse en una preocupación mundial frente a su potencial uso delictivo[133].

En sus comienzos, las primeras construcciones dogmáticas referidas a los delitos informáticos no fueron concebidas por sus autores, "en el sentido de un grupo autónomo de infracciones penales con caracteres sistemáticos"[134]. La

---

su costado informático a través de los *phreakers* (neologismo proveniente de las palabras en inglés freak, de rareza; *phone*, de teléfono; y free, gratis) donde a través de las llamadas blue box o cajas azules establecían comunicaciones en forma gratuita simulando los tonos de llamadas utilizadas por la Bell Corporation y la ATT, básicamente para comunicaciones de larga distancia. Con el correr del tiempo, estas técnicas de hacking alcanzaron un mayor grado de sofisticación, utilizadas también para las manipulaciones de transferencias de dinero por redes telefónicas vulnerables. En cuanto a la utilización de computadoras, la principal preocupación estaba dada por el manejo de la información a partir del almacenamiento y procesamiento de datos personales". SAIN, Gustavo, "Evolución histórica de los delitos informáticos", en *Revista Pensamiento Penal,* vol. 2, 2015, pp. 1-2.

[130] Siguiendo a JIMÉNEZ HERRERA, software es definido por la Real Academia Española como: "un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora, es decir es la parte lógica del ordenador". El software es desarrollado mediante distintos lenguajes de programación, que permiten controlar el comportamiento de una máquina. JIMÉNEZ HERRERA, *op. cit.,* p. 35.

[131] SAIN, Gustavo, *La estrategia gubernamental…*, *op. cit*., p. 8.

[132] *Idem.*

[133] *Ibid.,* p. 8.

[134] MIRÓ LLINARES, *El cibercrimen…, op. cit.*, p. 34.

misma estructura típica del delito informático y sus elementos objetivos lo enmarcaban dentro de aquellos comportamientos ejecutados a través de procesos electrónicos, y sobre aquellos comportamientos, que afectaban bienes relacionados con el *hardware* y el *software*[135].

A diferencia de la delincuencia tradicional, basada en la comisión de delitos clásicos, la cibercriminalidad supone un tipo de criminalidad característica especial que se materializa a través de los medios informáticos y telemáticos[136]. En sus comienzos la doctrina penal no se enfocó en establecer de forma categoría un bien jurídico común, como ámbito de protección, en este tipo de ilícitos penales[137]. Si no que, muy por el contrario, los bienes jurídicos, como el patrimonio y el orden socioeconómico, se consideraban protegidos por los delitos informáticos[138].

Según SAIN, en la actualidad los delitos informáticos se pueden clasificar en dos grupos: aquellos que requieren de una sofisticación técnica para su comisión, basados en *softwares* maliciosos desarrollados por los *hackers* con la finalidad de vulnerar dispositivos o redes para obtener un beneficio económico[139]; y la segunda está direccionada a aquellos delitos que adquieren una nueva vida en la nube y son intermediados por servicios aplicaciones web denominadas *ingeniería social*, que se diferencia de la *ingeniería técnica*, porque se basa en la modalidad del engaño[140]. Como refiere MIRÓ LLINARES, la denominación cibercriminalidad sirve para definir un ámbito de riesgo particular y específico que tiene mucha relación con el uso de las TIC.

---

[135] *Ibid.,* p. 35.

[136] FERNÁNDEZ BERMEJO y MARTÍNEZ ATIENZA, *op. cit.,* p. 116.

[137] MIRÓ LLINARES, *El cibercrimen…, op. cit.*, p. 35.

[138] *Ibid.,* p. 45.

[139] SAIN, Gustavo, *La estrategia gubernamental…, op. cit.,* p. 11.

[140] *Ibid*., p. 11.

VII. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS SEGÚN TEMPERINI

1. Los delitos de cuello blanco

En esta categoría se caracteriza y circunscribe solo a un grupo selecto de individuos que pueden acceder de forma privilegiada a determinados conocimientos tecnológicos y profesionales, para la comisión de delitos informáticos. Sin embargo, el mismo TEMPERINI señala que esta categoría ya no sería tan exacta porque "la evolución en materia de inseguridad informática ha llevado a que los conocimientos sean cada vez más accesibles y difundidos"[141]. Posición que compartimos, ya que, en la actualidad, el conocimiento de la informática es de fácil acceso para cualquier persona común, a través de Internet, tutoriales gratuitos, etc.

2. Transnacionales

Al igual que en el ciberespacio, la posibilidad tecnológica de la comunicación a distancia a través de las redes concibe que el delincuente se pueda ubicar en cualquier territorio o jurisdicción, muy alejado de las víctimas. Esta es una de las grandes problemáticas que presenta esta forma de delincuencia transnacional, ya que hay jurisdicciones que, por sus propias características o normativa interna, son poco cooperantes, lo que dificulta la persecución de la acción penal de este tipo de delitos. Acertado es TEMPERINI al establecer que "la internacionalidad como propiedad de los delitos informáticos, implica que los mismos no encuentren barreras jurisdiccionales para llevarse a cabo"[142]. En el plano de la pragmática, es técnicamente viable estar conectado a una red en el Perú y cometer el delito en España, sin duda que frente a esta fenomenología delictiva surgen interrogantes como lo son: qué legislación se debería aplicar al caso en concreto o si los canales de cooperación internacional entre los distintos Estados están cumpliendo con efectividad su razón de ser.

---

[141] TEMPERINI, *op. cit.*, p. 63.
[142] TEMPERINI, *op. cit.*, p. 63.

3. Instantáneos

Esta característica es propia de las nuevas tecnologías con las que se llevan a cabo los ciberdelitos, se materializa en lo instantáneo de la ejecución del delito; es decir, el delito se consuma con acción de ejecución del mismo[143], más allá con los actos preparatorios que pudieran haber demorado la elaboración de un ataque sistemático.

4. Masivos

Esta característica tiene relación directa, según TEMPERINI, con las posibilidades tecnológicas de difusión masiva de contenidos, haciendo la precisión que esta característica es independiente en relación con la instantaneidad anteriormente analizada[144].

5. Anonimato

Mediante esta característica nos referimos a la posibilidad de lograr distintos niveles de ocultamiento que ofrecen las nuevas tecnologías, y en especial los criptoactivos, que son de suma utilidad para los ciberdelincuentes al momento de perpetrar sus ataques. Este anonimato se da en dos vertientes: la primera dirigida al ocultamiento de la identidad del agente que comete el delito, y la

---

[143] *Idem.*

[144] *Ibid*., p. 63.

segunda enfocada en la utilización de la red[145], es decir, la verdadera conexión desde la cual se está ejecutando el ciberdelito[146].

6. Pluriofensivos

Siguiendo a VILLAVICENCIO, el bien jurídico tutelado en los delitos informáticos a la vez como es el caso de la intimidad, daños, seguridad nacional, etc.

7. Investigación compleja

El uso de las nuevas tecnologías en la comisión de ilícitos, sin duda que también significan un mayor desafío para los operadores de justicia, al momento de su ejecución. Este desafío se da en todos los estamentos, ya que este tipo de investigación compleja, revestida de un alto contenido tecnológico, requiere que las autoridades que intervienen en dichos actos de investigación tengan el conocimiento técnico suficiente para llevar a cabo una investigación eficaz[147].

VIII. CLASIFICACIÓN DE LOS CIBERCRÍMENES SEGÚN MIRÓ LLINARES

1. Los cibercrímenes económicos

Tienen como objetivo la obtención de un beneficio económico patrimonial, por parte de sus autores, por lo que todos los ataques están dirigidos a afectar el

---

[145] En ese sentido: "El Internet oculto o Dark Web es una porción de la red en la que necesitas determinadas aplicaciones para poder conectarte, y eso es precisamente a lo que te vamos a ayudar, a descargarte y configurar estas herramientas para entrar en ellas. La primera será la de TOR, que posiblemente es la más conocida y utilizada de todas. Pero también te enseñaremos a conectarte a ZeroNet, Freenet e I2P para que puedas explorarlas todas y decidirte por la que más te haya convencido, ya sea por utilizarla a fondo o simplemente por curiosear en ella como nosotros hemos hecho también varias veces". FERNÁNDEZ, Yúbal, "Cómo entrar en la Deep Web: guía 2023 para entrar en TOR, ZeroNet, Freenet e I2P", en *Xataka,* 23 de marzo del 2023. Disponible en: <https://www.xataka.com/basics/como-entrar-deep-web-guia-2020-para-entrar-tor-zeronet-freenet-e-i2p>.

[146] TEMPERINI, *op. cit.*, p. 63.

[147] *Ibid.,* p. 67.

patrimonio individual de un individuo o al sistema económico en relación con las transacciones comerciales en Internet[148]. Se dividen en ciberataques puros, ciberataques de réplica y ciberataques de contenido.

Los primeros se caracterizan, primordialmente, en que su ejecución únicamente se puede materializar en el ciberespacio[149]. Dentro de este tipo de ciberataques tenemos el *hacking, malware intrusito, malware destructivo, ataques de insiders, ataques DoS, spam, ciberocupación de red* y *antisocial, networks*.

Los ciberataques de réplica se tratan de réplicas llevadas a cabo en el ciberespacio de crímenes que ya se realizaban, de otro modo, en el espacio físico[150]. Dentro de los que tenemos a los *ciberfraudes (phishing, pharming, scam, auction fraud…), cyberspyware (uso de sniffers y demás spyware, ciberespionaje de empresa), Identity theft, Spoofing (DNS spoofing, ARP spoofing, IP spoofing, web spoofing), ciberblanqueo de capitales ciberextersión* y *ciberocupación*[151]. Los ciberataques de contenido se caracterizan, porque el centro de la infracción lo constituye el contenido que se comunica o se transmite a través de las redes sociales telemáticas del Internet[152]. En esta categoría tenemos a la distribución de *pornografía infantil a través del Internet* y la *ciberpiratería intelectual*[153].

2. Los cibercrímenes sociales

Este tipo de ciberdelito está vinculado con las redes sociales, ya que, en los últimos años, han pasado a convertirse en el eje central de la comunicación social en el planeta. Existen distintos *softwares* o aplicativos como el Facebook,

---

[148] MIRÓ LLINARES, Fernando, *Cibercrimen, cibercriminales…, op. cit.,* p. 9.

[149] *Ibid.*, p. 51.

[150] *Ibid.*, p. 68.

[151] MIRÓ LLINARES, *El cibercrimen…*, *op. cit.,* p. 50.

[152] *Ibid.*, p. 100.

[153] *Ibid*., p. 50.

WhatsApp, Instagram, MySpace, entre otros, permitiendo que todas las personas en el mundo estén interconectadas e intercambien todo tipo de información, desde imágenes, videos, audios, textos, archivos, etc. Sin embargo, estos avances de la tecnología están siendo utilizados de manera indebida, atacando la intimidad de las personas, a través de injurias y calumnias masivas, que afectan la intimidad y el honor. En esa línea, los cibercrímenes sociales se desenvuelven dentro del ámbito de los ciberataques como son: *spoofing, cyberstalking, cyberbullying, online harassment* (ciberamenazas, coacciones, injurias, etc.), *sexting, online grooming*[154].

3. Los cibercrímenes políticos

Este tipo de cibercriminalidad se caracteriza por la transmisión de información con fines de ataque ideológicos. De igual forma que las dos modalidades anteriores, estos se clasifican en ciberataques puros (*cyberwar* y *cyberhacktivism*), ciberataques (ciberespionaje terrorista y ciberguerra) y los ciberataques de contenido.

IX. LAVADO DE ACTIVOS Y EL CIBERESPACIO

Desde su concepción internacional inicial en la Convención de Viena de 1988, el lavado de activos, como se le dice en varios sistemas penales en Latinoamérica, se define por primera vez, a partir de lo descrito en el texto normativo regulado en el artículo 3, inciso b), literales i y ii, respectivamente, en esta construcción dogmática inicial tenía como verbos rectores nucleares a los actos de conversión y transferencia de bienes, partiendo del conocimiento que debía tener el agente sobre la procedencia ilícita de los mismos. Similar técnica legislativa se utilizó para los actos de ocultamiento, tenencia y transporte, siempre partiendo del conocimiento previo que debía tener el autor frente al origen ilícito de las propiedades o bienes reales o derechos relativos a tales bienes. Fue a partir de

[154] *Idem.*

dichos parámetros normativos que los Estados que suscribieron el Convenio de Viena optaron por incorporar en sus legislaciones penales internas la tipificación del delito de blanqueo de capitales, también conocido en otros ordenamientos jurídicos penales como lavado de dinero o *money laundering*.

En relación con la fenomenología del lavado de activos, son muchas las definiciones que se han venido manejando en la doctrina en los últimos años. El Grupo de Acción Financiera de Latinoamérica (GAFILAT) lo define de la siguiente manera: "El proceso a través del cual es encubierto el origen de los fondos generados mediante el ejercicio de algunas actividades ilegales o criminales"[155]. PRADO SALDARRIAGA, quien ya hace un tiempo ha venido desarrollando un concepto operativo, en el que define a este delito como: "un conjunto de operaciones comerciales o financieras que procuran la incorporación al circuito económico formal de cada país, sea de modo transitorio o permanente, de los recursos, bienes y servicios que se originan o están conexos con actividades criminales"[156]. De igual parecer, para LAMAS PUCCIO, el lavado de activos constituye todas aquellas operaciones dirigidas a ocultar la fuente o el destino del dinero o activos que se han obtenido a través de actividades ilegales[157]. En ambas definiciones se puede advertir que se trata de un proceso conformado por operaciones financieras comerciales de distinta índole, destinadas a macular activos que tiene su origen en una actividad criminal. Sin duda que en la actualidad son diversos los textos jurídicos que se han escrito sobre el delito de lavado de activos, por lo que se hubiera podido abarcar una mayor cantidad de definiciones desarrolladas por la doctrina actual. Sin embargo, para los objetivos que pretendo demostrar en esta investigación doctoral, considero que las definiciones referenciadas grafican, de forma acertada, el estado de la cuestión sobre la definición del lavado de activos en la actualidad y la necesidad de que esta sea reformulada a partir de un nuevo

---

[155] Concepto tomado del glosario de términos de la página web del GAFILAT. Disponible en: <https://www.gafilat.org/index.php/es/glosario-de-definiciones>.

[156] PRADO SALDARRIAGA, Roberto, *Lavado de activos y financiación del terrorismo*, Lima: Editora Jurídica Grijley, 2007, p. 9.

[157] LAMAS PUCCIO, Luis, *Lavado de activos y operaciones sospechosas*, Lima: Pacifico Editores, 2016, p. 89.

escenario delictivo dotado de nuevos componentes tecnológicos que no fueron tomados en cuenta al momento de su concepción jurídica.

Como se puede apreciar, en cada una de las distintas definiciones que han sido citadas, se hace referencia a un procedimiento basado en operaciones claramente diferenciadas por su funcionamiento en sus distintas fases o etapas de lavado, que tienen como finalidad dar una apariencia legítima a los activos o ganancias que han sido obtenidos en una actividad delictiva previa, para su posterior acoplamiento al sistema económico. De hecho, las definiciones señaladas en relación con el lavado de activos han venido funcionando de forma bastante armoniosa y consolidada bajo los esquemas actuales de criminalización de dicho fenómeno delictivo.

Sin embargo, en los últimos años viene dándose un fenómeno global de gran escala, en el que aparecen nuevas conductas criminógenas estrechamente asociadas con el uso de nuevas tecnologías, que se caracterizan principalmente por su ubicación y desenvolvimiento dentro del ciberespacio. En este nuevo escenario, el avance tecnológico permite, mediante la transnacionalidad, las operaciones electrónicas, desplazando la moneda tradicional por medios de pago electrónicos[158].

El lavado de activos no ha sido ajeno a este nuevo escenario, sino, muy por el contrario, empiezan a surgir nuevas formas de lavado a través del uso de las nuevas tecnologías en el ciberespacio. En el año 2014 el Grupo de Acción Financiera Internacional (GAFI) emitió un informe titulado *Virtual Currencies Key Definitions and Potential AML/CFT Risks,* en el que estableció que las monedas virtuales son potencialmente vulnerables para el lavado de activos y el financiamiento al terrorismo, ya que su misma estructura está compuesta por elementos que permiten un mayor anonimato que los métodos de pago en

[158] CALLEGARI, André Luis. *El delito de blanqueo de capitales en España y Brasil*, Bogotá: Universidad Externado de Colombia, 2003, pp. 104-105. Al respecto, sostiene Callegari que "resulta demasiado restrictivo hablar exclusivamente de blanqueo de dinero, ya que la noción de valores patrimoniales permite englobar en la noción de blanqueo no sólo el dinero en metálico obtenido de forma ilícita, sino también los títulos, los derechos de crédito, las piedras y metales preciosos, los bienes muebles e inmuebles, etc.".

efectivo. Otro factor de suma trascendencia se manifiesta en el riesgo potencial que ofrece la negociación y transacción de las monedas virtuales, mediante la utilización del ciberespacio, accediendo mediante la utilización del Internet, lo cual dificulta la identificación de los sujetos intervinientes[159] en la transacción.

Si bien, en su historia evolutiva, el lavado de activos ha ido evolucionando desde su concepción inicial como un delito en el que el agente realizaba actos de conversión, transferencia, tenencia y ocultamiento, así como de transporte de dinero ilícito. Si bien las tipologías mencionadas están estrechamente vinculadas con el sistema financiero, para su ejecución mediante actos de conversión y transferencia requieren el uso de lo que se denomina *banca por Internet* o *banca digital*, sistema que funciona desde larga data, y es lo que permite la realización de transferencias entre usuarios de una misma entidad financiera, interbancarias, pagos de servicios, cambio de tipo de moneda, pago de créditos, etc., situaciones que se dan de forma inmediata en tiempo real y de forma segura. Además, no podemos soslayar el control y supervisión rigurosa a la que son sometidas este tipo de transacciones por parte de los sujetos obligados de las mismas entidades bancarias.

Sin embargo, recientemente se empieza a conocer por un sector minoritario de la doctrina una nueva forma de blanqueo de dinero, la cual ha venido evolucionando a gran velocidad de forma extraordinaria, sin que existan fronteras que lo limiten, disponiendo del ciberespacio para tales fines[160], conocida por algunos autores[161] como el *ciberlavado, cyber laundering* o el

---

[159] Véase el Informe del GAFI: GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, "Virtual Currencies Key Definitions and Potential AML/CFT Risks", junio del 2014, p. 11.

[160] RUIZ-CLAVIJO GARCÍA, Teresa, "Recursos para la prevención de delitos relacionados con el blanqueo de capitales y cibercriminalidad", en Abel GONZÁLEZ y Daniel FERNÁNDEZ (coords.), *El blanqueo de capitales y su relación con la cibercriminalidad*, Pamplona: Editorial Aranzandi, 2019, p. 97.

[161] En ese sentido, han escrito sobre el particular los siguientes autores: Miró Llinares, *El cibercrimen…, op. cit.*, p. 83. FUENTES REQUENA, Ramón y GONZÁLES GARCÍA Abel, "*Modus operandi* en el ciberblanqueo. Experimento práctico", en Abel GONZÁLEZ y Daniel FERNÁNDEZ (dirs.), *El blanqueo de capitales y su relación con la cibercriminalidad*, Pamplona: Editorial Aranzandi, 2019, pp. 59-75. GONZÁLES GARCÍA, Abel y SANZ SIERRA, Javier, "Financiación del terrorismo y ciberblanqueo", en Abel GONZÁLEZ y Daniel FERNÁNDEZ (dirs.), *El blanqueo de capitales y su relación con la cibercriminalidad*, Pamplona: Editorial Aranzandi, 2019, pp. 107-

ciberblanqueo. Esta construcción dogmática tiene su origen en la unión de dos palabras *ciberespacio* y el *lavado* o *blanqueo*: la primera de ellas se define como un espacio virtual creado por medios digitales e informáticos, es decir, un espacio global virtual sin fronteras que funciona sobre la base de un conjunto de procedimientos tecnológicos que permiten la interconexión en lo que se conoce como una sociedad moderna. Por su parte, el término *lavado* se puede entender como aquellos actos tendientes a ocultar o camuflar ganancias de origen ilícito, a través de un proceso de estratificación para su posterior consolidación en el circuito económico.

Habiendo realizado estas precisiones de orden conceptual, podemos definir al ciberlavado de activos como aquella conducta delictiva que utiliza medios tecnológicos a través del ciberespacio para dotar de una apariencia legítima a todas aquellas ganancias ilícitas que tiene su origen en una actividad criminal previa. En la doctrina moderna sobre el lavado de activos, ANZOLA lo define "como proceso en virtud del cual los bienes de origen delictivo se integran al sistema económico legal mediante la utilización de las TIC a fin de darles una apariencia de licitud"[162]. Se advierte que esta nueva conceptualización del ciberlavado enmarca el proceso de lavado a partir del uso del factor tecnológico, como punto medular para la incorporación de los activos al sistema económico legal. PICOTTI, desde un sentido criminológico, lo define como todas aquellas actividades ilimitadas dirigidas a limpiar capitales, bienes o valores, recurriendo a medios cibernéticos, que otorgan las TIC[163].

Al día de hoy, el lavado de activos va evolucionando a la par con las TIC, situación que pone más en boga el uso de la acepción ciberlavado de activos, ya que, salvo los actos tradicionales de transporte de dinero o activos sucios, las

112. FERNÁNDEZ MARTÍNEZ, Juan Carlos, "Evasión de impuestos y ciberblanqueo", en Abel GONZÁLEZ y Daniel FERNÁNDEZ (dirs.), *El blanqueo de capitales y su relación con la cibercriminalidad*, Pamplona: Editorial Aranzandi, 2019, pp. 115-124.

[162] ANZOLA, Ayelén, "Ciberblanqueo de capitales: El especial caso de los activos virtuales old wine in new bottles", en *Desafíos contra la lucha contra la corrupción: Gestión de riesgos y paradigmas globales*, Coruña: Colex, 2023, p. 117.

[163] PICOTTI, Lorenzo, "Profili penali del cyberlaundering: Le nuove tecniche di riciclaggio", en *Rivista Trimestrale di diritto penale dell'economía*, 2018, p. 591.

otras tipologías clásicas siempre se han visto inmersas en el uso de las nuevas tecnologías para su operatividad o funcionamiento, y no cabe duda que este se materializa mediante la utilización del ciberespacio. Actualmente, existen infinidad de *fintechs,* que son tecnologías aplicadas al sector financiero, en las que el ciberespacio se ha vuelto de vital importancia para su aplicación y uso a través del ciberespacio.

En el caso específico del delito de lavado de activos, su ejecución va muy entrelazada con el sistema financiero, ya que me refiero a un conjunto de operaciones complejas y muy sofisticadas que permiten la colocación e integración de activos o capitales sucios en el orden económico, para posteriormente ser integrados en sistema económico. En este escenario, el fenómeno de las nuevas tecnologías se viene posicionado en el sistema financiero, por lo que poco a poco se van desplazando los pagos con dinero en efectivo por medios de pago virtuales.

Por intermedio de las TIC se puede verificar en tiempo real mediante un aplicativo denominado como banca móvil —que funciona en el teléfono celular— los saldos, estados de cuenta, la realización de transferencias bancarias, solicitud de préstamos crediticios, y, lo más importante, puedes operar desde cualquier lugar del mundo sin tener que movilizarte, logrando tener un mayor control financiero de tus activos, ya que puedes realizar un seguimiento conjunto de todas tus operaciones, situación muy similar ocurre con los criptoactivos, como veremos más adelante.

La posibilidad de poder transferir dinero de forma anónima e instantánea a través del Internet se ha vuelto un pilar clave para las organizaciones terroristas; mediante las operaciones *online*, se transfieren fondos que permiten que estas organizaciones puedan subsistir[164]. La falta de supervisión y transnacionalidad global que ofrece el Internet mediante el ciberespacio, al no existir una frontera establecida incrementa las facilidades para la ejecución de cibercrímenes y la

[164] GONZÁLES GARCÍA y SANZ SIERRA, *op. cit.*, p. 112.

movilización de las ganancias obtenidas de estos[165]. Sumado a ello, tenemos que la revolución permanente del ciberespacio y las TIC ha permitido el instrumentalizar herramientas adicionales para los terroristas, como es el caso de las monedas virtuales, o la minera ilegal a través de mercados *online*[166].

De lo expuesto, podemos señalar que se trata de un espacio de oportunidad delictiva inigualable, porque que los agentes tienen menos restricciones espaciales y temporales para delinquir, sumándole a ello características propias del ciberespacio, como son las transnacionalidad, neutralidad de la red y la descentralización, es decir, un espacio entendido como universal, global, colectivo, lo que le otorga una gran dimensión[167]. El ciberespacio no cambia los caracteres esenciales que hacen que determinados eventos se les pueda seguir denominando crímenes, pero sí modifica los parámetros espacio y tiempo en los que el crimen tiene lugar, por lo que se afecta el contexto espacial y temporal en el que se consuma el delito[168].

X. GRUPO DE ACCIÓN FINANCIERA Y LAS NUEVAS TECNOLOGÍAS

1. La recomendación n.º 13: Banca corresponsal

A modo de recuento evolutivo en cuanto a la preocupación mostrada por el Grupo de Acción Financiera Internacional (GAFI), podemos señalar lo siguiente: en el año 1996 el GAFI, se preocupó de lo referido a las nuevas tecnologías a partir de la recomendación n.º 13[169], ya que estas suponen un enorme peligro

---

[165] *Ibid.*, p. 112.

[166] *Idem*.

[167] GÓMEZ INIESTA, Diego, "Utilización de las nuevas tecnologías en la comisión del blanqueo de dinero", en *Revista Virtual USMP*, 2018, p. 5. Disponible en: <https://derecho.usmp.edu.pe/cedp/revista/articulos/internacional/terrorismo.pdf>.

[168] *Idem*.

[169] En ese sentido, véase la nota interpretativa de la recomendación 13 del GAFI refiere: "Entre las relaciones similares a las que las instituciones financieras deben aplicar los criterios (a) al (e) están, por ejemplo, las que se establecen para transacciones de valores o transferencias de

para el lavado de activos, porque se trata de operaciones financieras de un volumen bastante significativo, además de que estas se pueden realizar desde cualquier parte del mundo, revestidas de un anonimato y sin ningún tipo de control por parte de las entidades financieras[170]. Además, como refiere SOUTO, las técnicas de investigación tradicionales devienen en poco efectivas y obsoletas, por lo que el desafío que significaba para los lavadores clásicos el tener que licuar grandes cantidades de dinero físico o papel moneda[171] hoy en día ha sido reemplazado por dinero electrónico, justamente porque su misma esencia no genera una presencia física y complicación en su traslado mediante el uso del Internet, lo que hace que la detección de la operación sospechosa sea muy compleja.

2. La recomendación n.º 15: Nuevas tecnologías

En relación con el tema objeto de investigación en este trabajo, la novedad incorporada por el GAFI es la recomendación n.º 15, referida a las nuevas tecnologías, los países y las instituciones financieras que deben identificar y evaluar los riesgos de lavado de activos o financiamiento del terrorismo que pudieran surgir con respecto (a) al desarrollo de nuevos productos y nuevas prácticas comerciales, incluyendo nuevos mecanismos de envío, y (b) el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como los existentes. En el caso de las instituciones financieras, esta evaluación del riesgo debe hacerse antes del lanzamiento de los nuevos productos, prácticas comerciales o el uso de tecnologías nuevas o en desarrollo. Los países y las instituciones financieras deben tomar medidas apropiadas para administrar y mitigar esos riesgos. Para gestionar y mitigar los riesgos que surjan de los

fondos, ya sea para la institución financiera transfronteriza en calidad de principal o para sus clientes. El término cuentas de transferencias de pago en otras plazas se refiere a las cuentas corresponsales que son utilizadas directamente por terceros para hacer operaciones en nombre propio".

[170] ABEL SOUTO, Miguel, "Blanqueo, innovaciones tecnológicas, amnistía fiscal de 2012 y reforma penal", en *Revista Electrónica de Ciencia Penal y Criminología,* n.º 14-14, 2012, p. 14:5. Disponible en: <http://criminet.ugr.es/recpc/14/recpc14-14.pdf>.

[171] *Ibid.,* p. 14.

activos virtuales, los países deben garantizar que los proveedores de servicios de activos virtuales estén regulados para propósitos ALA/CFT y tengan licencia o registro y estén sujetos a sistemas de monitoreo efectivo, así como asegurar el cumplimiento de las medidas relevantes requeridos en las recomendaciones del GAFI"[172].

La nota interpretativa de la recomendación n.º 15 establece como criterio que los países deben considerar a los activos virtuales como "bienes", "productos", "fondos" "fondos y otros "activos" y otros activos de "valor equivalente". Los países deben aplicar las medidas pertinentes en virtud de las recomendaciones del GAFI a los activos virtuales y a los proveedores de servicios de activos virtuales (PSAV), recomendación que tiene incidencia directa con el uso y comercialización de criptomonedas, como veremos en el capítulo respectivo.

Con respecto a las medidas preventivas para los proveedores de activos virtuales, la nota interpretativa de la recomendación n.º 15, en el punto 7, establece dos presupuestos: el primero referido a la debida diligencia[173], en cuanto al umbral de las transacciones, el cual no deber superar los 1000 USD/EUR; y el segundo dirigido a la obtención y resguardo de la información obligatoria y precisa del originador y del beneficiario o, si la hubiera, de la institución financiera, y que esta se ha puesto de forma inmediata en conocimiento de la autoridad competente[174].

---

[172] Véase la recomendación n.º 15 del Grupo de Acción Financiera Internacional.

[173] En ese sentido, la recomendación n.º 10 establece: "Si, durante el establecimiento o en el curso de la relación comercial o cuando se realizan transacciones ocasionales, una institución financiera sospecha que las transacciones están relacionadas al lavado de activos o el financiamiento del terrorismo, la institución debe entonces:(a) tratar normalmente de identificar y verificar la identidad[1] del cliente y del beneficiario final, sea permanente u ocasional, e independientemente de alguna exención o umbral designado que pudiera de otro modo aplicarse; y (b) hacer un reporte de operación sospechosa (ROS) dirigido a la Unidad de Inteligencia Financiera (UIF), de conformidad con la Recomendación 20".

[174] La recomendación n.º 16 señala, en relación con las transferencias electrónicas, lo siguiente: "Los países deben de asegurar que las instituciones financieras incluyan información sobre el originado que se requiere, y que sea precisa, así como la información requerida sobre el beneficiario en las transferencias electrónicas y mensajes relacionados y que la información permanezca con la transferencia electrónica".

3. *Report of New Payment Methods*

En el año 2006 el GAFI elaboró un informe sobre nuevos métodos de pago: *Report of New Payment Methods.* En dicho documento se hace referencia a las nuevas innovaciones tecnológicas de pago que se llevan a cabo mediante el Internet, los dispositivos inalámbricos e incluso redes de pago, y cómo estos servicios pueden darse por proveedores de servicios nacionales o extranjeros. La finalidad del mismo es analizar los sistemas de pagos por Internet, móviles, con el objetivo de evaluar el potencial uso de las nuevas tecnologías frente al blanqueo de dinero[175]. Desde la publicación que elaboró el GAFI en el 2006, ha sido amplía la aceptación de los medios de pago que se realizan a través del uso de internet por parte de los usuarios[176].

4. *Money Laundering Using New Payment Methods*

En octubre del año 2010, el GAFI elabora un nuevo informe en el que, a diferencia del informe primigenio del año 2006, se describen los mecanismos de pago alternativos. Este nuevo documento se centra en los desarrollos de los mismos, así como en su reciente evolución; además, hace un análisis pormenorizado de los riesgos que estos presentan. El documento se divide en 6 capítulos: la primera parte, constituida por los capítulos 1 y 2, abordan temas

---

[175] FINANCIAL ACTION TASK FORCE, "Report of new payment methods", 13 de octubre del 2006. Disponible en: <http://www.fatf-gafi.org>. En ese sentido refiere GÓMEZ que hubo que esperar al 2006 para que el GAFI presentara un nuevo Informe sobre los peligros latentes que estas nuevas tecnologías suponían, al facilitar la realización de operaciones sin tener que identificarse. GÓMEZ INIESTA, *op. cit.,* p. 9.

[176] Véase el informe del GAFI *Money Laundering Using New Payment Methods.* En lo referido a objetivos refiere que "el aumento en el número de transacciones y el volumen de fondos que se movieron a través de los NPM desde 2006 ha ido acompañado de un aumento en el número de casos detectados en los que dichos sistemas de pago fueron utilizados indebidamente para fines de LA/FT. El informe del MNP de 2006 identificó posibles acciones legítimas y usos ilegítimos de los diversos MNP, pero hubo poca evidencia para respaldar esto. El informe actual comparará y contrastará los *riesgos potenciales* descritos en el informe de 2006 con los *riesgos reales* basados sobre nuevos estudios de casos y tipologías. No todos los riesgos potenciales identificados en 2006 fueron respaldados por caso estudios. Esto no significa que esos riesgos ya no sean motivo de preocupación, y las jurisdicciones deben continuar estar atento a la evolución del mercado para prevenir malos usos y detectar casos que antes pasaban desapercibidos".

generales de los Nuevos Métodos de Pago (*New Payment Methods*); la segunda, parte del texto abordada en los capítulos 3 y 4, aborda lo referente a riesgos y vulnerabilidades, así como sus tipologías; la sección tercera, el capítulo 5, aborda cuestiones referidas a la regulación y supervisión, así como realiza un enfoque legislativo de las normas antiblanqueo; la última parte de este informe, en el capítulo 6, establece las conclusiones.

El informe en sus conclusiones hace referencia a los supuestos de blanqueo en los que se compran tarjetas prepago en el mercado ilegal, haciendo énfasis que se debería prestar más atención a los servicios de pago por Internet y su utilización para el ciberblanqueo y la financiación del terrorismo. Según GÓMEZ INIESTA, "su propagación se ha debido fundamentalmente a que en muchos casos no están involucradas las instituciones financieras, porque permiten realizar todo tipo de operaciones bancarias, fuera de dicho entorno, como transferencias o pagos, o porque permiten, incluso sin necesidad de identificarse y sin disponer de una cuenta bancaria o tarjeta de crédito, extraer efectivo de cajeros automáticos"[177].

5. Guidance for a risk-based approach prepaid cards, mobile payments and Internet-Based Payment Services

En junio del 2013, se emitió una guía denominada *Guidance for a risk-based approach prepaid cards, mobile payments and Internet-Based Payment Services*. Mediante este documento, el GAFI propone una guía sobre el enfoque basado en el riesgo que generan las tarjetas prepago, teléfonos móviles y servicios de pago por Internet con relación al blanqueo de dinero. Debemos resaltar que los nuevos productos y servicios de pago juegan un rol preponderante en la inclusión financiera; también no se debe perder perspectiva desde un enfoque eminentemente de carácter preventivo.

[177] GÓMEZ INIESTA, *op. cit.,* p. 9.

X. CRIMINALIDAD ORGANIZADA Y TIC

El proceso de globalización no ha sido ajeno a la criminalidad. La reciente evolución de la criminalidad organizada transnacional ha supuesto un cambio que le está permitiendo desafiar el orden estatal a través del proceso de globalización[178], el mismo que está posibilitando nuevas formas de delincuencia mediante el uso de la informática y las telecomunicaciones[179]. En la actualidad, las organizaciones criminales dedicadas al narcotráfico, trata de personas, blanqueo de capitales, se vienen instrumentalizando de diversas tecnologías en la red, que generan muchas dificultades en al ámbito de imputación y atribución de responsabilidad penal. Como refiere GRANADOS, se trata de estructuras organizativas complejas en las que el derecho penal clásico poco puede hacer en materia de subsunción típica[180].

Se trata, pues, de un nuevo espacio público que ha favorecido nuevas formas de relación, que también incluyen nuevas formas delictivas como son las ciberamenazas, ciberataques, ciberespionaje, ciberterrorismo, etc., lo cual ha llevado a los estados a modificar sus ordenamientos jurídicos para poder dar respuesta a estas nuevas formas delictivas[181].

Según GRANADOS, este nuevo modelo de criminalidad organizada global tiene sus propias características: a) una operatividad a escala mundial, b) unas conexiones transnacionales extensivas, c) la capacidad de retar a la autoridad nacional e internacional[182].

Se puede definir a los grupos de ciberdelincuencia organizada como aquellos grupos delictivos organizados que cometen delitos cibernéticos. Según se define

---

[178] GRANADOS ROMERO, *op. cit.*, p. 67.

[179] *Ibid*., p. 68.

[180] *Ibid*., p. 69.

[181] FERNÁNDEZ BERMEJO y MARTÍNEZ ATIENZA, *op. cit*, p. 117.

[182] *Ibid*., p. 117.

en el artículo 2, apartado a), de la Convención contra la Delincuencia Organizada, un *grupo delictivo organizado* es "un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material"[183]. La Organización de las Naciones Unidas contra la Droga y el Delito ha señalado que, en el caso de la ciberdelincuencia organizada, se entiende que esta se da teniendo como punto de partida la comisión de un delito cibernético (un delito basado en la cibernética o un delito facilitado por ella) que sea: a) cometido por un grupo delictivo organizado, según se define en el artículo 2, apartado a), de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, aprobada en 2000; o b) que implique un delito tipificado con arreglo al artículo 5 de la Convención, que abarca la penalización de la participación en un grupo delictivo organizado. En las siguientes secciones se analizan cada uno de estos elementos[184].

Con respecto a las tipologías sobre los grupos criminales organizados dedicados a la ciberdelincuencia, la doctrina los ha clasificado de acuerdo con su estructura organizativa y a su grado de participación en actividades en dos: los que operan fuera de línea y los que operan en línea[185]. Dentro de los que operan en línea tenemos dos grupos:

El primer grupo son los *enjambres*, que pueden describirse como la fusión, durante un cierto tiempo, de personas para realizar tareas específicas con el fin de cometer un delito cibernético. Una vez que consuman la tarea o los objetivos asignados, o logran cometer el ciberdelito como un colectivo, algunas de las personas, la mayoría de ellas o todas pueden irse cada una por su lado y es

---

[183] OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO, *Compendio de ciberdelincuencia organizada*, Viena, febrero del 2022, p. 8. Disponible en: <https://www.unodc.org/documents/Cybercrime/tools-and-resources/Compendio_de_delincuencia_organizada_ES.pdf>.

[184] *Ibid.,* p. 8.

[185] *Idem*.

posible que se desarticule el grupo temporal que se había estructurado[186]. Su operatividad se manifiesta a través de redes descentralizadas, integradas generalmente (aunque no de manera exclusiva) por "grupos efímeros de personas", con un propósito común y mínimas cadenas de mando. Un propósito común de un enjambre es cometer un delito cibernético por razones ideológicas, y las personas que se unen a los enjambres tienden a hacerlo por esas razones[187].

El segundo es el conformado por los *nodos,* que está integrado por un núcleo de delincuentes rodeado de asociados delictivos periféricos. Está más estructurado que un enjambre; tiene una estructura de mando que puede reconocerse. Por lo general, las actividades de los nodos están orientadas a la obtención de beneficios[188].

Dentro de los que operan fuera de línea, son grupos delictivos organizados que solo utilizan las TIC para ampliar o apoyar las actividades y operaciones ilícitas fuera de línea. Estos grupos tienen una estructura jerárquica, suelen estar integrados por grupos delictivos organizados tradicionales y han tratado de ampliar ciertas actividades ilícitas en línea, como los juegos de azar, la extorsión, la prostitución y la trata de personas[189].

Por último, tenemos una categoría mixta o híbrido en la que los grupos organizados operan fuera y en línea. Dentro de híbridos tenemos, los grupos híbridos extendidos que están integrados por asociados y subgrupos que llevan a cabo diversas actividades delictivas y los híbridos agrupados y su composición es más compleja[190].

---

[186] *Ibid.,* p. 18.

[187] *Ibid.,* p. 19.

[188] *Idem*.

[189] *Idem*.

[190] *Idem.*

CAPÍTULO II
CONSIDERACIONES GENERALES RELATIVAS A LOS CRIPTOACTIVOS Y AL *BITCOIN*

I. DEFINICIONES TERMINOLÓGICAS EN RELACIÓN CON EL DINERO Y LOS CRIPTOACTIVOS

Para poder comprender con mayor claridad el fenómeno de los criptoactivos y su diferencia con el dinero tradicional, considero importante, para un mejor entendimiento del mismo, hacer una explicación de los distintos conceptos terminológicos vinculados a los criptoactivos, ya que en la actualidad existe una gran confusión al momento de referirnos a los criptoactivos, y estos se suelen confundir con otra amplitud de conceptos vinculados a las nuevas tecnologías. Sin embargo, uno de los grandes problemas que genera esta variedad de definiciones elaboradas es que no existe un consenso en la aceptación de una definición que se haya adoptado de forma general por todas las distintas entidades públicas y privadas que han venido construyendo un concepto sobre el tema en cuestión.

Como de forma acertada refiere BARRIO ANDRÉS, las criptofinanzas y sus aplicaciones han dado lugar a diferentes conceptos difíciles de definir y categorizar, tomando como ejemplo los siguientes nombres: criptoactivos, criptomonedas, monedas virtuales, monedas digitales, dinero electrónico, conceptos que se utilizan de forma indistinta como si se tratara de términos igualitarios, cuando realidad no es así, como veremos más adelante[191]. Por ello, empezaré definiendo al "dinero" y sus tipologías, para luego definir los criptoactivos y otros conceptos referidos a distintas tecnologías que tiene que ver con el tema objeto de investigación.

[191] BARRIO ANDRÉS, Moisés, "Concepto y clases de criptoactivos", en *Criptoactivos. Retos y desafíos normativos*, Madrid: Wolters Kluwer, 2021, p. 50.

1. Dinero

Se define al dinero como los "activos financieros que cumplen las funciones de medio de pago, reserva de valor y unidad de cuenta"[192]. Para poder cumplir estas funciones, el dinero debe tener idéntico valor en lugares distintos y mantener un valor estable a lo largo del tiempo: decidir si conviene vender un determinado bien o servicio es mucho más fácil si se tiene la seguridad de que la moneda recibida tiene un valor garantizado en términos de su capacidad adquisitiva tanto actual como futura[193].

En el caso del Perú, la Constitución Política, en su artículo 83, es la ley suprema que determina el sistema monetario de la República, y la emisión de billetes y monedas es facultad exclusiva del Estado, y este la ejerce por intermedio del Banco Central de Reserva del Perú[194]. En el caso de la Unión Europea, el Banco Central Europeo y los bancos centrales de la zona del euro son los que debidamente están autorizados para la emisión de billetes en euros.

2. Criptoactivos

El término *cripto* según la RAE proviene del griego *kryptos,* que significa 'oculto, encubierto'. Por su parte, el *activo,* desde un enfoque eminentemente económico, es el conjunto de todos los bienes y derechos con valor monetario que son propiedad de una empresa, institución o individuo[195]. Una característica

---

[192] En ese sentido, "el dinero desempeña tres funciones fundamentales y complementarias. Es (i) una unidad de cuenta, una vara de medir que facilita la comparación de precios de las cosas que compramos, así como del valor de las promesas que hacemos; (ii) un medio de cambio: un vendedor lo acepta como medio de pago, con la esperanza de que otra persona se lo acepte a él más adelante; y (iii) un depósito de valor, al permitir que los usuarios transfieran capacidad adquisitiva al futuro". BANK FOR INTERNATIONAL SETTLEMENTS, "V. Criptomonedas: más allá del fenómeno de moda", en *Informe Económico Anual 2018 del BPI*, p. 2.

[193] BANK FOR INTERNATIONAL SETTLEMENTS, *op. cit.*, p. 2

[194] El artículo 2 de la Ley Orgánica del Banco Central de Reserva establece: "Artículo 2.- La finalidad del Banco es preservar la estabilidad monetaria. Sus funciones son regular la cantidad de dinero, administrar las reservas internacionales, emitir billetes y monedas e informar sobre las finanzas nacionales".

[195] REAL ACADEMIA ESPAÑOLA, "Activo", 23.º ed., octubre del 2014. Disponible en: <https://dle.rae.es/activo?m=form>.

de los criptoactivos, según IBÁÑEZ JIMÉNEZ, es que su emisión se materializa en fichas digitales o *tokens* que nacen y circulan en la red, asociados a plataformas ya existentes que facilitan su ofrecimiento público a inversores[196].

En palabras de BARRIO ANDRÉS, el critptoactivo "es un activo digital que presenta cumulativamente tres características: a) Esta registrado en alguna forma de libro mayor digitalmente distribuido asegurado con la criptografía. b) Por lo general hace uso de la tecnología blockchain. c) Puede como un medio de pago con fines de inversión, para acceder a un producto o servicio, o bien una combinación de las anteriores"[197]. En líneas generales, se denominan criptoactivos a todas aquellas divisas virtuales protegidas por la técnica de la criptografía y que basan su funcionamiento en la utilización de técnicas de cifrado de clave pública y de técnicas numéricas de verificación[198].

Dentro de las más populares tenemos al *bitcoin, ethereum, litecoin, primecoin, namecoin, ripple dogecoin, dash,* entre otras.

El Comité de Basilea, en su documento consultivo sobre el tratamiento prudencial de las exposiciones a criptoactivos, los define como "activos digitales privados que dependen principalmente de la criptografía y el libro mayor distribuido o tecnología similar"[199].

La propuesta del reglamento del Parlamento Europeo y del Consejo, relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE)

---

[196] IBÁÑEZ JIMÉNEZ, Javier, "Emisión, representación y gestión de criptoactivos", en *Criptoactivos. Retos y desafíos normativos*, Madrid: Wolters Kluwer, 2021, pp. 218 y 219.

[197] BARRIO ANDRÉS, *op. cit.*, p. 53.

[198] RAMÍREZ MORÁN, David, "Riesgos y regulación de las divisas virtuales" en *Instituto Español de Estudios Estratégicos*, 19 de marzo del 2014, p. 5. Disponible en: <http://www.ieee.es/Galerias/fichero/docs_analisis/2014/DIEEEA182014_ImplicacionesFuturoDivisasElectronicas_DRM.pdf>.

[199] COMITÉ DE BASILEA DE SUPERVISIÓN BANCARIA, *Documento consultivo. Tratamiento prudencial de las exposiciones a criptoactivos*, junio del 2021, p. 20.

2019/1937 (MICA), define a los criptoactivos como “una representación digital de valor o derechos que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o una tecnología similar”[200].

El Grupo de Acción Financiera define a la moneda virtual convertible (o abierta) como aquella que “tiene un valor equivalente en moneda real y se puede intercambiar de acá para allá por moneda real”[201].

3. Monedas virtuales centralizadas

Todas aquellas monedas se consideran centralizadas, ya que son emitidas y administradas por un tercero que establece las reglas para su circulación. De igual forma, este tercero, que cumple un rol de administrador, tiene la potestad para retirarla de circulación en el momento que él lo decida. En cuanto al valor de la moneda, este es fijado por la oferta y la demanda o también se puede fijar por el administrador central[202]. Para entender mejor de qué se trata una moneda virtual centralizada, usaremos el siguiente ejemplo: un banco[203] central[204] crea

---

[200] Véase el artículo 3 del “Reglamento del parlamento europeo y del consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937 (Mica)”.

[201] GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Directrices para un Enfoque Basada en Riesgo. Monedas Virtuales*, junio del 2015, p. 29. Disponible en: <https://www.fatf-gafi.org/media/fatf/documents/Directrices-para-enfoque-basada-en-riesgo-Monedas-virtuales.pdf>.

[202] *Ibid*., p. 29.

[203] En ese sentido, el informe emitido por BIS establece: “Algunos bancos centrales han comenzado a sopesar la posibilidad de emitir en algún momento monedas digitales propias. Aunque ampliar el acceso a formas digitales de pasivos de bancos centrales no es una idea totalmente nueva, en los últimos tiempos el debate ha estado motivado por varios factores. Entre ellos cabe citar: (i) el interés por las innovaciones tecnológicas aplicables al sector financiero, (ii) la aparición de nuevos participantes en los mercados de servicios de pagos e intermediación, (iii) el descenso del uso del efectivo en algunos países y (iv) la creciente atención que reciben los llamados tokens digitales privados. En respuesta al creciente interés de los bancos centrales, el sector privado y el público en general, el Comité de Pagos e Infraestructuras del Mercado (CPMI) y el Comité de los Mercados (MC) emprendieron sendos estudios complementarios sobre las consecuencias de la emisión de monedas digitales de bancos centrales (CBDC)”. Cfr. COMITÉ DE PAGOS E INFRAESTRUCTURAS DEL MERCADO Y COMITÉ DE LOS MERCADOS, *Monedas digitales emitidas por bancos centrales*, marzo del 2018, p. 4. Disponible en: <https://www.bis.org/cpmi/publ/d174_es.pdf>.

una criptomoneda similar al *bitcoin*; sin embargo, a diferencia de lo que ocurre con este, en relación con que puede ser creado por cualquier participante de la red *bitcoin,* en este caso el banco es el único organismo central que puede crearlas y controlarlas, además de la regulación de su valor la misma, que ya no estaría en manos de los usuarios, sino que este sería otorgado por el organismo emisor central.

4. Monedas virtuales descentralizadas

Más conocidas como criptomonedas, estas monedas virtuales son distribuidas de fuentes abiertas que se basan en la ciencia de la matemática. La principal característica es que no cuentan con un administrador, ni están sujetas a ningún tipo de control, ni de supervisión[205], entre las más destacadas tenemos al *bitcoin, litecoin, dogecoin, dash, ripple, ethereum*, etc.

5. Esquemas cerrados de moneda virtual

Estos esquemas casi no tienen ningún vínculo con la economía real y a veces se denominan esquemas "solo en el juego". Bajo este esquema, los usuarios suelen pagar una cuota de suscripción y luego ganar dinero virtual en función de su rendimiento de juego en línea. La moneda virtual solo se puede gastar mediante la compra de bienes y servicios virtuales ofrecidos dentro de la

[204] Son dos los modelos de Moneda Digital Centralizada que se manejan como posibles opciones para su emisión por parte de los bancos centrales: la primera es la de pagos para mayoristas, "cuyo uso estaría limitado a cierto grupo de participantes, principalmente para transacciones en el mercado interbancario y la liquidación de valores. Este diseño no implica un cambio muy significativo a lo que actualmente existe), teniendo en cuenta que los bancos comerciales tienen cuentas corrientes en los bancos centrales con las cuales pueden realizar transacciones sin necesidad de hacer uso de dinero físico (billetes y monedas)". La segunda es la de pagos para pagos minoristas, "este tipo de moneda digital estaría disponible para todos los agentes de la economía y podría considerarse, en cierta forma, un sustituto de los actuales billetes y monedas. Para su diseño existen dos alternativas, digitalizar los actuales billetes y monedas (token) o crear cuentas para todos los agentes de la economía directamente en el banco central". BANCO CENTRAL DE RESERVA DEL PERÚ, "Monedas digitales de bancos centrales", en *Moneda*, n.º 178, junio del 2019, p. 5. Disponible en: <https://www.bcrp.gob.pe/docs/Publicaciones/Revista-Moneda/moneda-178/moneda-178.pdf>.

[205] *Ibid*. p. 5.

comunidad virtual[206]. Dentro del ejemplo más relevante, tenemos el juego World of Warcraft, que es un juego multijugador masivo en línea desarrollado por Blizzard Entertainment, el cual utiliza su propia moneda virtual denominada Gold, que es necesaria como medio de intercambio en el juego, por ejemplo, para que los jugadores se equipen lo suficientemente bien como para alcanzar niveles más altos[207].

6. Esquemas de moneda virtual con flujo unidireccional

Este tipo de moneda virtual se puede comprar directamente utilizando moneda real a un tipo de cambio específico, pero no se puede volver a cambiar a la moneda original. Las condiciones o cláusulas de conversión a moneda fíat las establece el titular del régimen. Los esquemas permiten que la moneda se emplee para comprar bienes y servicios virtuales, pero algunos puede que también permitan que sus monedas se utilicen para comprar bienes y servicios reales[208]. Por ejemplo, los créditos de la red social Facebook. La moneda virtual de Facebook se introdujo en el año 2009 con la finalidad de permitir a sus usuarios el comprar bienes virtuales en cualquier aplicación en la plataforma de dicha red social. Era posible comprar esta moneda utilizando una tarjeta de crédito, una cuenta de PayPal o una variedad de otros métodos de pago. Otro ejemplo de este esquema lo encontramos en la moneda virtual establecida por consola de videojuegos Nintendo, en la que su moneda virtual se llama Nintendo Points, y pueden ser canjeados de forma virtual o en las tiendas de Nintendo y en sus juegos[209].

---

[206] EUROPEAN CENTRAL BANK, *Virtual Currency Schemes*, Frankfurt am Main, octubre del 2012, p. 13. Disponible en: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>.

[207] *Ibid*., p. 13.

[208] *Ibid.,* p. 14.

[209] *Idem*.

7. *Altacoins*

Se les llama así, a todas aquellas criptomonedas alternativas (*alternative coins*) al *bitcoin*, como por ejemplo *ethereum, ripple, cardano, litecoin, dash.*

8. *Stablecoins*

Las *stablecoins* o monedas estables son unidades digitales de valor que se basan en un conjunto de herramientas de estabilización[210], con la finalidad de intentar minimizar las fluctuaciones en su precio[211]. Esto tiene lógica ya que el sentido de crear una moneda estable radica en la minimización de la volatilidad de los precios de la misma. Para GARCÍA DEL POYO, las *stablecoins* podrían considerarse como derechos de participación que se ven representados en tokens de cualquier índole, ya que los criptoactivos, al igual que cualquier activo, se pueden tokenizar en distintas modalidades ya sea en *commodity tokens*, *tokens de utilidad* y *tokens de seguridad*[212].

9. *Tokens* de pago

Es un activo virtual convertible descentralizado que sirve como un medio de pago para adquirir bienes o servicios, o como un medio de transferencia de dinero o valor. Los tokens de pago más utilizados incluyen *bitcoin, ethereum* y *ripple*. En algunas jurisdicciones, los *tokens* de pago no se tratan como valores[213].

---

[210] En ese sentido, GARCÍA DEL POYO refiere lo siguiente: "Las stablecoins suelen definirse como criptoactivos creados con la finalidad de mantener un valor estable a lo largo del tiempo, para lo que necesitan un respaldo que algunos casos, se obtiene mediante su vinculación al mercado de otro tipo de activos". GARCÍA DEL POYO, Rafael, "Algunos casos de uso", en *Criptoactivos. Retos y desafíos normativos,* Madrid: Wolters Kluwer, 2021, p. 87.

[211] KOŁODZIEJCZYK, Hanna y JARNO Claudia, "Stablecoin - the stable cryptocurrency", *en Studia BAS*, vol. 3, n.º 63, 2020, p. 157.

[212] GARCÍA DEL POYO, *op. cit*., p. 87.

10. *Tokens* de activos

Se representan en activos análogos a acciones, bonos o derivados, que implican un reclamo o que están directamente vinculados a activos, que pueden ser mercancía o acciones de una empresa o portafolio. Los *tokens* de activos representan la propiedad legal y prometen una participación en las ganancias futuras de la empresa o futuros flujos de capital[214].

11. *Tokens* de utilidad

Están destinados a proporcionar derechos de acceso digital a una aplicación o servicio Los *tokens* de utilidad crean una economía interna dentro de la cadena de bloques de la aplicación o servicio y no tienen relación con la valoración de la organización emisora. En la mayoría de las jurisdicciones, si el único propósito de los *tokens* de servicios públicos es conferir derechos de acceso digital a una aplicación o servicio, no califican como valores[215].

12. *Tokens* no fungibles (NFT)

Los *tokens* no fungibles son un tipo de criptoactivo único del mundo físico o virtual cuyas unidades no resultan intercambiables, por lo que, como refiere GARCÍA DEL POYO, este tipo de token se utiliza para representar activos escasos y únicos, así como su propiedad y la interoperabilidad de los mismos en distintas plataformas, todo respaldado por la tecnología *blockchain*[216].

---

[213] SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP, "Activos virtuales y proveedores de servicios de activos virtuales: Diagnóstico situacional, legislación comparada y exposición a los riesgos de LA/FT en el Perú", 2009, p. 22.

[214] *Ibid.* p. 22.

[215] *Idem*.

[216] GARCÍA DEL POYO, *op. cit.,* p. 90.

II. OTROS CONCEPTOS RELEVANTES EN EL ENTORNO DE LOS CRIPTOACTIVOS

1. Intercambio de moneda virtual (IMV) o intercambiador (*exchanger*)

Se le considera a aquella "persona o entidad que se dedica como empresa al intercambio de AV por moneda real, fondos u otras formas de AV y también metales preciosos, y viceversa"[217]. El Grupo de Acción Financiera Internacional (GAFI) las define como aquella "persona o entidad operando como un negocio en el intercambio de moneda virtual para moneda real, fondos u otras formas de moneda virtual y también metales preciosos y viceversa, para un honorario (comisión)"[218].

2. Administrador

Es la persona o entidad que se dedica como empresa a emitir (poner en circulación) criptoactivos[219].

3. Minero

Minero es aquella persona o entidad que participa en una red activos virtuales descentralizados mediante la ejecución de un *software* especial para resolver algoritmos complejos en un sistema de prueba distribuido utilizado para validar transacciones en el sistema[220].

---

[217] *Ibid.,* p. 26.

[218] GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Directrices…, op. cit.,* p. 31.

[219] *Ibid.*, p. 31.

[220] *Idem*.

4. Criptografía

La criptografía es la rama de las matemáticas que nos permite crear pruebas matemáticas que proporcionan altos niveles de seguridad. En el caso de *bitcoin*, la criptografía se utiliza para hacer imposible que alguien pueda gastar los fondos del monedero de otro usuario o que se pueda corromper la cadena de bloques. También se utilizada para encriptar un monedero, de manera que no se pueda utilizar sin una contraseña[221].

5. Billeteras o monederos virtuales

La denominada *digital wallet*, palabra del idioma inglés que traducida al español significa 'billetera digital', es un *software* que sirve para guardar, mantener, almacenar y transferir *bitcoins*. A diferencia de lo que significaría una cuenta bancaria tradicional de ahorro, la billetera digital no está resguardada por ninguna entidad financiera que la controle. Técnicamente se trata de un archivo que contiene las claves criptográficas que permiten a un usuario enviar y recibir *bitcoins*[222].

6. Monederos *online*

Existen distintas empresas que, a través de sus plataformas virtuales, dan el servicio de almacenaje *online* de *bitcoins* a cambio de un porcentaje. Para poder acceder a este servicio es necesario la apertura de una cuenta, para lo cual la plataforma que presta el servicio requerirá algunos datos personales del solicitante; sin embargo, para hacer las transferencias de *bitcoins* hacia tu monedero digital no se requiere ningún proceso de verificación por parte de la empresa que otorga el servicio[223]. Dentro de las plataformas más conocidas que

---

[221] BITCOIN, "Algunas palabras en Bitcoin que usted puede escuchar". Disponible en <https://bitcoin.org/es/vocabulario>.

[222] SÁNCHEZ, Óscar, *Bitcoin: Qué son las criptomonedas y cómo ganar dinero fácil con ellas*, San Bernardino CA, 2017, p. 71.

dan servicio *online* de almacenaje de bitcoins tenemos: *coinbase, mycelium, xapo, exodus, jax, electrum, breadwallet, armory, airbitz, copay, bitcoin wallet.*

7. Monederos instalados en dispositivos móviles

También existen aplicaciones de monederos que permiten guardar bitcoins en los dispositivos móviles, dentro de las que tenemos: *Bit-coin Knots, Bitcoin Core, Bither, Armony,* etc.

8. Monederos físicos

Del mismo modo, también existe la posibilidad de almacenar o guardar *bitcoins* en monederos físicos, en dispositivos similares a las de un *pendrive* como son: *trezor*[224], *ledger nano*[225]o *keepkey*[226].

9. Monederos fríos

Se conoce como monederos fríos o *cold wallets* a aquellos que utilizan claves generadas por una fuente que no está conectada al registro *blockchain* y, por tanto, tampoco a Internet[227]. Este tipo de *wallet* ofrece una enorme ventaja sobre las demás, ya que, al no estar conectadas a la red, su nivel de seguridad y resguardo es muy seguro frente a los ataques de los *hackers* o *malwares* que buscan hurtar criptoactivos. Otra ventaja está relacionada con la capacidad de almacenaje que tienen para guardar criptomonedas, porque no están sujetas a ningún tercero para el resguardo del monedero.

---

[223] *Ibid.,* p. 72.

[224] Véase: <https://trezor.io/?a=reviewsera.com>.

[225] Véase: <https://www.ledgerwallet.com>.

[226] Véase: <https://www.keepkey.com/>.

[227] BIT2ME ACADEMY, "¿Qué son las *cold wallets*?", 14 de febrero del 2020. Disponible en: <https://academy.bit2me.com/que-son-cold-wallets/>.

10. Monederos calientes

Es un tipo de monedero que se caracteriza principalmente por su permanente conexión a Internet[228]. Su principal utilidad es que ofrece un rápido acceso a las criptomonedas custodiadas, debido a su constante conexión a Internet. Sin embargo, esto representa también un mayor riesgo, ya que son muy apetecibles para los ciberdelincuentes, que pueden intentar hurtarlas mediante a través de la Internet.

11. Monederos de papel (*paper wallets*)

Son planchas de papel o de otro material en el que se imprimen, mediante un programa de monedero de criptoactivos, las direcciones y el juego de claves pública/privada con las que se gestiona el intercambio de esta, se pueden dar ya sea en formato *plaintext* o en forma de código QR[229].

12. Monederos de firma múltiple (*multi-signature wallets*)

"Son aplicaciones que brindan un nivel de seguridad adicional al requerir el uso de múltiples claves privadas para autorizar una transacción, reduciendo de ese modo el riesgo de robo de criptomonedas si se compromete una única clave privada"[230].

[228] BIT2ME ACADEMY, "¿Qué son las *hot wallets*?", 11 de febrero del 2020. Disponible en: <https://academy.bit2me.com/que-son-hot-wallets/>.

[229] *Idem*

[230] *Idem.*

13. Monederas controladas por el Estado

"Se trata de un monedero (de cualquier clase) que está bajo control de una autoridad gubernamental (puede ser una agencia estatal especializada en el manejo de activos incautados, una agencia de cumplimiento de la ley, una fiscalía, un órgano jurisdiccional o incluso una compañía privada colaborando con el Estado), a la cual se transfieren los AV que se incautan o decomisan"[231].

14. Árboles de Merkle

El árbol de Merkle es un tipo de árbol binario, compuesto por un conjunto de nodos con una gran cantidad de nodos hoja en el parte inferior del árbol que contiene los datos subyacentes, un conjunto de nodos intermedios donde cada nodo es el hash de sus dos hijos, y finalmente un único nodo raíz, también formado a partir del hash de sus dos hijos, que representa el "parte superior" del árbol[232].

15. Contratos inteligentes (*smart contracts*)

MORA ASTABURUAGA define a los contratos inteligentes o *smart contracts* de la siguiente manera: "Son secuencias de código informático destinadas a ejecutar prestaciones de un contrato de manera automática una vez que se cumplan una serie de circunstancias previstas por las partes"[233].

---

[231] *Idem.*

[232] BUTERIN, Vitalik, "Ethereum white paper: A Next-Generation Smart Contract and Decentralized Application Platform", en *First versión,* vol. 53, 2014, p. 9.

[233] MORA ASTABURUAGA, Aitor, "Smart Contracts. Reflexiones sobre su concepto, naturaleza y problemática en el derecho contractual", en *Revista de Derecho Uned*, n.º 27, 2021, p. 64.

16. DeFi (finanzas descentralizadas)

Las finanzas descentralizadas (DeFi) es un término general para una colección de productos financieros que se clasifican en seis categorías principales de servicios DeFi: monedas estables, intercambios, crédito, derivados, seguros y gestión de activos, así como servicios auxiliares como billeteras y oráculos[234], que se basan en contratos inteligentes (*smart contracts*) y cadenas de bloques[235] (*blockchain*) para permitir servicios financieros abiertos entre pares (P2P) y automatizar procedimientos específicos[236]. Los servicios de las DeFi generalmente operan sin intermediarios o instituciones centralizados, y utilizan protocolos abiertos que permiten que los servicios se combinen programáticamente de manera flexible.

17. Agentes centralizados (CEX)

Es un tipo de *exchange* o intercambiador centralizado. Su centralización está dada por la participación que tiene el *exchange* en la intervención entre compradores y vendedores. Se fijan las tasas de cambio y la tasa de comisión que se debe pagar por las transacciones que se realizan a través de la plataforma. Dentro de los servicios que ofrecen están los servicios propiamente del *exchange*, los del *wallet, staking,* entre otros[237].

---

[234] WHARTON BLOCKCHAIN AND DIGITAL ASSET PROJECT Y WORLD ECONOMIC FORUM, "Defi Beyond the Hype. The Emerging World of Decentralized Finance", mayo del 2021, p. 1.

[235] En ese sentido, "libros mayores distribuidos que sirven como capa de liquidación para las transacciones. Actualmente, la mayoría de los servicios DeFi operan en la red Ethereum, debido a sus capacidades y adopción por parte de los desarrolladores. La actividad de DeFi también está creciendo en otras cadenas de bloques". Cfr. WHARTON BLOCKCHAIN AND DIGITAL ASSET PROJECT Y WORLD ECONOMIC FORUM, *op. cit.*, p. 2.

[236] THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM, *Decentralised Finance (DeFi)*, 2022, p. 6.

[237] ALEJANDRO VADELL, Gabriel, "Las Finanzas Descentralizadas (Defi) ¿La evolución de las cuentas off shore?", en *Centro de Estudios de Administración Tributaria CIAT*, 2021, p. 3.

18. Agentes descentralizados (DEX)

Este tipo de agente se caracteriza por tener un funcionamiento descentralizado que basa en el uso de la *blockchain*, a través de contratos inteligentes o *smart contracts,* es decir, se trata de programas autónomos que permiten ejecutar una serie de instrucciones o cláusulas de acuerdo con el cumplimiento de condiciones preestablecidas. La característica más importante es que estos contratos, una vez programados, se ejecutan de forma automática y descentralizada[238].

19. Dirección de criptoactivos

Es un código alfanumérico asociado a una determinada cantidad de activos virtuales, la cual es necesaria para poder enviar o recibir criptoactivos. Funciona como una cuenta bancaria en el sistema financiero tradicional para recibir o enviar transferencias[239].

20. Oferta inicial de moneda (ICO)

Se trata de un mecanismo que capta criptoactivos, como *bitcoin*, *ether* y moneda fíat para el financiamiento de un nuevo proyecto de criptoactivo a cambio de nuevos tokens[240].

---

[238] *Ibid.,* p. 4.

[239] GRUPO DE ACCIÓN FINANCIERA DE LATINOAMÉRICA, *Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales*, Buenos Aires, diciembre del 2021, p. 19.

[240] NAVARRO CARDOSO, Fernando, "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", en *Revista Electrónica de Ciencia Penal y Criminología*, n.º 21, 2019, p. 2. Disponible en: <http://criminet.ugr.es/recpc>.

III. EL BITCOIN, SUS ELEMENTOS Y FUNCIONAMIENTO

El respaldo de la creación del *bitcoin* habría sido avalado inicialmente por un sector de la población mundial conformado por cyberactivistas, que, de acuerdo con su línea de pensamiento liberatorio, buscan salir de ese control ejercido por los intermediarios financieros, recurriendo a la técnica de la criptografía como un instrumento de protección[241]. Esta corriente del libertarismo[242], según SOLÍS UMAÑA, "presupone como moral y políticamente insostenible que un determinado Estado (o cuerpo institucional con atribuciones de Estado) imponga a sus ciudadanos derechos y deberes de bienestar o derechos sociales (llamados también derechos positivos)"[243]. En materia económica, este pensamiento filosófico defiende que toda actividad se regule naturalmente, sin intervención de los poderes públicos[244]. Bajo esta corriente de pensamiento, refiere AHOMED CHÁVEZ, "el bitcóin debe ser respetado, y el Estado debe mantenerse aislado de cualquier intento de intervención, atendiendo que la aceptación de esta moneda digital es la expresión de una decisión libre de realizar operaciones que no sean respaldadas por ningún Estado, a pesar de que esto pueda constituir un riesgo patrimonial"[245].

---

[241] GUAITA, Martínez, J., "El fenómeno de las criptomonedas", en *Las criptomonedas: Digitalización del dinero 2.0*, Pamplona: Editorial Aranzandi, 2019, p. 42.

[242] En ese sentido Mario Solis refiere: "En ese las tesis que se defienden constantemente en nombre del libertarismo. Por un lado, se sostiene que la libertad individual es un valor absoluto (ahistórico), en donde libertad es entendida como la ausencia de coerción y los individuos son vistos como agentes autónomos. Por otro lado, en el lenguaje de los derechos, los defensores del libertarismo sostienen que cada individuo goza de derechos absolutos a la vida, libertad y propiedad; y que éstos activan o soportan estrictamente deberes negativos, esto es, deberes de no interferencia. Tales derechos son entendidos también como derechos naturales, i.e. como derechos que pertenecen a cada ser humano independientemente de cualquier forma de consenso colectivo o marco socio-político". SOLÍS UMAÑA, Mario, "Libertarismo y justicia social: La libertad como valor político", en *Revista Humanidades*, vol. 1, n.º 1, 2011, p. 2. Disponible en: <file:///C:/Users/Estudio%20Lamas%20Puccio/Downloads/Dialnet-LibertarismoYJusticiaSocial-4920531.pdf>.

[243] SOLÍS UMAÑA, *op. cit.,* p. 2.

[244] CHÁVEZ, O. A., "Análisis jurisprudencial del Bitcóin", en *Giuristi: Revista de Derecho Corporativo,* vol. 2, n.º 3, 2021, p. 7. Disponible en: <https://doi.org/10.46631/Giuristi.2021.v2n3.02>.

[245] *Ibid.,* p. 10.

La segunda corriente filosófica, basada en el liberalismo, establece como valor central la libertad y de forma conexa la protección de la propiedad privada. Bajo esa premisa la esencia del *bitcoin*, no debe enfocarse en constituir organismos públicos reguladores, pero sí considera necesaria la existencia de mecanismos legales que tutelen el cumplimiento de las transacciones y eviten cualquier fraude[246].

Por último, tenemos la corriente del ordoliberalismo. Esta corriente defiende una postura intermedia, es decir, defiende la libertad de la persona en la medida que esta no se vuelva una amenaza para el bienestar común de la sociedad[247]. Bajo esta escuela de pensamiento, se respeta la existencia del *bitcoin* como innovación tecnológica y medio de pago, siempre y cuando las transacciones en dicho activo digital sean objeto de regulación y supervisión estatal, con la finalidad de no afectar el bien del orden económico y financiero de la nación[248].

En relación con el origen del *bitcoin*, este se remonta al 31 de octubre del 2008, fecha en la que su creador o creadores conocidos con el pseudónimo de Satoshi NAKAMOTO elaboró un documento denominado *Bitcoin: A Peer-to-Peer Electronic Cash System*[249]. En este documento primigenio[250], NAKAMOTO refiere que el

---

[246] *Idem.*

[247] *Ibid,* p. 10.

[248] *Idem*.

[249] En ese sentido, NAKAMOTO refiere que "el comercio en el Internet ha venido a depender exclusivamente de instituciones financieras las cuales sirven como terceros confiables para el procesamiento de pagos electrónicos. Mientras que el sistema funciona lo suficientemente bien para la mayoría de las transacciones, aún sufre de las debilidades inherentes del modelo basado en confianza. Transacciones completamente no-revertibles no son realmente posibles, dado que las instituciones financieras no pueden evitar mediar disputas. El costo de la mediación incrementa costos de transacción, limitando el tamaño mínimo práctico por transacción y eliminando la posibilidad de pequeñas transacciones casuales, y hay un costo más amplio en la pérdida de la habilidad de hacer pagos no-reversibles por servicios no-reversibles. Con la posibilidad de revertir, la necesidad de confianza se expande. Los comerciantes deben tener cuidado de sus clientes, molestándolos pidiendo más información de la que se necesitaría de otro modo. Un cierto porcentaje de fraude es aceptable como inevitable. Estos costos e incertidumbres de pagos pueden ser evitadas en persona utilizando dinero físico, pero no existe un mecanismo para hacer pagos por un canal de comunicación sin un tercero confiable". NAKAMOTO, Satoshie, "Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario", 2008, p. 1. Disponible en: <https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf>.

"internet ha venido a depender exclusivamente de instituciones financieras las cuales sirven como terceros confiables para el procesamiento de pagos electrónicos"[251].

De forma operativa, el *bitcoin* aparece por primera vez en una lista de correo electrónico de *cryptography*, donde un usuario con el pseudónimo Satoshi NAKAMOTO anunció, el 1 de noviembre de 2008, que había desarrollado un nuevo sistema de dinero electrónico, resumiendo los alcances y contenido del artículo original[252]. El 11 de febrero de 2009, un perfil creado en el portal P2P Foundation, la cual es una organización que promueve las prácticas del sistema *peer-to-peer*, publicó un mensaje titulado: "Bitcoin open source implementation of P2P currency". En el texto, nuevamente el seudónimo de Satoshi NAKAMOTO daba a conocer el portal oficial de Bitcoin, el documento, donde se describía el diseño e, incluso, el cliente inicial con el que iba a comenzar a participar en la red[253].

En este primer constructo, NAKAMOTO crea un nuevo concepto del dinero privado, y lo hace mediante tres instrumentos: un *software* libre, una red de pares (P2P) y la criptografía[254]. GUTIÉRREZ y MORENO refieren que el *bitcoin* se trata de un protocolo tecnológico basado en un *software* libre, que está a disposición de

[250] Véase el Abstract del documento inicial elaborado por Nakamoto en el que describe la tecnología bitcoin como: "una versión puramente electrónica de efectivo permitiría que los pagos en línea fuesen enviados directamente de un ente a otro sin tener que pasar por medio de una institución financiera. Firmas digitales proveen parte de la solución, pero los beneficios principales se pierden si existe un tercero confiable para prevenir el doble-gasto. Proponemos una solución al problema del doble gasto utilizando una red usuario-a-usuario. La red coloca estampas de tiempo a las transacciones al crear un hash de las mismas en una cadena continua de pruebas de trabajo basadas en hashes, formando un registro que no puede ser cambiado sin volver a recrear la prueba de trabajo. La cadena más larga no solo sirve como la prueba de la secuencia de los eventos testificados, sino como prueba de que vino del gremio de poder de procesamiento de CPU más grande. Siempre que la mayoría del poder de procesamiento de CPU esté bajo el control de los nodos que no cooperan para atacar la red, estos generarán la cadena más larga y le llevarán la ventaja a los atacantes. La red en sí misma requiere una estructura mínima. Los mensajes son enviados bajo la base de mejor esfuerzo, y los nodos pueden irse y volver a unirse a la red como les parezca, aceptando la cadena de prueba de trabajo de lo que sucedió durante su ausencia".

[251] *Ibid.,* p. 158.

[252] CARMONA BORJAS, Juan Cristóbal, *Mundo jurídico de las criptomonedas*, Caracas: Juan Cristóbal Carmona, 2019, p. 158.

[253] *Ibid.,* p. 158.

[254] GOMA GARCÉS, Ignacio, *¿Qué es realmente Bitcoin?*, Madrid: Editorial Rasche, 2018, p. 23.

cualquier usuario, su código fuente puede ser usado, copiado, modificado y redistribuido, de modo que se pueden crear nuevos proyectos de *software* libre a partir de él[255]. Además, en el documento original NAKAMOTO explicaba otros aspectos referidos a la problemática, que se presentan en las transacciones financieras tradicionales como son: la falta revertibilidad de las operaciones, así como los conflictos entre las entidades bancarias y los usuarios, el alto costo que le significa a las entidades financieras, todas aquellas operaciones que contienen montos dinerarios pequeños o insignificantes, por último hace referencia al alto grado de fraudes y del *hacking* informático que se viene dando por parte de los cibercriminales[256].

Es en este escenario, es que el autor plantea como solución la necesidad de crear un sistema de pago electrónico, protegido por la criptografía, viabilizando la posibilidad de que dos partes interesadas puedan realizar transacciones sin la necesidad de la intervención de un intermediario o tercero confiable[257], que controle y perciba algún tipo de beneficio económico por las transacciones en las que partícipe[258].

Coincidencia o no, el *bitcoin* fue lanzado el mismo año de la quiebra del Banco estadounidense Lehman Brothers. Para muchos analistas, la caída de esta

---

[255] GUTIÉRREZ, Omar y MORENO, Abraham, *El bitcoin: consideraciones financieras y legales sobre su naturaleza y propuesta de enfoque para su regulación*, Lima: Esan Ediciones, 2018, p. 27.

[256] *Ibid.,* p. 27.

[257] "Lo que se necesita es un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiéndole a dos partes interesadas en realizar transacciones directamente sin la necesidad de un tercero confiable. Las transacciones que son computacionalmente poco factibles de revertir protegerían a los vendedores de fraude, y de mecanismos y depósitos de fideicomisos de rutina podrían ser fácilmente implementados para proteger a los compradores". Véase en NAKAMOTO, Satoshie, *op. cit.,* p. 1.

[258] En ese sentido García del Poyo Vizcaya refiere que: "finalidad inicial y más básica fue aquella para la que fue concebido el Bitcoin, que en principio pretendía sencillamente establecer un sistema de pagos e intercambio de valor no supervisado por ninguna autoridad, de manera que la privacidad de los usuarios quedará asegurada. Esta característica, sin embargo, ha servido a determinados operadores malintencionados para la compraventa de determinados bienes y servicios de dudosa licitud, pese a no ser uno de los usos previstos por su creador". GARCÍA DEL POYO, *op. cit.,* p. 84.

entidad bancaria fue el punto de partida del inicio de la crisis financiera[259] del 2008[260].

Fue recién en enero del 2009[261] que "Nakamoto distribuyó al público la primera versión de su *software*, con el que se empezaron a crear de forma oficial las primeras criptoactivos del sistema *bitcoin*. A este primer bloque se le conoció con el nombre de génesis, y contenía la cantidad exacta de 50 criptoactivos *bitcoin*, que tenían como dueño a Nakamoto"[262]. Luego de ese primer momento, una persona conocida con el nombre Hal Finney descarga el *software bitcoin*, con el cual se crea el segundo nodo de *bitcoin*. A esta persona NAKAMOTO le envía 10 *bitcoin*, del grupo de las 50 primeras creadas, realizándose la primera transferencia oficial de bitcoin. Después de esta primera transacción, los usuarios empezaron a descargar el software, con lo cual fueron apareciendo nuevos nodos o mineros, los cuales explicaremos con mayor precisión en el acápite respectivo.

---

[259] En ese sentido Carmona refiere: "ese nefasto episodio al que se llamó "Subprime Mortgage Crisis", arrastró consigo a Lehman Brothers una de las principales firmas de servicios financieros de Wall Street. Aquella firma para el año 2003 comenzó un proceso de reorganización corporativo con miras a incursionar fuertemente en el financiamiento de proyectos inmobiliarios y de compra de inmuebles ya construidos. Para el año 2003, llegó a otorgar préstamos por la cantidad de US$ 18,2 billones, en tanto que para el año 2006 alcanzaba un promedio de US$ 50 billones mensuales. En contrapartida, Lehman Brothers contaba con activos por US$ 680 billones, sólo que soportados por 22,5 billones de capital firme. registraba así un riesgo comercial tres veces más alto que su capital". CARMONA BORJAS, *op. cit.,* p. 106

[260] BOAR, Andrei, *Descubriendo el bitcoin*, España: Profit Editorial, 2018, p. 23. El 15 de septiembre del 2008, en plena crisis financiera mundial se dio el derrumbe de una de las más grandes firmas de banca de inversión del mundo, se trataba del banco Lehman Brothers, el cual se derrumbaba y desaparecía de forma abrupta, al mismo tiempo un grupo significativo de corporaciones, empresas que iban colapsando, ahogados en deudas millonarias y productos financieros tóxicos, generado a partir de una expansión exuberancia de los mercados, lo que llevó a un colapso inminente del sistema financiero, permitiendo este comprobar que los sistemas de regulación del mismo habrían fracasado. Cediel, Ana y Perez Pombo Emilio, Fiscalidad de las Criptomonedas, Barcelona: Atelier, 2020, p. 11.

[261] En ese sentido "la red bitcoin se puso en marcha el 3 de enero de 2009 con el bloque génesis, justamente unos pocos meses antes de que el proyecto fuera registrado, el 8 de noviembre de 2008", Márquez Solís, Santiago, Bitcoin Guía completa de la moneda del futuro, Madrid: RA-MA Editorial, p. 117.

[262] DOMINGO, CARLOS, *Todo lo que querías saber sobre Bitcoin, Criptomonedas y Blockchain y no te atrevías a preguntar,* Barcelona: Editorial Planeta, 2018, p. 50.

Como resumen de todo lo explicado anteriormente, con respecto al funcionamiento del bitcoin[263], CARLOS DOMINGO señala que "es una red mundial descentralizada de ordenadores que actúan P2P, todos los componentes de la red se comunican con todos, sin que nadie centralice la comunicación y cada uno de estos ordenadores constituye un nodo, comportándose todos como entre sí, es decir todo conectados con todo"[264].

1. Concepto de *bitcoin*

El *bitcoin* es un tipo de criptoactivo descentralizado, ya que su creación y validación se realiza mediante los miembros de la red *bitcoin*; es convertible, ya que se intercambia por otra criptoactivo o por dinero; es libre de intermediarios, ya que no hay ningún organismo central que lo pueda controlar; su funcionamiento se basa en un *software* libre, una red de pares y la criptografía como mecanismo de protección de las transacciones. El Tribunal Supremo español en la STC 2109/219 estableció que "el bitcoin no es sino una unidad de cuenta de la red del mismo nombre. A partir de un libro de cuentas público y distribuido, donde se almacenan todas las transacciones de manera permanente en una base de datos denominada Blockchain, se crearon 21 millones de estas unidades, que se comercializan de manera divisible a través de una red informática verificada"[265]. Esta ha sido la primera conceptualización que se ha dado a nivel jurisprudencial por parte de un órgano jurisdiccional en el mundo; sin duda que marca una pauta de gran trascendencia frente a la normativización de los criptoactivos. Si bien el tribunal, más que definir, describe la tecnología en

---

[263] En ese sentido "El bitcoin es una innovación reciente en las tecnologías de pago. Esta aplicación es un tipo de moneda virtual que aporta un nuevo sistema de pago y puede usarse como nuevo medio de intercambio. Destaca en la rama de sistemas de pago gracias a su protocolo tecnológico (el Bitcoin) que, principalmente, hace posible que su creación no la controle persona alguna y permite su intercambio por bienes y servicios sin la necesidad de un tercero que supervise la liquidación de cada transacción. Esto ocurre porque ese protocolo cuenta con un proceso de validación de transacciones que opera de modo descentralizado". Cfr. GUTIÉRREZ y MORENO, *op. cit.,* p. 9.

[264] *Ibid.,* p. 58.

[265] Véase el fundamento tercero de la STC 2109/219 de fecha 20 de junio del 2019.

la que está acaparado el funcionamiento *bitcoin*, dejando en claro cuál es naturaleza tecnológica.

2. Protocolo *bitcoin*

Los protocolos son conjuntos básicos de reglas que permiten compartir datos entre computadoras[266]. En el caso concreto del *bitcoin*, su protocolo está compuesto de un procedimiento de código abierto que opera en una red entre pares (*peer-to-peer*). Utiliza una cadena llamada *blockchain*[267] para registrar todas las transacciones e impedir el doble gasto. Para GUTIÉRREZ y MORENO, el protocolo *bitcoin* está compuesto de "un programa (*software*) libre. Pone a disposición de sus usuarios su código fuente con el fin de que estos puedan usarlo, copiarlo, modificarlo y redistribuirlo, de modo que se pueden crear nuevos proyectos de software libre a partir de él"[268].

3. Bitcoin Core

Se trata de un *software* de código abierto que cualquiera puede descargar a su ordenador o computador para ejecutar las reglas de consenso del protocolo *bitcoin.* Este *software* libre, llamado Bitcoin Core, es la continuación del código inicial elaborado por NAKAMOTO entre el 2008 y 2009, hasta su desaparición, posteriormente el proyecto *bitcoin* fue mejorado por un grupo de desarrolladores[269]. A los ordenadores que corren este programa se les suele

---

[266] Véase: <www.coinbase.com>.

[267] En ese sentido refieren GUTIÉRREZ y MORENO: "La piedra angular de Bitcoin es Blockchain, un archivo transaccional, electrónico, compartido, copiado, distribuido (organizacional y territorialmente) y descentralizado. Ha sido diseñado con base en un conjunto de tecnologías modernas como Internet, protocolos de código abierto par-a-par". GUTIÉRREZ y MORENO, *op. cit.,* p. 28.

[268] *Ibid., 28.*

[269] En ese sentido, NAKAMOTO participó en el desarrollo y mejora de Bitcoin Core hasta la versión 0.3.19 en 2010, luego abandonó el proyecto, dejándolo en manos de Gavin Andresen. Fue Andresen quien posteriormente, en 2014, cedió el proyecto a Wladimir Van Der Laan y otros desarrolladores principales. BIT2ME ACADEMY, "¿Qué es Bitcoin Core?", 2 de enero del 2020. Disponible en: <https://academy.bit2me.com/que-es-bitcoin-core/>.

llamar nodos, y el conjunto de nodos que interactúan entre sí conforman la red de *bitcoin*.

4. Nodos

En la informática en términos generales, los nodos son dispositivos conectados a una red que transmiten, procesan y almacenan información. En el caso específico del *bitcoin,* los nodos funcionan como ordenadores que ejecutan el *software* libre de *bitcoin* y a su vez están conectados a la red de *bitcoin*, para validar las transacciones de *bitcoin.* Estos monitorean de forma continua la cadena de bloque y su registro de transacciones como un mecanismo de seguridad para evitar transacciones fraudulentas y el doble gasto[270].

5. Las transacciones

Entendidas estas como la unidad básica del funcionamiento del *bitcoin*. La transacción[271] refleja un movimiento de un *bitcoin* de una dirección de origen a otra dirección de destino. Cada movimiento del *bitcoin* se representa en una clave pública[272], compuesta por números y letras. Como refieren PÉREZ-SOLÀ y HERRERA-JOANCOMARTÍ, para gastar bitcoin es necesaria la clave privada asociada a la clave pública que contenga un saldo de bitcoin[273].

---

[270] DECRYPT, "¿Cuáles son los Diferentes Tipos de Nodos de Bitcoin? Conoce Cómo se Mantiene la Red Bitcoin", 31 de julio del 2022. Disponible en: <https://decrypt.co/es/resources/cuales-son-los-diferentes-tipos-de-nodos-de-bitcoin-conoce-como-se-mantiene-la-red-bitcoin>.

[271] En ese sentido, refiere NAKAMOTO que "cada dueño transfiere la moneda al próximo al firmar digitalmente un hash de la transacción previa y la clave pública del próximo dueño y agregando estos al final de la moneda. Un beneficiario puede verificar las firmas para verificar la cadena de propiedad". NAKAMOTO, Satoshie, *op. cit.*, p. 2.

[272] PÉREZ-SOLÀ, Cristina y HERRERA-JOANCOMARTÍ, Jordi, "Bitcoins y el problema de los generales bizantinos", Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información (RECSI XIII), Universidad de Alicante, 2-5 de septiembre del 2014, p. 241. Disponible en: <https://web.ua.es/en/recsi2014/documentos/papers/bitcoins-y-el-problema-de-los-generales-bizantinos.pdf>.

[273] *Ibid*., p. 241.

Las transacciones[274] se pueden realizar en forma de pago, donación o como una retribución por un servicio prestado. El único requisito indispensable para viabilizar la transacción es conocer la combinación alfanumérica del receptor o destinatario, para poder realizar la transferencia, ya sea a través del *software* Bitcoin Core, o de alguna plataforma intermediarias (*exchange*) de cambio de divisas[275]. Una de las principales características de la transacción es el total anonimato con el que cuentan los usuarios del sistema *bitcoin*, lo que de ninguna manera genera una total falta de identificación y aseguramiento de la operación, ya que todo el movimiento transaccional queda registrado en la cadena de bloque, como veremos más adelante[276].

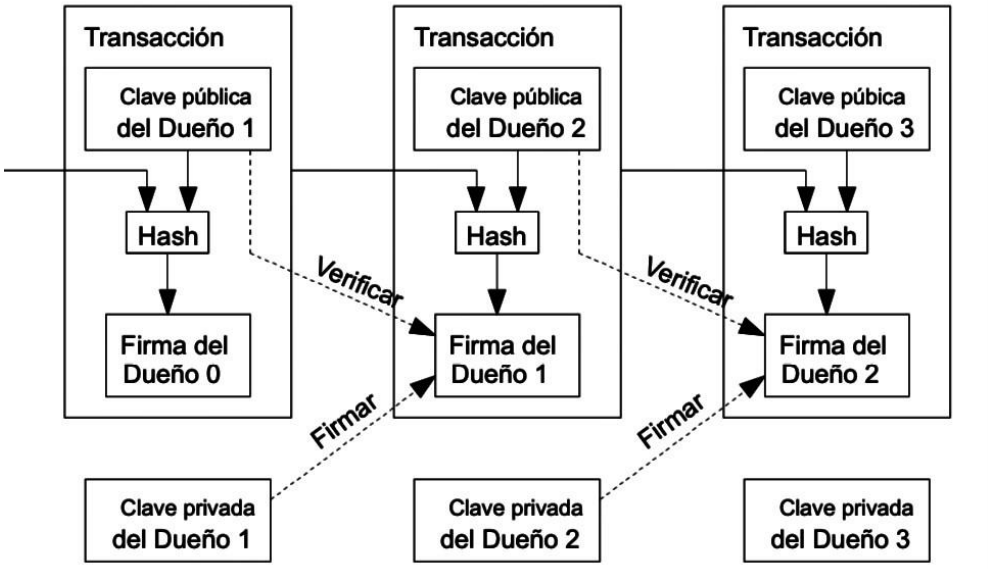

Imagen tomada de "Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario" de NAKAMOTO.

---

[274] "La unidad básica de funcionamiento de Bitcoin son las llamadas transacciones. Una transacción indica un movimiento de Bitcoins de una dirección de origen a una dirección de destino. Cada dirección de Bitcoins representa una clave pública (Bitcoin se basa en criptografía de curvas elípticas). Para gastar Bitcoins es necesario conocer la clave privada asociada a la clave pública que contenga un saldo en Bitcoins. Entonces, se pueden gastar esos Bitcoins, es decir, transferirlos a otra dirección, firmando digitalmente con la clave privada la transmisión de esta información y enviando la nueva transacción a toda la red". PÉREZ-SOLÀ y HERRERA-JOANCOMARTÍ, *op. cit.,* p. 242.

[275] BOAR, ANDREI, *op. cit.,* p. 45.

[276] *Ibid.,* p. 45.

6. Funcionamiento de la cadena de bloques en *Bitcoin*

Se puede definir a la *blockchain* o la cadena de bloques[277] como un protocolo fiable de registros, globalmente distribuidos llamado cadena de bloques[278]. ESPARZA y NICASTRO lo definen como una "cadena de bloques de información interconectados por el uso de la criptografía, de esta manera cada modificación realizada a un bloque queda registrada siempre y exclusivamente en un bloque posterior, sumando bloques a la cadena, por ellos la información contenida en la blockchain es irrefutable, ya que cada modificación ha sido registrada y anotada en un nuevo eslabón y no el previo, bríndanos así la posibilidad de rastrear cada paso como verdadero hasta el bloque inicial"[279].

Para NIEVES PACHECO, la *blockchain* "puede definirse como un libro digital compartido que abarca una lista de bloques conectados y almacenados en una red distribuida, descentralizada y protegida mediante criptografía, sirviendo como un depósito de información irreversible e incorruptible"[280].

La importancia de este protocolo está circunscrita a la posibilidad de trazabilidad de un producto, el cual nos permite conocer toda su historia y los procesos previos a su fabricación[281].

---

[277] "Los *bloques* proporcionan seguridad sobre la existencia de las transferencias sin permitir conocer el nombre de la persona ni la prestación realizada. Este libro contable digital, sin embargo, permite verificar el movimiento contable de los bitcoins utilizados". Cfr. CHÁVEZ, *op. cit.,* p. 6. En ese sentido, refiere Nieves Pacheco que "una cadena de bloques (*blockchain*) es una base de datos distribuida que registra bloques de información y los entrelaza para facilitar la recuperación de dicha información y la verificación de que esta no ha sufrido cambios. Estos bloques de información se entrelazan mediante apuntadores o algoritmos de resumen (*hash*) *que conectan el bloque actual con el anterior y así sucesivamente hasta llegar al denominado bloque génesis*". PACHECO JIMÉNEZ, María, "De La Tecnología Blockchain a La Economía Del Token", en *Derecho PUCP*, n.º 83, 2019, p. 64. Disponible en: <https://revistas.pucp.edu.pe/index.php/derechopucp/article/view/21468>.

[278] TAPSCOTT, Don y TAPSCOTT, Alex, *La revolución Blockchain*, Bogotá: Editorial Planeta, 2017, p. 27.

[279] ESPARZA, Marco y NICASTRO, Maximiliano, *Blockchain is Life*, Lima: Saxo, 2018, p. 33.

[280] PACHECO JIMÉNEZ, *op. cit.*, p. 64.

[281] *Ibid.,* p. 64.

A través de este protocolo, se puede enviar dinero de manera directa y segura de un usuario a otro usuario, sin la necesidad de contar con un intermediario financiero (tarjeta de crédito, al tratarse de un código abierto de fuente libre, cualquier usuario puede descargarlo de Internet y utilizarlo[282]. Uno de los mayores retos que presentan los criptoativos, PayPal, etc.).

Dentro de sus principales funciones se encuentra el registro de información de manera estructurada, de tal forma que es el de la realización de un doble gasto por parte de los usuarios; es decir, crea transacciones que tienen direcciones de destino diferentes utilizando la misma dirección de origen. Ahí es donde entra a tallar el denominado la *blockchain*, que es un tipo de bitácora o libro de registros virtual público, en el que se registran y graban todas las transacciones que realizan los usuarios de *bitcoin*.

Nermin HAJDARBEGOVIC refiere que la cadena de bloques de *bitcoin* "es la columna vertebral de la red y proporciona una estructura de datos inviolable, proporcionando un libro de contabilidad público compartido y que está abierto a todos"[283]. En términos sencillos, la cadena de bloques *bitcoin* es la espina tecnológica de red y proporciona una estructura de data a prueba de alteraciones, la cual proporciona a su vez un libro de contabilidad público abierto a todos.

7. Función de *hash*

La ciencia de las matemáticas y el uso de *hardware* especializado son lo que permite la construcción de la cadena de bloques protegidos por la criptografía, lo cual imposibilita su réplica. Todas las transacciones confirmadas forman parte de la cadena de bloques de *bitcoin*. El uso de la criptografía SHA-256, el algoritmo SHA o Secure Hash Algorithm fue desarrollado por la Agencia de

---

[282] TAPSCOTT y TAPSCOTT, *op. cit.,* p. 27

[283] HAJDARBEGOVIC, Nermin "Tecnología de Cadena de Bloques Explicada: Impulsando Bitcon", Disponible en: <https://www.toptal.com/bitcoin/tecnologia-de-cadena-de-bloques-explicada-impulsando-bitcoin>.

Seguridad Nacional de los Estados Unidos (NSA**)** y el National Institute of Standards and Technology (NIST). Su función primordial es generar *hashes*[284] o códigos únicos con base en un estándar, con el que se pudieran asegurar documentos o datos informáticos frente a cualquier agente externo que desee modificarlos[285]. Para DOMÍNGUEZ GÓMEZ, este algoritmo determina la integridad de los datos de entrada, es decir, cualquier cambio en los datos de entrada producirá un *digest*; además, refiere que este sistema es útil en la generación y verificación de firmas digitales y códigos de autenticación[286].

El *blockchain* es un sistema de registro, es público y cualquier persona puede acceder a verificar la información contenida en él, respecto a las transferencias de *bitcoin*[287]. Este registro único cuenta con la aceptación de todas las personas que ofrecen sus ordenadores voluntariamente, razón por la que no existe una base de datos central que pueda ser atacada. Los usuarios intervinientes de la red *bitcoin* no requieren de ninguna autoridad central para que controle el registro de operaciones del *blockchain*. Cada bloque de la cadena contiene un registro de información, el mismo que con el tiempo se va incrementando a medida que se realizan más transacciones[288].

Se puede resumir la utilidad de la tecnología *blockchain* dentro de la estructura del *bitcoin* de la siguiente forma: Don y Alex TAPSCOTT refieren que "el bitcoin o cualquier otra moneda digital no se guardan en archivos, que están en un lugar

---

[284] El *hash* es una función unidireccional, una forma de identificar algo de longitud arbitraria (como bloques que pueden ser bastante grandes) en un espacio finito. Podemos decir que una función *hash* es comparable a una firma en un documento. Pongamos un ejemplo de una función *hash*. Cfr. HERENCIA ANTÓN, Jesús, "Fundamentos tecnológicos de los criptoactivos", en *Criptoactivos. Retos y desafíos normativos*, Madrid: Walter Kluwers, 2021, p. 69.

[285] BIT2ME ACADEMY, "¿Qué es el SHA-256?", 23 de julio del 2018. Disponible en: <https://academy.bit2me.com/sha256-algoritmo-bitcoin/>.

[286] DOMÍNGUEZ GÓMEZ, Javier, "Criptografía: Función SHA-25", 2018, p. 2. Disponible en: <https://docplayer.es/169481186-Criptografia-funcion-sha-256.html>.

[287] *Ibid*., p. 2.

[288] *Ibid.,* p. 2. En ese sentido, una de las características de esta tecnología es que lo se escribe en el *blockchain* no puede desaparecer jamás, se registra de forma inmutable y permanente. No se puede modificar ni borrar nada de lo escrito. Esto lo hace invulnerable a falsificaciones de copia. SÁNCHEZ, *op. cit.,* pp. 41 y 42.

concreto, sino que los mismos, están representados por transacciones que se registran en una cadena de bloques, que es una especie de hoja de cálculo o registro que usa los recursos de una amplia red entre iguales para verificar y aprobar todas y cada una de las transacciones hechas en bitcoin"[289].

8. Firma digital

Se puede definir a la firma digital como "aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada"[290]. Es decir, podremos describir el funcionamiento de la firma digital como un código vinculado a un mensaje o documento[291].

En el caso específico de *bitcoin* el sistema criptográfico se basa en dos claves, la primera es eminentemente privada y la segunda de dominio público. Como refiere GONZÁLES BRIONES, las funciones de cifrado que utilizan estas claves permiten ocultar la información aplicando la clave pública sobre un conjunto de datos, lo que será validado única y exclusivamente por el tenedor de la clave privada, quien podrá realizar la función de descifrado. En el caso de bitcoin no se utiliza el cifrado, sino la denominada forma digital que será la que válida al autor de esos datos[292]. En síntesis, al utilizar la firma digital con la clave privada, se obtiene un *hash* de datos que pueden ser verificados aplicando la clave pública generada por el propietario original.

---

[289] TAPSCOTT y TAPSCOTT, *op. cit.,* p. 28.

[290] Artículo 3 de la Ley N.º 27269, Ley de Firmas y Certificados Digitales, del 8 de mayo del 2000.

[291] Véase: <https://academy.binance.com/es/articles/what-is-a-digital-signature>.

[292] GONZÁLES BRIONES, Alfonso, "Fundamentos de programación e introducción a la tecnología blockchain*"* en *Economía digital y criptoactivos*, DoinGlobal y Fundación General de Universidad de Salamanca, p. 6.

9. La prueba de trabajo o *proof of work*

La prueba de trabajo o *proof of work*[293] es el mecanismo de consenso que utilizan las criptomonedas para verificar nuevas transacciones, agregarlas a la cadena de bloques y crear nuevos *tokens*[294]. La prueba de trabajo, iniciada por primera vez por Bitcoin, utiliza la minería para lograr esos objetivos. La prueba de trabajo y la minería son ideas estrechamente relacionadas. La razón por la que se llama *prueba de trabajo* es porque la red requiere una gran cantidad de potencia de procesamiento. Las cadenas de bloques de prueba de trabajo están aseguradas y verificadas por mineros virtuales de todo el mundo que compiten para ser los primeros en resolver un acertijo matemático.

El ganador puede actualizar la cadena de bloques con las últimas transacciones verificadas y la red lo recompensa con una cantidad predeterminada de criptografía. Para Bitcoin, este método permite garantizar una forma el mantener una cadena de bloques descentralizada y segura, ya que en la medida que el valor de la criptomoneda va subiendo, mayor es la cantidad de mineros que se animan a formar parte de la red. Este incentivo se podría traducir en la teoría de los juegos del "problema de los generales bizantinos"[295], que buscan el consenso entre las distintas entidades, enfocados hacia un objetivo común.

---

[293] En ese sentido la prueba de trabajo o *proof-of-work*, se entiende "consiste en demostrar que se ha realizado una cantidad de trabajo para conseguir el bloque. Por lo tanto, la probabilidad de conseguir minar un bloque depende del poder de cómputo empleado en el trabajo. En este ámbito, las mejoras se centran en dos alternativas. Por un lado, proponer funciones que no requieran una inversión en hardware para el minado de bloques (como sucede actualmente con la función SHA256), para democratizar el proceso de minado y evitar así grandes clústers de minado que pudieran llegar a controlar la red. Dentro de esta alternativa se encuentran funciones hash, como por ejemplo scrypt que requieren un volumen elevado de memoria para su cálculo, haciendo poco viable la creación de hardware específico. Otro enfoque, mucho más ambicioso, es la propuesta de una función de proof-of-work tal que su propio cálculo permita resolver problemas útiles computacionalmente costosos". PÉREZ-SOLÀ, PÉREZ-SOLÀ y HERRERA-JOANCOMARTÍ, *op. cit.,* p. 245.

[294] COINBASE, "What is *proof of work* or *proof of stake*?". Disponible en: <https://www.coinbase.com/es/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake>.

[295] En ese sentido, refieren PÉREZ-SOLÀ y HERRERA-JOANCOMARTÍ lo siguiente: "El problema de los generales bizantinos es un experimento mental creado para ilustrar el dilema de lograr un consenso entre un conjunto de entidades con un objetivo común cuando entre ellas pueden existir traidores, es decir, entidades con objetivos opuestos que intenten dinamitar el proceso. Además, se supone que las comunicaciones entre dichas entidades son limitadas e inseguras". PÉREZ-SOLÀ y HERRERA-JOANCOMARTÍ, *op. cit.,* p. 241.

10. La red

Los pasos para gestionar la red son como sigue:

> *1) Transacciones nuevas son emitidas a todos los nodos.*
> *2) Cada nodo recolecta nuevas transacciones en un bloque.*
> *3) Cada nodo trabaja en encontrar una prueba-de-trabajo difícil para su bloque.*
> *4) Cuando un nodo encuentra una prueba-de-trabajo, emite el bloque a todos los nodos.*
> *5) Los nodos aceptan el bloque si todas las transacciones en el bloque son válidas y no se han gastado ya.*
> *6) Los nodos expresan su aceptación del bloque al trabajar en crear el próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash previo*[296].

11. La minería *bitcoin*

La minería en términos informáticos se le denomina a aquel proceso de verificación de transacciones realizado por el minero, mediante la resolución de problemas matemáticos[297]. Este problema de índole matemático siempre es el mismo, pero las variables son diferentes y solo se puede resolver combinando distintos números al azar, hasta dar con el resultado. La función primordial del minero[298] es la verificación de la transacción[299], así como dar con la solución al

---

[296] Esquema tomado del documento inicial donde se desarrolla el *bitcoin*. NAKAMOTO, Satoshie, *op. cit.,* p. 3.

[297] En esa misma línea, "un minero está a la escucha de las diversas transacciones que son enviadas a través de la red Bitcoin, las mismas que van siendo incorporadas en un bloque de datos, el minero comienza a resolver el desafío criptográfico y una vez resuelto el mismo, lo enlaza al bloque junto con los previos, difundiendo el resultado a través de la red". ARROYO GUARDEÑO, David, DÍAZ VICO, Jesús y HERNÁNDEZ ENCINAS, Luis, *¿Qué sabemos de Blockchain?*, Madrid: Catarata, 2019, p. 14.

[298] En ese sentido refiere ARROYO: "Los usuarios involucrados en esta tarea son los denominados mineros, y el desafío sobre el que trabajan tiene por objeto el registro de transacciones realizadas por otros usuarios de la red". Cfr. ARROYO GUARDEÑO *et al., op. cit.,* p. 13. En ese sentido Ohamed refiere: "paralelamente, existe un grupo o red de personas —los ya mencionados *mineros*— que se encargan de certificar continuamente las operaciones efectuadas mediante bitcoines. Este registro contable digital se conoce como *bloque*, y para tal certificación se requiere la conformidad de todos los *mineros*, quienes reciben a cambio una determinada cantidad de bitcoines; y estos, a su vez, pueden ser adquiridos por los interesados en realizar transacciones con esta moneda digital. No hay un organismo regulador de dicho registro: su elaboración dependerá de la confirmación consensual de los *mineros*". CHÁVEZ, *op. cit.,* p. 5.

problema matemático[300]. Una vez realizadas estas dos funciones operativas, el mismo *software* emitirá de forma automática una recompensa que será plasmada con un incentivo[301] que será materializado en nuevos *bitcoins*. Este procedimiento es el único proceso válido para la creación de monedas digitales *bitcoins*. Para el proceso de validación de las transacciones en un bloque, se realizan las siguientes comprobaciones[302]: a) que no exista doble gasto, b) que la transacción anterior que se intenta gastar exista, c) que la clave pública especificada se corresponda a la de dirección de salida especificada, d) que la firma sea la correcta al momento de validarla con la clave pública. Con respecto a cuál es la cantidad tope de *bitcoin* que se pueden crear a través del minado, Satoshie NAKATOMO, su creador, ha puesto como tope la cifra de veintiún millones (21 000 000.00) de *bitcoins.*

[299] PÉREZ-SOLÀ y HERRERA-JOANCOMARTÍ, en cuanto a la validación, refieren que los mineros validan cada una de las transacciones que se incluyen en el bloque, para de esa forma evitar que no exista doble gasto; que la transacción anterior que se intente gastar existe; que la clave pública especificada en la entrada se corresponde a la dirección de salida especificada; y que la firma es correcta al validarla con la clave pública especificada. PÉREZ-SOLÀ y HERRERA-JOANCOMARTÍ, *op. cit.,* p. 243.

[300] En relación con el doble gasto, "los usuarios que se dedican a crear bloques en la red Bitcoin son conocidos como mineros, y son una pieza fundamental del esquema. Cualquier usuario de la red puede ser un minero. Su trabajo consiste en validar las transacciones que se envían por la red P2P, incluyendo las válidas en nuevos bloques y descartando las inválidas. De este modo, si una transacción intenta gastar un importe ya gastado, o bien un usuario intenta gastar una transacción que no le pertenece (generando por lo tanto una firma inválida), esta nueva transacción nunca sería incluida en un bloque y, de este modo, no habría existido para el sistema. Por lo tanto, se necesita asegurar que los mineros hacen su trabajo correctamente, es decir, que aunque existan algunos mineros traidores que actúen en contra del interés común, se asegura que los mineros leales consigan acordar una cadena única, que contenga únicamente transacciones válidas". PÉREZ-SOLÀ y HERRERA-JOANCOMARTÍ, *op. cit.,* pp. 242 y 243.

[301] Al respecto, NAKAMOTO refiere: "El incentivo también puede ser fundado con costos de transacción. Si el valor de salida de una transacción es menor que la entrada, la diferencia es una tarifa de transacción que se le añade al valor de incentivo del bloque que contiene la transacción. Una vez que un número predeterminado de monedas han entrado en circulación, el incentivo puede transicionar enteramente a tarifas de transacción y ser completamente libre de inflación. El incentivo puede ayudar a animar a los nodos a mantenerse honestos. Si un atacante egoísta es capaz de reunir más potencia de CPU que todos los nodos honestos, este tendría que elegir entre utilizarla para defraudar a la gente robando sus pagos de vuelta, o en utilizarla para generar monedas nuevas. Debería encontrar más rentable jugar por las reglas, tales reglas lo favorecen a él con más monedas que a todos los demás combinados, que socavar el sistema y la validez de su propia riqueza". Cfr. NAKAMOTO, *op. cit.*, p. 4.

[302] PÉREZ-SOLÀ y HERRERA-JOANCOMARTÍ, *op. cit.,* p. 243.

12. P2P o punto a punto

SANTÍN GONZALES define al P2P (*peer-to-peer*) de la siguiente manera: "Aquella red informática que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan a la vez como clientes y como servidores de los demás nodos de la red. Este modelo de red contrasta con el modelo cliente-servidor tradicionalmente empleado en las aplicaciones de Internet. Así, en una red P2P todos los nodos se comportan igual y pueden realizar el mismo tipo de operaciones; pudiendo no obstante diferir en configuración local, velocidad de proceso, ancho de banda y capacidad de almacenamiento"[303].

La característica fundamental de la red P2P[304] está en su unidad de procesamiento básico, ya que un par es una entidad capaz de desarrollar algún trabajo útil y de comunicar los resultados de ese trabajo a otra entidad de la red, ya sea de forma directa o indirectamente.

---

[303] SANTÍN GONZALES, Abel, "Peer to Peer. Sistemas Operativos Distribuidos", p. 3. Disponible en: <http://www.dit.upm.es/~joaquin/so/p2p/p2p.pdf>. En ese sentido, Bonilla Egido y Meler Playan la definen como las "Redes descentralizadas y distribuidas en las cuales las aplicaciones pueden comunicarse entre sí, intercambiando información sin la intervención de un servidor central". BONILLA EGIDO, Antonio y MELER PLAYAN, Javier, "Aplicaciones Distribuidas P2P (Seminaris de Caso)", p. 2. Disponible en: <http://docencia.ac.upc.es/FIB/CASO/seminaris/2q0304/M9.pdf>.

[304] Bitcoin utiliza una red P2P totalmente distribuida para propagar la información. Bloques y transacciones son transmitidos a través de esta red. Cuando un nodo quiere realizar una transacción (o bien encuentra un bloque válido), este lo envía a toda la red. Para hacerlo, lo envía a los nodos que se encuentran directamente conectados con él y éstos, a su vez, lo reenvían a sus vecinos, siempre que el objeto en cuestión (bloque o transacción) sea válido. De este modo, la información se propaga por toda la red. Dado que, a diferencia de los bloques, las transacciones no contienen ninguna prueba de trabajo, un nodo malicioso podría crear un gran número de transacciones válidas con la intención de desbordar la red. Para evitar este tipo de ataques, los nodos estándar de Bitcoin aplican una política de retransmisión de transacciones, que obliga a incorporar una comisión a las transacciones que cumplen ciertas características que las hacen ideales para este tipo de ataques. Aún así, los usuarios que realizan transacciones tienen libertad para decidir si pagan o no una comisión y, en caso de hacerlo, del importe que esto conlleva. Estas comisiones afectan, como hemos comentado, la retransmisión de la transacción, además de su inclusión en un bloque. Esto último es debido a que el minero, además de cobrar la recompensa por encontrar un bloque, también obtiene todas las comisiones que las transacciones que contiene el bloque incorporan. Por este motivo, incluir comisiones en las transacciones puede crear incentivos adicionales para que los mineros las incluyan en sus bloques. PÉREZ-SOLÀ y HERRERA-JOANCOMARTÍ, *op. cit.,* p. 243.

Se clasifican en dos modelos. El modelo "puro", en el que los nodos pueden cumplir tres funciones: 1) la de servidor, cuando un nodo requiere información de otro; 2) la de cliente, cuando éste pide información a un par; 3) la de ruteador, cuando el nodo se encuentra como intermediario entre otros dos[305]. El modelo "híbrido", "donde un nodo, puede realizar una consulta a un servidor para saber dónde están los otros nodos en la red. Una vez hecha la consulta, el nodo podrá establecer la conexión directa con otro nodo para compartir su información. La aplicación P2P debe informar a este servidor, de su conexión y desconexión para mantener la integridad del servicio"[306].

13. Privacidad

Una de las principales características del *bitcoin* es el anonimato[307] que existe por parte de sus usuarios, ya que si bien es cierto las operaciones o transferencias de *bitcoin* quedan registradas en el *blockchain*, no hay forma de saber las identidades o nombres de los usuarios que formaron parte de esa transferencia virtual, porque se trata de una transferencia de datos de un punto A ha un punto B. Esta mecánica se puede repetir infinidad de veces sin la necesidad de contar con los datos personales de los intervinientes.

Sin embargo, el supuesto blindaje de identidad con el que *bitcoin* blinda a sus usuarios es muy relativo[308], ya que, como refieren algunos especialistas en la

[305] BONILLA EGIDO y MELER PLAYAN, *op. cit.,* p. 6.

[306] *Ibid*., p. 7.

[307] "El modelo bancario tradicional logra un nivel de privacidad al limitar el acceso a la información de las partes envueltas y del tercero confiado. La necesidad de anunciar todas las transacciones públicamente se opone a este método, pero la privacidad aún puede ser mantenida al romper el flujo de la información en otro lugar: al mantener las claves públicas anónimas. El público puede ver que alguien está enviando una cantidad a otra persona, pero sin información que relacione la transacción a ninguna persona". NAKAMOTO, *op. cit.*, p. 2.

[308] En ese sentido: "Bitcoin no difunde información personal sobre los titulares de los fondos sino direcciones Bitcoin (similares a las direcciones de correo electrónico), lo cual permite la reserva de la identidad del usuario detrás de cada cuenta privada; no obstante, debe advertirse que existen técnicas que permiten adquirir cierto conocimiento acerca de los usuarios de las direcciones Bitcoin". GUTIÉRREZ y MORENO, *op. cit.,* p. 28.

técnica de la criptografía, se puede asociar al usuario, al IP desde donde se realiza la operación.

Aunque otro sector discrepante establece que el anonimato que brinda *bitcoin* a sus usuarios cuenta con cierta relatividad, ya que cualquier usuario podría haber utilizado cualquier computador u ordenador en cualquier lugar del planeta para transferir *bitcoin*[309], con lo cual existirían infinidad de fórmulas para mantenerse en un total y absoluto anonimato, sin poder ser detectado o identificado.

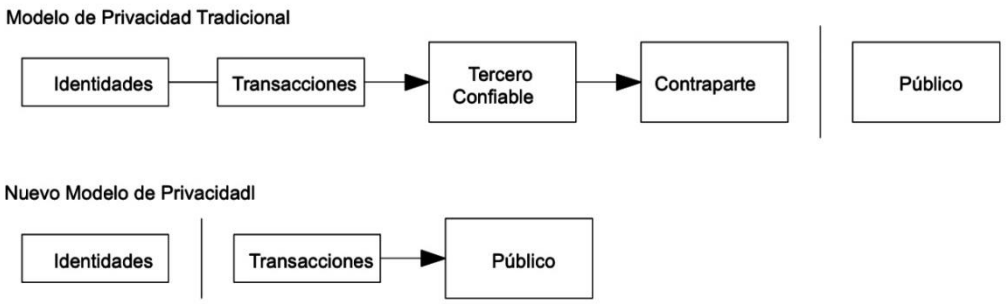

Imagen tomada de “Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario”

12. Volatilidad

Al ser el *bitcoin* una criptoactivo descentralizado, su misma naturaleza monetaria la hace independiente de estar sujeta a algún tipo de control formal por parte del gobierno o del banco central, a diferencia de lo que significa la moneda fíat, que tiene todo el respaldo gubernamental y de la banca mundial.

El *bitcoin,* muy por el contrario, se autorregula con base en la oferta y la demanda que promueven sus mismos usuarios. Esto se da primordialmente por la falta de regulación y control, por lo que se vuelve extremadamente volátil respecto a su valor. Al día de hoy 25 de mayo del 2022, a las 12:06 a. m., en que redacto esta

[309] ELBITCOIN.ORG, *op. cit.,* posición en Kindle 704-722.

tesis el precio del *bitcoin,* según la plataforma web CoinMarketCap[310], es de $29.558.017 dólares.

Un estudio del Banco de Pago Internacionales (BPI)[311] revela el impacto que tienen las noticias en los precios de las criptoactivos. Como refiere el informe, existe una incidencia intradía que las noticias generan en el precio del *bitcoin*, expandiendo sus efectos sobre los precios de otros criptoactivos y sobre otros aspectos de los mercados de criptoactivos. Los precios tienen carácter prospectivo, por lo que con frecuencia se utilizan para evaluar la posible incidencia de operaciones societarias e iniciativas de las administraciones, por medio de una metodología estándar de estudio de eventos[312].

Acá un recuento del historial de precios más altos alcanzados por el *bitcoin* desde su creación al día 22 de febrero del 2022: precio del *bitcoin* en el 2009 = $ 0; precio del *bitcoin* en el 2010 = $ 0.39; precio del *bitcoin* en el 2011[313] = $ 1; precio del *bitcoin* en el 2012 = $ 13,5; precio del *bitcoin* en el 2013 = $ 727; precio del *bitcoin* en el 2014 = $ 317; precio del *bitcoin* en el 2015 = $ 429; precio del *bitcoin* en el 2016 = $ 966; precio del *bitcoin* en el 2017[314] = $ 13,170; precio del

---

[310] Véase: <https://coinmarketcap.com/es/currencies/bitcoin/>.

[311] En ese sentido, refiere el informe Trimestral del PBI que "a menudo se cree que las criptomonedas operan fuera del alcance de la regulación nacional, pero en realidad sus valoraciones, volúmenes de transacciones y bases de usuarios reaccionan con fuerza a las noticias sobre iniciativas de las autoridades reguladoras. La repercusión depende de la categoría regulatoria concreta a la que se refiera la noticia: las noticias sobre posibles prohibiciones generales de las criptomonedas o su sujeción a la legislación sobre valores son las que tienen un mayor efecto negativo, seguidas de las noticias sobre la lucha contra el blanqueo de capitales y la financiación del terrorismo y las relativas a restricciones de la interoperabilidad de las criptomonedas con los mercados regulados. Las noticias que apuntan al establecimiento de marcos jurídicos específicos adaptados a las criptomonedas y las ofertas iniciales de criptomonedas coinciden con fuertes avances en el mercado. De estos resultados se desprende que los mercados de criptomonedas dependen para su funcionamiento de instituciones financieras reguladas y que están segmentados por jurisdicciones, por lo que sí se encuentran dentro del radio de acción de la regulación nacional". AUER, Raphael y CLAESSENS, Stijin, "Regulación de las criptomonedas: evaluación de reacciones del mercado", en *Informe Trimestral del BPI*, septiembre del 2018, p. 1

[312] AUER y CLAESSENS, op. cit., p. 6.

[313] Véase: <https://www.buybitcoinworldwide.com/es/precio/>.

[314] *Idem*.

bitcoin en el 2018[315] = $ 10,109; precio del *bitcoin* en el 2021= $ 68,789.63[316]; precio del bitcoin en el 2022 = $ 28,774.00[317].

14. La falta de territorialidad

La falta de territorialidad es unas de las principales características que hacen muy atractivo para los usuarios la compra de *bitcoin,* ya que una persona puede adquirir *bitcoin* en cualquier parte del mundo, sin ningún tipo de control por parte de las entidades reguladoras. El *bitcoin* no se encuentra ubicado en un servidor específico, ni tiene un dueño identificado, sino muy por el contrario se encuentra distribuido de forma descentralizada[318], ya que la toma de esas decisiones se realiza de acuerdo con las reglas de consenso que el responsable del nodo ha elegido libremente, por ello la suma de todos los nodos y sus decisiones se materializan en una respuesta única. Como señala HERENCIA ANTÓN, hay que diferenciar un sistema descentralizado[319] de un sistema distribuido; en este último, el trato de los datos se distribuye con buena parte de la red y los nodos, por lo que las decisiones son centralizadas con pleno conocimiento de la totalidad del estado del sistema[320].

---

[315] Véase: <https://www.coingecko.com/es/tabla_de_precios/bitcoin/usd>.

[316] Véase: <https://finance.yahoo.com/>.

[317] *Idem*.

[318] "Debido a su descentralización, Bitcoin ha creado una clase diferente de pago en la red con un incremento en flexibilidad y redundancia. Bitcoin puede manejar millones de dólares en intercambios sin necesitar protección militar. Sin un punto central que pueda fallar, atacar la red es una tarea muy difícil. Bitcoin podría representar un gran paso en asegurar sistemas financieros locales" y globales". BITCOIN, "Innovación en sistemas de pago". Disponible en: <https://bitcoin.org/es/innovacion>.

[319] En ese sentido, HERENCIA ANTÓN refiere: "Se dice de aquel que no tiene un controlador de decisiones único, es decir, un solo centro de mando. Los nodos que forman un sistema descentralizado no son conscientes del mapa completo del sistema, no lo necesitan, y son capaces de tomar las decisiones que más se ajusten a sus necesidades con la información que han obtenido hasta un momento determinado del tiempo". HERENCIA ANTÓN, *op. cit.,* p. 67.

[320] *Ibid*., p. 67.

15. La falta de intermediarios

Las operaciones en *bitcoin* no están sujetas a algún tipo de control central por parte de un administrador o tercero que regule las transacciones. He ahí unas de las grandes críticas que presenta el *bitcoin* al no estar sujeto a ningún tipo de control por parte del sistema financiero. Esta falta de organismos centrales controladores descansa en la apuesta hecha por NAKAMOTO de evitar la existencia de una autoridad central alguna, lo que supone eliminar el papel preponderante de los bancos en la intermediación de una operación financiera. En ese sentido, AHOMED CHÁVEZ refiere que "para comprender la motivación que generó la creación del bitcóin, es necesario comparar las actuales transacciones electrónicas bancarias de débito o de crédito. Tales actividades ahorran tiempo, pero conllevan una comisión que cobra el banco o la entidad financiera en desmedro del patrimonio del titular de la cuenta bancaria o financiera"[321].

Sin embargo, la falta de trazabilidad de las operaciones de un criptoactivo supone un problema mayor en lo que se refiere a la regulación vigente en prevención de blanqueo de capitales, como veremos más adelante[322].

16. Criptografía

La criptografía se remonta a hace más de 4000 años, el origen de la palabra criptografía lo encontramos en la palabra de origen griego *krypto,* que significa 'oculto', y *graphos*, 'escribir'. La criptografía se encarga de cifrar o codificar los mensajes para evitar que su contenido pueda ser leído por un tercero no autorizado; es decir, la generación de códigos y algoritmos de cifrado que buscan ofuscar la información y protegerla de "ojos curiosos" es el cometido principal de esta disciplina[323].

---

[321] CHÁVEZ, *op. cit.,* p. 5.

[322] ARROYO GUARDEÑO *et al., op. cit.,* p. 13.

[323] JESÚS VELASCO, Juan, "Breve historia de la criptografía", en *Diario.es*, 20 de mayo del 2014. Disponible en: <https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html>.

La BITCOIN la define como "la rama de las matemáticas que nos permite crear pruebas matemáticas que proporcionan altos niveles de seguridad. El comercio en línea y los bancos ya utilizan criptografía. En el caso de Bitcoin, la criptografía se utiliza para hacer imposible que alguien pueda gastar los fondos del monedero de otro usuario o que se pueda corromper la cadena de bloques. También se utilizada para encriptar un monedero, de manera que no se pueda utilizar sin una contraseña"[324].

17. La falta de regulación del bitcoin en el sistema financiero

Una de las principales características que presenta el *bitcoin* es la falta de regulación por parte del sistema financiero bancario y no bancario. Al respecto, ya se han emitido distintos pronunciamientos, por parte de un sector importante de las autoridades financieras y de supervisión de la banca mundial, sobre cuáles son las implicancias negativas que generan las transacciones y operaciones con bitcoin, al no estar sometida a ningún tipo de control bancario.

El Banco Europeo Central (European Central Bank) ha señalado que son varios las desventajas e inconvenientes que presenta el bitcoin para sus usuarios dentro de las que enumera: la falta de transparencia, la volatilidad, anonimato del beneficiario[325]. Si bien es cierto las monedas virtuales presentan aspectos positivos con relación a la innovación financiera como medio de pago, no podemos soslayar que también existe un alto riesgo de que pueden afectar la estabilidad financiera, pero lo más grave es que puedan ser utilizadas para fines criminales, como veremos más adelante el ítem referente a ese punto.

Uno de los principales problemas que plantea el *bitcoin* es que los bancos centrales del denominado Eurosistema no reconocen el concepto de moneda

---

[324] BITCOIN, "Algunas palabras en Bitcoin que usted puede escuchar". Disponible en <https://bitcoin.org/es/vocabulario>.

[325] EUROPE CENTRAL BANK, *op. cit.,* p. 4.

virtual, ya que estos términos no pertenecen al mundo del dinero o moneda tradicional que se utilizan en la economía, enfocado desde una perspectiva legal[326].

Desde un enfoque eminentemente económico, las monedas virtuales, como es el caso del *bitcoin,* no responden a las tres funciones del dinero que tienen mayor aceptación por la doctrina mayoritaria, los cuales son: i) el *medio de cambio o intercambio,* que diferencia al dinero del resto de activos financieros, ya que tiene total aceptación como forma de pago de bienes y servicios[327]; ii) el *depósito o reserva de valor,* porque es utilizado para guardar poder adquisitivo o de compra a lo largo del tiempo[328]; iii) *unidad de cuenta*, ya que simplifica la fijación de los precios de los bienes y servicio[329].

Desde un enfoque jurídico regulatorio, el *bitcoin* o monedas virtuales*,* a diferencia de las monedas y billetes tradicionales que son de curso legal en los distintos países del globo terráqueo, no han sido declaradas como monedas oficiales por ninguna entidad financiera, salvo el caso de los países del El Salvador y República Centroafricana, como veremos.

18. El *bitcoin* en El Salvador

El 7 de septiembre del 2021, El Salvador se convirtió en el primer país del mundo en adoptar *bitcoin* como moneda de curso legal, con la finalidad de reducir los costos en los envíos de remesas. La referida ley fue aprobada el 8 de junio de 2021 por la Asamblea Legislativa de El Salvador, y tiene como su antecedente el Dictamen N.º 03, que contiene la iniciativa del presidente de la república de

---

[326] *Ibid.,* p. 23.

[327] JIMÉNEZ, Félix, *Elementos de teoría y políticas macroeconómicas para una economía abierta,* Lima: Fondo Editorial - Pontificia Universidad Católica del Perú, 2012, p. 193.

[328] *Ibid.,* p. 193.

[329] *Idem*.

dicho país, Nayib Bukele, solicitando se emita La Ley Bitcoin, que tiene como objeto la regulación del *bitcoin* como moneda de curso legal, irrestricto con poder liberatorio, ilimitado en cualquier transacción y a cualquier título que las personas naturales o jurídicas, públicas o privadas, requieran realizar[330].

La Ley Bitcoin de El Salvador está compuesta por un marco normativo de 16 artículos que desarrollan de forma general el funcionamiento de la misma. Dentro de los dispositivos que conforman la Ley Bitcoin, se hace referencia que el control de tipo de cambio entre el dólar norte americano y el bitcoin será libremente definido por el mercado[331]; de igual forma, se establece que todo precio, es decir, todo ofrecimiento de servicios y productos que se ofrecen el mercado, podrá ser expresado en bitcoin[332].

En materia de recaudación tributaria la norma refiere que todas las contribuciones realizadas al fisco podrán ser pagadas en bitcoin[333], y que todos los intercambios en bitcoin no estarán sujetos al impuesto de ganancia de capital[334]; además, la norma conmina a todos los agentes económicos (personas físicas o jurídicas que forman parte del proceso de una operación económica) a la obligatoria aceptación de bitcoin como forma de pago absoluto por el otorgamiento de un bien o servicio[335]. Sumado a ello el texto proveerá de todas las herramientas necesarias para viabilizar la convertibilidad automática a bitcoin, para lo cual creará un fideicomiso[336] en el Banco Central de El Salvador.

Con posterioridad a la promulgación del Decreto N.º 57, denominado como la Ley Bitcoin, publicado el 08 de junio del 2021 en el *Diario Oficial* de la República

---

[330] Artículo 1 del Decreto N.º 57, Ley Bitcoin, de fecha 09 de junio del 2021.

[331] Artículo 2 del Decreto N.º 57, Ley Bitcoin, de fecha 09 de junio del 2021.

[332] Artículo 3 del Decreto N.º 57, Ley Bitcoin, de fecha 09 de junio del 2021.

[333] Artículo 4 del Decreto N.º 57, Ley Bitcoin, de fecha 09 de junio del 2021.

[334] Artículo 5 del Decreto N.º 57, Ley Bitcoin, de fecha 09 de junio del 2021.

[335] Artículo 7 del Decreto N.º 57, Ley Bitcoin, de fecha 09 de junio del 2021.

[336] Artículo 14 del Decreto N.º 57, Ley Bitcoin, de fecha 09 de junio del 2021.

del Salvador en América Central, el Banco Central del Salvador publicó un documento con las normas técnicas para poder facilitar la aplicación de la Ley Bitcoin entre los distintos agentes económicos que permitan ofrecer servicios ágiles, competitivos e inclusivos para la población[337].

Dicho cuerpo normativo tiene por objeto regular los derechos y obligaciones en las relaciones comerciales entre entidades financieras y proveedores que contraten para el adecuado funcionamiento de transacciones y pagos digitales únicamente con *bitcoin* o dólares por medio de distintos mecanismos electrónicos[338].

Dentro de los sujetos obligados al cumplimiento de las normas técnicas, el reglamento hace referencia a los bancos, bancos cooperativas, sociedades de ahorro y crédito que estén interesados de cambio de dólares por *bitcoin* y viceversa, esto a través de proveedores de: a) billeteras digitales de *bitcoin* y dólares; b) casas de intercambio digitales o *exchange* para *bitcoin* y dólares; c) proveedores de servicios de pagos para *bitcoin* y dólares; y d) cualquier otro agente en la cadena de valor del producto o servicio relacionado a esta norma, tales como custodios y proveedores de tecnología relacionadas con *bitcoin*[339]. Las normas técnicas[340] también hacen especial referencia a las obligaciones específicas en materia de prevención de blanqueo de capitales, acápite que desarrollaremos el capítulo 4 de la presente tesis. Sin duda que, para poder viabilizar la legalización del *bitcoin* como moneda de curso legal, El Salvador se ha tenido que ver en la necesidad de adquirir *bitcoin* dentro del mundo cripto,

---

[337] Véase el preámbulo del Comité de Normas del Banco Central de Reserva, en el que se establece "que la aprobación de la Ley Bitcoin hace necesario la entrada en operación de distintos agentes económicos que permitan ofrecer servicios financieros ágiles, competitivos e inclusivos para la población en general, considerando las transacciones en monedas de curso legal para el territorio de El Salvador".

[338] Véase el artículo 1 de las Normas Técnicas para Facilitar la Aplicación de Ley Bitcoin

[339] Véase el artículo 2 de las Normas Técnicas para Facilitar la Aplicación de Ley Bitcoin

[340] Art. 1.- Las presentes Normas tienen por objeto regular los derechos y obligaciones en las relaciones comerciales entre entidades financieras y proveedores que contraten para el adecuado funcionamiento de las transacciones y pagos digitales únicamente con bitcoin o dólares por medio de distintos mecanismos electrónicos.

para lo cual al 09 de mayo del 2022 se han hecho de unos 2301[341] *bitcoin*, una inversión millonaria por parte de este gobierno, si tenemos en cuenta que un *bitcoin* ha llegado a valer $ 68 789.63.

La justificación de esta medida según el gobierno salvadoreño sería de orden eminentemente económico, ya que el *bitcoin* tiene un mercado de capitalización de 600 000 millones de dólares (504 000 millones de euros) a nivel global, buscando con esta normativa incentivar a que los inversores y los turistas que tengan *bitcoin* inviertan y viajen al Salvador, beneficiando a la economía de dicho Estado.

Respecto al almacenamiento de criptomonedas, el gobierno de El Salvador ha desarrollado la Chivo Wallet[342], que es la billetera oficial de bitcoin y dólar que apoya el Gobierno de El Salvador. Esta tecnología permite enviar y recibir, sin comisión, *bitcoin* y/o *dólar* entre salvadoreños; de la misma manera, permite a los usuarios intercambiar *bitcoin* por *dólar* o viceversa; todas estas operaciones no están sujetas a ningún tipo de comisión[343].

---

[341] EL ECONOMISTA, "El Salvador compra 500 bitcoines aprovechando baja en su previo", 9 de mayo del 2022. Disponible en: <https://www.eleconomista.com.mx/internacionales/El-Salvador-compra-500-bitcoines-aprovechando-baja-en-su-precio-20220509-0078.html>.

[342] "Chivo Wallet es la billetera oficial de *bitcoin* y dólar que apoya el Gobierno de El Salvador. Chivo Wallet permite enviar y recibir *bitcoin* y/o dólar entre Salvadoreños sin comisión, de la misma manera le permite a los usuarios intercambiar Bitcoin por Dolar o viceversa sin comisión. Adicionalmente Chivo es compatible con otras billeteras Bitcoin On-Chain y Lightning Network. Chivo permite la posibilidad de conectarse con el sistema bancario de El Salvador para depositar o retirar dólares de la plataforma, y con una red de cajeros Chivo para depositar y retirar dólares en efectivo. Chivo posee una versión de empresas que permite cobrar, asignar terminales de cobro para empleados, y pagar impuestos de forma rápida y fácil. Para hacer uso de la billetera y sus Servicios, el Usuario debe estar registrado en Chivo Wallet y tener una cuenta vigente (en adelante el Usuario Registrado). CHIVO S. A. DE C. V. declara, y así lo acepta el Usuario, que no proporciona ningún tipo de servicio de asesoría financiera. Así como tampoco, posee alianzas o vinculación alguna con empresas que ofrezcan servicios de asesoría financiera que involucren o no transacciones con Bitcoin. Dependiendo del país de residencia, se puede dar el caso que un Usuario no deba usar todas las funciones de Chivo Wallet. Es responsabilidad del Usuario respetar las reglamentaciones y leyes propias del país donde reside, o el país desde donde está accediendo a Chivo Wallet, incluyendo, pero sin limitarse al régimen cambiario y de transferencias de cada uno de los países. En esa medida, el Usuario no puede usar Chivo Wallet y/o sus Servicios para transgredir directa o indirectamente cualquier disposición del ordenamiento jurídico". CHIVO WALLET, "Términos y condiciones". Disponible en: <https://chivowallet.com/terminos-y-condiciones.html>.

[343] CHIVO WALLET, *op. cit.*

Esta *ballet* o billetera digital se conecta con el sistema bancario de El Salvador para depositar o retirar dólares de la plataforma, y con una red de aproximadamente 200 cajeros[344] Chivo para depositar y retirar dólares en efectivo. Se registran un promedio entre 6000 a 15000 transacciones[345] diarias desde este aplicativo, el cual también cuenta con una versión diseñada para las personas jurídicas que les permite cobrar, asignar terminales de cobro para empleados, y pagar impuestos. Los miembros registrados pueden realizar pagos ilimitados, incluidas las conversiones, de forma gratuita. No se imponen tarifas adicionales ni tarifas de transacción.

Para incentivar a la población al uso de este monedero virtual, el gobierno otorga un bono de $30 dólares americanos a todos aquellos ciudadanos que lo descarguen.

Sobre el particular, los directores del Fondo Monetario Internacional mediante el Comunicado de Prensa 22/13 resaltaron la importancia de promover la inclusión financiera y reconocieron que los medios digitales de pago, como la billetera electrónica Chivo, pueden tener un rol. Sin embargo, enfatizaron la necesidad de fortalecer la regulación y la supervisión del nuevo ecosistema de Chivo y Bitcoin. Subrayaron que hay grandes riesgos asociados al uso de Bitcoin para la estabilidad financiera, la integridad financiera y la protección del consumidor, así como las posibles contingencias fiscales. Instaron a las autoridades a limitar el alcance de la ley Bitcoin eliminando su calidad de moneda de curso legal. Algunos directores también manifestaron su preocupación sobre los riesgos asociados a la emisión de bonos respaldados por Bitcoin[346].

---

[344] PASTRÁN, Rosa María, "Athena Bitcóin provee la red de cajeros Chivo al gobierno", en *El Economista,* 18 de noviembre del 2021. Disponible en: <https://www.eleconomista.net/economia/Athena-Bitcoin-provee-la-red-de-cajeros-Chivo-al-gobierno-20211118-0008.html>.

[345] BARRERA, José, "Chivo Wallet registra un promedio de 6,000 transacciones por día, según experto argentino", en *Diario el Mundo*, de fecha 24 de noviembre del 2021. Disponible en: <https://diario.elmundo.sv/economia/chivo-wallet-registra-un-promedio-de-6000-transacciones-por-dia-segun-experto-argentino>.

[346] FONDO MONETARIO INTERNACIONAL, "Comunicado de Prensa No. 22/13: El Directorio Ejecutivo del FMI concluye la Consulta del artículo IV con El Salvador correspondiente a 2021", 25 de

19. El *bitcoin* en República Centroafricana (RCA)

La República Centroafricana ha sido el segundo país en el mundo en adoptar el *bitcoin* como moneda de curso legal. Mediante la Asamblea Nacional del país se ha aprobado por unanimidad la Ley N.º 22004, del 22 de abril del 2022, que regula las criptomonedas en dicho Estado.

El texto normativo compuesto por 26 artículos utiliza una técnica legislativa muy similar a la utilizada por El Salvador en su Ley Bitcoin. Establece el objeto, alcances, y lo referente a la regulación de operaciones en criptomonedas dentro del territorio de ese país. La Ley N.º 22004 se aplica a todas personas naturales o jurídicas de derecho público o privado que realicen actividades de comercio en línea relacionado con criptomonedas, y actividades que brinden acceso a servicios de criptomonedas al público a través de las tecnologías de la información y la comunicación, mediante la tecnología *blockchain* que da lugar a la celebración de contratos inteligentes para la obtención de bienes o servicios[347].

Esta iniciativa legislativa sería reforzada en un futuro según el presidente Faustin-Archange Touaderá, quien, en un anuncio en redes, lanzó la noticia del proyecto Sango, que busca atraer inversión en *bitcoin* al país, haciendo mayor énfasis en la adquisición de terrenos. Ya el Banco Mundial ha manifestado su rechazo en relación con este proyecto, por considerarlo inviable[348].

20. BitLicence

El 8 de agosto del 2015, el Departamento de Servicios Financieros de la ciudad de Nueva York (DFS) emitió la BitLicence bajo el reglamento de la

enero del 2022. Disponible en: <https://www.imf.org/es/News/Articles/2022/01/25/pr2213-el-salvador-imf-executive-board-concludes-2021-article-iv-consultation>.

[347] Véase: Loi n° 22.004 du 22 avril 2022, régissant la cryptomonnaie en République Centrafricaine

[348] COGHLAN, Jesse, "El Banco Mundial no apoyará el centro de criptomonedas Sango de la República Centroafricana", en *Cointelegrah*, 26 de mayo del 2022. Disponible en: <https://es.cointelegraph.com/news/world-bank-won-t-support-central-african-republic-s-sango-crypto-hub>.

Superintendencia de Servicios Financieros para regulación de moneda virtual 23 NYCRR, Parte 200, bajo la Ley de Servicios Financieros de Nueva York (Virtual Currency Regulation 23 NYCRR Part 200 under the New York Financial Services Law). Se trata de los requisitos para la obtención de una licencia comercial destinada a todas aquellas personas jurídicas que desean realizar actividades relacionadas con criptomonedas[349].

Desde ese entonces, la Ley Bancaria de Nueva York sobre sociedades fiduciarias de propósito limitado, ha otorgado numerosas licencias y estatutos de moneda virtual para garantizar que los neoyorquinos tengan una forma bien regulada de acceder al mercado de moneda virtual. El documento normativo en mención tiene como finalidad regular todos aquellos negocios que se realizan con monedas virtuales.

21. Cajero automático de *bitcoin*

El GAFI lo define como "una máquina automatizada utilizada para el cambio de moneda fíat para bitcoin y/o otra moneda virtual y viceversa"[350]. Hasta finales del 2014 había un aproximado de 300 cajeros de *bitcoin* operando a nivel mundial[351]. En la actualidad, hay unos 30 000 cajeros automáticos de *bitcoin* en todo el mundo, la mayoría de ellos se ubica en Estados Unidos de Norteamérica[352]. En España, hay alrededor de 3600 cajeros *bitcoin* posicionando en segundo lugar después de Estados Unidos[353]. Los cajeros *bitcoin* necesitan estar conectados a

---

[349] Véase la New York State Department of Financial Services Proposed New York Codes, Rules and Regulations, title 23. department of financial services chapter i. regulations of the superintendent of financial services part 200. virtual currencies.

[350] GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Directrices para un Enfoque*…, *op. cit*., p. 48.

[351] *Ibid.,* p. 48.

[352] COINTELEGRAPH, "Cajeros automáticos de Bitcoin: Guía para principiantes sobre los cajeros de Bitcoin". Disponible en: <https://es.cointelegraph.com/bitcoin-for-beginners/bitcoin-atms-a-beginners-guide-to-bitcoin-teller-machines>.

[353] HERRERA, Jesús, "3000 cajeros automáticos en España añaden compra bitcoin", en *Criptonoticias*, 15 de septiembre del 2022. Disponible en: <https://www.criptonoticias.com/comunidad/espana-3000-cajeros-automaticos-funcionan-bitcoin/>.

la Internet para poder funcionar e intercambiar criptomonedas por dinero en efectivo. Los cajeros automáticos de *bitcoin* también están sujetos a un proceso de verificación, especialmente cuando se realizan transacciones de grandes cantidades. Dependiendo del tipo de cajero, se puede comprar o vender *bitcoin*, o ambas funciones.

22. Algunas reflexiones en torno a los conceptos señalados

Una primera conclusión que podemos establecer, después de haber realizado una explicación del dinero electrónico y su regulación en el ordenamiento jurídico peruano, es su diferencia con los criptoactivos, ya que en la actualidad existe una confusión en la terminología de ambos conceptos. Como ya expliqué al comienzo en este punto, el dinero electrónico es dinero digital almacenado en un soporte electrónico, por el mismo valor que se recibe; el dinero digital también lo encontramos en todas aquellas transferencias que se ejecutan a través de la banca electrónica o las *fintech.* Todas las monedas de curso legal en el mundo pueden mutar a la forma digital sin perder su valor físico o reserva de valor. Los criptoactivos o monedas virtuales, como ya se explicó, son representaciones digitales que se pueden comercializar digitalmente a través del ciberespacio, pero no tiene estatus o amparo para ser consideradas de curso legal, salvo en el caso de las jurisdicciones del El Salvador y República Centroafricana. Otra diferencia sustancial se da con respecto a la creación de los criptoactivos, ya que son creados por los propios usuarios en redes centralizadas y descentralizadas.

IV. OTROS CRIPTOACTIVOS DE RELEVANCIA

Si bien el *bitcoin* sigue siendo el criptoactivo con mayor valor económico en el mercado, algunos atribuyen esta alza permanente en su valor a su escasez, ya que su protocolo establece una creación máxima de 21 millones de unidades, y cada vez habría menos, situación que encarecería su valor. Sin embargo, no podemos soslayar que en el mercado de criptoactivos, desde el auge de *bitcoin* en el mercado de criptoactivos, se han venido creando otros proyectos de criptoactivos con sus propias particularidades tecnológicas, que han tenido una

acogida bastante interesante por parte de la comunidad interesada en estas representaciones digitales. Se calcula un estimado de más de 8000 tipos de criptoactivos que son objeto de comercialización en las distintas plataformas. Por ello, considero pertinente y útil hacer referencia a otros criptoactivos que actualmente están circulando en el mercado.

1. Ethereum

El proyecto Ethereum fue creado en el año 2015 por el programador Vitalik Buterin[354]. El Ethereum funciona como una plataforma de código abierto basado en la tecnología *blockchain*, muy similar a la del bitcoin; sin embargo, su lenguaje de programación les permite a sus desarrolladores crear un *software* para gestionar las transacciones y automatizar las operaciones, lo que se conoce como "contrato inteligente"[355] o *smart contract*.

El propósito de Ethereum es crear un protocolo alternativo para construir aplicaciones descentralizadas y colaborativas. La criptomoneda de la red Ethereum es el *ether*[356] y, al igual que bitcoin, existe como parte de un sistema

---

[354] En relación con su biografía, "Vitalik Buterin es un escritor y programador ruso-canadiense. Vitalik ha estado involucrado en la comunidad Bitcoin desde 2011, cofundando y escribiendo artículos para la revista Bitcoin. Pero se le conoce principalmente como el niño genio detrás de Ethereum, la segunda plataforma de criptomoneda más valorada y reconocida del mundo después de Bitcoin". COINTELEGRAPH, "¿Quién es Vitalik Buterin?". Disponible en: <https://es.cointelegraph.com/ethereum-for-beginners/who-is-vitalik-buterin>.

[355] En los contratos inteligentes de Ethereum, "el código en los contratos de Ethereum está escrito en un lenguaje de bajo nivel bytecode basado en pila, conocido como *código de máquina virtual de Ethereum* o *código de la EVM*. El código consiste en una serie de bytes, donde cada byte representa una operación. En general, la ejecución del código es un bucle infinito que consiste en ejecutar repetidamente la operación en el contador actual de programa (que comienza en cero) y luego incrementar el contador del programa en uno, hasta que se alcance el final del código o se detecte un error o una instrucción STOP o RETURN. Las operaciones tienen acceso a tres tipos de espacio en el que almacenar datos: La pila, un contenedor *último en entrar, primero en salir* cuyos valores se pueden apilar y retirar, el Memoria, un array de bytes expandible infinitamente, el almacenamiento a largo plazo del contrato, un almacén de clave/valor. A diferencia de la pila y la memoria, que se restablecen una vez termina la computación, el almacenamiento persiste a largo plazo". ETHEREUM.ORG, "Guía de Ethereum". Disponible en: <https://ethereum.org/es/whitepaper/#notes>.

[356] En ese sentido: "la red Ethereum incluye su propia moneda incorporada: ether, el cual cumple el doble propósito de proporcionar una capa de liquidez primaria para permitir un intercambio eficiente entre varios tipos de activos digitales y, aún más importante, el proporcionar un

financiero autónomo de pares, libre de intervención gubernamental. Al igual que *bitcoin*, el *ether* utiliza una *blockchain*[357] o cadena de bloques pública donde se registran todas sus transacciones. También utiliza un sistema de verificación de transacciones basado en la minería. Una vez realizado el proceso de verificación, los nuevos bloques se enlazan a la cadena de bloques anterior y el minero en cuestión recibe una recompensa en *tokens* de *ether*. Normalmente son 5 unidades de *ether*, aunque esta cifra puede verse afectada dependiendo de la volatilidad del *ether*, es decir, si este sufre un alza, la recompensa será menor.

Hay dos tipos de aplicaciones que resaltan dentro del cúmulo de posibilidades, que se pueden realizar en *ethereum*. La primera categoría, referida a las aplicaciones de índole financieras, ofrece a los usuarios formas más potentes de gestionar y suscribir contratos con su dinero fíat. Esto incluye submonedas, derivados financieros, contratos de cobertura, carteras de ahorros, testamentos e incluso, en última instancia, algunas clases de contratos de empleo a gran escala. La segunda categoría está referida a las aplicaciones semifinancieras, en las que el dinero está presente, pero también hay una destacada parte no monetaria[358].

A manera de resumen, podemos señalar que el protocolo Ethereum fue concebido originalmente por su por su creador Vitalik Buterin, como una versión mejorada de Bitcoin. Cuenta con un sistema de contratos inteligentes que le permite gestionar de forma más eficiente las transacciones. Además de lo referido es considerada la segunda criptomoneda más importante del mundo: su valor de mercado la posiciona en el segundo lugar después de *bitcoin*.

---

mecanismo para pagar tarifas de transacción. Para comodidad y para evitar futuras discusiones (ver el debate actual mBTC/uBTC/satoshi en Bitcoin), las denominaciones se preetiquetarán:1: wei, 1012: szabo, 1015: finney, 1018: ether". ETHEREUM.ORG, "Guía de Ethereum". Disponible en: <https://ethereum.org/es/whitepaper/#notes>.

[357] "La blockchain de Ethereum es en muchas maneras similar a la blockchain de Bitcoin, aunque tiene algunas diferencias. La diferencia principal entre Ethereum y Bitcoin en relación a la arquitectura blockchain es que, a diferencia de Bitcoin (que solo contiene una copia de la lista de las transacciones), los bloques de Ethereum contienen una copia tanto de la lista de transacciones como del estado más reciente". ETHEREUM.ORG, "Guía de Ethereum". Disponible en: <https://ethereum.org/es/whitepaper/#notes>.

[358] ETHEREUM.ORG, "Guía de Ethereum". Disponible en: <https://ethereum.org/es/whitepaper/#notes>.

Recientemente Ethereum realizó una fusión mediante la cual a partir de ahora se cambia la forma en la que ejecuta una cadena de bloques de forma de trabajo (*proof of work*) a prueba de participación (*proof of stake*). Este cambio significa para Ethereum un ahorro de energía de 99,9 % menos del que consumía antes de la fusión[359].

El precio de *ethereum* al día de hoy es de 1 285,73 USD, con un volumen de operaciones de 24 horas de 18 974 622 092 USD. En el ranking actual de CoinMarketCap es el n.° 2, con una capitalización de mercado en vivo de 157 493 722 025 USD. Tiene un suministro en circulación de 122 493 377 monedas ETH[360].

2. Solana

El origen de Solana comienza con el proyecto desarrollado por Anatoly Yakovenko[361], quien es un desarrollador de *software* con una amplia experiencia de desarrollo de sistemas operativos como son: Qualcomm (Brew OS), sistemas distribuidos en Mesosphere y sistemas de compresión en Dropbox. El proyecto Solana[362] es un código abierto altamente funcional que se basa en la naturaleza

---

[359] KESSLER, Sam, "La fusión de Ethereum ya es un hecho y abre una nueva era para la segunda blockchain más grande", en *CoinDesk*, del 15 setiembre del 2022. Disponible en: <https://www.coindesk.com/tech/2022/09/15/la-fusion-de-ethereum-ya-es-un-hecho-y-abre-una-nueva-era-para-la-segunda-blockchain-mas-grande/>.

[360] El 23 de septiembre del 2022 fue consultado el precio *ether*, en el siguiente enlace <https://coinmarketcap.com/currencies/ethereum/>.

[361] En ese sentido, "Anatoly Yakovenko es un ingeniero informático ruso y cofundador del proyecto Solana. Fue autor del libro blanco de Solana. Al crecer en la Unión Soviética, estuvo obsesionado con las computadoras desde los cinco años. Yakovenko finalmente se mudó a los Estados Unidos para construir su propia vida". COINTELEGRAPH, **"**Anatoly Yakovenko. Co-founder of Solana". Disponible en: <https://cointelegraph.com/top-people-in-crypto-and-blockchain-2022/anatoly-yakovenko>.

[362] Véase el resumen o abstract del documento, "Solana: A new architecture for a high performance blockchain v0.8.13", en el que se establece lo siguiente: "Este documento propone una nueva arquitectura de cadena de bloques basada en Prueba de Historia (PoH), una prueba para verificar el orden y el paso del tiempo entre eventos. PoH se utiliza para codificar el paso del tiempo sin confianza en un libro mayor, una estructura de datos solo para agregar. Cuando se usa junto con un algoritmo de consenso como Prueba de trabajo (PoW) o Prueba de participación (PoS), PoH puede reducir la sobrecarga de mensajería en una máquina de estado

descentralizada de la tecnología *blockchain*, para proporcionar soluciones financieras descentralizadas (DeFi).

Solana fue puesta en circulación oficialmente en marzo del 2020 por la Fundación Solana con sede en Ginebra, Suiza. La Fundación Solana ha anunciado que se pondrán en circulación un total de 489 millones de *tokens* SOL; por ahora unos 260 millones de estos ya están en circulación en el mercado[363]. Al día de hoy, de solana tiene un precio de 31,72 USD con un volumen de operaciones de 24 horas de 839 940 671 USD. En el ranking actual de CoinMarketCap es el n.° 9, con una capitalización de mercado en vivo de 11 243 724 814 USD. Tiene un suministro circulante de 354 521 531 monedas SOL[364].

3. Cardano

El proyecto Cardano se inició en el año 2015 por su fundador Charles Hoskinson. El nombre del proyecto tiene su origen en Girolamo Cardano, un erudito y médico italiano conocido por los primeros cálculos sistemáticos de probabilidades. Su token nativo es el ADA; deriva su nombre de Ada Lovelace, quien fue una reconocida matemática y escritora inglesa, conocida principalmente por su trabajo en la computadora mecánica de propósito general propuesta por Charles Babbage, la máquina analítica[365].

---

replicada tolerante a fallas bizantinas, lo que resulta en tiempos de finalización inferiores a un segundo. Este documento también propone dos algoritmos que aprovechan las propiedades de mantenimiento del tiempo del libro mayor PoH: un algoritmo PoS que puede recuperarse de particiones de cualquier tamaño y una prueba de replicación (PoRep) de transmisión eficiente. La combinación de PoRep y PoH proporciona una defensa contra la falsificación del libro mayor con respecto al tiempo (pedido) y el almacenamiento".

[363] Véase: <https://coinmarketcap.com/currencies/solana/>.

[364] El 23 de septiembre del 2022 fue consultado el precio SOL en el siguiente enlace: <https://coinmarketcap.com/currencies/solana/>.

[365] Véase: <https://academy.bit2me.com/que-es-cardano-ada/>.

Su funcionamiento se basa en un protocolo[366] *blockchain* de prueba de participación de código abierto, que tiene dentro de sus desafíos la creación y desarrollo de criptomonedas[367], así como el poder proporcionar un ecosistema con mayor equilibrio que responda a las necesidades de sus usuarios[368]. Su objetivo principal es proporcionar un ecosistema más equilibrado y sostenible que responda mejor a las necesidades de sus usuarios, así como a otros sistemas que buscan la integración[369].

Se trata de una cadena de bloques de tercera generación, ya que plantea una evolución en relación con las generaciones anteriores y evoluciona para satisfacer todas las necesidades que surjan de los usuarios[370]. El precio de Cardano al día de hoy es de 0,451076 USD con un volumen de operaciones de 24 horas de 1.033.483.159 USD. Su ranking actual de CoinMarketCap es el n.º 8, con una capitalización de mercado en vivo de 15 439 006 994 USD. Tiene un suministro circulante de 34 227 045 077 monedas ADA y un suministro máximo de 45.000.000.000 monedas ADA[371].

---

[366] El resumen del libro blanco de Cardano establece lo siguiente: presentamos “Ouroboros”, el primer protocolo blockchain basado en prueba de participación con rigurosas garantías de seguridad. Establecemos propiedades de seguridad para el protocolo comparables a las logradas por el protocolo blockchain de bitcoin. Como el protocolo proporciona una disciplina de cadena de bloques de "prueba de participación", ofrece ventajas de eficiencia cualitativas sobre las cadenas de bloques basadas en la prueba de recursos físicos (por ejemplo, prueba de trabajo). También presentamos un mecanismo de recompensa novedoso para incentivar los protocolos de prueba de participación y demostramos que, dado este mecanismo, el comportamiento honesto es un equilibrio de Nash aproximado, lo que neutraliza ataques como la minería egoísta. También presentamos evidencia inicial de la practicidad de nuestro protocolo en entornos del mundo real al proporcionar resultados experimentales sobre la confirmación y el procesamiento de transacciones”. KIAYIAS, Aggelos, RUSSELL, Alexander, DAVID, Bernardo y OLIYNYKOV, Roman, “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol”, 21 de agosto del 2017. Disponible en: <https://app.box.com/s/eui5ayv98rw5m9ysvtnkrirlm5wpm7og>.

[367] Véase: <https://docs.cardano.org/new-to-cardano/why-use-cardano>.

[368] *Idem.*

[369] *Idem.*

[370] *Idem.*

[371] El 23 de septiembre del 2022 fue consultado el precio ADA en el siguiente enlace: <https://coinmarketcap.com/currencies/cardano/>.

4. Polkadot

En el año 2016, Gavin Wood desarrolló un código para múltiples aplicaciones especializadas en criptodivisas, publicando el *white paper* de Polkadot. Se trata de un proyecto de código abierto que ha estado desarrollando la Fundación Web3[372]. Este es un protocolo compartido que posibilita que las redes *blockchains* puedan operar juntas. Con ello se busca, crear una red unificada configurada por la unión de varias *blockchains*.

El token de *polkadot* es el DOT y tiene tres finalidades concretamente esctablecidas:

La *gobernanza*: "Los usuarios que poseen tokens de Polkadot ejercen completo control sobre el protocolo de la plataforma. Pasando de ser un protocolo donde el control lo ejercen los mineros del mismo, a un protocolo donde el control recae sobre quienes poseen recursos (*tokens*) invertidos en el mismo, y por extensión, en las personas más interesadas en el correcto funcionamiento del sistema".

La *operación*: en este sentido se incentiva a los titulares de *tokens* DOT, mediante la teoría de juegos, a mantener comportamientos honestos. A través de este mecanismo, la red se asegura el correcto funcionamiento. Esto gracias a que el comportamiento deshonesto, de algún participante, es castigado con la pérdida de la participación.

La *vinculación*: "Este aspecto de Polkadot consiste en eliminar aquellas parachains obsoletas o inutilizadas que se encuentran enlazadas al sistema. De esta manera, no solo se elimina la parachain sino también los *tokens* vinculados

[372] La Fundación Web3 se creó para fomentar y administrar las tecnologías y aplicaciones en los ámbitos de los protocolos de software de web descentralizados, en particular los que utilizan métodos criptográficos modernos para salvaguardar la descentralización, en beneficio y para la estabilidad del ecosistema de la Web3. Polkadot es el protocolo insignia de la Fundación Web3. Polkadot es el protocolo principal de la Fundación Web3. Polkadot. Light Paper, Una Introducción a Polkadot, abril del 2020, p. 14. Disponible en : <https://assets.polkadot.network/Polkadot-lightpaper_es.pdf>.

a éstas. Estos tokens pueden unirse o migrar a nuevas parachains dentro de la red". El precio de *polkadot* al día de hoy es el 6,68 USD con un volumen de comercio de 24 horas de 310 859 897 USD, con una capitalización de mercado de 7 485 730 213 USD. Tiene un suministro circulante de 1 120 833 217 de monedas[373].

5. Decentraland

El proyecto Decentraland está compuesto de una plataforma de realidad virtual impulsada por una cadena de bloques de Ethereum. En él los usuarios pueden comprar parcelas de tierra[374], crear, experimentar y monetizar contenido y aplicaciones. La tierra en Decentraland es propiedad permanente de sus usuarios, solo ellos pueden controlar sus creaciones[375]. Los usuarios reclaman la propiedad de la tierra virtual en un libro mayor de parcelas basado en *blockchain*[376]. MANA es el primer token de *decentraland* que sigue el estándar ERC-20 de Ethereum y se utiliza para comprar parcelas de LAND y para pagar bienes y servicios en el mundo Decentraland. El segundo token es LAND, que es un token no fungible que sigue el estándar ERC-721. La idea es que cada token LAND identifique de forma única las propiedades de una parcela de tierra que es propiedad de un usuario de Decentraland[377]. El precio de *decentraland* al

---

[377] El 27 de septiembre del 2022 fue consultado el precio POLKADOT en el siguiente enlace: <https://coinmarketcap.com/currencies/polkadot/>.

[374] Se puede definir al LAND como: "Los espacios con los que el usuario interactúa en Decentraland se llaman LAND (tierra). Son activos digitales no tangibles que los usuarios pueden comprar en el juego. Una vez el usuario posee un trozo de LAND es libre de decidir qué hacer con este. Puede crear juegos, aplicaciones, servicios de juego o incluso escenas dinámicas en 3D. Sin poner límites a la imaginación, los usuarios pueden crear cualquier servicio basado en LAND que puede ser de carácter educativo, de desarrollos profesionales, turismo, etc.". DIARIO BITCOIN, ¿Qué es *decentraland*? Disponible en: <https://www.diariobitcoin.com/glossary/decentraland/>.

[375] DIARIO BITCOIN, ¿Qué es *decentraland*? Disponible en: <https://www.diariobitcoin.com/glossary/decentraland/>.

[376] En ese sentido Decentraland proporciona una infraestructura para admitir un mundo virtual compartido, también conocido como metaverso. Consiste en un libro mayor descentralizado para la propiedad de la tierra, un protocolo para describir el contenido de cada parcela de tierra y una red entre pares para las interacciones de los usuarios. Decentraland White Paper, p. 4.

día de hoy es el de 0,706680 USD con un volumen de comercio de 24 horas de 120 059 026 USD, con una capitalización de mercado de 1 310 950 946 USD. Tiene un suministro circulante de 1 855 084 192 de monedas[378].

V. PROPUESTA DEL REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVO A LOS MERCADOS DE CRIPTOACTIVOS Y POR EL QUE SE MODIFICA LA DIRECTIVA (UE) 2019/1937 (MICA)

El 20 de abril del 2023 el Parlamento Europeo aprobó por mayoría la votación del Reglamento sobre los Mercados de Criptoactivos, mejor conocido como Ley MICA. El origen de esta propuesta normativa, regulada en el Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937, se encuentra amparado en la progresiva digitalización que viene sufriendo el sector financiero en los últimos 10 años dentro de la Unión Europea[379]. Esta situación ha sido abordada por su actual presidenta, Ursula Von del Leyen, al emitir, el 24 de septiembre del 2020, un paquete normativo de medidas denominado como Digital Finances Package[380], que tiene dentro de sus objetivos, como sostiene NOVELLA GONZÁLES

[377] BIT2ME ACADEMY, "¿Qué es decentraland (MANA)?", 15 de junio del 2021. Disponible en: <https://academy.bit2me.com/que-es-decentraland-mana/>.

[378] El 27 de septiembre del 2022 fue consultado el precio DECENTRALAND en el siguiente enlace: <https://coinmarketcap.com/currencies/decentraland/>.

[379] NOVELLA GONZÁLES DEL CASTILLO, Eduardo, "Hacia una nueva regulación europea: El Digital Finance Package", en *Criptoactivos. Retos y desafíos normativos*, Madrid: Wolters Kluwer, 2021, p. 99.

[380] En ese sentido, véase las razones y objetivos de la propuesta contenida en la exposición de motivos del Reglamento del Parlamento Europeo y del Consejo Relativo a los Mercados de Criptoactivos y por el que se modifica la Directiva (UE) 2019/1937: "La presente propuesta se integra en el paquete de finanzas digitales, cuyas medidas están dirigidas a explotar en mayor grado y apoyar el potencial de las finanzas digitales en términos de innovación y competencia, reduciendo al mismo tiempo los riesgos. Está en consonancia con las prioridades de la Comisión de adaptar Europa a la era digital y forjar una economía con visión de futuro al servicio de las personas. El paquete comprende una nueva Estrategia de Finanzas Digitales para el sector financiero de la UE cuyo objetivo es garantizar que la Unión adopte la revolución digital y la lidere con la ayuda de empresas europeas innovadoras a la vanguardia, de manera que los beneficios de las finanzas digitales estén al alcance de los consumidores y las empresas de Europa. Además de la presente propuesta, el paquete incluye una propuesta de régimen piloto sobre infraestructuras del mercado basadas en la tecnología de registro descentralizado (TRD), una propuesta relativa a la resiliencia operativa digital3 y una propuesta para aclarar o modificar determinadas normas conexas de la UE en materia de servicios financieros".

DEL CASTILLO, el lograr la transición hacia una Europa financiera digital y sostenible[381].

Para los fines de nuestra investigación, hemos decidido abordar únicamente la propuesta del reglamento sobre mercados disputables y equitativos en el sector digital o conocido en sus siglas en inglés como MICA (Market in Crypto Assets), que tiene como finalidad brindarle regulación a un grupo de criptoactivos que carecen de soporte normativo dentro de la Unión Europea.

En el reglamento MICA, se incluye una taxonomía o clasificación de los criptoactivos, así como el otorgamiento de información con el que deben contar cada criptoactivo, es decir, el denominado libro blanco o *white paper* en el que se desarrolla el contenido y funcionamiento de cada criptoactivo, además de un procedimiento de autorización para la emisión de criptoactivos[382]. Si bien el reglamento MICA se presenta como una propuesta normativa muy ambiciosa con relación a la regulación de criptoactivos, lo cierto y lo concreto es que su alcance jurídico normativo no le da solución a todas las problemáticas que pueden surgir en torno a los criptoactivos, sino únicamente se centra: (i) en el proceso de emisión de criptoactivos y (ii) en la prestación de servicios sobre criptoactivos[383]. Dentro de sus novedades MICA, presenta un conjunto de definiciones con relación a los criptoactivos y sus distintos tipos[384].

La primera definición que se puede resaltar en el reglamento es el de criptoactivo, y lo define como una representación digital de valor o derechos que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o una tecnología similar[385]. Como ya señalamos, esa taxonomía sirve para poder diferenciar los regímenes y obligaciones que serán

---

[381] NOVELLA GONZÁLES DEL CASTILLO, *op. cit.,* p. 100.

[382] *Ibid.,* pp. 113 y 114.

[383] NOVELLA GONZÁLES DEL CASTILLO, *op. cit.,* p. 120.

[384] *Ibid.,* p. 120.

[385] Véase el artículo 3, inciso 2, de la propuesta del Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la directiva (UE) 2019/1937.

aplicables a cada uno de los criptoactivos regulados por MICA, los cuales se encuentran clasificados en tres categorías de criptoactivos[386]:

- Ficha referenciada a activos (*asset-referenced tokens*): un tipo de criptoactivo que, a fin de mantener un valor estable[387], se referencia al valor de varias monedas fíat de curso legal, una o varias materias primas, uno o varios criptoactivos, o una combinación de dichos activos.

- Ficha de dinero electrónico (*electronic money tokens*): un tipo de criptoactivo cuya principal finalidad es la de ser usado como medio de intercambio y que, a fin de mantener un valor estable, se referencia al valor de una moneda fíat de curso legal.

- Ficha de servicio (*utility tokens*): un tipo de criptoactivo utilizado para dar acceso digital a un bien o un servicio, disponible mediante TRD, y aceptado únicamente por el emisor de la ficha en cuestión.

Es importante resaltar que la propuesta MICA no aplica a los criptoactivos que se consideren instrumentos financieros, de acuerdo con la definición del artículo 4, apartado 1, punto 15, de la Directiva 2014/65/UE; no aplicara a aquellos que se consideren dinero electrónico, de acuerdo con la definición del artículo 2, punto 2, de la Directiva 2009/110/CE, excepto cuando se consideren fichas de dinero electrónico en virtud del presente Reglamento; ni tampoco será aplicable a aquellos que se consideren depósitos, de acuerdo con la definición del artículo 2, apartado 1, punto 3, de la Directiva 2014/49/UE del Parlamento Europeo y del

---

[386] Véase el artículo 3, incisos 3,4 y 5, de la Propuesta MICA

[387] En ese sentido véase la exposición de motivos del Reglamento del Parlamento Europeo y del Consejo Relativo a los Mercados de Criptoactivos MICA refiere que: En ese sentido “en los últimos tiempos ha aparecido un subtipo relativamente nuevo de criptoactivos, las denominadas *criptomonedas estables*, que ha atraído la atención tanto del público como de los reguladores de todo el mundo. El mercado de criptoactivos sigue teniendo un tamaño modesto y por ahora no plantea ninguna amenaza para la estabilidad financiera; sin embargo, la situación podría cambiar con la llegada de las *criptomonedas estables mundiales*, que, al incorporar características para estabilizar su valor y aprovechar los efectos de red derivados de las empresas que promueven estos activos, aspiran a una mayor difusión”.

Consejo; ni aplicará a aquellos que se consideren depósitos estructurados, de acuerdo con la definición del artículo 4, apartado 1, punto 43, de la Directiva 2014/65/UE; ni aplicará a aquellos que se consideren titulizaciones, de acuerdo con la definición del artículo 2, punto 1, del Reglamento (UE) 2017/2402 del Parlamento Europeo y del Consejo.

Tampoco aplicarán al Banco Central Europeo y a los bancos centrales nacionales de los Estados miembros, cuando actúen en su condición de autoridad monetaria, ni otras autoridades públicas; ni a las empresas de seguros ni las empresas que ejerzan las actividades de reaseguro y de retrocesión definidas en la Directiva 2009/138/CE del Parlamento Europeo y del Consejo, cuando ejerzan las actividades contempladas en dicha Directiva; ni al liquidador o administrador que intervenga en el marco de un procedimiento de insolvencia, excepto a los fines del artículo 42; ni a las personas que presten servicios de criptoactivos, exclusivamente a sus empresas matrices, a sus filiales o a otras filiales de sus empresas matrices; ni al Banco Europeo de Inversiones; ni a la Facilidad Europea de Estabilidad Financiera y al Mecanismo Europeo de Estabilidad; ni a las organizaciones internacionales públicas.

1. Ficha de servicio (*utility tokens*)

El título II de la propuesta MICA está dirigida a las fichas de servicios (*utility tokens*), es decir, un tipo de activo digital que permite acceder a una plataforma como por ejemplo el Basic Attention Token (BAT) o el Golem (GNT). Este se podría considerar un nivel bajo de emisión de criptoactivos, ya que representan un menor riesgos para los usuarios, y por ende el régimen de regulación es mucho menos estricto[388], como veremos.

Dentro de la propuesta MICA para *utility tokens*, se exige, para la comercialización de este tipo de criptoactivos que se lleva a cabo mediante una plataforma de negociación, que esto se dé a través de una persona jurídica; que

[388] NOVELLA GONZÁLES DEL CASTILLO, *op. cit.,* p. 122.

sea haya elaborado el libro blanco o *white paper*[389] que contendrá las características principales del cripotoactivo a negociar. Además, dentro del procedimiento establecido por el reglamento, se establece que las autoridades competentes no exigirán la aprobación previa del libro blanco de criptoactivos, ni de las comunicaciones publicitarias al respecto antes de su publicación[390].

Con relación a la publicidad de emisores de criptoactivos distintos de fichas referenciadas a activos o fichas de dinero electrónico, estos publicarán sus libros blancos de criptoactivos y, en su caso, las comunicaciones publicitarias en su sitio web, las mismas que serán de acceso público, a más tardar en la fecha de inicio de la oferta pública de los criptoactivos correspondientes o de su admisión o negociación en una plataforma de negociación de criptoactivos. El libro blanco de criptoactivos, y, en su caso, las comunicaciones publicitarias, permanecerán disponibles en el sitio web del emisor mientras los criptoactivos estén en manos del público[391]. Por último, el MICA propone una regulación directa frente a la ética con la que se deben manejar los proveedores de criptoactivos[392], frente a las distintas situaciones que pudieran surgir[393], basadas en la honestidad, profesionalidad e imparcialidad.

La presente normativa no considera como *utility token:* a aquellos criptoactivos que se oferten gratuitamente como es el caso de los criptoactivos que se creen automáticamente mediante minería, como recompensa por el mantenimiento de la tecnología de registro descentralizada o la validación de operaciones; a los criptoactivos que sean únicos y no fungibles respecto de otros criptoactivos; a los criptoactivos que se oferten a menos de ciento cincuenta personas físicas o jurídicas por el Estado miembro, cuando estas personas actúen por cuenta propia; a lo largo de un período de doce meses, y la contraprestación total de

---

[389] Véase el artículo 4, inciso 1 (c), de la Propuesta MICA.

[390] Véase el artículo 7, inciso 1, 2 y 3, de la Propuesta MICA.

[391] Véase el artículo 8, inciso 1, 2, de la Propuesta MICA.

[392] Véase el artículo 13, inciso 1 (a, b, c, y d), de la Propuesta MICA.

[393] Véase el artículo 13, inciso 1 (a, b, c, y d), de la Propuesta MICA.

una oferta pública de criptoactivos en la Unión no exceda de 1.000.000 EUR, o la cantidad equivalente en otra moneda o en criptoactivos; la oferta pública de criptoactivos se dirija exclusivamente a inversores cualificados y solo estos puedan ser titulares de los criptoactivos[394].

2. Ficha referenciada a activos (*asset-referenced tokens*)

Una diferencia significativa con los *utility tokens* es que la autorización de los *asset-referenced tokens* está sujeta a una autorización *ex ante*[395], es decir, un emisor de fichas referenciadas a activos no podrá ofretar en la Unión Europea, las fichas al público ni solicitar su admisión a negociación en una plataforma de negociación de criptoactivos a menos que así lo haya autorizado la autoridad competente de su Estado miembro[396].

Sin embargo, este precepto normativo no aplicará en dos supuestos claramente delimitados por el MICA: a) cuando en un período de doce meses, calculado al final de cada día natural, el importe medio de las fichas referenciadas a activos en circulación no exceda de 5.000.000 EUR o el importe equivalente en otra moneda; b) cuando la oferta pública de fichas referenciadas a activos se dirija exclusivamente a inversores cualificados y solo estos puedan ser titulares de las fichas. Como señala NOVELLA GONZÁLES DEL CASTILLO, el régimen normativo propuesto por MICA se basa en el principio de *one-stop-shop* o ventana única, con lo cual solo se requiere una única autorización por la autoridad competente para poder operar dentro de toda la Unión Europea[397].

El procedimiento para la obtención de la autorización se requiere la documentación estipulada en la norma, junto con la presentación de libro blanco

---

[394] Véase el artículo 4, inciso 2 (a, b, c, d, e y f) de la Propuesta MICA.

[395] NOVELLA GONZÁLES DEL CASTILLO, *op. cit.,* p. 125.

[396] Véase el artículo 15, inciso 5, de la Propuesta MICA.

[397] NOVELLA GONZÁLES DEL CASTILLO, *op. cit.,* p. 125.

o *white paper*[398] describiendo todo el contenido[399] exigido por MICA, para su aprobación. Es importante resaltar que esta autorización puede ser revocable, cuando el emisor no haga uso de la misma durante el plazo de los 6 meses consecutivos desde su otorgamiento[400]. Asimismo, si la obtención de la autorización ha sido expedida mediante algún medio irregular o infracción grave que contravenga en el reglamento MICA, esta también será revocada[401].

3. Ficha de dinero electrónico (*Electronic money tokens*)

El tercer tipo de criptoactivo al que hace referencia la propuesta MICA son los denominados *e-money tokens*, que se caracterizan porque su valor se determina haciendo referencia a una única moneda fiduciaria, por lo que su función es más similar a la de un medio de pago[402]. En ese sentido, la propuesta MICA pone como límite a la condición de emisor de ficha de dinero electrónico en la Unión o ser admitida a negociación, siempre y cuando esté autorizado como entidad de crédito o como "entidad de dinero electrónico", en el sentido del artículo 2, apartado 1, de la Directiva 2009/110/CE[403]. En relación con la autorización para *e-money tokens*, esta es bastante similar a la de los *asset-referenced tokens,* en cuanto a la exigencia de una autorización *ex ante* y exime a aquellos emisores que vayan destinadas a inversores cualificados o bien durante un plazo de 12 meses y que tengan una capitalización inferior a 5.000.000 euros[404].

---

[398] Véase el artículo 15 de la Propuesta MICA.

[399] Véase el artículo 17 de la Propuesta MICA.

[400] Véase el artículo 20 de la Propuesta MICA.

[401] Véase el artículo 20 de la Propuesta MICA.

[402] NOVELLA GONZÁLES DEL CASTILLO, *op. cit.,* p. 127.

[403] Véase el artículo 43, de la Propuesta MICA.

[404] NOVELLA GONZÁLES DEL CASTILLO, *op. cit.,* p. 128.

4. Proveedores de servicios de criptoactivos según la propuesta MICA

En relación con la obtención de la autorización para dar el servicio como proveedores de criptoactivos, el reglamento MICA restringe esta posibilidad de prestación solo a las personas jurídicas que tengan su domicilio social en un Estado miembro de la Unión y que hayan sido autorizadas como proveedores de servicios de criptoactivos, de conformidad con el artículo 55 del mismo texto. Como de forma acertada señala NOVELLA GONZÁLES DEL CASTILLO, el reglamento MICA establece un *numerus clausus* de actividad que tendrán la consideración de prestación de servicios sobre criptoactivos[405], enumerando de la siguiente forma:

- La custodia y administración de criptoactivos en nombre de terceros.
- Operar una plataforma de comercialización para criptoactivos.
- Realizar el intercambio de criptoactivos por monedas fiduciarias de curso legal o por otros criptoactivos.
- Ejecutar órdenes por criptoactivos en nombre de terceros.
- La colocación de criptoactivos.
- Recibir y transmitir criptoactivos en nombre de un tercero.
- Prestar asesoramiento en criptoactivos[406].

5. Otros puntos relevantes a tener en cuenta en la propuesta MICA

Otro punto importante que plantea la propuesta MICA es el derecho a recurrir ante el órgano jurisdiccional, garantizándole a toda persona natural o jurídica que participe en el procedimiento establecido por MICA para la obtención de una autorización el derecho al recurso. Obligando a todo los Estados miembros a velar porque toda decisión adoptada de conformidad con el presente reglamento se motive adecuadamente y pueda ser objeto de recurso judicial. El derecho a recurrir a los tribunales será igualmente de aplicación cuando, sobre una solicitud

[405] *Ibid.,* p. 129.

[406] *Idem*.

de autorización como proveedor de servicios de criptoactivos que contenga todos los elementos requeridos, no se haya adoptado ninguna resolución en los seis meses siguientes a su presentación[407].

Por último, el reglamento establece un régimen sancionador. Pone a disposición de las autoridades encargadas un conjunto de mecanismos de disuasorios y coercitivos, con la finalidad de garantizar que los actores señalados en el reglamento hagan cumplimientos de la normativa especificada dentro de la Unión Europea[408].

VI. COMITÉ DE BASILEA: "UN TRATAMIENTO PRUDENCIAL DE LA EXPOSICIÓN DE CRIPTOACTIVOS"

El documento en cuestión es producto del debate y las respuestas recibidas de una amplia gama de partes interesadas, así como de las iniciativas en curso emprendidas por la comunidad internacional. El Comité publica este documento de consulta en el que recaba las opiniones de las partes interesadas sobre una propuesta preliminar del tratamiento prudencial para los criptoactivos. Dada la naturaleza, rapidez y evolución de los criptoactivos, el Comité opina que es probable que el desarrollo de políticas para criptoactivos sea un proceso iterativo, que involucre más de una consulta[409].

El tratamiento prudencial de los criptoactivos establecido en el documento se ha llevado a cabo siguiendo los siguientes principios generales:

---

[407] Véase el artículo 94, de la Propuesta MICA.

[408] NOVELLA GONZÁLES DEL CASTILLO, Eduardo, "El futuro reglamento europeo para de criptoactivos (propuesta Mica)", en *Criptoactivos. Retos y desafíos normativos*, Madrid: Wolters Kluwer, 2021, p. 132.

[409] COMITÉ DE BASILEA DE SUPERVISIÓN BANCARIA, *Documento consultivo. Tratamiento prudencial de las exposiciones a criptoactivos*, junio del 2021, p. 1.

1. Mismo riesgo, misma actividad, mismo tratamiento

Un criptoactivo que proporciona funciones económicas equivalentes y presenta los mismos riesgos en comparación con un "activo tradicional", debe estar sujeto a los mismos requisitos de capital, liquidez y otros, al igual que el activo tradicional. Como punto de partida, el marco prudencial debe aplicar el concepto de "neutralidad tecnológica" y este no debe estar diseñado de tal manera que abogue o desaliente explícitamente el uso de tecnologías específicas relacionadas con los criptoactivos. Sin embargo, el tratamiento prudencial debe tener en cuenta cualquier riesgo adicional que surja de las exposiciones a los criptoactivos en relación con los activos tradicionales[410].

2. Sencillez

El diseño del tratamiento prudencial de los criptoactivos debe ser simple. Los criptoactivos son actualmente una clase de activos relativamente pequeños para los bancos. Dado que el mercado, las tecnologías y los servicios relacionados con los criptoactivos aún están evolucionando, razón por la que vale la pena comenzar con un tratamiento simple y cauteloso, que, en principio, podría revisarse en el futuro dependiendo de la evolución de los criptoactivos[411].

3. Estándares mínimos

Cualquier tratamiento prudencial de los criptoactivos especificado por el Comité constituiría un estándar mínimo para los bancos con actividad internacional. Las jurisdicciones serían libres de aplicar medidas adicionales y/o más conservadoras si se justifica. Como tal, se consideraría que las jurisdicciones

---

[410] *Ibid*., p. 2

[411] *Idem*.

que prohíben que sus bancos tengan exposiciones a criptoactivos cumplen con un estándar prudencial global[412].

Con el fin de determinar los requisitos mínimos de capital en función del riesgo para el crédito y el riesgo de mercado, los criptoactivos se examinan de forma continua y se clasifican en dos grupos:

Los criptoactivos del grupo uno estarán sujetos a requisitos de capital basados en el riesgo, al menos equivalentes en función de las ponderaciones de riesgo de las exposiciones subyacentes según lo establecido en el marco de capital de Basilea existente. La sección segunda describe cómo interpretar y aplicar el marco de capital de Basilea existente a los criptoactivos del grupo uno. Los criptoactivos del grupo 1 incluyen activos tradicionales tokenizados (grupo 1a) y criptoactivos con mecanismos de estabilización efectivos (grupo 1b)[413].

Los criptoactivos del grupo dos son los que no cumplen con ninguno de los requisitos de clasificación del grupo uno, ya que presentan riesgos adicionales y más altos en comparación con los criptoactivos del grupo uno y, en consecuencia, estarán sujetos a un tratamiento de capital conservador recientemente prescrito establecido en la sección 3[414].

Para ser clasificado en el grupo 1, se debe cumplir con las siguientes condiciones[415]:

1. Se debe tratar de criptoactivos que tienen un mecanismo de estabilización que es efectivo en todo momento para vincular su valor a un activo tradicional subyacente o a un grupo de activos tradicionales.

---

[412] *Ibid.,* p. 2.

[413] *Idem*.

[414] *Ibid*., p. 4.

[415] *Ibid*., pp. 4 y 5.

2. Todos los derechos, obligaciones e intereses que surjan de los acuerdos de criptoactivos que cumplan con la condición anterior están claramente definidos y son legalmente exigibles en las jurisdicciones donde se emite y canjea el activo. Además, el(los) marco(s) legal(es) aplicable(s) asegura(n) la firmeza de la liquidación.

3. Las funciones de los criptoactivos y la red en la que opera, incluido el libro mayor distribuido o tecnología similar en la que se basa, están diseñadas y operadas para mitigar y gestionar suficientemente cualquier riesgo material.

4. De igual forma, se exige que se regulan y supervisan las entidades que ejecutan rescates, transferencias o liquidación definitiva del criptoactivo.

Los criptoactivos del grupo 2 presentan riesgos únicos en comparación con los criptoactivos del grupo 1 y, como tales, están sujetos al requisito de capital recientemente prescrito establecido en esta sección. Los requisitos solo se aplican a los criptoactivos del grupo 2 que no se han deducido del capital de nivel 1 común (CET1); por ejemplo, los criptoactivos clasificados como intangibles según el marco contable aplicable. Los fondos de criptoactivos del grupo 2 (por ejemplo, ETF de criptoactivos del grupo 2) y otras entidades, cuyo valor material se deriva principalmente del valor de los criptoactivos del grupo 2, deben tratarse en esta categoría. Las inversiones de capital, los derivados o las posiciones cortas en estos fondos o entidades también deben tratarse en esta categoría[416].

[416] *Ibid*., p. 13.

VII. ALGUNAS REGULACIONES DE LOS CRIPTOACTIVOS EN AMÉRICA

1. Estados Unidos

A pesar de en los Estados Unidos existen una gran cantidad de inversores en criptoactivos y empresas de la tecnología *blockchain*, aún no se ha desarrollado un marco regulatorio claro y preciso para dicha clase de activos digitales. Si bien varios reguladores ya se han vendio pronunciado, como es el caso de la Comisión de Bolsa y Valores o U.S. Securities and Exchange Commission (SEC), quien considera a los criptoactivos como un valor[417]; por su parte, la Comisión de Comercio de Futuros de Commodities o Commodity Future Trading Commission (CFTC) considera al Bitcoin como un *commodity*[418].

En cuanto a los intercambios de criptoactivos, estos se encuentran regulados por la Ley de Secreto Bancario o Bank Security Act (BSA) y deben registrarse en la Red de Ejecución de Delitos Financieros. También están obligados a cumplir con las obligaciones contra lavado de activos o Anti Money Laundering (AML) y la lucha contra la financiación del terrorismo (CFT)[419].

Sin embargo, recientemente, las senadoras Kirsten Gillibard del partido demócrata y Cynthia Lummis del partido republicano presentaron el 6 de junio del 2022, ante el Senado de los Estados Unidos, un amplio proyecto de ley bipartidista que busca regular las criptomonedas y otros activos digitales como las *stablescoins.* La ley tiene por objeto[420] el abordar el papel de la Comisión de Comercio de Futuros de Materias Primas (CFTC) y de la Comisión de Valores (SEC) en lo que respecta a la regulación de las criptomonedas, junto con la

---

[417] BANCO CENTRAL DE RESERVA DE PERÚ, *Reporte de estabilidad financiera*, Lima: noviembre del 2021, p. 87.

[418] *Ibid.,* p. 87.

[419] *Idem*.

[420] GALINDO, German, "Las senadoras de EE. UU. Kirsten Gillibrand y Cynthia Lummis presentan proyecto de ley sobre criptomonedas en Criptotendencias", en *Criptotendencias.com*, 7 de junio del 2022. Disponible en: <https://www.criptotendencias.com/actualidad/las-senadoras-de-eeuu-kirsten-gillibrand-y-cynthia-lummis-presentan-proyecto-de-ley-sobre-criptomonedas/>.

regulación de las *stablecoins***,** la banca, el tratamiento fiscal de los activos digitales y la coordinación entre agencias[421]; además, proponen que la supervisión de los criptoactivos se realice por parte del Comercio de Futuros de Commodities (CFTC)[422].

La denominada *Cypto bill outlining sweeping plan for future rules* o denominada o por sus siglas en español Ley de Innovación Financiera Responsable, propone las definiciones legales de *activos digitales* y *monedas virtuales* y lo referente a las *stablecoins.*

Además del señalado, se le requeriría al Servicio de Rentas Internas o *Internal Revenue Services* (IRS), es decir, la agencia de impuestos de Estados Unidos, que adopte una guía sobre la aceptación comercial de activos digitales y contribuciones caritativas. Además, propone una exoneración para todas aquellas transacciones que no superen los 200 dólares[423].

Recientemente, la Casa Blanca de los Estados Unidos ha publicado un marco integral para el desarrollo responsable de los criptoactivos. El informe refiere lo siguiente: "El mercado de activos digitales ha crecido significativamente en los últimos años. Millones de personas en todo el mundo, incluido el 16 % de los estadounidenses adultos, han comprado activos digitales, que alcanzaron una capitalización de mercado de 3 billones de dólares en todo el mundo en noviembre pasado. Los activos digitales presentan oportunidades potenciales para reforzar el liderazgo de EE. UU., en el sistema financiero global y permanecer en la frontera tecnológica. Pero también presentan riesgos reales, como lo demuestran los eventos recientes en los criptomercados"[424] .

QUARMBY Brian, "El proyecto de ley Lummis-Gillibrand sobre criptomonedas probablemente se aplace hasta el año que viene", en *Cointelegraph*, 20 de julio del 2022. Disponible en: <https://es.cointelegraph.com/news/lummis-gillibrand-crypto-bill-likely-deferred-to-next-year>.

[422] GALINDO, German, *op. cit.*

[423] *Idem.*

[424] THE WHITE HOUSE, "FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets", setiembre del 2022. Disponible en: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-

El gobierno liderado por John Biden siempre ha apuntado a la protección de los consumidores, garantizando un mercado seguro para la inversión en el mercado de activos digitales. En esa misma línea de garantismo, es que los activos digitales plantean riesgos significativos para los consumidores, los inversores y las empresas. Los precios de estos activos pueden ser muy volátiles: la capitalización de mercado global actual de las criptomonedas es aproximadamente un tercio de su pico de noviembre de 2021.

Aun así, los vendedores suelen engañar a los consumidores sobre las características de los activos digitales y los rendimientos esperados, y el incumplimiento de las leyes y regulaciones aplicables sigue siendo generalizado. El fraude, las estafas y los robos absolutos en los mercados de activos digitales van en aumento: según las estadísticas del FBI, las pérdidas monetarias reportadas por estafas de activos digitales fueron casi un 600 % más altas en 2021 que el año anterior[425]. Asimismo, propone, a través un trabajo conjunto entre las distintas entidades públicas, desarrollar un marco integral que haga énfasis en mitigar los riesgos con relación al blanqueo de dinero, terrorismo y cibrefraudes mediante el uso de criptoactivos, para poder luchar frontalmente contra el uso indebido de activos digitales[426].

2. Perú

En el 2018, la Superintendencia del Mercado de Valores del Perú emitió un comunicado advirtiendo sobre los peligros que presentan los ICO o por sus siglas en inglés como Initial Coin Offerings advirtiendo lo siguiente[427]:

house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/>.

[425] *Idem.*

[426] *Idem.*

[427] SUPERINTENDENCIA DE MERCADO DE VALORES, "Comunicado advertencia sobre la adquisición de monedas virtuales o criptomonedas y la participación en esquemas conocidos como ICOs". Disponible en: <https://www.smv.gob.pe/uploads/COMUNICADO%20ICOS%2021_11_2.pdf>.

a) No existe una regulación específica en el Perú que ampare la oferta o promoción de criptomonedas o monedas virtuales, o de unidades de valor denominadas “tokens”, las que no cuentan con el respaldo de autoridad financiera o entidad gubernamental alguna, y no están por tanto las empresas que realizan tales ofertas o promociones bajo supervisión.

b) De acuerdo al artículo 2 de la Ley 30050 la publicidad u ofrecimiento de compra, venta o suscripción de activos financieros en territorio nacional y empleando medios masivos de comunicación, sólo puede realizarse por empresas autorizadas o supervisadas por la SMV o por la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones. Se puede consultar el Directorio de entidades autorizadas por dichas Instituciones en sus respectivos portales.

c) A nivel internacional, diversas autoridades financieras se han pronunciado advirtiendo sobre los riesgos y factores especulativos asociados con la adquisición de criptomonedas o tokens, sobre los riesgos de fraude y su posible vinculación con actividades ilícitas, así como sobre las precauciones que se deben tener respecto a la adquisición de los mismos.

El 20 de diciembre del 2021, se elaboró, por parte de un congresista de la república José Luis Elías Ávalos, el Proyecto de Ley N.º 1042/2021-CR, denominado “Proyecto de Ley Marco de Comercialización de Criptoactivos”. El objeto de esta ley era establecer los lineamientos para la operación y funcionamiento de las empresas de servicios de intercambio de criptoactivos a través de plataformas tecnológicas[428].

Este marco normativo persigue el establecer una regulación para todas aquellas personas jurídicas, ya sean bancarias o no bancarias, nacionales o extranjeras que se dediquen dentro del territorio nacional a la comercialización de criptoactivos, ya sea a la venta, compra o intercambio[429]. El texto establece los siguientes requisitos para poder operar en el Perú:

[428] Artículo 1 del Proyecto de Ley N.º 1042/2021-CR, Proyecto de Ley Marco de Comercialización de Criptoactivos.

[429] Artículo 5 del Proyecto de Ley N.º 1042/2021-CR, Proyecto de Ley Marco de Comercialización de Criptoactivos.

- Estar constituido como persona jurídica domiciliada en el territorio nacional. También aplica para aquellas sucursales de una sociedad extranjera. Estas empresas a su vez deben estar debidamente inscritas ante la Superintendencia de Banca y Seguros (SBS)[430].

- Establecer en su constitución que el objeto social únicamente se dedicará al servicio de intercambio de criptomonedas, incluidos servicios como el *staking* y *holding*[431].

- Establecer un programa de seguridad informática para resguardar toda la información objeto de almacenamiento[432].

- La creación de un registro único de plataforma de intercambio de criptomonedas (Rupic)[433].

- La adopción de un sistema antiblanqueo para detectar y prevenir el lavado[434], además del reporte de operaciones sospechosas, a través de los oficiales de cumplimiento ante la Unidad de Inteligencia Financiera del Perú[435] .

Sin embargo, este proyecto de ley ha recibido una serie de observaciones por parte de la Superintendencia de Banca y Seguros (SBS), quien, mediante Oficio

---

[430] Artículo 6.1 del Proyecto de Ley N.º 1042/2021-CR, Proyecto de Ley Marco de Comercialización de Criptoactivos.

[431] Artículo 6.2 del Proyecto de Ley N.º 1042/2021-CR, Proyecto de Ley Marco de Comercialización de Criptoactivos.

[432] Artículo 6.3 del Proyecto de Ley N.º 1042/2021-CR, Proyecto de Ley Marco de Comercialización de Criptoactivos.

[433] Artículo 6.5 del Proyecto de Ley N.º 1042/2021-CR, Proyecto de Ley Marco de Comercialización de Criptoactivos.

[434] Artículo 6.4 del Proyecto de Ley N.º 1042/2021-CR, Proyecto de Ley Marco de Comercialización de Criptoactivos.

[435] Artículo 6.6 del Proyecto de Ley N.º 1042/2021-CR, Proyecto de Ley Marco de Comercialización de Criptoactivos.

N.º 05294-2022-SBS, concluye que “la SBS por su naturaleza y funciones no puede ser competente para ejercer algún tipo de fiscalización sobre las empresas que no pertenecen el sistema financiero y que realizan las actividades de intercambio de criptoactivos, ya que la función de la Superintendencia como supervisor del sistema financiero consiste en cautelar la solvencia de las entidades que captan y resguardan los ahorros del público, tal como se observa con las empresas bancarias, empresas financieras, cajas municipales y cajas rurales, según se regula en la Ley N.º 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros[436].

3. Colombia

En el caso de Colombia, desde el año 2021, la Superintendencia Financiera de Colombia se encuentra realizando el plan piloto en el cual siete entidades del sistema financiero vigiladas por este ente de control, a través de nueve proyectos, y en alianza con plataformas de criptoactivos se encuentran ejecutando pruebas temporales en la arenera (*sandbox*) de la Superintendencia Financiera de Colombia. Dicho proyecto se culminará en el primer trimestre del año 2022[437].

Sin embargo, actualmente en Colombia no existe ninguna ley que regule los criptoactivos. Sin embargo, la Dirección de Impuesto y Adunas Nacionales (DIAN), el Banco de la República, la Superintendencia Financiera, el Consejo Técnico de Contaduría Pública, entre otras organizaciones, se han pronunciado frente al tema.

Es de mencionar que la Superintendencia Financiera, mediante la Carta Circular 29 del 2014, señaló que las monedas virtuales no se encuentran reguladas por

---

[436] Oficio N.º 05294-2022-SBS, 9 de febrero del 2022, p. 8.

[437] MARTÍNEZ MERCHÁN, Mary Luz, “Regulación de los criptoactivos en Colombia”, en *BDO,* 22 febrero de 2022. Disponible en: <https://www.bdo.com.co/es-co/publicaciones/boletines-audit/regulacion-de-los-criptoactivos-en-colombia>.

la Ley, ni se encuentran sujetas a control, vigilancia e inspección de la Superintendencia Financiera[438].

Adicionalmente, en el año 2021, se presentó el Proyecto de Ley "Por la cual se regulan los servicios de intercambio de criptoactivos ofrecidos a través de las plataformas de intercambio de criptoactivos".

La Unidad de Análisis e Información Financiera (UIAF) de Colombia expidió él la Resolución 314, por medio de la cual las personas naturales y jurídicas que provean servicios de activos virtuales tienen la obligación de enviar reportes de operaciones sospechosas a la Unidad cuando adviertan posibles operaciones de lavado de activos y/o financiamiento del terrorismo en las transacciones o actividades[439].

Asimismo, Colombia busca crear un Registro Único de Plataformas de Intercambio de Criptoactivos (RUPIC). Este registro será manejado por las cámaras de comercio de Colombia y funcionará como una base de datos en donde se darán de alta todas las empresas que manejan *bitcoin* en Colombia que cumplan con los requerimientos de la ley[440].

4. Argentina

El único avance de índole conceptual que se ha dado en la Argentina, hasta el momento, tiene que ver con el concepto de "moneda virtual" establecido por la Unidad de Información Financiera (UIF) mediante la Resolución 300/2014 (B.O. 10/07/2014). Siguiendo los lineamientos estipulados por el Grupo de Acción Financiera Internacional (GAFI, 2014)[441], la UIF en su artículo 2 las define como "la representación digital de valor que puede ser objeto de comercio digital y

---

[438] Véase la Carta Circular 29 del 2014.

[439] Véase el art. 1 de la resolución N.º 314 del 2021 de la Unidad de Información y Análisis Financiero.

[440] MARTÍNEZ MERCHÁN, *op. cit.*

[441] ZOCARO MARCOS, "El marco regulatorio de las criptomonedas en Argentina. Comparativa con otros países", en *Centro de Estudios de Administración Tributaria*, p. 8.

cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción"[442].

Además, con la Resolución 300, la UIF mediante el artículo 4 incorpora el artículo 15 de la Resolución-UIF 70/2011, en el que se exige a los sujetos obligados enumerados en los incisos 1, 2, 3, 4, 5, 7, 8, 9, 11, 12, 13, 18, 19, 20, 21, 22 y 23 del artículo 20 de la Ley N.º 25246 a informar, a través del sitio <www.uif.gob.ar> de la UIF, todas las operaciones efectuadas con monedas virtuales. Estos reportes deben efectuarse mensualmente, hasta el día 15 de cada mes, y contener la información correspondiente a las operaciones realizadas en el mes calendario inmediato anterior[443].

En el ámbito bancario, el Banco Central de la República Argentina (BCRA) emitió la comunicación 6823, que obliga los emisores de tarjetas de crédito a contar con la aprobación del BCRA, cuando estas sean utilizadas para la adquisición de criptoactivos[444]. En el plano tributario, se promulgó la Ley N.° 27430, la cual modificó varios artículos de la ley de impuesto a las ganancias y se incorporó a las monedas digitales en el listado[445].

---

[442] Véase el artículo 2 de la Resolución 300/2014 de la Unidad de Información Financiera (B.O. 10/07/2014).

[443] CARO CORIA, Carlos, "La regulación de los criptoactivos en Latinoamérica", en *Criptoactivos. Retos y desafíos normativos*, Madrid: Wolters Kluwer, 2021, p. 138.

[444] *Ibid.,* p. 138.

[445] *Idem*.

CAPÍTULO III
LAVADO DE ACTIVOS Y CRIPTOACTIVOS

I. LAVADO DE ACTIVOS MEDIANTE CRIPTOACTIVOS

Desde su concepción inicial, el blanqueo de dinero ha sido entendido como un delito mediante el cual se busca blanquear ganancias ilícitas que han sido obtenidas en un hecho delictivo previo que tenga la potencialidad necesaria para generar ganancias dinerarias, y darle una apariencia lícita dentro del circuito económico. Si bien esta definición inicial sigue estando vigente en los distintos libros, tratados, artículos científicos, y sentencias judiciales que han desarrollado el delito de blanqueo en sus distintas tipologías, dejando de lado la discusiones interminables de orden dogmático, temática que no es objeto de esta investigación de esta tesis, podemos señalar que el delito de lavado de activos al día de hoy se presenta de forma evolucionada y teniendo como un nuevo aliado dentro de sus componentes al factor tecnológico.

Me refiero a una nueva forma de lavar dinero sucio obtenido en una actividad criminal previa, específica, mediante la utilización del ciberespacio, aprovechando todo el componente tecnológico que este les ofrece a los lavadores, para poder camuflar todas las ganancias ilícitas obtenidas. De igual parecer es NAVARRO CARDOSO, quien refiere que las nuevas tecnologías vienen potenciando delitos como el blanqueo de dinero, la evasión tributaria, justamente por dotar las mismas de cierto anonimato, virtualidad y transnacionalidad[446].

No podemos soslayar que los criptoactivos también han obtenido un rol protagónico en este nuevo escenario virtual criminal. Todos los días salen noticias en distintos medios de comunicación e información relacionadas a la utilización de criptoactivos vinculados a la comisión del delito de blanqueo de dinero, como ejemplo podemos citar algunos casos. Recientemente, la DEA detectó un cartel mexicano que se dedicaba al tráfico con metanfetaminas

[446] NAVARRO CARDOSO, *op. cit.,* p. 16.

utilizando criptoactivos para ocultar sus ganancias[447]. En Reino Unido, la Autoridad de Conducta Financiera del Reino Unido (FCA) reveló que durante el año 2018 las pérdidas por estafas, relacionadas con inversiones en los mercados de divisas, acciones, bonos y criptoactivos, ascendió a 197 millones de libras esterlinas, o lo que es igual a unos 254 millones de dólares estadounidenses[448]. El conocimiento adquirido a partir de estos casos, como los referidos en ejemplo anterior, es un porcentaje mínimo con relación al número real de casuística criminal en materia de criptoactivos, ya que a la fecha tenemos un número significativo de actos criminales mediante la utilización de criptoactivos.

II. EL DELITO PREVIO EN EL LAVADO DE ACTIVOS MEDIANTE CRIPTOACTIVOS

La construcción típica del delito de blanqueo ha sido desarrollada por la dogmática penal contemporánea, de tal forma que en su configuración se requiere la comisión de dos hechos delictivos, un primer suceso delictivo, sin el cual no se puede consumar el segundo momento o hecho. A esta categoría dogmática se le ha denominado, según refiere BALMACEDA QUIRÓS, como tipos penales *conexos-subsiguientes* o *subsecuencia delictiva*, que son "las relaciones entre dos o más conductas (hechos) con relevancia jurídico penal concatenadas unas a otras, dependiendo la segunda de la primera (respecto a su existencia

[447] En ese sentido: "La Administración de Control de Drogas (DEA) de Estados Unidos identificó a una organización criminal mexicana que utilizó al exchange de bitcoin (BTC) y criptomonedas Binance para lavar entre 15 y 42 millones en ganancias ilícitas. El cártel mexicano que se dedica a traficar metanfetamina y cocaína a Estados Unidos, Europa y Australia, utilizó bitcoin y otras criptomonedas para ocultar sus transacciones en Binance desde el 2020, de acuerdo al reporte de Forbes". PLAZA, Nickolas, "Cártel de México lavó dinero a través de Binance usando bitcoin, reveló Forbes", en *Criptonoticias,* 21 de diciembre del 2022. Disponible en: <https://www.criptonoticias.com/seguridad-bitcoin/cartel-mexico-lavo-dinero-binance-usando-bitcoin-revelo-forbes/>.

[448] GÓMEZ LA TORRE, Rafael, "Estafas con bonos y criptoactivos dejan pérdidas de $254 millones en Reino Unido", en *Criptonoticias*, 7 de febrero del 2019. Disponible en: <https://www.criptonoticias.com/seguridad-bitcoin/estafas-bonos-criptoactivos-reino-unido/>.

general o de algún elemento que emana de esta), pero autónoma en función del sentido penal que adquiere al relacionarse con la primera"[449].

Respecto al delito previo, este se considera como la fuente u origen de algo. La palabra *previo* deriva del latín *praevius,* que significa 'anticipado, que va adelante o que sucede primero'[450]. Cuando nos referimos a la palabra subyacente, esta significa que está por debajo o detrás de otra cosa. El concepto clásico tripartito de la teoría del delito define al ilícito como toda conducta típica, antijurídica y culpable. Cuando hablamos de delito fuente o previo, nos referimos a toda conducta típica, antijurídica (desvalor sobre el hecho) y culpable (desvalor sobre el autor del hecho), que fue cometida con anterioridad a la consumación del delito de lavado de activos. En algunos delitos, como es el caso del encubrimiento y la receptación, se requiere para su configuración típica de la preexistencia de un delito fuente o previo[451].

El primer componente del lavado de activos se origina en una actividad ilícita que sea capaz de generar un ingreso para el delincuente. Estas conductas ilícitas tienen como finalidad la obtención de un beneficio de orden económico[452]. Un requisito indispensable para que se configure el denominado delito fuente o previo es que este se haya cometido con anterioridad. La comisión de ese delito anterior habilita los bienes que posteriormente van a ser blanqueados[453]. El delito previo viene a ser de antecedente en tiempo y espacio respecto al delito de lavado, es decir, tiene necesariamente que haberse cometido con anterioridad.

---

[449] BALMACEDA QUIRÓS, Justo, *Delitos conexos y subsiguientes*, Barcelona: Atelier, 2014, p. 322.
[450] REAL ACADEMIA ESPAÑOLA, "Previo", 23.º ed., octubre del 2014. Disponible en: <https://dle.rae.es/previo>.

[451] MUÑOZ CONDE, Francisco, *Derecho penal. Parte general*, Valencia: Tirant lo Blanch, 2004, p. 42.

[452] ZAMORA SÁNCHEZ, Pedro, *Marco jurídico del lavado de dinero*, México: Editorial Mexicana, 2000, p. 10.

[453] BLANCO CORDERO, Isidoro, *El delito de blanqueo de capitales*, Pamplona: Aranzandi, 2012, p. 273.

El delito de lavado de activos, al igual que los delitos de encubrimiento y receptación, tiene dentro de su estructura típica un presupuesto especial referido a la comisión de un hecho delictivo previo; es en este hecho que va a tener origen el objeto material sobre el cual recae la conducta típica respectiva[454]. Una de las características más importantes del delito de blanqueo de dinero, tanto en la legislación peruana como en la extranjera, es reclamar que las conductas típicas de adquirir, utilizar, custodiar, recibir, administrar, etc., tengan un origen ilícito de procedencia delictiva[455]. Es esta procedencia delictiva la que le da sentido al delito de blanqueo de capitales, ya que sin delito previo el blanqueo no tendría razón de ser[456].

En el ámbito de los tratados o convenios internacionales, debemos hacer referencia al Convenio sobre Blanqueo, Investigación, Embargo y Comiso del Producto de Delitos, que fue aprobado en la ciudad francesa de Estrasburgo el 8 de noviembre de 1990. El artículo 6 del convenio en mención hace referencia a que obliga a las partes a penalizar una serie de conductas vinculadas con el lavado de las ventajas económicas procedentes de la comisión de delitos, sea cual fuere la naturaleza de estos. FABIÁN CAPARRÓS afirma "que la parte más importante del artículo en mención es, pues, la existencia misma de una ganancia ilícita; no la cualidad concreta del delito previo". Esto significa que no puede haber blanqueo de dinero sin la preexistencia de un delito fuente previo o actividad criminal previa que dio origen a esas ganancias ilícitas que posteriormente serán objeto de blanqueo[457].

---

[454] CALLEGARI Luis, *El delito de blanqueo de capitales en España y Brasil*, Bogotá: Sigma, 2003, p. 163.

[455] CASTILLO ALVA, José Luis, "La necesidad de determinación del 'delito previo' en el delito de lavado de activos, una propuesta constitucional", en *Gaceta Penal & Procesal Penal*, n.º 4, Lima, octubre 2009, pp. 339 y 340.

[456] CASTILLO ALVA, José Luis, *op. cit.,* p. 340.

[457] FABIÁN CAPARRÓS, *op. cit.*, p. 203.

III. DELITOS FUENTE GENERADORES DE GANANCIAS ILÍCITAS EN CRIPTOACTIVOS

Ya adentrándonos en el objeto de nuestra investigación, debemos establecer qué delitos previos pueden generar ganancias ilícitas en criptoactivos a partir de su ejecución. En primer término, debemos diferenciar aquellos delitos fuentes que utilizan el ciberespacio para su comisión delictiva de los que no lo utilizan, ya que como su misma construcción terminológica refiere el ciberblanqueo requiere para su ejecución de actos de conversión, transferencia u ocultamiento, de ganancia ilícitas, obtenidas en actividades criminales vinculadas al ciberespacio virtual. En esa línea, MIRÓ LLINARES clasifica a los delitos de los que se puede obtener un beneficio económico patrimonial como *cibercrímenes económicos*[458].

En esta categoría se engloban a todos aquellos comportamientos criminales que tienen la finalidad de obtener un beneficio patrimonial, por lo que tienen cabida todas las conductas delictivas basadas en ataques que tienen una afectación directa al patrimonio individual o al orden económico en relación con las transacciones comerciales en Internet, pero también aquellos que afectan a otros bienes jurídicos, como la intimidad, seguridad de los sistemas, etc., pero que tienen el objetivo final de obtener un beneficio económico[459] y que pueden generar ganancias en criptoactivos a partir de su consumación. La diferencia con los delitos de orden convencional está en la ejecución de estos actos ilícitos a través del ciberespacio. Dentro de estos delitos tecnológicos podemos mencionar algunos:

[458] MIRÓ LLINARES, Fernando, *Cibercrimen, cibercriminales…, op. cit.,* p. 9.

[459] *Ibid.,* p. 9.

1. *Hacking*

Se puede definir al *hacking* como aquella conducta realizada por el *hacker* en la que se accede directamente a sistemas informáticos o incluso a la entidades públicas y privadas o de particulares, para realizar el ataque, generalmente aprovechando las vulnerabilidades del sistema o las que ha ido creando la propia víctima. Me refiero a cualquier forma de destrucción o modificación[460].
En el caso del Perú, el artículo 2 de la Ley N.º 30096 tipifica el delito de acceso ilícito[461] o intrusismo blanco[462]. Dentro de los casos más típicos tenemos el hackeo a los *exchange* de criptoactivos.

2. Ciberextorsión

En este caso nos referimos a un tipo de extorsión ejecutada por cibercriminales, que consiste en la solicitud de una cantidad de criptoactivos. Normalmente se piden *bitcoins*, para realizar un determinado ciberataque; también se da la figura inversa, en la que se piden los criptoactivos para no ejecutar el ataque.

3. Estafa

Como refiere de forma acertada ARÁNGUEZ SÁNCHEZ, desde una perspectiva criminológica, las propias características del *bitcoin* lo convierten en un objeto idóneo para la estafa. Dentro de las modalidades que más se suscitan en materias de estafa en criptoactivos tenemos: sitios web falsos, estafas en el trading, esquemas Ponzi en los que se ofrecen grandes ganancias y se les paga

[460] MIRÓ LLINARES, *El cibercrimen…, op. cit.*, p. 53 y ss.

[461] Artículo 2.- El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.

[462] VEGA AGUILAR, Alberto y ARÉVALO MINCHOLA, Maguín, *Ciberdelitos. Análisis del Sistema Penal,* Lima: Editorial Iustitas, 2022, p. 248.

a los viejos inversionistas con el dinero de los nuevos inversionistas. Uno de los casos más recientes de esquema Ponzi en criptoactivos es el de la empresa Bitconnect, en la sentencia dictada por el Tribunal del Distrito de EE. UU. Para el Distrito Sur de California, Bitconnect era una plataforma de préstamos de criptoactivos que ofrecía tecnología patentada y que garantizaba un alto rendimiento a sus inversores; sin embargo, lo que ocurría era que se les paga a los primeros inversores con el dinero de los más recientes, generándose un colapso[463]. En esa misma línea hay que diferenciar la estafa piramidal con criptoactivos del criptoactivo *bitcoin* como estafa piramidal; es decir, si la creación de este tipo de criptoactivo mediante tecnología puede conllevar a establecer que estamos antes una estafa piramidal. Según ARÁNGUEZ SÁNCHEZ, el *bitcoin* como tal no es nada más que la solución a un problema matemático, y en ello radica su relevancia, ya que la principal diferencia entre una estafa piramidal y una empresa multinivel es la existencia o no de un producto real o un verdadero activo que justifique ese negocio[464]. Además de lo señalado, otra dificultad surge con base a la complejidad de las investigaciones y juzgamiento, debido a la carga probatoria con alto contenido tecnológico.

4. *Cryptojacking*

La Interpol define al *cryptojacking* o criptosecuestro como un tipo de ciberdelito que consiste en el uso de manera subrepticia de la potencia de los ordenadores para generar criptoactivos[465]. Se puede configurar cuando el usuario sin darse cuenta instala un programa con secuencias de comando maliciosas que permiten al ciberdelincuente acceder al ordenador o cualquier otro dispositivo de

---

[463] ASMAKOV Andrew, "Víctimas del Esquema Ponzi Bitconnect Recibirán $17 Millones en Compensaciones" en *Decrypt*, 13 de enero del 2023. Disponible en: <https://decrypt.co/es/119171/victimas-del-esquema-ponzi-bitconnect-recibiran-14-millones-en-compensaciones>.

[464] ARÁNGUEZ SÁNCHEZ, Carlos, "El bitcoin como instrumento y objeto de delitos", en *Cuadernos de Política Criminal,* n.° 131, segunda época, septiembre del 2020, p. 85.

[465] INTERNATIONAL CRIMINAL POLICE ORGANIZATION, "Cryptojacking makes Money for Criminals", INTERPOL General Secretariat, Lyon, 2020, p. 1.

la víctima que esté conectado a Internet, para generar o extraer criptoactivos. Al tratarse de divisas digitales, para crearlas solo es necesario disponer de programas informáticos y de la potencia de los ordenadores. Las criptoactivos que más se ven extraídos a partir de ordenadores personales son los moneros[466].

5. *Ilegal cryptomarkets*

No cabe duda que dentro de los casos más notorios con relación al uso ilegal de criptoactivos, el caso más conocido es el *Silk Road* o Ruta de la Seda. En octubre del 2013, Ross Ulbritch, de 30 años de edad, fue condenado a cadena perpetua por la comisión de los delitos de lavado de activos, actividad criminal organizada y piratería informática, por haber creado el mayor mercado negro virtual de la historia, que utilizaba como medio pago *bitcoins*, primordialmente por la encriptación que ofrece este tipo de criptodivisa, que la hizo indetectable por parte del gobierno de los Estados Unidos[467].

La página Web *Silk Road* o la Ruta de la Seda fue puesta en circulación en el año 2011, funcionaba como un mercado negro virtual para la venta de bienes y servicios ilícitos. La mayoría de sus usuarios eran comercializadores de drogas que usaban la plataforma para ofrecer sus productos en todo el mundo, la mayoría de estos usuarios pertenecían a los Estados Unidos, y otro tanto al resto del mundo[468]. Los ingresos generados por la Ruta de la Seda ascienden a un aproximado de 1,2 billones de dólares, que serían un aproximado de 600000

---

[466] En ese sentido, "Monero fue lanzado en 2014, y su objetivo es simple: permitir que las transacciones se realicen de forma privada y con anonimato. A pesar de que comúnmente se cree que BTC puede ocultar la identidad de una persona, a menudo es fácil rastrear los pagos a su fuente original porque las cadenas de bloques son transparentes. Por otro lado, XMR está diseñado para ocultar a remitentes y destinatarios por igual mediante el uso de criptografía avanzada". Véase: <https://coinmarketcap.com/es/currencies/monero/>.

[467] GÓMEZ ECHAVARRÍA, Cristina, "Todo lo que tienes que saber sobre Ross Ulbricht y Silk Road", en *Vice***.** Disponible en: <https://www.vice.com/es_co/article/qbqax5/todo-lo-que-tienes-que-saber-sobre-ross-ulbricht-y-el-silk-road>.

[468] GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Directrices para un Enfoque…, op. cit.,* p. 37.

bitcoins en comisiones por las transacciones realizadas. La razón por la que Ulbritch escogió el *bitcoin* como medio pago fue por la característica principal del anonimato y encriptación que hace indetectable la transacción por parte de terceros. Nos referimos al registro de la transacción, ya que el mismo *software bitcoin* protege la identidad del usuario y lo mantiene en un anonimato absoluto. Por lo que millones de dólares fueron blanqueados a través del portal de la Ruta de la Seda, sin que puedan ser detectados.

Además, también existieron otros componentes que coadyuvaron en el proceso de lavado como son la utilización de red oculta Tor y la utilización de anonymisers[469]. El 31 de mayo del año 2017 un Tribunal de Apelaciones de la ciudad de Nueva York confirmó la sentencia de cadena perpetua impuesta por el juez distrital en contra de Ross Ulbritch. El 28 de junio del 2018, el Tribunal Supremo de los Estados Unidos ha negado la revisión de la cadena perpetua de Ross Ulbricht, también conocido como Dread Pirate Roberts del mercado de la *dark web*, *Silk Road.*

Otro caso muy sonado fue el del ciudadano alemán Maximilian Schmitd, quien en el año 2013 creó una plataforma web en la que se dedicaba a la comercialización de sustancias ilegales, desde marihuana, cocaína, éxtasis, hasta medicamentos bajo receta médica. El método de pago utilizado en la para las transacciones ilegales fue el *bitcoin*. Si bien fue procesado y condenado por parte de la justicia alemana, la gran parte de sus ganancias en *bitcoins*, estaba almacenada en billeteras virtuales.

[469] "El sistema de pago Silk Road funcionaba como un banco interno de Bitcoin, donde cada usuario tenía que tener una cuenta para realizar transacciones en el sitio. Cada usuario de Silo Road tenía al menos una dirección de Silk Road de Bitcoins (y posiblemente miles) asociadas a la cuenta de SilK Road, almacenadas en carteras mantenidas en servidores controlados por Silk Road. Para realizar las compras un usuario obtenía bitcoins (normalmente a través de un cambiador de Bitcoin) y lo enviaba a una dirección Bitcoin asociada a su cuenta Silk Road para financiar la cuenta. Cuando se hacía una compra, Silk Road transferencia los bitcoins del usuario a una cuenta de fideicomiso que mantenía, en espera de la finalización de la transacción y luego se transfería los bitcoins del usuario/comprador de la cuenta de fideicomiso a la dirección de bitcoin Silk Road del vendexdor". GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Directrices para un Enfoque…, op. cit.,* p. 37.

IV. POLÍTICA CRIMINAL PREVENTIVA EN RELACIÓN CON LOS CRIPTOACTIVOS

Han transcurrido 14 años desde que el seudónimo de NAKAMOTO lanzó el *paper* denominado *Bitcoin: A Peer-to-Peer Electronic Cash System.* Durante el transcurso de ese tiempo, solo dos países han adoptado al citado criptoactivo como una moneda virtual de curso legal, hablamos de El Salvador y República Centro Africana; sin embargo, hasta la fecha, salvo las dos excepciones señaladas, no existe una regulación jurídica general unitaria global y una normativa con relevancia jurídico penal, sino, muy por el contrario, encontramos legislación discontinua y totalmente fragmentada. Esta situación, según NIETO MARTÍN y GARCÍA MORENO, complica la descripción de los riesgos penales derivados de la creación y el funcionamiento de los criptoactivos[470].

Además de la problemática señalada, existe un crecimiento desmedido en la creación de nuevos proyectos de criptoactivos con sus propias características y grado de control[471]. En la actualidad, esta falta de política de regulación se percibe socialmente, como señala PÉREZ LÓPEZ, como una "actitud cautelosa por parte de las autoridades de supervisión y de triunfalismo por parte de sus promotores y de parte de sus comunidades de usuarios, que a menudo las identifican con la realización de un ideal anarcoliberal de liberación del individuo de la supervisión financiera estatal mediante la tecnología"[472]. Si bien organismos como el GAFI, ya han venido emitiendo distintos pronunciamientos, los cuales se ven plasmados en los distintos documentos y recomendaciones. Estos difícilmente se podrían considerar vinculantes en términos técnicos jurídicos; sin embargo, no dejamos de reconocer que su capacidad de influencia

---

[470] NIETO MARTÍN, Adam y GARCÍA MORENO, Beatriz, "Criptomonedas y derecho penal: más allá del blanqueo de capitales", en *Revista Electrónica de Ciencia Penal y Criminología*, n.º 23-17, 2021, p. 2. Disponible en: <http://criminet.ugr.es/recpc/23/recpc23-17.pdf>.

[471] *Ibid.* p. 2.

[472] PÉREZ LÓPEZ, Xesús, "Las criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento para el blanqueo de capitales en la Unión Europea y España", en *Revista de Derecho Penal y Criminología*, 3.° época, n.° 18, 2017, p. 145.

ha hecho posible que muchos países tomen en cuenta las recomendaciones para aplicarlas en su legislación penal interna[473].

En la Unión Europea es donde se pueden apreciar los avances más significativos en materia de regulación de criptoactivos, tanto de forma jurídica general como desde una respuesta penal preventiva-punitiva. En esa línea, tenemos la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, que es en la actualidad el mayor instrumento jurídico en prevención de utilización de criptoactivos para el blanqueo de capitales. Asimismo, tenemos la Directiva (UE) 2019/713, relativa a la falsedad de medios de pago distintos al efectivo, en la que se han incluido los criptoactivos. Por último, tenemos la propuesta MICA, la cual tiene como finalidad regular las monedas estables o *stablecoins.* En el caso de América Latina, salvo algunas iniciativas propuestas por parte de las Unidades de Inteligencia Financiera, a la fecha no existe ninguna legislación preventiva en materia de criptoactivos.

V. LA DIRECTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

Si bien en el capítulo I hicimos una breve reseña de esta directiva, consideramos que, dada su trascendencia en el tema objeto de investigación, en relación con el blanqueo y los criptoactivos, es importante hacer un análisis profundo de la misma. El 5 de julio del 2016, los avances en materia de ciberdelincuecia empujaron a la Comisión Europea a presentar al Parlamento Europeo una

[473] FABIÁN CAPARRÓS, Eduardo, *Combate contra el lavado de activos desde el sistema judicial*, Washington DC: Fimart, p. 12.

propuesta Directiva que reformase[474] la Directiva (UE) 2015/849, relativa a la utilización del sistema financiero para el blanqueo de capitales[475].

Las propuestas iniciales tenían como finalidad detectar con efectividad los flujos de financiación de la delincuencia y el terrorismo, por lo que deberán:

- Crear una mayor seguridad jurídica para las entidades obligadas, en lo que se refiere a las medidas reforzadas de diligencia debida con respecto al cliente que deben aplicarse en relación con terceros países de alto riesgo.
- Mejorar la detección de transacciones sospechosas con monedas virtuales.
- Reducir el uso indebido de instrumentos de prepago anónimos.
- Mejorar el acceso de las UIF a la información en poder de las entidades obligadas y el intercambio de esa información entre las UIF.
- Asegurar un rápido acceso a la información pertinente sobre la identidad de los titulares de cuentas bancarias y de pago, con el fin de prevenir y detectar transacciones vinculadas al blanqueo de capitales y la financiación del terrorismo.
- Aumentar la transparencia de la titularidad real de las estructuras societarias y jurídicas[476].

El 19 de junio del 2018, se publicó en el *Diario Oficial de la Unión Europea* la Directiva (UE) 2018/843. El preámbulo del texto hace énfasis en los recientes atentados terroristas, los cuales han revelado la aparición de nuevas tendencias, especialmente en lo que se refiere a la manera en que se financian y ejecutan

---

[474] En ese sentido la Comisión Europea determinó que "si bien la Directiva (UE) 2015/849 supone un gran paso adelante en la prevención del blanqueo de capitales y la financiación del terrorismo en la UE, los recientes atentados terroristas y revelaciones sobre ciertas deficiencias en el sistema financiero mundial (los *papeles de Panamá*) ponen de manifiesto la necesidad de nuevas medidas que mejoren este marco. Desde esa perspectiva, es preciso abordar cinco problemas relacionados con la financiación del terrorismo". Véase la ficha resumen del documento de trabajo elaborado por la Comisión. Disponible en: <https://eur-lex.europa.eu/legalcontent/ ES/TXT/?uri=CELEX%3A52016SC0224>.

[475] CECCARELLI, Cristina, "Criptoactivos en el punto de mira de los blanqueadores de capitales: España e Italia", en *Revista Electrónica de Estudios Penales y de Seguridad*, n.º 7, Sevilla, 2021 p. 5. Disponible en: <https://www.ejc-reeps.com/Cecarelli.pdf>.

[476] Véase la ficha resumen del documento de trabajo elaborado por la Comisión. Disponible en: <https://eur-lex.europa.eu/legalcontent/ ES/TXT/?uri=CELEX%3A52016SC0224>.

las operaciones de los grupos terroristas. Estos servicios basados en el uso de nuevas tecnologías están ganando popularidad como sistemas de financiación alternativos. Si bien permanecen fuera del ámbito de aplicación del derecho de la Unión o se benefician de exenciones de requisitos jurídicos que podrían haber dejado de estar justificadas, razón por la que para seguir el ritmo de evolución de estas tendencias, es preciso adoptar nuevas medidas destinadas a garantizar una mayor transparencia de las transacciones financieras, de las sociedades y otras entidades jurídicas, así como de los fideicomisos (del tipo *trust*) e instrumentos jurídicos de estructura o funciones análogas a las de tales fideicomisos, con el fin de mejorar el marco preventivo vigente y de luchar más eficazmente contra la financiación del terrorismo[477].

En lo que respecta al blanqueo mediante criptoactivos, la directiva incorpora a los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias (es decir, las monedas y billetes de designados como medio legal y el dinero electrónico de un país aceptado como medio de cambio en el país expedidor), así como a los proveedores de servicios de custodia de monederos electrónicos.

El documento advierte que los grupos terroristas pueden ser capaces de transferir dinero hacia el sistema financiero de la Unión o dentro de las redes de monedas virtuales, ocultando transferencias o gozando de cierto grado de anonimato en esas plataformas. Razones fundadas por las que resulta indispensable ampliar el ámbito de aplicación de la Directiva (UE) 2015/849 para incluir en él a los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias, así como a los proveedores de servicios de custodia de monederos electrónicos. Asimismo, las autoridades competentes deben estar facultadas, a través de las entidades obligadas, para vigilar el uso de las monedas virtuales. Dicha vigilancia aportaría un enfoque equilibrado y proporcionado que salvaguarde los avances técnicos y el alto grado de

[477] Véase el preámbulo de la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, del 30 de mayo del 2018.

transparencia logrado en el ámbito de la financiación alternativa y el emprendimiento social.

Otro punto al que hace énfasis el documento es el referente al anonimato de las monedas virtuales, ya que este permite su posible uso indebido con fines delictivos. Además, advierte que la inclusión de los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias y de los proveedores de servicios de custodia de monederos electrónicos no resolverá totalmente la cuestión del anonimato asociado a las transacciones con monedas virtuales, al mantenerse el anonimato en gran parte del entorno de la moneda virtual, puesto que los usuarios pueden llevar a cabo transacciones al margen de tales proveedores de servicios.

Para combatir los riesgos relacionados con ese anonimato, la Directiva establece que a través de las Unidades de Inteligencia Financiera (UIF) nacionales deben poder obtener informaciones que les permitan asociar las direcciones de las monedas virtuales a la identidad del propietario de la moneda virtual.

Por último, en lo que se refiere a criptoactivos, las monedas virtuales no deben confundirse: con dinero electrónico, tal como se define en el artículo 2, punto 2, de la Directiva 2009/110/CE del Parlamento Europeo y del Consejo; con el concepto más amplio de “fondos”, tal como se define en el artículo 4, punto 25, de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo; con el valor monetario almacenado en instrumentos exentos, tal como se especifica en el artículo 3, letras k) y l), de la Directiva (UE) 2015/2366; ni con las monedas de juegos, que solo pueden utilizarse en el contexto específico de un juego. Aunque las monedas virtuales pueden utilizarse frecuentemente como medio de pago, también podrían utilizarse con otros fines y encontrar aplicaciones más amplias, tales como medios de cambio, inversión, productos de reserva de valor o uso en los casinos en línea. Por último, el objetivo de la presente directiva es abarcar todos los posibles usos de las monedas virtuales, y su prevención frente al blanqueo de capitales.

Las modificaciones realizadas a la Directiva (UE) 2015/849 son las siguientes:

El artículo 1 de la directiva incorpora a los siguientes sujetos y sus definiciones:

- Los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias.
- Los proveedores de servicios de custodia de monederos electrónicos.
- Monedas virtuales: representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos;
- Proveedor de servicios de custodia de monederos electrónicos: una entidad que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales[478].

La transposición de esta directiva en España se materializó mediante el Anteproyecto de Ley del año 2020, por la que se modifica la ley 10/2010, del 28 de abril del 2021, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, y se Transponen Directivas de la Unión Europea en materia de prevención de blanqueo de capitales y financiación del terrorismo. En concreto, el proyecto procede transponer la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, del 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 (en adelante, la V Directiva o Directiva UE 2018/843). En segundo lugar, deben incorporarse las novedades en estas materias aprobadas por la Directiva (UE) 2019/2177 del Parlamento Europeo y del Consejo, del 18 de diciembre de 2019, por la que se modifica la Directiva 2009/138/CE, sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II); la Directiva 2014/65/UE, relativa a los mercados de instrumentos financieros; y la Directiva (UE) 2015/849, relativa a la

[478] Artículo 1 de la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, del 30 de mayo del 2018

prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. Todo ello con el doble objetivo de perfeccionar los mecanismos de prevención del terrorismo, y mejorar la transparencia y disponibilidad de información sobre los titulares reales de las personas jurídicas y otras entidades sin personalidad que actúan en el tráfico jurídico. Precisamente esta ley tiene el propósito fundamental de transponer esta nueva Directiva UE 2018/843[479].

En lo que se refiere a la incorporación de los proveedores de servicios de cambio entre diferentes monedas virtuales (y no únicamente entre moneda virtual y real) como sujetos obligados en las legislaciones nacionales, así como su regulación y registro, según los estándares del GAFI es necesaria la regulación de los proveedores de servicios financieros que permitan la emisión y negociación de activos virtuales que tengan la consideración de valores negociables (*security tokens*). Sin embargo, no es correcto realizar modificaciones adicionales a la presente ley para dar cobertura a esta previsión, debido a que su consideración como valor negociable por parte de la Comisión Nacional del Mercado de Valores supone la aplicación del mismo régimen existente para el resto de los valores negociables que se encuentran ya sujetos a la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo.

Mediante el Real Decreto Ley 7/2021, del 27 de abril, se realizó la transposición de la directiva de la Unión Europea en materia de prevención del blanqueo de capitales, modificándose el artículo tercero de la Ley 10/2010, del 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, en los siguientes términos: se añaden los nuevos apartados 5, 6 y 7 al artículo 1, con la siguiente redacción:

[479] Véase el preámbulo del Anteproyecto de Ley --/2020, por la que se modifica la Ley 10/2010, del 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, y se transponen directivas de la Unión Europea en materia de prevención de blanqueo de capitales y financiación del terrorismo.

- Se entenderá por moneda virtual aquella representación digital de valor no emitida ni garantizada por un banco central o autoridad pública, no necesariamente asociada a una moneda legalmente establecida y que no posee estatuto jurídico de moneda o dinero, pero que es aceptada como medio de cambio y puede ser transferida, almacenada o negociada electrónicamente.

- Se entenderá por cambio de moneda virtual por moneda fiduciaria la compra y venta de monedas virtuales mediante la entrega o recepción de euros o cualquier otra moneda extranjera de curso legal o dinero electrónico aceptado como medio de pago en el país en el que haya sido emitido.

- Se entenderá por proveedores de servicios de custodia de monederos electrónicos aquellas personas físicas o entidades que prestan servicios de salvaguardia o custodia de claves criptográficas privadas en nombre de sus clientes para la tenencia, el almacenamiento y la transferencia de monedas virtuales[480].

Asimismo, el real decreto establece como disposición adicional segunda el registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos a las personas físicas o jurídicas que, cualquiera que sea su nacionalidad, ofrezcan o provean en España servicios de los descritos en los apartados 6 y 7 del artículo 1 de la ley; esas personas deberán estar inscritas en el registro constituido al efecto en el Banco de España.

Se señala en el real decreto que se inscribirán en el registro:

[480] Véase el Real Decreto-ley 7/2021, del 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores.

- Las personas físicas que presten estos servicios, cuando la base, la dirección o la gestión de estas actividades radique en España, con independencia de la ubicación de los destinatarios del servicio.
- Las personas jurídicas establecidas en España que presten estos servicios, con independencia de la ubicación de los destinatarios.

Por último, la inscripción en el registro estará condicionada a la existencia de procedimientos y órganos adecuados de prevención previstos en esta ley.

Tras el análisis cronológico realizado a la Directiva (UE) 2018/843, se puede apreciar que el legislador español ha dado pleno cumplimiento a las exigencias establecidas por la Unión Europea, respecto la incorporación en el ordenamiento jurídico español de nuevas definiciones tecnológicas en materia de criptoactivos o monedas virtuales, así como la inclusión de nuevos sujetos obligados.

VI. LOS CRIPTOACTIVOS COMO OBJETO DEL DELITO DE LAVADO DE ACTIVOS

Como antecedente normativo internacional en relación con el *objeto material* del delito en el blanqueo de capitales, debemos tomar en cuenta a lo establecido en la Convención de las Naciones Unidas Contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas del año 1988, conocida como la Convención de Viena, que establece en el artículo 1, incisos p y q, lo siguiente: “p) por “producto” se entiende los bienes obtenidos o derivados directa o indirectamente de la comisión de un delito tipificado de conformidad con el párrafo 1 del artículo 3; q) por “bienes” se entiende los activos de cualquier tipo, corporales o incorporales, muebles o raíces, tangibles o intangibles, y los documentos o instrumentos legales que acrediten la propiedad u otros derechos sobre dichos activos”.

La descripción de la citada convención se circunscribe únicamente de forma directa o indirecta al tráfico ilícito de drogas como delito fuente generador de

ganancias[481]. Sin embargo, esta definición inicial con el paso de los años y la evolución del delito de lavado de activos a nuevas construcciones típicas a partir de los actos de blanqueo producto de una variedad de actividades criminales previas, generó una preocupación internacional de ampliar la gama de actividades delictivas generadoras de ganancias ilegales, distintas al narcotráfico. En ese sentido, la Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional y sus Protocolos, conocida como la Convención de Palermo, del año 2000, establece en sus artículos 2, incisos d y e: "d) por *bienes* se entenderá los activos de cualquier tipo, corporales o incorporales, muebles o inmuebles, tangibles o intangibles, y los documentos o instrumentos legales que acrediten la propiedad u otros derechos sobre dichos activos; e) por *producto del delito* se entenderá los bienes de cualquier índole derivados u obtenidos directa o indirectamente de la comisión de un delito".

La interrogante que debemos plantearnos es si cabe la posibilidad de incorporar a los criptoactivos como bienes objeto del delito de blanqueo de capitales a partir de una interpretación de los convenios internacionales adoptados por el Perú, los cuales han sido plasmados en el Decreto Legislativo N.° 1106, en los artículos 1[482], 2[483] y 3[484]. Lo primero que debemos señalar es qué entiende el regulador

---

[481] MENDOZA LLAMACPONCCA, Fidel, *Lavado de activos y criminalidad empresarial*, Lima: Jurista Editores, 2022, pp. 330 y 331.

[482] Artículo 1.- *Actos de conversión y transferencia*
El que convierte o transfiere dinero, bienes, efectos o ganancias cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa.

[483] Artículo 2.- *Actos de ocultamiento y tenencia*
El que adquiere, utiliza, guarda, administra, custodia, recibe, oculta o mantiene en su poder dinero, bienes, efectos o ganancias, cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa.

[484] Artículo 3.- *Transporte, traslado, ingreso o salida por territorio nacional de dinero o títulos valores de origen ilícito*
El que transporta o traslada dentro del territorio nacional dinero o títulos valores cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso; o hace ingresar o salir del país tales bienes con igual finalidad, será reprimido con pena privativa de libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa.

peruano por criptoactivos. En ese esa línea, el Banco Central de Reserva del Perú los define como "activos digitales no regulados, que no tienen la condición de moneda de curso legal ni son respaldadas por bancos centrales. Asimismo, no cumplen plenamente las funciones del dinero como medio de cambio, unidad de cuenta y reserva de valor"[485]. A partir de esta definición otorgada por el ente regulador y al margen de su significado financiero y alta potencialidad delictiva[486], el problema de orden dogmático penal se centra en determinar, en primer término, si estamos ante un activo digital y, en segundo término, si este puede ser subsumido como parte de los elementos normativos del tipo penal de blanqueo. Según MAX ERNST MAYER, los elementos normativos son partes esenciales de un resultado típico que solo tiene una importancia valorativa determinada[487], asimismo tales expresiones forman parte de la descripción contenidos en los tipos penales y que se llaman normativos, por implicar una valoración que es necesaria para poder captar el sentido de la norma[488].

Estos elementos se caracterizan porque en ellos predomina una valoración que no es perceptible por los sentidos[489]. Como refiere ROXIN, no hay percepción sensorial, ni comprobación solo en virtud de la valoración[490]. MEZGER los clasifica en tres grupos: jurídicos, culturales y subjetivos[491]. Los elementos normativos del tipo de contenido jurídico implican una valoración eminentemente jurídica en

---

[485] BANCO CENTRAL DE RESERVA, "Riesgos de las criptomonedas". Disponible en: <https://www.bcrp.gob.pe/sistema-de-pagos/articulos/riesgos-de-las-criptomonedas.html>.

[486] PRADO SALDARRIAGA, Víctor, "Lavado de Activos en el Perú: problemas y alternativas", en *Lex: Revista de la Facultad de Derecho y Ciencia Política de la Universidad Alas Peruanas*, vol. 17, n.º 24, 2019, p. 174.

[487] REYES ECHANDÍA, Alfonso, *La tipicidad*, Bogotá: Temis, 1989, p. 89.

[488] *Ibid.,* p. 90

[489] BACIGALUPO Enrique, *Manual de derecho penal*, Bogotá: Temis, 1989, p. 84. "La teoría del penal tuvo un significativo impulso como consecuencia del descubrimiento de los elementos normativos del tipo hecha por Max Ernst Mayer. La gran transformación surge de los elementos normativos del tipo. Ellos hacen vacilar por primera vez la teoría de la neutralidad valorativa del tipo penal. Mayer menciona como ejemplos la falsedad de un hecho, la honestidad y la peligrosidad". ROXIN, Claus, *Teoría del tipo penal: Tipos abiertos y elementos jurídicos del deber*, Buenos Aires: Depalma, 1979, p. 60 y ss.

[490] ROXIN, *op. cit.,* p. 63.

[491] *Loc. cit.*

cuanto se trata de conceptos que pertenecen al ámbito del derecho[492]. Los otros elementos tienen un contenido cultural, por lo que requieren una valoración de orden ético social[493]. Para JESCHEK, los elementos normativos del tipo "aluden a premisas que solo pueden ser imaginadas y pensadas bajo los presupuestos lógicos de una norma"[494]. Menciono algunos ejemplos que pertenecen a conceptos jurídicos dentro de los tipos penales como son el matrimonio, el deber legal de prestación de alimentos, los datos, el documento, la ventaja patrimonial, el funcionario público, entre otros[495].

En cuanto a la primera problemática descrita, debemos dilucidar si el concepto de *muebles* es lo suficientemente amplio para abarcar a los criptoactivos como objeto material del delito, para determinar si su utilización sirve como instrumento para la ocultación de bienes que tienen su origen en una actividad delictiva previa[496]. En esa línea de pensamiento, PRADO SALDARRIGA, realizando una interpretación progresista y funcional de la naturaleza jurídica de los criptoactivos, establece que sí es posible identificarlas como un objeto del delito de blanqueo, rechazando cualquier cuestionamiento formalista que pueda darse[497]. Coincidimos con esta posición, ya que los criptoactivos se pueden subsumir mediante un juicio de tipicidad dentro de los elementos normativos de las tipologías descritas en los artículos 1 y 2 del Decreto legislativo N.º 1106, y a partir de ello efectuarse actos propios del blanqueo, como son actos de conversión, transferencia, tenencia y ocultamiento. Además, están los acuerdos internacionales suscritos por el Perú en materia de represión del blanqueo de capitales, tanto en la Convención de Viena como en la de Palermo, que le

---

[492] REYES ECHANDÍA, *op. cit.,* p. 91.

[493] *Loc. cit.*

[494] WEIGEND Thomas y JECHECK, Hans, *Tratado de derecho penal. Parte general*, Granada: Comares, 2003, p. 289.

[495] WEIGEND y JECHECK, *op. cit.*, p. 63.

[496] MORALES GARCÍA, Oscar, "Riesgos penales de la posesión, adquisición, venta e intercambio de criptoactivos", en *Criptoactivos retos y desafíos normativos*, Madrid: Wolter Klawuers, 2021, p. 275.

[497] PRADO SALDARRIAGA, Víctor, "Lavado de Activos en el Perú…, *op. cit.,* p. 174.

otorgan la flexibilidad necesaria al órgano judicial para hacer una interpretación extensiva sobre los bienes objeto del delito. Siguiendo esa línea interpretativa, se pueden definir a los criptoactivos como un activo digital intangible.

En cuanto al segundo problema, tampoco se advierte mayores dificultades de orden dogmático típico, ya que las transacciones financieras requieren del ciberespacio para su materialización; es decir, todos los actos propios del blanqueo como son la conversión, transferencia, tenencia y ocultamiento se pueden realizar mediante la instrumentalización de criptoactivos. Como de forma acertada señala PRADO SALDARRIAGA, solo se trata de construir interpretación funcional o normativa de dicho *modus operandi* y de su conexión y eficacia para la realización de las conductas típicas[498].

En el derecho comparado, España ya ha delimitado la naturaleza jurídica de los criptoactivos, tal como se advierte en la sentencia emitida por el Tribunal Supremo, Sala de lo Penal, teniendo como ponente al magistrado LLORENA CONDE. En la sentencia se ha establecido que "el bitcoin no es sino un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica denominada bitcoin, cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta que de estas unidades se realiza a través de las plataformas de trading Bitcoin"[499]. La Sala Suprema reconoce dos aspectos en relación con el criptoactivo *bitcoin:* el primero es que se trata de unidades de cuenta y el segundo es que se trata de un activo patrimonial inmaterial, y en ello radica su no restituibilidad, pero sí intercambiabilidad, al tener un valor patrimonial inherente al mismo activo en sí[500].

Otro aspecto por resaltar respecto a los criptoactivos como objeto material de delito de blanqueo de capitales que se debe tener en cuenta es en relación con

[498] *Ibid.,* p. 174.

[499] Véase el fundamento tercero de la STS 2019/20, del 20 de junio del 2019.

[500] MORALES GARCÍA, *op. cit.,* p. 276.

la restitución del bien como parte de la responsabilidad civil. Este aspecto jurídico. En esa línea, el artículo 110 del Código Penal de España dispone que la responsabilidad civil derivada del hecho descrito por la ley como delito debe materializarse en la restitución de la cosa objeto del delito. La imposibilidad de hacerlo da lugar al derecho a obtener una reparación equivalente al daño sufrido. En el presente caso, si bien la Sala Suprema de España recoge al criptoactivo *bitcoin* como el objeto del delito de estafa y su valor como un activo patrimonial, el problema se suscita, ya que los agraviados no fueron despojados de *bitcoins* en sentido estricto, por ende la restitución patrimonial se debe dar en euros. Este razonamiento perfectamente se podría aplicar por parte del operador de justicia en el Perú, ya que el artículo 94 del Código Penal peruano, establece, que la restitución se hace con el mismo bien, aunque se halle en poder de terceros, sin perjuicio del derecho de estos para reclamar su valor.

VII. CARACTERÍSTICAS QUE HACEN A LOS CRIPTOACTIVOS ÚTILES PARA EL LAVADO DE ACTIVOS

1. Fácil acceso

Existen distintas formas de obtener criptoactivos; ello depende del tipo de protocolo con el que se elabore el mismo. ÁLVAREZ LARRONDO clasifica la adquisición de criptoactivos en dos modalidades[501]: la adquisición de manera originaria, es decir a través de la minería, creando la moneda a través de la prueba de trabajo (*proof of work*); y la adquisición derivada.

En la adquisición originaria o directa, solo está habilitada para algunos criptoactivos como es el caso del *bitcoin*, ya que se puede minar con equipos de minería específicos. Además, hay otros criptoactivos que se pueden minar como son: *bitcoin cash* (BCH), *kadena* (KDA), *dogecoin* (DOGE), *zcash* (ZEC), *dash* (DASH), *litecoin* (LTC), *horizen* (ZEN), *nicehash blake* (14r), *decred* (DCR), *axe* (AXE), *pirate* (ARRR), *groestlcoin* (GRS), *litecoin cash* (LCC), *komodo* (KMD),

[501] ÁLVAREZ LARRONDO, Federico, *Entendiendo al bitcoin y sus desafíos jurídicos y sociales*, Buenos Aires: Thomson Reuters Aranzandi, 2022, p. 77.

hush (HUSH), *DigiByte* (DGB), *Verge-Scrypt* (XVG), *nervos* (CKB), *NiceHash Eaglesong* (STC), *DGB-Scrypt* (DGB), *einsteinium* (EMC2), *bitgesell* (BGL), *actinium* (ACM), *Nicehash-Lyra2zDGB-Skein* (DGB), *SmartCash* (SMART), *Verge-Groestl* (XVG), *NicehashKeccakSibcoin* (SIB), *DGB-SHA* (DGB), *peercoin* (PPC), *MyriadGroestl* (XMY) *bytecoin* (BCN), *BitcoinDiamond* (BCD), *monacoin* (MONA), *Verge-Lyra2REv2* (XVG), *Myriad-scrypt* (XMY), *viacoin* (VIA), *LBRY* (LBC), *Myriad-SHA* (XMY), *sia* (SC), etc. Sin embargo, no todos los criptoactivos son susceptibles de ser creados mediante el proceso de minería, ya que no todos se basan en el protocolo de *prueba de trabajo*, y por lo tanto no pueden ser objeto de este proceso. Algunos ejemplos son *polkadot* (DOT), *cardano* (ADA), *solana* (SOL), *polygon* (MATIC), *avalanche* (AVAX), *binance coin* (BNB), etc.

La *adquisición derivada* puede darse de distintas formas, como veremos[502]. Para un mejor entendimiento de este acápite, tomaremos como ejemplo el *bitcoin*. La primera forma de adquisición derivada se da cuando la transacción para la obtención de la moneda se da entre usuarios de la misma red *bitcoin*, ya sea por los servicios prestados o bienes transados, y estos sé intercambian directamente entre las partes utilizando la red P2P o red entre pares. La segunda forma se da a través de operadores o casas de cambio virtuales, para lo cual se requiere realizar una transferencia bancaria desde nuestra cuenta con destino a la cuenta del operador; en algunos casos, operadores disponen de la opción de cargar el saldo vía tarjeta de crédito, con lo cual una adquiere los criptoactivos en el instante. Además, estas plataformas o *exchanges* también ofrecen la posibilidad de proporcionarle al usuario una billetera electrónica, para que pueda almacenar los criptoactivos adquiridos en la misma plataforma. También cuentan con el sistema P2P, para transar directamente sin intermediarios[503]. En la gran mayoría de los casos, estos intercambiadores operan de forma virtual y su titularidad se encuentra cubierta bajo un entorno societario, con su real ubicación en lugares recónditos, situación que los usuarios no advierten por desconocimiento al momento de hacer uso de sus servicios.

---

[502] *Ibid.,* p. 78.

[503] *Idem*.

Los cajeros ATM en los últimos años han surgido como un servicio para facilitar la conversión de moneda fíat en criptoactivos y viceversa. En el año 2020, el informe emitido por la Administración de Control de Drogas (DEA), titulado "Evaluación Nacional de Amenaza a las Drogas 2020", hace énfasis en que cada vez más las organizaciones criminales utilizan cajeros automáticos de moneda virtual (ATM) para fines de blanqueo. Estos cajeros automáticos son específicamente diseñados para aceptar dinero fiduciario a cambio de criptoactivos, y se encuentran sujetos a distintas regulaciones en materia de prevención de blanqueo dependiendo el país en el que estén situados[504]. A pesar de estas normas, estos cajeros ATM se están instrumentalizando para el blanqueo de dinero proveniente del tráfico ilícito de drogas, entre otros delitos. Los agentes blanqueadores depositan grandes volúmenes de dinero en efectivo, para su posterior conversión a monedas virtual; ese efectivo ingresado en la máquina ATM luego es integrado en el flujo de ingresos del propietario del cajero para ocultar el origen ilícito de los fondos[505].

2. Descentralización

La descentralización de algunos criptoactivos como parte de su propio protocolo es lo que evita el control por parte de un organismo central controlador que pueda verificar las transacciones, es decir la confianza de la validez de las transacciones se deposita en terceras personas, las cuales validadas dichas operaciones. Esta característica permite a las organizaciones criminales el poder transferir criptoactivos dentro de la misma red, escapando del control estatal, debilitando los sistemas gubernamentales en materia de prevención contra el blanqueo[506].

---

[504] DRUG ENFORCEMENT ADMINISTRATION, *2020 National Drug Threat Assessment*, marzo del 2021, p. 89.

[505] *Ibid.,* p. 89.

[506] SALDAÑA TABOADA, Patricia, "¿Por qué las organizaciones criminales utilizan criptomonedas? Los bitcoins en el crimen organizado", en *El Criminalista Digital. Papeles de Criminología*, n.º 6, 2017, p. 28.

3. Red entre pares (*peer-to-peer*)

La red entre pares (P2P), por sus siglas en inglés *peer-to-peer*, es una tecnología que permite a un individuo de la red cripto el poder transar con otro individuo de la misma red o ecosistema cripto, sin ningún intermediario u organismo controlador central. No cabe duda de que este método directo para realizar operaciones que ofrece esta tecnología es la que genera mayor atención por parte de las organizaciones criminales, ya que, al darse la operación dentro de la misma red, sin convertirse el criptoactivo en dinero fíat, es casi imposible de detectar o controlar la transacción hacia el exterior.

4. Coste cero en las transacciones

De igual forma que el sistema P2P entre pares, el ecosistema cripto permite realizar las transacciones entre miembros de una misma red o protocolo, sin cobrar ninguna comisión por realizar la transferencia. Situación que se vuelve muy atractiva para las organizaciones criminales, ya que no solo evitan el control o fiscalización de un organismo central, sino que, además, la operación en sí no les genera ningún gasto.

5. Transnacionalidad en las transacciones

Al tratarse de activos virtuales, todas las operaciones que se realizan mediante el uso del P2P se realizan a través del Internet. Este hecho —además de los dos referidos anteriormente, como son el uso de P2P a un costo cero por transacción, y ahora la posibilidad de transferir criptos a cualquier parte del mundo, sin un organismo central controlador, es decir, sin la necesidad de recurrir al sistema financiero bancario tradicional, y ello unido a la disparidad de las distintas jurisdicciones— genera la posibilidad de operar con múltiples cuentas[507], siendo

[507] NAVARRO CARDOSO, *op. cit.,* p. 33.

ello muy atractivo para los delincuentes, ya que facilita el ocultamiento del origen ilícito del dinero fíat convertido en criptoactivos.

6. Anonimato

Desde el punto de vista del cripotactivo *bitcoin*, las transacciones no presentan características de privacidad, de acuerdo con como lo establece el secreto bancario, pero sí de anonimidad, es decir, las identidades no se registran en ninguna parte del protocolo *bitcoin*; sin embargo, cada transacción realizada es visible en un "libro electrónico público y distribuido", conocido como *blockchain* o cadena de bloques. La tecnolgía *blockchain* no brinda la identificación de los intervinientes de cada operación, solo se limita al registro de las direcciones de origen y destino de todas las transferencias[508], ya que la *blockchain*, funciona como un libro contable donde se asientan las operaciones, permite la trazabilidad de las transacciones[509].

7. Falta de regulación

Actualmente, solo hay dos países donde se ha regulado el *bitcoin*, me refiero a El Salvador y República Centroafricana. Son los únicos estados en que el criptoactivo *bitcoin* es una representación digital de curso legal y de obligatoria aceptación por parte de su sociedad, como ya se explicó en el capítulo respectivo. En lo que respecto a otros países como, por ejemplo, lo es el caso de España, si bien no hay una regulación sobre la materia, esto no quita las autoridades bancarias, tanto locales como europeas, hayan emitido algunos informes que han contribuido al esclarecimiento de la posible naturaleza jurídica de los criptoactivos, como es el caso del Banco de España, de la CNMV, y de la Estrategia de Seguridad Nacional y Ciberseguridad Nacional[510].

---

[508] BELÉN LINARES, María, "Criptomoneda como herramienta para lavar activos criminales", en *Ciberdelito nuevas tecnologías y derecho penal*, Ciudad de México: Editorial Flores, 2002, p. 65.

[509] NAVARRO CARDOSO, *op. cit.,* p. 13.

[510] PEREZ LOPEZ, *op. cit.*, p. 169.

Sin embargo, no existen más países que hayan decidido enrumbarse hacia la regularización de los criptoactivos, situación que se torna muy atractiva en el ámbito delictivo, ya que esta falta de normatividad facilita los actos de blanqueo por parte de las organizaciones criminales, para encubrir el patrimonio, ya que esa falta de legislación o vacío legal sirve como escudo para encubrir actos destinados a proteger el origen ilícito de los activos. Además, esta carencia regulatoria está siendo capitalizada por personas que se dedican a la compra y venta de criptoactivos, con fines de elusión tributaria, generándose un enriquecimiento desmedido por un puñado de personas que, amparadas en esta carencia normativa, se viene beneficiando. Si bien hay muchos proyectos e iniciativas regulatorias, lo real y concreto es que hasta la fecha en la gran mayoría de países no hay una normativa específica y armonizada sobre el fenómeno de los criptoactivos.

8. Tokens no fungibles (NTF)

Como ya lo explicamos en el capítulo II, el token no fungible (*non-fungible tokens*) significa que no se puede sustituir, es decir, nos referimos a que no puede ser intercambiado por otro, ya que posee características únicas y distintas a todos los demás tokens. Este se representa un en un activo único que se registra en la cadena de bloques, lo cuales pueden ser de dos formas: una es de índole digital y la otra es una versión digitalizada de un activo real. RIVERA JIMÉNEZ los define como "una unidad única de datos almacenada en un libro de registros, que es descentralizado, electrónico y público, con la que se crea un registro inalterable de transacciones encriptadas, distribuidas a través de una cadena de bloques de información de manera descentralizada, mejor conocida como blockchain"[511]. Por su parte, MENÉNDEZ PASTORELLI los define como un tipo de criptoactivo consistente en un activo digital único, comerciable, transferible a lo largo de mercados digitales de finanzas descentralizadas (DeFi), respaldados a través de

[511] RIVERA JIMÉNEZ, Adriana, DE LA MORA MONDRAGÓN, Maritza, GISHOLT AVILÉS, Pamela y CAMACHO HERNÁNDEZ, Salvador, *Los NFT en la propiedad intelectual,* en blog *AMPPI,* n.° 45, junio-julio del 2021, p. 1. Disponible en: <https://amppi.org.mx/wp-content/uploads/2021/07/45Blg_7aArtCmtTICS-NFTs_JunJul2021.pdf>.

contratos inteligentes y se aloja en el ecosistema digital conocido como *blockchain*. La tecnología *blockchain* (cadena de bloques) es una red de servidores descentralizada, con bloques o nodos enlazados y asegurados usando criptografía[512].

No cabe duda que hoy en día los NTF se presentan como una forma de nueva tecnología que viene captando la atención del mundo debido a su funcionalidad y flexibilidad. Los NFT se han convertido en una oportunidad de inversión, tanto para los coleccionistas como para los artistas, que están incursionando en la venta de obras digitales. Sin embargo, alrededor de ocho mil millones han sido blanqueados a través de plataformas NFT desde el 2017 al 2021, ilicitud que se ampara, según el mismo autor, en la alta volatilidad que actualmente experimenta el mercado de criptoacticvos, ya que esa especulación en las subidas de los precios es aprovechada por los blanqueadores para justificar transferencia de dinero vinculado al tráfico de drogas, pero encubiertas en la adquisición de un NFT[513].

9. Irreversibilidad de las operaciones

La irreversibilidad de las transferencias en el caso de *bitcoin* se caracteriza por no poder ser anulables con posterioridad, el mismo sistema de validación por parte de los mineros genera una pared blindada que no permite revertir las transferencias, situación que dificulta la labor persecutoria de las fuerzas del orden[514].

---

[512] MENÉNDEZ PASTORELLI, Paola, "NFTS (not fungible tokens) desde una perspectiva jurídica", en *Biblioteca Nacional del Congreso de Chile - Asesoría Técnica Parlamentaria*, julio del 2022, p. 1.

[513] JOFFRE CALASICH, Fabio, "Cripto criminalidad. NFT's, DEX's, *cross chain bridges*, nuevos datos e innovaciones en la tecnología blockchain de uso criminal", en *Ilícitos económicos y evidencia digital*, Argentina: Editores Fondo Editorial, 2022, p. 16.

[514] PÉREZ LÓPEZ, *op. cit.,* p. 154.

VIII. FASES DEL LAVADO Y CRIPTOACTIVOS

Como ya se explicó en el capítulo I de forma bastante pormenorizada, el delito de blanqueo de capitales está compuesto de tres etapas o fases operativas conocidas como la *colocación*, *ensombrecimiento* e *integración,* en las que se produce lo que se conoce como el ciclo del blanqueo o lavado. Bajo este esquema, los criptoactivos pueden perfectamente ser instrumentalizados como una herramienta útil en el proceso de blanqueo de fondos de origen ilícito, como veremos.

1. Colocación de criptoactivos

En este caso nos referimos a todas aquellas operaciones destinadas a la obtención de criptoactivos, por parte del agente lavador. Se considera que la misma compra de criptoactivos puede ser una excelente vía de blanqueo de dinero[515]. Esta adquisición se puede dar mediante las plataformas de cambio (*exchangers*), los vendedores locales (*local traders*), los cajeros automáticos (ATM), las tarjetas *bitcoin* y, por último, el proceso de minería.

a) Plataforma de cambio

Me refiero a empresas de intercambio de monedas virtuales por dinero fiduciario y viceversa. Usualmente estos *exchangers* dan el servicio de billetera a sus clientes, actuando como entidad depositante de los fondos de su cliente. Como señala la *Guía de investigación en el lavado de activos mediante criptodivisas*, se han identificado algunas empresas intercambiadoras en América del Sur, porque allí no están sujetas a las limitaciones y restricciones regulatorias[516].

---

[515] NAVARRO CARDOSO, *op. cit.,* p. 29.

[516] BODOQUE AGREDANO, Ángel y Orduna LANAU, Alberto, *Guía de investigación en el lavado de activos mediante criptodivisas*, Madrid: El PAcCTO, 2022, p. 21.

b) Vendedores locales

Son personas que se publicitan para llevar a cabo el cambio de moneda virtual a moneda real, en un intercambio P2P (*peer-to-peer*). Actúan a modo de los antiguos cambistas de moneda tradicional, por divisas o incluso por oro u otros activos. A través de su actividad, que puede ser *online*, se cambia el efectivo de una actividad criminal[517].

c) Cajeros automáticos BTC

Con ello se hace referencia a los cajeros utilizados para poder introducir efectivo, transformarlo en BTC y enviarlo a un determinado monedero del usuario que realiza la operación (y viceversa). Lo ampliaremos en apartado diferenciado, dado que ya hay investigaciones activas sobre esta tipología[518].

d) Tarjetas bitcoin

Básicamente, dichas tarjetas se recargan con *bitcoin* y con ellas se pagan en euros o dólares instantáneamente, o bien permite su extracción en efectivo por cajeros de la red bancaria. Estas tarjetas se usan o bien para pagos *online* o reales a vendedores que no aceptan el pago en criptomonedas, pero sí aceptan el pago con Visa o Mastercard, o bien para hacer el cambio de criptomonedas a moneda real a través de cajeros de la red bancaria convencional que sí permiten la extracción con tarjetas Visa o Mastercard[519].

e) Minería

La obtención de beneficios mediante la práctica de actividades criminales podría ser empleado por aquellos para la adquisición de equipos de minería, para con

[517] *Ibid.,* p. 22.

[518] *Idem.*

[519] *Idem*.

ello conseguir el minado de bitcoins, y una vez obtenidos ser reinvertidos en cualquier bien[520].

2. Ensombrecimiento de criptoactivos

En esta etapa la finalidad operativa, está circunscrita a efectuar diversas operaciones con la finalidad de ocultar los activos. En el caso de los criptoactivos, el ensombrecimiento se entiende innecesaria en tanto implícito en la opacidad de la *blockchain*[521], o se lleva a cabo mediante el uso de mezcladores, que son un tipo de programa anónimo que oscurece la cadena de transacciones en la cadena de bloques vinculados a las transacciones de una misma dirección de *bitcoin* y enviándolas de manera conjunta, de manera que parece que hubieran sido enviadas desde otra dirección[522].

3. Integración de criptoactivos

Conocida como la fase de inversión o goce de lo capitales[523]. A modo de resumen, en relación con el blanqueo mediante criptoactivos, podemos desarrollar el proceso de blanqueo de la siguiente forma. Se recoge el dinero fíat de origen ilícito, posteriormente se adquieren los criptoactivos, ya sea en un intercambiador, un cajero ATM, o directamente mediante la tecnología P2P, para su posterior conversión, ya sea en otro tipo de criptoactivo o nuevamente a moneda fíat para su posterior goza adquiriendo otros activos limpios.

---

[520] *Ibid.,* p. 21.

[521] *Ibid*., p. 22.

[522] *Idem*.

[523] PRADO SALDARRIAGA, Roberto, *Lavado de activos…, op. cit.*, p. 29.

IX. EL DECRETO LEGISLATIVO N.° 1106 Y LOS CRIPTOACTIVOS

Como de forma acertada refiere PRADO SALDARRIAGA, el problema dogmático en nuestra legislación penal contra el blanqueo de capitales en relación con los criptoactivos se presenta en dos niveles[524]. Primero, en establecer si los criptoactivos son un tipo de activo y por tanto pueden ser instrumentalizados en la configuración de típica de las tipologías previstas en la sistemática de los artículos 1, 2 y 3 del Decreto Legislativo N.° 1106[525]. El segundo aspecto está circunscrito a la flexibilidad típica, es decir, al juicio de tipicidad en relación con dichas tipologías[526].

Con relación a la primera interrogante, tal como lo explicamos en el punto VII del presente capítulo, el Banco Central de Reserva del Perú ya emitió un pronunciamiento en que señala que los criptoactivos son "activos digitales no regulados, que no tienen la condición de moneda de curso legal ni son respaldadas por bancos centrales. Asimismo, no cumplen plenamente las funciones del dinero como medio de cambio, unidad de cuenta y reserva de valor"[527]. A partir de esta definición otorgada por el ente regulador, podemos afirmar, de forma positiva, que sí estamos ante un activo digital y que este sí puede someterse a un juicio de subsunción, como parte de los elementos normativos del tipo penal de blanqueo.

Respecto a la segunda interrogante, en relación con la configuración típica del delito de blanqueo en el Perú. Tampoco vemos ningún problema de orden dogmático en la instrumentalización de los criptoactivos como parte de los elementos normativos de las conductas típicas descritas en los artículos 1, 2 y 3, si tenemos en cuenta que hoy por hoy las transacciones se realizan a través del ciberespacio, para adquirir, convertir, transferir, tener, ocultar, criptoactivos

---

[524] PRADO SALDARRIAGA, Víctor, "Lavado de Activos en el Perú…, *op. cit.,* p. 174.

[525] *Ibid.,* p. 174.

[526] *Idem*.

[527] BANCO CENTRAL DE RESERVA, "Riesgos de las criptomonedas", *op. cit.*

que tienen un origen ilícito en una actividad criminal, conductas que perfectamente se pueden calzar en las tipologías del citado Decreto Legislativo N.° 1106. Se trata, simplemente, de construir una interpretación funcional o normativa de dicho *modus operandi* y de su conducción y eficacia para la realización de dichas conductas. Como ya lo explicado en el punto XI, el proceso de blanqueo de capitales pasa por tres fases, es decir, la *colocación*, *ensombrecimiento* y *consolidación*, etapas que se pueden perfeccionar mediante la utilización de criptoactivos.

1. Los actos de conversión y transferencia

El artículo 1 del Decreto Legislativo N.° 1106 sanciona al que "convierte o transfiere dinero, bienes, efectos o ganancias cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa". Se entiende por conversión "toda colocación de bienes o capitales, mientras que en sentido restringido es la operación económica que consiste en colocar bienes y capitales con el fin de lograr un determinado beneficio económico"[528]. En la conversión no se requiere que todos activos o capitales que se están colocando en el sistema financiero sean de procedencia ilícita, ya que, sin ningún cuestionamiento de orden jurídico, estos pueden mezclarse con activos de origen lícito[529]. En el caso concreto de los criptoactivos, los actos de conversión involucran todas las formas posibles de colocación o movilización primaria de dinero líquido para la adquisición de criptoactivos, ya sea mediante intercambiadores, Cajeros atm, comercialización directa, P2P, etc. Así como ya habíamos hecho referencia, en la fase de colocación, al agente del delito de blanqueo. Cuando nos referimos a actos de transferencia de activos obtenidos ilícitamente, el agente transfiere o traspasa los activos cuya procedencia ilícita

[528] GÁLVEZ VILLEGAS, Tomas, *El delito de lavado de activos*, Lima: Editorial Pacífico, 2014, p. 168.

[529] *Ibid.,* p. 168.

conoce o debía presumir a otras personas naturales o jurídicas[530]. Mediante esta modalidad, el agente o lavador de criptoactivos busca hacer la mayor cantidad de transacciones con la finalidad de poder borrar cualquier evidencia, ya sea de forma directa mediante el P2P, sin necesidad de salir del protocolo del criptoactivo que haya elegido o a través de los intercambiadores.

2. Actos de ocultamiento y tenencia

El artículo 2 establece: "El que adquiere, utiliza, posee, guarda, administra, custodia, recibe, oculta o mantiene en su poder dinero, bienes, efectos o ganancias, cuyo origen ilícito conoce o debía presumir, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa". Los actos de ocultamiento y tenencia son aquellos que representan en la legislación penal a la fase final del proceso de lavado de activos. Esto es, la etapa que conocemos como de integración[531]. En esta fase, los criptoactivos ya han sido maculados, integrándose al sistema económico, como dinero de curso legal, completándose de esta forma el proceso de lavado, sin que este deje rastros o huellas que puedan presumir su ilicitud. El legislador en el tipo penal referido a los actos de ocultamiento y tenencia establece, dentro de los elementos normativos del tipo, los verbos rectores tales como "adquiere, utiliza, guarda, administra, custodia, recibe, oculta o mantiene"[532].

---

[530] SALAS BETETA, Christian, "El delito de lavado de activos y su dificultad probatoria en el CPP de 2004. Comentarios al Decreto Legislativo N.° 1106", en *Gaceta Penal & Procesal Penal*, n.º 35, mayo del 2012, Lima, p. 23.

[531] PRADO SALDARRIAGA, Roberto, *Lavado de activos…, op. cit.*, p. 146.

[532] Artículo 2 del Decreto Legislativo N.º 1106.

3. Actos de transporte, traslado, ingreso o salida por territorio nacional de dinero o títulos valores de origen ilícito

El artículo 3 sanciona al "que transporta o traslada consigo o por cualquier medio dentro del territorio nacional dinero en efectivo o instrumentos financieros negociables emitidos *al portador* cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso; o hace ingresar o salir del país consigo o por cualquier medio tales bienes, cuyo origen ilícito conoce o debía presumir, con igual finalidad, será reprimido con pena privativa de libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa". El tipo penal sanciona como figura típica el desplazamiento dentro del territorio nacional de dinero en efectivo o títulos valores de origen ilícito. La conducta se configura con el transporte, traslado, ingreso o salida de bienes muebles de origen delictivo[533]. El tipo penal no tiene como finalidad el sancionar actos de conversión o transferencia, ya que dichas conductas están debidamente reguladas en los artículos 1 y 2 de Decreto Legislativo N.° 1106, lo que se reprime es el acto de desplazar activos dentro del territorio nacional o sacarlos afuera de este. En relación con el desplazamiento de criptoactivos, hablamos de un desplazamiento material, que puede dar en cualquiera de los distintos dispositivos descritos en el punto 3 del capítulo III, es decir, monederos físicos o de papel, que contienen criptoactivos, como son un *pendrive*, computadora o incluso mediante aplicativo de un teléfono móvil.

[533] GARCÍA CAVERO, Percy, *El delito de lavado de activos, op. cit.,* pp. 91-92.

X. DECOMISO E INCAUTACIÓN DE CRIPTOACTIVOS

En los últimos años, la institución jurídica del decomiso ha significado, como de forma acertada señala ANZOLA, la piedra angular en la recuperación de activos provenientes del crimen organizado transfronterizo[534]. En el caso de los ordenamientos jurídicos sustantivos del Perú[535] y España[536], la institución jurídica del decomiso opera como una consecuencia accesoria del delito impuesta en la sentencia. Una vez que se ha finiquitado con el proceso penal, el decomiso puede recaer sobre los instrumentos, objetos y efectos del delito[537]. Es importante señalar que el decomiso no opera en todos los casos, ya que su aplicabilidad está sujeta a un control jurisdiccional, en la cual se debe medir la peligrosidad de los instrumentos frente reutilización en la comisión de un delito.

En relación con el decomiso de criptoactivos como instrumento del delito de blanqueo de capitales, surgen varias interrogantes que se encuentran justificadas en la propia naturaleza tecnológica y funcionamiento de los activos virtuales. Como ya hemos explicado en el punto VII del presente capítulo, los criptoactivos sí pueden ser objeto del delito de blanqueo de capitales, por ende

---

[534] ANZOLA, Ayelén, "La ejecución de las resoluciones de decomiso de activos virtuales en España", en *Revista Procesal,* n.° 57, 2022, p. 2.

[535] El artículo 102 del Código Penal del Perú regula el decomiso de bienes provenientes del delito de la siguiente forma: "el juez, siempre que no proceda el proceso autónomo de extinción de dominio, resuelve el decomiso de los instrumentos con que se hubiere ejecutado el delito, aun cuando pertenezcan a terceros, salvo cuando estos no hayan prestado su consentimiento para su utilización. Los objetos del delito son decomisados cuando, atendiendo a su naturaleza, no corresponda su entrega o devolución. Asimismo, dispone el decomiso de los efectos o ganancias del delito, cualesquiera sean las transformaciones que estos hubieren podido experimentar. El decomiso determina el traslado de dichos bienes a la esfera de titularidad del Estado. El juez también dispone el decomiso de los bienes intrínsecamente delictivos, los que serán destruidos. Cuando los efectos o ganancias del delito se hayan mezclado con bienes de procedencia lícita, procede el decomiso hasta el valor estimado de los bienes ilícitos mezclados, salvo que los primeros hubiesen sido utilizados como medios o instrumentos para ocultar o convertir los bienes de ilícita procedencia, en cuyo caso procederá el decomiso de ambos tipos de bienes. Si no fuera posible el decomiso de los efectos o ganancias del delito porque han sido ocultados, destruidos, consumidos, transferidos a tercero de buena fe y a título oneroso o por cualquier otra razón análoga, el juez dispone el decomiso de los bienes o activos de titularidad del responsable o eventual tercero por un monto equivalente al valor de dichos efectos y ganancias".

[536] ANZOLA, Ayelén, *op. cit.,* p. 2.

[537] GARCÍA CAVERO, P., "El decomiso de bienes relacionados con el delito en la legislación penal peruana", en *Derecho PUCP*, n.º 1, 2018, p. 115.

también son susceptibles de aplicárseles medidas de coerción reales, para su aseguramiento, así como la consecuencia accesoria del decomiso, en el entendido de que estos activos virtuales son bienes, efectos o ganancias del delito o cualquier transformación que estos hayan podido experimentar.

Sin embargo, en el plano pragmático, se presentan varias dificultades de orden operativo. La efectividad del decomiso está supeditada a una acuciosa investigación patrimonial en el marco de un proceso penal, es decir, logrando un correcto aseguramiento de los bienes, efectos o ganancias del delito que se esté juzgando[538]. En el caso de la recuperación de activos tradicionales, tenemos que esta se da en cuatro fases: 1) localización de los bienes de origen ilícito, 2) el embargo o incautación cautelar, 3) el decomiso, y 4) la compensación de la víctima. Etapas que perfectamente se puedan extrapolar a la recuperación de criptoactivos, como veremos.

1. Fase de localización

No cabe duda de que la localización de criptoactivos es uno de los mayores desafíos a los que se enfrentan los investigadores, al momento de establecer quién es el propietario real de un criptoactivo. El primer problema a resolver es en determinar quién es el titular de la denominada billetera o (*wallet*), en la que se almacenan los criptoactivos, ya que puede pertenecer a una persona jurídica o en su defecto a una persona natural[539]. Una de las mayores dificultades que se afrontan al momento de la trazabilidad de la detección de operaciones en criptoactivos no está vinculada a su anonimato o pseudoanonimato, sino el mayor problema se da al no existir un organismo central que las supervise frente a cualquier contingencia o irregularidad[540].

---

[538] ANZOLA, Ayelén, *op. cit.,* p. 13.

[539] NAVAS BLÁNQUEZ, JUAN JOSÉ, "Embargo y decomiso de criptomonedas en el Espacio Judicial Europeo", en *Revista de Estudios Europeos*, n.º extraordinario monográfico 1, Ediciones Universidad de Valladolid, 2023, p. 367.

[540] *Ibid.,* p. 367.

2. La clave pública

Otro de los problemas tiene relación directa con la averiguación de la clave pública. Nos referimos a dos sistemas de claves que son las siguientes: la clave pública, la cual permite recibir transacciones, mientras que la clave privada es necesaria para enviarlas. El uso de dos claves diferentes (una pública y otra privada) es lo que se conoce como la criptografía asimétrica, que es un aspecto fundamental de la cadena de bloques. Las dos claves están conectadas entre sí en términos matemáticos[541].

Las claves públicas son comparables a los números de cuenta bancaria, conformada por un conjunto de números y letras generados aleatoriamente que representan un tipo de número único similar al número de una cuenta bancaria y pueden ser compartidos libremente con todos, y cualquiera puede enviarles transacciones. Las claves privadas, por el contrario, deben mantenerse privadas, tal y como su nombre indica; existe una total discrecionalidad por parte del propietario del usuario, de mantener en secreto la clave, ya que de ello depende en última instancia que se pueda acceder a esa billetera[542].

Ejemplo: la primera dirección de *bitcoin* de la historia: **1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa**.

Una vez obtenida la clave pública, el siguiente paso en las pesquisas realizadas por los investigadores apunta a las personas jurídicas de proveedores de servicios de monederos electrónicos para criptoactivos, que a su vez pueden ser de dos tipos: *intercambiadores descentralizados* y *centralizados.* Los primeros funcionan de forma automatizada mediante contratos inteligentes o *smart contracts* firmados por las partes y registrados en la *blockchain.* En este tipo

[541] BITPANDA, "¿Qué son las claves públicas, las claves privadas y las direcciones de monedero?". Disponible en: <https://www.bitpanda.com/academy/es/lecciones/que-son-las-claves-publicas-las-claves-privadas-y-las-direcciones-de-monedero/>.

[542] BITPANDA, *op. cit.*

intercambiador, la problemática en la identificación se suscita a partir de la dificultad de conocer la identidad del sujeto firmante, ya que la operación se ejecuta mediante el sistema P2P o red entre pares, por lo que en estos casos la principal vía de averiguación será el IP desde el ordenador en el que se ha autorizado la transacción[543].

En esa línea preventiva contra el blanqueo de capitales, es que la Unión Europea, mediante la Directiva (UE) 2018/843, modifica la Directiva (UE) 2015/849, incorporando como sujetos obligados a los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias y a los proveedores de servicios de custodia de monederos electrónicos. Con lo cual, estas personas jurídicas están obligados bajo este marco legal a realizar una debida diligencia en identificar a todas aquellas personas físicas y jurídicas que se dediquen a este rubro. En el derecho comparado español, esta directiva ha sido objeto de transposición al ordenamiento jurídico español; mediante el Real Decreto 7/2021 se incorporó al artículo 1 de la Ley 10/2010 del 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, las siguientes definiciones:

> 5. Se entenderá por moneda virtual aquella representación digital de valor no emitida ni garantizada por un banco central o autoridad pública, no necesariamente asociada a una moneda legalmente establecida y que no posee estatuto jurídico de moneda o dinero, pero que es aceptada como medio de cambio y puede ser transferida, almacenada o negociada electrónicamente[544].
>
> 6. Se entenderá por cambio de moneda virtual por moneda fiduciaria la compra y venta de monedas virtuales mediante la entrega o recepción de euros o cualquier otra moneda extranjera de curso legal o dinero electrónico aceptado como medio de pago en el país en el que haya sido emitido[545].

---

[543] NAVAS BLÁNQUEZ, *op. cit.,* p. 369.

[544] Artículo 1, inciso 5, de la Ley 10/2010, del 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

[545] Artículo 1, inciso 6, de la Ley 10/2010, del 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

> 7. Se entenderá por proveedores de servicios de custodia de monederos electrónicos aquellas personas físicas o entidades que prestan servicios de salvaguardia o custodia de claves criptográficas privadas en nombre de sus clientes para la tenencia, el almacenamiento y la transferencia de monedas virtuales[546].

Sin embargo, si bien estas reformas legislativas suponen un gran avance regulatorio en materia de represión del delito de blanqueo de capitales mediante criptoactivos, las mismas que deberían ser objeto de réplica por parte de otros ordenamientos jurídicos. Aún quedan muchas aristas por resolver como, por señalar algunos, las referentes la titularidad real del propietario del monedero electrónico o la ausencia de registro dentro de territorio nacional de dichas personas jurídicas[547], situaciones que generan grandes escollos legales que dificultan la detección de los criptoactivos para su eventual decomiso.

3. La clave privada

Las claves privadas, muy por el contrario, son aquellas que escapan del dominio público, y se encuentran encriptadas por una clave compuesta de palabras que solo es de conocimiento por parte del titular de la misma, es decir, depende única exclusivamente del titular el mantener en secreto la clave, ya que de ello depende en última instancia que se pueda acceder a esa billetera[548]. Bajo esta hipótesis, solo quedaría el aplicar técnicas de investigación, como son la videovigilancia, allanamiento, incautación de bienes, documentos bajo el amparo de las restricciones de derechos fundamentales, con el objetivo de la búsqueda de pruebas que permitan obtener la clave privada que da acceso a los criptoactivos, para de esta forma lograr los fines del esclarecimiento del proceso penal.

---

[546] Artículo 1, inciso 7, de la Ley 10/2010, del 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

[547] NAVAS BLÁNQUEZ, *op. cit.,* p. 372.

[548] *Ibid.,* p. 373.

XI. CASOS INTERNACIONALES RELEVANTES EN MATERIA PENAL SOBRE CRIPTOACTIVOS

1. *United States of America v. Ross William Ulbricht,* No. 15-1815-cr (2d Cir. May 31, 2017)

El caso de la Ruta de la Seda o *Silk Road*, involucra la comisión delictiva de varios ciberdelitos vinculados con el crimen organizado por parte de su creador de Ross William Ulbricht. *Silk Road* era un cibermercado masivo en línea que vendía bienes y servicios ilícitos, en particular drogas. *Silk Road* se creó en enero de 2011 y funcionaba hasta que las autoridades policiales capturaron a su creador y administrador Ross Ulbricht en octubre de 2013. Se trataba de un mercado criminal en línea con la intención de facilitar a sus usuarios la compra y venta de bienes y servicios ilegales de forma anónima y bajo el radar de las fuerzas del orden[549].

El acusado tenía como objetivo anonimizar las transacciones en *Silk Road* a través de la red The Onion Router o Tor, una red especial de computadoras en Internet, distribuida en todo el mundo, diseñada para ocultar las verdaderas direcciones IP y, por lo tanto, identidades de sus usuarios; la particularidad de esta plataforma es que operaba mediante un sistema de pago basado en *bitcoin* que ocultaba las identidades y ubicaciones de los usuarios. El autor supervisaba todos los aspectos de *Silk Road*, y manejaba un equipo de administradores en línea pagados, junto con programadores de computadoras que ayudaban con la operación diaria del sitio. Las ganancias ilícitas obtenidas por las ventas de bienes y servicios ilegales ascendían a un valor de más de 13 millones de dólares.

[549] UNITED NATIONS OFFICE ON DRUGS AND CRIME, *United States of America v. Ross William Ulbricht*, No. 15-1815-cr (2d Cir. May 31, 2017). Disponible en: <https://sherloc.unodc.org/cld/en/case-law-doc/cybercrimecrimetype/usa/2017/united_states_of_america_v._ross_william_ulbricht_no._15-1815-cr_2d_cir._may_31_2017.html>.

El gobierno de EE. UU se enteró *de Silk Road* en el año 2011, luego de interceptar un paquete de drogas en el aeropuerto O'Hare de Chicago, e inició una investigación sobre el mercado en línea. Los agentes descubrieron que *Silk Road* estaba dirigido y administrado por alguien con el nombre de pantalla de Dread Pirate Roberts (DPR). En el año 2012, los agentes investigaron a varias personas que se creía eran Dread Pirate Roberts, incluidos Ross Ulbricht, Anand Athavale y Mark Karpeles. En última instancia, Ulbricht se convirtió en el principal sospechoso en el año 2013 después de una serie de órdenes de actos de investigación que llevaron a los agentes del orden público de EE. UU. a recopilar pruebas en forma de IP datos de dirección de la red inalámbrica doméstica de Ulbricht. La evidencia adicional provino de investigaciones encubiertas, en las que los agentes de la ley se hicieron cargo de las cuentas de los administradores de *Silk Road* de bajo nivel e interactuaron con D.P.R. en línea, en un intento de exponer a Ulbricht.

Ross Ulbricht fue acusado y condenado por distribuir narcóticos a través de Internet, conspirar para distribuir narcóticos, participar en una empresa delictiva continua, conspirar para cometer piratería informática, conspirar para traficar con documentos de identidad falsos y conspirar para cometer dinero lavado, Además, fue acusado de solicitar seis asesinatos a sueldo en relación con la operación del sitio, aunque no hubo evidencia de que estos asesinatos realmente se llevaran a cabo.

La importancia casuística de este caso radica en el componente transfronterizo de las operaciones en línea de *Silk Road*. Mientras estuvo en funcionamiento, *Silk Road* fue utilizada por miles de traficantes de drogas y otros vendedores ilegales para distribuir cientos de kilogramos de drogas ilegales y otros bienes y servicios ilegales a más de 100000 compradores, y para blanquear cientos de millones de dólares derivados de estas transacciones ilegales. Solo entre 2011 y 2013, el gobierno de EE. UU. estimó que los compradores que operaban en la Ruta de la Seda vendieron aproximadamente USD 183 millones en bienes y servicios ilegales.

La mayoría de los artículos a la venta eran drogas ilícitas, que se publicitaban abiertamente como tales en el sitio. Al 23 de septiembre de 2013, *Silk Road* contenía casi 13.000 listados de sustancias controladas, incluidas en categorías como “Cannabis”, “Disociativos”, “Éxtasis”, “Intoxicantes”, “Opioides”, “Precursores”, “Prescripción”, “Psicodélicos” y “Estimulantes”. El sitio web también proporcionó servicios de piratería, *software* malicioso y ofertas para producir documentos de identificación falsos. Desde noviembre de 2011 hasta septiembre de 2013, los agentes encargados de hacer cumplir la ley realizaron más de 60 compras individuales encubiertas de sustancias controladas a vendedores de la Ruta de la Seda, lo que convierte el caso en un ejemplo significativo de técnicas especiales de investigación en virtud del artículo 20 de las Convenciones contra el Crimen Organizado Transnacional y sus Protocolos.

Se utilizaron agentes encubiertos, los mismos que compraron varias drogas ilegales a los vendedores ubicados en más de diez países diferentes, incluidos Austria, Canadá, Francia, Alemania, Irlanda, Italia, Países Bajos, España, Reino Unido, Estados Unidos, lo que demuestra el alcance internacional de las operaciones de *Silk Road* y la naturaleza inherentemente transnacional del ciberdelito.

La sentencia se emitió el 29 de mayo del 2015, interviniendo los magistrados Mallory McGee, Lindsay Lerner y Rivka Mandel, del John Jay College of Criminal Justice, City University of New York.

El Tribunal de Distrito tuvo que abordar las siguientes cuestiones jurídicas:

- Si el acuerdo requerido para respaldar los cargos de conspiración podría establecerse cuando las partes solo interactuaron a través de transacciones automatizadas y anónimas.

- Si se puede demostrar que los compradores y vendedores en un mercado en línea actúan de manera concertada bajo la dirección de una persona en un puesto de gestión.

- Si las transacciones financieras se pueden realizar con *bitcoins* y, por lo tanto, se pueden utilizar en el blanqueo de dinero.

El Tribunal de Distrito razonó que los acuerdos de conspiración no requieren necesariamente un acuerdo expreso con todos los detalles de la conspiración; basta con ponerse de acuerdo sobre el objetivo o el fin ilícito de la conspiración. En el presente caso, la fiscalía pudo demostrar que Ulbricht recaudó decenas de millones de dólares en comisiones por transacciones de drogas ilícitas, así como transacciones por *software* informático malicioso y documentos de identificación falsos. El Tribunal determinó que Ulbricht creó *Silk Road* con el propósito expreso de facilitar transacciones anónimas e ilegales, y que sin que terceros acepten usar el sitio y participar en esas transacciones ilegales, *Silk Road* no tendría ningún uso. El hecho de que estos acuerdos ocurrieran en la computadora no significa que no pueda ocurrir una reunión de mentes: las acciones realizadas por la computadora son realizadas por un ser humano. Por lo tanto, el Tribunal de Distrito determinó que el acuerdo requerido podría establecerse en casos de transacciones automatizadas y anónimas.

Del mismo modo, el Tribunal sostuvo que no se requería que Ulbricht participara en una forma particular de conducta con cada uno de aquellos con los que actuaba en concierto en su continua empresa criminal. Fue suficiente para mostrar que miles de traficantes de drogas realizaron transacciones en la Ruta de la Seda con miles de compradores. Además, Ulbricht no solo diseñó y creó la Ruta de la Seda, sino que también controló las operaciones diarias, incluida la fijación de reglas para compradores y vendedores, la determinación de las tasas de comisión y la vigilancia de las infracciones de las reglas, etc.;

En lo que se refiere a *bitcoins*, el Tribunal estableció que el único valor de *bitcoin* es como un medio de pago para pagar por cosas. El *bitcoin* puede usarse directamente para pagar cosas, o puede convertirse en moneda y luego usarse para pagar cosas. Los bitcoins se diseñaron específicamente para proteger las ganancias del descubrimiento por parte de terceros de su origen ilegal. Si bien es posible que *bitcoin* no se haya incluido en las definiciones tradicionales de "moneda" o "transacciones financieras", el Tribunal sostuvo que son

funcionalmente equivalentes y, por lo tanto, pueden utilizarse para blanquear dinero. Por las razones anteriores, el Tribunal condenó al acusado por los siete cargos no violentos y lo condenó a cadena perpetua, la misma que fue objeto de apelación, y rechazada por parte de la Corte de Apelaciones de Estados Unidos.

2. STS 326/2019 - Tribunal Supremo en lo Penal

Se trata de la sentencia de fecha 20 de junio del 2019, en la que se resolvió el Recurso de Casación N.° 998/2018, emitida por la Sala Suprema en lo Penal de Madrid integrada por los magistrados D. Pablo Llerena Conde (ponente) y los magistrados D. Julián Sánchez Melgar, D. Francisco Monterde Ferrer, D. Pablo Llarena Conde, D.ª Susana Polo García, D.ª Carmen Lamela Diaz.

En relación con la sentencia, podemos señalar que este fallo judicial marca un hito en materia jurisprudencial de criptoactivos, ya que establece por primera vez lineamientos doctrinales que nunca habían sido tocados a nivel judicial en el sistema de justicia español y del mundo.

Los hechos se circunscriben a una estafa sistemática a través de una empresa que suscribió diversos contratos de trading de alta frecuencia *(high-frequency trading*), en virtud de los cuales se comprometía a gestionar los *bitcoins* que le fueron entregados en depósito por cada uno de los contratantes, debiendo reinvertir los eventuales dividendos y entregar al vencimiento del contrato las ganancias obtenidas, a cambio de una comisión que retendría.

Un primer criterio, resaltado por parte de la sala en la sentencia, es en relación con el dinero. Sobre el particular, la Sala establece lo siguiente: “Aun cuando la jurisprudencia de esta Sala ha expresado la obligación de restituir cualquier bien objeto del delito, incluso el dinero, los acusados no fueron despojados de bitcoins que deban serles retornados, sino que el acto de disposición patrimonial que debe resarcirse se materializó sobre el dinero en euros que, por el engaño inherente a la estafa, entregaron al acusado para invertir en activos de este tipo.

Por otro lado, tampoco el denominado bitcoin es algo susceptible de retorno, puesto que no se trata de un objeto material, ni tiene la consideración legal de dinero"[550]. Bajo este análisis interpretativo, la Sala deja sentado que el bitcoin no es una moneda de curso legal y, por ende, el resarcimiento del objeto del delito debe ser en dinero de curso legal.

Un segundo criterio que establece la Sala es en relación con establecer una definición legal de bitcoin: "El bitcoin no es sino una unidad de cuenta de la red del mismo nombre. A partir de un libro de cuentas público y distribuido, donde se almacenan todas las transacciones de manera permanente en una base de datos denominada Blockchain, se crearon 21 millones de estas unidades, que se comercializan de manera divisible a través de una red informática verificada"[551].

Como tercer criterio, la Sala Penal, en aras de reforzar el concepto establecido, decide adentrarse en el fenómeno cripto y explicar la tecnología sobre la que funciona el criptoactivo *bitcoin,* estableciendo que "el bitcoin no es sino un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica denominada bitcoin, cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta que de estas unidades se realiza a través de las plataformas de trading bitcoin"[552].

[550] Véase el fundamento tercero de la STS 326/2019 de fecha 20 de junio.

[551] Véase el fundamento tercero de la STS 326/2019 de fecha 20 de junio.

[552] Véase el fundamento tercero de la STS 326/2019 de fecha 20 de junio.

CAPÍTULO IV
PREVENCIÓN DE LAVADO DE ACTIVOS Y CRIPTOACTIVOS

I. SISTEMA DE GESTIÓN DE PREVENCIÓN DE LAVADO DE ACTIVOS PARA PLATAFORMAS DE INTERCAMBIO DE CRIPTOACTIVOS

Antes de adentrarnos en establecer y desarrollar los pilares o cimientos sobre los que debe descansar un sistema de prevención de lavado de activos, debemos establecer las características de las personas jurídicas que se dedican al intercambio de monedas virtuales. Actualmente, en el mundo existen más de 229 intercambiadores de criptoactivos, a los que se le conoce como *exchange.*

Los *exchanges* son personas jurídicas que operan mediante una plataforma virtual y se dedican al intercambio de criptoactivos. Dentro de sus servicios, está el otorgarles a sus usuarios la posibilidad de comprar, vender y custodiar activos virtuales. Algunas de estas compañías permiten realizar operaciones más complejas como el *staking*, *P2P*, *bots de trading*, *farming swap*, préstamos, etc. Con un esquema muy similar al de una plataforma de trading tradicional, los usuarios ingresan los montos con lo que van a operar y el intercambiador ejecuta las órdenes de forma automatizada, cobrando comisiones por todas las operaciones que se ejecutan. Las formas de poder comprar al intercambiador después de registrarse son diversas, desde hacer el dinero en efectivo (*cash in*) del dinero mediante una tarjeta de crédito, billetera electrónica, transferencia, etc. El dinero por cobrar (*cash out*) también se hace a través de diversas modalidades, P2P o transferencia bancaria a diversos bancos vinculados al intercambiador.

Si bien en la mayoría de las jurisdicciones de Latinoamérica los *exchange* no cuentan con una regulación específica, al día de hoy se está dando un proceso de autorregulación propia por parte de las personas jurídicas que otorgan este tipo de servicio, más aún sí tenemos en cuenta la evolución dogmática y normativa que se vienen dando en materia de responsabilidad penal de personas jurídicas.

Como veremos, los pilares clásicos sobre los que se realiza la elaboración de un sistema de cumplimiento contra el lavado de activos, el cual permite la atenuación o exención de responsabilidad penal de la persona jurídica, se pueden aplicar perfectamente para los intercambiadores o *exchange* de criptoactivos, con algunas particularidades que son inherentes a la propia tecnología con la que funcionan los criptoactivos. En el plano jurídico normativo, nos referimos a un conjunto de normas que surgen desde el derecho administrativo regulatorio y sancionador. En el caso del Perú, esta normativa se materializa en la Ley N.º 27693 de fecha 12 de abril del 2002, Ley que crea la Unidad de Inteligencia Financiera (UIF) y sus modificatorias, y su Reglamento de fecha 6 de octubre de 2017, aprobado mediante Decreto Supremo N.º 020-2017-JUS y recientemente la Resolución SBS N.° 02351-2023.

Las persona naturales o jurídicas están obligadas a informar a la UIF-Perú, según el artículo 3 de la Ley N.º 29038, incorporado por la Superintendencia de Banca y Seguros conforme a las facultades conferidas a través del numeral 3.4 del artículo 3 de la Ley N.º 29038, lo que incluye a las sucursales en el Perú de las personas jurídicas extranjeras que son sujetos obligados. De igual forma, la Ley N.° 30424, que regula la responsabilidad administrativa de las personas jurídicas por la comisión del delito de lavado de activos entre otro más, establece como eximente de responsabilidad penal a aquellas personas jurídicas que hayan implementado con anterioridad a la comisión del hecho delictivo un programa de cumplimiento adecuado a su naturaleza, riesgos, necesidades y características, consistente en medidas de vigilancia y control idóneas para prevenir el delito o para reducir significativamente el riesgo de su comisión.

Debemos precisar que si bien estas normas desarrollan los elementos sobre los que se debe elaborar un programa de cumplimiento antilavado tradicional, no fueron pensadas en personas jurídicas que se dedican al rubro de intercambiadores de monedas virtuales, por lo que para la elaboración del mismo debemos recurrir a normas de *soft law*, que han sido proporcionadas por el Grupo de Acción Financiera Internacional, a través de sus distintas guías, informes donde se establecen los criterios a tomar en cuenta en la creación de

un sistema de prevención de lavado para intercambiadores de criptoactivos, como veremos.

II. RECOMENDACIONES DEL GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE PREVENCIÓN DE LAVADO DE ACTIVOS PARA INTERCAMBIADORES DE CRIPTOACTIVOS

Los criptoactivos empiezan a llamar la atención del GAFI a partir del año 2014. No cabe duda que el hecho de que estas monedas virtuales pudieran ser intercambiadas por dinero fíat, generó una particular atención por parte de la entidad mencionada, más aún si hablamos de una tecnología caracterizada principalmente por su operatividad mediante el anonimato de las transacciones realizadas dentro del mismo protocolo. En ese sentido, los informes del GAFI desarrollan los riesgos potenciales de los criptoactivos frente al lavado de activos y la financiación al terrorismo. Asimismo, establecen cuáles son los criterios operativos que deben tener en cuenta los operadores de activos virtuales frente a las alertas de operaciones sospechosas generadas mediante la adquisición de criptoactivos. Nos hemos permitido, para un mejor entendimiento de la problemática descrita, desarrollar de forma cronológica los distintos pronunciamientos del GAFI frente a los riesgos potenciales del lavado de activos mediante el uso de criptoactivos, para luego adentrarnos en lo que abarcaría un sistema de prevención de lavado de activos y criptoactivos.

1. *Monedas virtuales: Definiciones claves y riesgos potenciales de LA/FT*

En el 2014 el Grupo de Acción Financiera Internacional emitió un informe denominado *Monedas virtuales: Definiciones claves y riesgos potenciales de la/ft*[553], en el que se hacía especial referencia al poder cambiario[554] de las monedas virtuales convertibles, y cómo estas pueden ser canjeadas por dinero real o por otras monedas virtuales y ser potencialmente vulnerables a abusos para el blanqueo de dinero y financiación del terrorismo. El informe hace referencia en primer término al anonimato con el que cuentan las monedas virtuales, protección con la cual no cuentan los métodos de pago tradicionales. De otro lado, refiere que "las monedas virtuales pueden ser intercambiadas en Internet, y se caracterizan generalmente por las relaciones entre clientes no presenciales y por permitir la financiación anónima (uso de efectivo o de terceros a través de intercambiadores virtuales que no identifiquen correctamente la fuente de financiación). También pueden permitir las transferencias anónimas, si el remitente y el destinatario no se identifican adecuadamente"[555].

De igual forma, el informe hace referencia de forma genérica a los sistemas descentralizados, ya que son especialmente vulnerables ante los riesgos del anonimato. Otro aspecto muy importante al que hace referencia el documento es con respecto a la falta de un organismo de control central o *software* antilavado de activos para monitorear e identificar transacciones sospechosas. En el entendido de que no se puede monitorear internamente el protocolo de la moneda virtual y eso dificulta la persecución e investigación penal del delito de blanqueo de dinero por parte de las autoridades, a pesar de que existe la

[553] En su parte introductoria el informe refiere lo siguiente: "Las monedas virtuales descentralizadas matemáticamente fundamentadas—especialmente Bitcoin2 — han ido ganado cada vez más atención; han surgido dos tendencias argumentativas populares al respecto: (1) las monedas virtuales son el futuro de los sistemas de pago; y (2) las monedas virtuales proporcionan una nueva y poderosa herramienta para que criminales, financiadores del terrorismo y otros evasores de sanciones puedan mover y almacenar fondos ilícitos, fuera del alcance de las fuerzas del orden y otras autoridades". Véase la introducción del informe GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Monedas virtuales: Definiciones claves y riesgos potenciales de LA/FT,* Unión Europea, 2014.

[554] PRADO SALDARRIAGA, Víctor, "Lavado de Activos en el Perú…, *op. cit.,* p. 167.

[555] GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Monedas virtuales…, op. cit.,* p. 9.

posibilidad de indagar preliminarmente a nivel de los intercambiadores o *exchangers* de criptoactivos.

De otro lado, se resalta el aspecto transnacional de alcance global de la moneda virtual; esto hace que se incremente de igual forma sus riesgos potenciales de LA/FT. Se puede acceder desde cualquier parte a los sistemas de moneda virtual a través de Internet, y se pueden utilizar para hacer pagos transfronterizos y transferencias de fondos de forma instantánea[556].

2. Directrices para un Enfoque Basado en Riesgo. Monedas Virtuales

En el año 2015, el GAFI emite un segundo documento en que se establecen las *Directrices para un Enfoque Basado en Riesgo. Monedas Virtuales*, en relación con el esquema de pagos de monedas virtuales. Se parte de un enfoque gradual, con especial énfasis en los cambiadores de moneda virtual convertible[557]. Estas directrices pretenden explicar la aplicación del enfoque basado en riesgo a las medidas de prevención de blanqueo de capitales y financiamiento al terrorismo, en el contexto del uso monedas virtuales o criptoactivos, es decir, partir de la identificación de las entidades que participan en productos de servicios de pago de moneda virtual. Las directrices incorporan un glosario de términos dentro del marco conceptual clave adoptado por el GAFI en su informe primigenio de junio del 2014[558].

Dentro de sus objetivos las directrices pretenden:

- Mostrar como recomendaciones del GAFI específicas deben aplicar a cambiadores de moneda virtual convertible en el contexto de VCPPS,

---

[556] *Ibid.*

[557] GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Directrices…, op. cit.,* p. 3.

[558] *Ibid.*, p.3.

identificar medidas de ALA/CFT que podrían ser requeridas y dar ejemplos.

- Identificar los obstáculos a la aplicación de medidas atenuantes basados en la tecnología de VCPPS y/o modelos de negocio y en marcos legales heredados[559].

Las recomendaciones específicas a las que hace mención el GAFI —que deben tomar en cuenta las entidades que sirven como nodos cuando las transacciones en criptoactivos salen de la esfera del sistema financiero y esto dificulta su trazabilidad— son las siguientes:

La *recomendación n.º 1:* basada en identificar, evaluar y tomar medidas efectivas para mitigar sus riesgos de LA/FT. La *recomendación n.º 10:* la aplicación de una debida diligencia por parte de los cambiadores de monedas virtuales a sus clientes, es decir, una debida identificación mediante documentación fiables como establecer un control transaccional teniendo como umbral los 15,000 $ o euros. La *recomendación n.º 11, n.º 20 y n.º 22:* para la detección de todas aquellas transacciones sospechosas en criptoactivos que pudieran estar vinculados a una actividad criminal previa; esta identificación incluirá, identificación de los usuarios, direcciones, claves públicas, montos, fecha, tomando como ayuda a la *blockchain*. *La recomendación n.º 14:* registro y otorgación de licencias de funcionamiento de servicios de transferencias de valores. La *recomendación n.º 15:* identificar y mitigar los riesgos vinculados a uso de las nuevas tecnologías (TIC)

La *recomendación n.º 18:* la cual establece los parámetros para un sistema de prevención contra el blanqueo y el financiamiento al terrorismo. Por último, la *recomendación n.º 20:* se ciñe al reporte de operaciones sospechosas[560].

---

[559] *Ibid.,* p. 4.

[560] *Ibid.,* p. 12.

El informe también recomienda las medidas adoptadas por la organización internacional del Banco de Pagos Internacionales

> a) Imponer restricciones a las entidades reguladas para hacer frente a las monedas virtuales;
>
> b) Adoptar medidas legislativas/regulatorias, tales como la necesidad plataformas de cambio que tratan con Moneda virtual ser objeto de regulación como los remitentes de dinero, o la propuesta regulación de los intermediarios de MV en algunas jurisdicciones para fines de ALA/CFT;
>
> c) Publicar declaraciones advirtiendo a los usuarios sobre los riesgos asociados con la MV y/o clarificar la posición de las autoridades con respecto a la MV;
>
> y d) Monitorear y estudiar los acontecimientos[561].

3. *Ejercicio Bienal de Tipologías Regionales: Casos y tipologías regionales 2017-2018*

En el año 2018, como resultado de un trabajo conjunto entre el GAFILAT Y varios países miembros del GAFI, así como de la Unidad de Análisis Financiero y Económico (UAFE) del Ecuador, con la asistencia técnica de la Cooperación Alemana GIZ, se elaboró el denominado *Informe de Tipologías Regionales Gafilat 2017-2018,* que fue producto del *Ejercicio Bienal de Tipologías Regionales* del GAFILAT. Mediante la información obtenida como resultado del trabajo plasmado en el informe, se podrán diseñar mejores instrumentos de control y señales de alerta que permitan a las autoridades diseñar o ajustar mecanismos encaminados a protegerse de la posibilidad de ser utilizadas por los legitimadores de capitales o para financiar grupos terroristas o delictivos, o actividades de proliferación de armas de destrucción masiva[562].

---

[561] GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Directrices…, op. cit.,* p. 16.

[562] GRUPO DE ACCIÓN FINANCIERA DE LATINOAMÉRICA, Ejercicio Bienal de Tipologías Regionales: Casos y tipologías regionales 2017-2018, Quito, p. 3. Disponible en: <https://pplaft.cnbs.gob.hn/wp-content/uploads/2015/05/Informe-Tipologias-Regionales-GAFILAT-2018.pdf>.

En lo que se refiere al uso ilegítimo de criptoactivos, el informe desarrolla dos tipologías. La primera hace referencia al blanqueo de dinero proveniente del tráfico ilícito de drogas mediante el uso de criptomonedas, en el que los traficantes venden drogas a través de tiendas de fachada y posteriormente compran el criptoactivo *bitcoin*. El informe describe la tipología fáctica de la siguiente manera: "La persona física, registrada en la institución financiera como vendedor, pasa a mover recursos voluminosos en su cuenta corriente. Los recursos proceden de depósitos en especie procedentes de diversas localidades, así como de transferencias de personas jurídicas diversas, en particular del sector tecnológico. Casi la totalidad de los recursos recibidos se transfieren inmediatamente a las empresas intercambiadoras de bitcoin"[563].

La segunda tipología desarrollada por el informe es referida a la Pirámide Financiera o Esquema Ponzi, basado en criptoactivos. Bajo este esquema se constituye un fondo de inversión en el que se les ofrece a los inversores una rentabilidad en moneda virtual, incompatible con las ganancias de mercado. La tipología descrita es graficada por el informe de la siguiente manera: "La empresa registrada como de la rama de intermediación de y agenciamiento de servicios registrada recientemente pasa a mover recursos incompatibles con su capacidad financiera. En investigación, se verifica que sus socios, de cerca de 20 años, tendrían como últimos vínculos de empleo frentista y empaquetador, respectivamente. Los socios de la empresa de intermediación habrían creado otra empresa del ramo de portales y proveedores de servicios de internet que actuaría supuestamente como *exchanger* de moneda virtual. Ambas empresas están ubicadas en la misma dirección. Según el sitio de la empresa de intermediación, ella realizaría la gestión de un fondo de inversiones, buscando la rentabilidad en moneda virtual […]"[564].

---

[563] *Ibid.,* p. 79.

[564] *Ibid.,* p. 81.

4. Nota interpretativa de la recomendación n.° 15

En el año 2018 el GAFI inicia un proceso de actualización de sus recomendaciones y su glosario de términos, específicamente en relación con la recomendación n.° 15[565] y su nota interpretativa, ya que los Gobiernos miembros del G20, así como el sector privado, exigen una mayor claridad en lo que se refiere a activos virtuales, y cuáles deben ser los parámetros interpretativos que se deben seguir para poder abordarlos[566].

Se trata de implementar acciones concretas para gestionar y mitigar los riesgos que surjan de los activos virtuales, tomando como ejemplo lo relativo a la debida diligencia, así como regulación mediante el otorgamiento de licencias y su registro por parte del país expedidor de la misma con la finalidad de garantizar que los proveedores de servicios de activos virtuales estén regulados para propósitos ALA/CFT. Como parte de ese monitoreo se debe resaltar lo referente al reporte de operaciones sospechosas.

La nota interpretativa establece que, para la aplicación de las recomendaciones del GAFI, los países miembros deben considerar los activos virtuales como "bienes", "productos", "fondos", "fondos y otros activos" u otros activos de "valor equivalente". Los países deben aplicar las medidas pertinentes en virtud de las recomendaciones del GAFI a los activos virtuales y a los proveedores de servicios de activos virtuales (PSAV)[567].

---

[565] "Los países y las instituciones financieras deben identificar y evaluar los riesgos de lavado de activos o financiamiento del terrorismo que pudieran surgir con respecto a (a) el desarrollo de nuevos productos y nuevas prácticas comerciales, incluyendo nuevos mecanismos de envío, y (b) el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como los existentes. En el caso de las instituciones financieras, esta evaluación del riesgo debe hacerse antes del lanzamiento de los nuevos productos, prácticas comerciales o el uso de tecnologías nuevas o en desarrollo. Los países y las instituciones financieras deben tomar medidas apropiadas para administrar y mitigar esos riesgos". GRUPO DE ACCIÓN FINANCIERA DEL CARIBE, "Nota Interpretativa de la Recomendación N.° 15". Disponible en: <https://www.cfatf-gafic.org/index.php/es/documentos/gafi40-recomendaciones/421-fatf-recomendacion-15-nuevas-tecnologias>.

[566] NAVARRO CARDOSO, *op. cit.,* p. 26.

[567] GRUPO DE ACCIÓN FINANCIERA DEL CARIBE, *op. cit.*

En ese sentido, la nota interpretativa establece que los países deben identificar, evaluar y comprender los riesgos del blanqueo de dinero y financiamiento del terrorismo que surgen de las actividades de activos virtuales y las actividades u operaciones de los proveedores de servicios de activos virtuales (PSAV). Asimismo, aplicar un enfoque basado en el riesgo para garantizar que las medidas para prevenir o mitigar el lavado de activos y el financiamiento del terrorismo sean proporcionales a los riesgos identificados.

La licencia también puede requerir que los PSAV que ofrecen productos y/o servicios a los clientes en su jurisdicción o que realizan operaciones desde su jurisdicción, que tengan una licencia o estén registrados en esta jurisdicción. Por ellos, los países deben tomar medidas para identificar a las personas físicas y jurídicas que lleven a cabo actividades sin la licencia o el registro necesarios, y aplicar las sanciones apropiadas.

Un punto importante por tomar en cuenta son las medidas preventivas en las recomendaciones n.^{os} 10 al 21 del GAFI, de acuerdo con los siguientes estándares:

> R.10 – El umbral designado para transacciones ocasionales por encima del cual los PSAV deben llevar a cabo DDC es de USD/EUR 1 000.
>
> R.16 – Los países deben asegurarse de que los PSAV de origen obtengan y mantengan la información obligatoria y precisa del originante y la información obligatoria del Beneficiario sobre las transferencias de activos virtuales, envíen la información anterior al PSAV beneficiario o institución financiera (si la hubiera) de forma inmediata y segura, y la pongan a disposición de las autoridades competentes, previa solicitud. Los países deben asegurarse de que los PSAV beneficiarios obtengan y mantengan la información obligatoria del originante y la información obligatoria y precisa de los beneficiarios sobre las transferencias de activos virtuales y la pondrán a disposición de las autoridades competentes, previa solicitud. Otros requisitos de R. 16 (incluido el seguimiento de la disponibilidad de información, la adopción de medidas de congelamiento y la prohibición de las transacciones con personas y entidades designadas) se aplican sobre la misma base que se establece en la R. 16. Las mismas obligaciones se aplican a las instituciones financieras al enviar o recibir transferencias de activos virtuales en nombre de un cliente[568].

[568] *Idem.*

5. Indicadores de bandera roja de activos virtuales de lavado de dinero y financiamiento del terrorismo

En el año 2020, el GAFI emitió el informe denominado *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing,* sobre las señales de alerta de LD/FT asociados con los activos virtuales, con la finalidad de ayudar a los sujetos obligados, incluidas las instituciones financieras, las actividades y profesiones no financieras designadas y los proveedores de servicios de activos virtuales. Además, el informe también facilita, por parte de los sujetos obligados, la aplicación de un enfoque basado en riesgos para sus requisitos de debida diligencia del cliente, que requieren saber quiénes son sus clientes y los beneficiarios finales, comprender la naturaleza y el propósito de la relación comercial y comprender la fuente de los recursos[569]. El informe enumera un grupo de señales de alerta de actividades sospechosas de activos virtuales a partir de la casuística recopilada por toda la red global del GAFI desde el año 2017. El informe clasifica las tipologías de la siguiente manera:

- Múltiples transferencias inmediatas de una gran cantidad de AV a VASP en el extranjero[570].
- Múltiples AV y múltiples transferencias a VASP extranjeros[571].

---

[569] FATF REPORT, "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing", París, 14 de setiembre del 2020, p. 2.

[570] Esta modalidad se presentó en Sudáfrica. Se trata de un VASP local que presentó un ROS tras sospechas sobre la compra de grandes cantidades de AV por parte de varias personas y sus posteriores transferencias inmediatas a VASP en una jurisdicción extranjera. En varios casos, las personas compartieron la misma dirección residencial; y se accedió a la mayoría de las direcciones de AV desde la misma dirección IP, lo que indica el posible uso de "mulas" por parte de los lavadores de dinero profesionales para lavar las ganancias ilícitas. Además, se organizaron múltiples capas de los fondos fiduciarios antes de la compra de AV por las mulas. Para disfrazar el origen de los recursos, primero se depositó efectivo en varias cuentas en diferentes IF a lo largo del país. Posteriormente, esos recursos se transfirieron a varias cuentas a nombre de entidades registradas en la jurisdicción. Los pagos electrónicos se realizaron en las cuentas en cantidades menores. Después de eso, los recursos se transfirieron a otro grupo de cuentas antes de llegar a las cuentas de las mulas en los VASP locales. Los AV se compraron inmediatamente y se transfirieron a VASP extranjeros. Más de 150 personas estuvieron involucradas en este caso, responsables de transferir un total de aproximadamente USD 108 352 900 (o BTC 11,960) a múltiples cuentas de AV mantenidas por dos VASP en el extranjero. FATF REPORT, *op. cit.,* p. 5.

[571] Casuística obtenida de Corea del Sur. Una oficina de cambios local de AV informó que aproximadamente KRW 400 millones (EUR 301,170) fueron robados a víctimas de *phishing* y

- Depósito inicial inconsistente con el perfil del cliente[572].
- Transferencias realizadas en un tiempo recurrente[573].
- Uso de la dirección IP asociada con el mercado negro en la red - AlphaBay[574].
- Uso de mezcla y volteo - Helix[575]

finalmente se intercambiaron por AV como una técnica de estratificación. Lo que desencadenó el reporte fue las múltiples operaciones de alto valor transferidas a un VASP extranjero en una sola cartera. Los recursos robados en moneda fiduciaria se intercambiaron primero a tres tipos diferentes de AV y luego se depositaron en la cartera AV del sospechoso en un VASP local. Luego, el sospechoso intentó ocultar la fuente de los recursos transfiriéndolos 55 veces adicionales a través de 48 cuentas separadas en diferentes VASP locales, y luego a una cartera AV diferente ubicada en el extranjero. FATF REPORT, *op. cit.,* p. 5.

[572] En República Checa, según una investigación, el titular de la cuenta personal parecía ser una mula reclutada por criminales en una plataforma de redes sociales para ayudar a recibir pagos reclamados por productos vendidos en línea. Sin embargo, esos recursos parecían haber sido depositados por otras empresas víctimas y no eran pagos por bienes. Los recursos depositados se transfirieron inmediatamente desde la cuenta bancaria personal a través de varios pagos divididos a otra cuenta de una sociedad anónima en la República Checa, y se cambiaron a AV (Bitcoin) en varios VASP locales. Estos VASP se retiraron inmediatamente de la cuenta. Además de presentar un ROS, el banco también suspendió las transferencias sospechosas, lo que hizo posible la posterior incautación de recursos. El VASP local también notó irregularidades en los recursos recibidos y brindó información útil para ayudar en la investigación. La información incluía: circunstancias en las que se compraron los AV; operación y otra información de DDC como la dirección de la cartera, copia del documento de identificación mal usado para la compra y nombre del supuesto comprador. Estos permitieron a las autoridades solicitar información adicional a los bancos (por ejemplo, extractos bancarios). FATF REPORT, *op. cit.,* p. 6.

[573] En Isla Caimán, una IF (empresa de valores) local presentó un ROS con respecto a los pagos no autorizados entre las cuentas de AV de su corredor y un ciudadano extranjero. La empresa de valores informó la actividad después de que determinó que el ciudadano extranjero tenía la intención de realizar transferencias por un total de USD 4.8 millones (dos operaciones separadas que ocurrieron con seis minutos de diferencia el mismo día), y presentó una solicitud al corredor para una cuenta comercial en el siguiente día hábil. La cartera no estaba alojada en las Islas Caimán. El informe de ROS condujo a un intercambio de información exitoso con las UIF extranjeras y a la devolución exitosa de la mayoría de los recursos a la víctima, ya que la plataforma en línea en una jurisdicción extranjera había podido congelar la cuenta del sospechoso antes de que se completara el delito. FATF REPORT, *op. cit.,* p. 7.

[574] En Estados Unidos, AlphaBay, el mercado negro en la red más grande desmantelado por las autoridades en 2017, fue utilizado por cientos de miles de personas para comprar y vender drogas ilegales, documentos de identificación y dispositivos de acceso robados y fraudulentos, productos falsificados, *malware* y otras herramientas de piratería informática, armas de fuego y productos químicos tóxicos durante un período de dos años. El sitio operaba como un servicio oculto en la red TOR para ocultar las ubicaciones de sus servidores subyacentes, así como las identidades de sus administradores, moderadores y usuarios. FATF REPORT, *op. cit.,* p. 8.

[575] En Estados Unidos, un VASP basado en *darknet*, Helix, proporcionó un servicio de mezcla o rotación que ayudó a los clientes a ocultar la fuente o los propietarios de los AV por una tarifa durante un período de tres años. Helix supuestamente transfirió más de 350,000 *bitcoin*, con un valor en el momento de la transmisión de más de USD 300 millones. El operador anunció específicamente el servicio como una forma de ocultar operaciones en el mercado negro en la red a las fuerzas del orden. En febrero de 2020, se presentaron cargos criminales que incluían conspiración de LD y operación de un negocio de transmisión de dinero sin licencia contra una persona que operaba Helix. FATF REPORT, *op. cit.,* p. 8.

- Uso de cartera descentralizada[576].
- Cliente rechazando proveer información sobre la fuente de los recursos[577].
- El perfil del cliente no coincide con el comercio habitual de AV de alto valor[578].
- Víctimas de estafa convertidas en mulas[579].

---

[576] Este caso demuestra cómo los criminales hacen uso de una cartera descentralizada para disfrazar la fuente de recursos ilícitos generada por actividades de tráfico de sustancias ilícitas. En este caso, los criminales realizaron una gran cantidad de venta de drogas en Internet, solicitando el pago no solo en dinero fiduciario, sino también en forma de AV (*bitcoins*, Códigos EX, Cheques EXMO). Los recursos ilícitos recibidos en forma de divisas fiduciarias fueron convertidos a AV con la ayuda de una cuenta anónima en una plataforma de transacciones en línea de Blockchain. Dichos recursos, en la forma de AV, se convierten de vuelta a divisas fiduciarias a través de un cambiario, antes de ser transferidas nuevamente a las cuentas bancarias personales de los criminales. Por su parte, los recursos ilícitos recibidos en la forma de AV, primero fueron transferidos a carteras descentralizadas de Bitcoin en poder de los criminales en cuestión. FATF REPORT, *op. cit.,* p. 9.

[577] Una IF (banco) presentó un ROS en relación con una cuenta de una compañía local que contaba con recursos generados por la venta de cupones que podían ser comercializados con un producto (en este caso, bioplástico). Los recursos eran depositados tanto por personas físicas como morales, algunos originalmente como AV. A pesar de pesquisas posteriores realizadas por el banco, los representantes del propietario de la cuenta no proveyeron información sobre el origen de los recursos. Un análisis subsecuente por parte de las autoridades reveló que los recursos enviados por la compañía mostraban vínculos con sujetos conectados al crimen organizado y con recursos recibidos de un proyecto fraudulento. FATF REPORT, *op. cit.,* p. 9.

[578] Un VASP (cambiador) y una IF (instituto de pago) presentaron ROS ante la UIF relacionados con la comercialización de AV de alto valor que comenzó cuando se abrió la cuenta con el cambiador. De manera específica, el propietario de la cuenta había estado llevando a cabo varias transacciones de compra y venta de AV por más de 180,000 euros, lo cual no coincidía con el perfil del propietario de la cuenta (incluyendo ocupación y salario). Los análisis realizados hallaron que los AV posteriormente fueron usados para (i) transacciones en un mercado de darknet; (ii) apuestas en línea; (iii) transacciones con VASP que no tenían controles adecuados de PLD/CFT o que tenían investigaciones previas sobre lavado de dinero por millones de dólares; (iv) operaciones en plataformas que ofrecían transacciones de AV entre pares; y (v) "mezclando". FATF REPORT, *op. cit.,* p. 10.

[579] En estas estafas de inversión, los ciudadanos extranjeros contactaron a pensionados o adultos mayores a través de llamadas telefónicas, correos electrónicos o a través de redes sociales, ofreciéndoles oportunidades de inversión en Bitcoin o algunos otros AV con la promesa de generar grandes ganancias dada la creciente popularidad de los AV y su aumento de precio. La inversión inicial en pequeñas cantidades (en muchos casos no más de 250 euros) fue hecha desde la cuenta bancaria de la víctima, su tarjeta de crédito u otros medios de servicios de pagos y terminaron en las manos de los criminales. De manera alternativa, las víctimas fueron instruidas a intercambiar divisas fiduciarias a *bitcoin* usando un cajero automático de AV y enviar los recursos a una dirección proporcionada por los criminales. Las víctimas no eran muy adeptas tecnológica y generalmente no comprendían la tecnología de los AV o qué era en realidad en lo que estaban invirtiendo. Los delincuentes también solicitaron a las víctimas instalar una aplicación de escritorio remoto en sus dispositivos para que los criminales pudieran ayudar a transferir los recursos de manera correcta a cuentas específicas. Esto comprometió los dispositivos de las víctimas, ocasionando que los delincuentes pudieran realizar transferencias no autorizadas de dinero sin el conocimiento de la víctima hasta que él o ella notaran el dinero

- El uso de compañías ficticias - DeepDotWeb[580].
- El uso de múltiples intercambios de AV, documentos de identificación falsos para la Debida Diligencia del Cliente y tarjetas de prepago[581].
- Distribuidor de Bitcoin opera empresas de transmisión de dinero sin licencias (elementos transfronterizos)[582].

---

faltante en la cuenta. En algunos casos, los delincuentes también creaban artículos en los que aseguraban que celebridades famosas, importantes empresarios o locutores estaban promocionando las inversiones en AV, generando un sentimiento de confianza y legitimidad de las víctimas hacia estas "inversiones". FATF REPORT, *op. cit.,* p. 11.

[580] En mayo de 2019, Agencias del Orden Público de EE. UU. incautaron un sitio web, DeepDotWeb (DDW), de conformidad con una orden judicial. Los supuestos propietarios y operadores de DDW estaban a cargo de una conspiración de LD relacionada con millones de dólares en sobornos que recibieron por referir a individuos a mercados de la *darknet* a través del sitio de DDW. A través de enlaces de referencia, los supuestos propietarios y operadores de DDW recibieron pagos de sobornos, lo que representaba comisiones sobre las ganancias generadas de la venta de bienes ilegales, como el fentanilo o la heroína, hecha por individuos referidos a mercados de la *darknet* a través del sitio DDW. Estos pagos de sobornos fueron hechos en AV a una cartera de Bitcoin controlada por DDW. Para encubrir y disimular la naturaleza y la procedencia de las ganancias ilícitas, que superaban los 15 mdd, los propietarios y operadores transferían sus pagos ilegales de sobornos de su cartera de Bitcoin de DDW a otras carteras de Bitcoin, así como a cuentas bancarias que controlaban a través de compañías ficticias. Los acusados utilizaron estas compañías ficticias para mover sus ganancias ilícitas y realizar otra actividad relacionada con DDW. FATF REPORT, *op. cit.,* p. 12.

[581] Los acusados en este asunto supuestamente operaban un esquema de LD en conexión con criminales cibernéticos que hackearon un intercambio de AV y robaron 250 mdd en AV. Supuestamente, los dos acusados lavaron cerca de 91 mdd de los AV robados, así como 9.5 mdd de otro delito cibernético. Posteriormente, los activos virtuales robados fueron enviados a través de cientos de transacciones automáticas de AV y múltiples intercambios de AV. Los lavadores utilizaron fotografías manipuladas y documentos de identificación falsificados en algunos casos para eludir los procedimientos de KYC en los intercambios de AV. En última instancia, cerca de 35 mdd de los recursos ilícitos fueron transferidos a cuentas bancarias extranjeras y también fueron usados para comprar tarjetas de prepago, las cuales podían ser intercambiadas por AV. Los acusados operaban tanto con cuentas vinculadas como independientes, y prestaban servicios de transmisión de AV, como convertir AV en divisas fiduciarias para los clientes a cambio de una cuota. Los acusados también realizaban negocios en EE. UU., pero en ningún momento con registro ante FinCEN. FATF REPORT, *op. cit.,* p. 12.

[582] En abril del 2019, el acusado recibió una sentencia de dos años en prisión por operar una empresa de transmisión de dinero sin licencia, luego de vender cientos de miles de dólares de AV (*bitcoin*) a más de mil clientes en EE. UU. Al acusado también se lo ordenó pagar una multa por 823 357 dólares en ganancias. El acusado anunciaba sus servicios en sitios para usuarios de AV, llegando incluso a reunirse en persona con algunos clientes para aceptar dinero en efectivo a cambio de AV. Otros clientes le pagan a través de cajeros nacionales o de servicios de transferencia de dinero. El acusado recibía una prima del 5 % sobre el tipo de cambio vigente por sus servicios. Primero adquirió *bitcoin* a través de un cambiario estadounidense, pero una vez que sus actividades generaron sospecha y su cuenta fue clausurada, el acusado se cambió a un cambiario en Asia. Utilizando ese cambiario, el acusado compró 3.29 mdd en *bitcoin* entre marzo de 2015 y abril del 2017 a través de cientos de transacciones por separado. El acusado también admitió que intercambió sus dólares en efectivo, los cuales mantuvo en otra jurisdicción fronteriza con EE. UU., con un distribuidor de metales preciosos, y que entre finales de 2016 y principios de 2018, él, junto con otras personas, ingresaron a EE. UU. un total de más de un mdd en cantidades ligeramente por debajo del requisito de reporte de 10,000 dólares". FATF REPORT, *op. cit.,* p. 13.

Las tipologías advertidas en el presente acápite mediante la detección de reportes de operaciones sospechosas, en la gran mayoría de la casuística, señala que se pone en evidencia la potencialidad e instrumentalización de los criptoactivos para el blanqueo de dinero. Me refiero a un tipo de criminalidad transnacional apoyada en el uso del factor tecnológico. Como se puede apreciar en los distintos casos, el uso de los distintos componentes que forman parte de la estructura de los criptoactivos, como son cuentas anónimas, intercambiadores de activos virtuales establecidos en jurisdicciones poco reguladas, viabilizan su utilidad para poder realizar actos propios del blanqueo de dinero, lo que pone en evidencia las vulnerabilidades inherentes vinculados a los activos virtuales[583].

6. Guía de activos virtuales y proveedores de servicios de activos virtuales

En octubre de 2021, el GAFI actualizó el documento denominado *Guía actualizada para un enfoque basado en el riesgo activos virtuales y proveedores de servicios de activos virtuales*, con la finalidad de ofrecer a los sectores público y privado orientaciones basadas en estándares del GAFI. El equipo que conformó el proyecto se conformó por más de 200 jurisdicciones entre miembros del GAFI y organismos regionales con similares políticas a la del GAFI, además de la participación del sector privado y los representantes de la comunidad de activos virtuales.

La Guía está organizada de la siguiente manera: la sección II examina cómo las actividades de AV y los PSAV entran en el ámbito de aplicación de las Recomendaciones del GAFI; la sección III describe la aplicación de las Recomendaciones del GAFI a los países y a las autoridades competentes; la sección IV explica la aplicación de las Recomendaciones del GAFI a los PSAV y a otros sujetos obligados que realizan o prestan actividades cubiertas de AV, incluidas las IF, como los bancos y los agentes de valores, entre otros; la sección V ofrece ejemplos de enfoques jurisdiccionales para regular, supervisar y hacer

[583] *Ibid.,* p. 14.

cumplir las actividades cubiertas de AV y los PSAV (y otros sujetos obligados) en materia ALA/CFT; y la sección VI establece los principios para la cooperación internacional y el intercambio de información entre los supervisores de los PSAV.

La Guía abarca los siguientes puntos[584]:

1) Aclarar las definiciones de AV y PSAV para dejar claro que estas definiciones son amplias y que no debería haber un caso en el que un activo financiero relevante no esté cubierto por los Estándares del GAFI (ya sea como AV o como otro activo financiero).
2) Proporcionar orientación sobre cómo se aplican los estándares del GAFI a las monedas estables (*stablecoins*) y aclarar que una serie de entidades involucradas en estructuras de moneda estable podrían calificar como PSAV bajo los estándares del GAFI.
3) Proporcionar orientación adicional sobre los riesgos y las herramientas disponibles para que los países aborden los riesgos de LA/FT para las transacciones entre pares, que son transacciones que no involucran a ningún sujeto obligado.
4) Proporcionar orientaciones actualizadas sobre la concesión de licencias y el registro de PSAV.
5) Proporcionar orientación adicional para los sectores público y privado sobre la aplicación de la "regla del viaje".
6) Incluir los principios de intercambio de información y cooperación entre los supervisores de PSAV. Este documento incorpora y sustituye a la Guía del 2019.

La primera parte trata de una ampliación de la *Guía sobre monedas virtuales* del 2015 y explica con mayor detalle la aplicación del enfoque basado en el riesgo de las medidas ALA/CFT para los AV; asimismo, identifica a las entidades que realizan actividades u operaciones relacionadas con los AV, es decir, los PSAV;

[584] GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Guía actualizada: EBR a los Activos Virtuales y Proveedores de Servicios de Activos Virtual,* París 2021, p. 5.

y aclara la aplicación de las recomendaciones del GAFI a los AV y PSAV[585]. Si bien el GAFI advierte que algunos países han implementado regímenes regulatorios para los criptoactivos, también es una realidad insoslayable que muchas jurisdicciones aún no cuentan con marcos antilavado eficaces para mitigar los riesgos asociados a las actividades de los criptoactivos en particular[586].

El rápido desarrollo y la creciente funcionalidad, sumado al aumento de la adopción y la naturaleza global y transfronteriza de los AV, hace que las acciones urgentes por parte de los países para mitigar los riesgos de LA/FT que presentan las actividades de los AV y los PSAV sea una prioridad clave del GAFI. El uso de activos virtuales por parte de las redes de *ransomware* es también una preocupación crítica, y el crecimiento de los ataques de este tipo ha aumentado la importancia del esfuerzo para introducir marcos ALA/CFT eficaces a nivel mundial[587].

La guía se centra en los AV que son convertibles a otros fondos o valores, incluyendo AV que son convertibles a otros AV y AV que son convertibles a monedas fiduciarias o que se entrelazan con el sistema financiero de monedas fiduciarias.

Sin embargo, no aborda otras cuestiones relativas a la regulación de la protección al consumidor y al inversor, como son la seguridad y solidez prudencial, las cuestiones impositivas, antifraude o anti-manipulación del mercado, las normas de seguridad de redes IT, o las cuestiones de estabilidad financiera[588]. La guía tampoco aborda lo referente a monedas digitales emitidas por el banco central, ya que el GAFI considera que estas no son AV, sino la representación digital de monedas de curso legal emitida por entidades reguladas. Pero cabe precisar que los estándares del GAFI sí se aplican a

---

[585] *Ibid.,* p. 8.

[586] *Ibid.,* p. 9.

[587] *Ibid.,* p. 10.

[588] *Ibid.,* p. 11.

monedas digitales emitidas por bancos centrales, similares a cualquier otra forma de moneda fiduciaria emitida por un banco central, y ante monedas de curso legal[589].

La guía establece, para los países en los que se ofrecen PSAV, así como los sujetos obligados que participan u ofrecen actividades cubiertas de AV, que deberán recordar los principios claves que subyacen al diseño y la aplicación de las recomendaciones del GAFI y que son relevantes en el contexto de los AV:

- Equivalencia funcional y enfoque basado en objetivos[590]

  Los requisitos del GAFI, incluidos los que se aplican en el ámbito de los AV, son compatibles con una variedad de sistemas jurídicos y administrativos diferentes. Explican en términos generales, pero no de manera excesivamente específica, cómo debe llevarse a cabo la aplicación, a fin de permitir diferentes opciones, en caso necesario. Cualquier aclaración de los requisitos no debe exigir a las jurisdicciones que ya han adoptado medidas adecuadas para alcanzar los objetivos de las recomendaciones del GAFI que cambien la forma o el fondo de sus leyes y regulaciones. La guía pretende apoyar la aplicación de las recomendaciones del GAFI en función de los fines o los objetivos, en lugar de imponer un régimen normativo rígido y único para todas las jurisdicciones.

- Neutralidad tecnológica y preparación para el futuro[591]

  Los requisitos aplicables a los AV, como valor o fondos, a las actividades cubiertas de los AV y a los PSAV se aplican con independencia de la plataforma tecnológica de que se trate.

---

[589] *Ibid.,* p. 11

[590] *Ibid.,* p. 12.

[591] *Idem.*

- Igualdad de condiciones (tratamiento funcional)[592]

  Los países y sus autoridades competentes deben tratar todas las variedades de PSAV, independientemente del modelo de negocio, en igualdad de condiciones desde el punto de vista de la reglamentación y la supervisión cuando presten servicios fundamentalmente similares y planteen riesgos parecidos. Sin embargo, cuando sus perfiles de riesgo difieran, el tratamiento puede ser diferente en línea con el EBR.

La segunda parte del informe también analiza el concepto de las denominadas monedas estables o *stablecoins*, entendidas por mantener un valor estable en relación con algún activo o activos de referencia. Además, resalta que, debido a su potencial anonimato, alcance global y uso para estratificar fondos ilícitos, cuenta con un gran potencial para LA/FT. Otro aspecto que resalta el documento es en relación con la adopción masiva, lo que podría aumentar los riesgos de LA/FT. En esa línea, refiere "la adopción masiva es un factor de riesgo de LA/FT importante a considerar debido a que la capacidad de los delincuentes de usar AV como medio de cambio depende en gran medida de que sea libremente intercambiable y líquida, algo que la adopción masiva podría facilitar"[593].

Otro punto que desarrolla la guía es el referido a las transacciones entre pares o sistema P2P, elemento que al día de hoy es uno de los que genera mayor polémica frente a la falta de control transaccional en el mundo de los criptoactivos. El GAFI define las transacciones entre pares (P2P) "como las transferencias de activos virtuales realizadas sin el uso o la participación de un intercambiador u otro sujeto obligado"[594]. Las transacciones P2P, por su misma naturaleza tecnológica, no están sujetas explícitamente a controles ALA/CFT en el marco de los estándares del GAFI, ya que los estándares suelen imponer obligaciones a los intermediarios en lugar de a los propios individuos[595].

---

[592] *Ibid.,* p. 12.

[593] *Ibid.,* p. 16.

[594] *Ibid.,* p. 17.

[595] *Idem.*

La tercera parte explica cómo se aplican las recomendaciones del GAFI relacionadas con los AV y PSAV a los países y a las autoridades competentes, y se concentra en la identificación y mitigación de los riesgos asociados con las actividades cubiertas de AV, la aplicación de medidas preventivas, la aplicación de requisitos de otorgamiento de licencias y registro, la implementación de una supervisión efectiva a la par de la supervisión de las actividades financieras relacionadas de las IF, la provisión de una variedad de sanciones efectivas y disuasivas, y la facilitación de la cooperación nacional e internacional. Casi todas las recomendaciones del GAFI son directamente pertinentes para entender cómo deben usar los países a las autoridades gubernamentales y a la cooperación internacional para abordar los riesgos de LA/FT asociados a los AV y los PSAV, mientras que otras recomendaciones están menos directa o explícitamente vinculadas a los AV o los PSAV, aunque siguen siendo relevantes y aplicables[596].

La cuarta parte está referida a cómo las recomendaciones del GAFI se aplican tanto a los países como a los PSAV y a otros sujetos obligados que prestan servicios relacionados con AV cubiertos o realizan actividades u operaciones financieras, incluidos los bancos, los agentes de valores y otras IF. En consecuencia, la sección ofrece orientaciones adicionales específicas para los PSAV y otros sujetos obligados que pueden realizar actividades cubiertas de AV. Estas orientaciones se enmarcan dentro de lo que es:

- Debida diligencia del cliente
- Personas expuestas políticamente
- Banca corresponsal y otras relaciones similares
- Transferencias electrónicas y la “regla del viaje”
- Controles internos y filiales y subsidiaria
- Reporte de ROS y *tipping-off*

[596] *Ibid.,* p. 36.

La quinta parte desarrolla ejemplos de países y sus regulaciones adoptadas frente al uso de criptoactivos. Se desarrolla el enfoque basado en el riesgo aplicable a los activos virtuales y los proveedores de servicios de activos virtuales[597].

La sexta parte desarrolla los principios del intercambio de información y la cooperación entre supervisores de PSAV, que son:

- Identificación de supervisores y PSAV
- Intercambio de información
- Cooperación

7. Actualización dirigida en implementación de estándares del GAFI sobre virtual activos y activo virtual proveedores de servicio *(travel rule*)

En junio del 2022, el GAFI adoptó oficialmente lo que se conoce como la regla de viaje o *travel rule*. El informe proporciona una tercera revisión específica de la implementación del enfoque de la regla de viaje, en la que se le requiere al sector privado que obtenga/intercambie información sobre el beneficiario y el originador con transferencias de los criptoactivos[598].

Durante los últimos años, los Estados parte del GAFI han logrado un progreso limitado en la introducción de la regla de viaje del GAFI, que es un requisito clave que permite al sector privado cumplir con los requisitos de sanciones y detectar transacciones sospechosas. Sin embargo, esta brecha deja a los activos virtuales y proveedores de activos virtuales vulnerables frente al uso ilícito de los mismos y demuestra la necesidad urgente de que las jurisdicciones aceleren la

[597] *Ibid.,* p. 102.

[598] GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Actualización dirigida en Implementación de Estándares del GAFI sobre Activos Virtuales y Proveedores de Servicios de Activos Virtuales*, París, 2022, p. 13.

implementación y el cumplimiento de esta regla en materia prevención de blanqueo de dinero.

Como parte del denominado *problema del amanecer*, que tiene que ver con la contradicción que se da entre la tecnología disruptiva de descentralización y la centralización normativa que conlleva la regulación, además de la falta de adaptación en la legislación de cada país. Algunas jurisdicciones han introducido solicitudes de orientaciones para aclarar cómo sus proveedores de activos virtuales locales deben interactuar con contrapartes extranjeras sin licencia/o no registradas[599]. GAFI enfoca esta problemática en dos dimensiones. La primera referida a si los proveedores de activos virtuales nacionales están autorizados a realizar transacciones con esos otros proveedores. La segunda, si los proveedores de activos virtuales nacionales están obligados a enviar información sobre transacciones y clientes relacionada con la regla de viaje[600].

Sobre el particular, en relación con la primera interrogante, la mayoría de las jurisdicciones han decidido permitir que los proveedores nacionales de activos virtuales efectúen transacciones con cualquier proveedor extranjero, ya sea que estén autorizados/registrados o no lo estén. Un grupo minoritario de jurisdicciones han optado por exigir a los proveedores nacionales que limiten las transacciones únicamente a los proveedores extranjeros que cuentan con licencia/registrados y/o aplican la regla de viaje del GAFI[601]. En relación con la segunda interrogante, sobre la exigencia de envío de información, la gran mayoría de las jurisdicciones aún no han tomado una decisión sobre este tema. Sin embargo, de las que lo han hecho, han decidido exigir a los proveedores nacionales de activos virtuales que apliquen la regla de viaje con todos los proveedores extranjeros, ya sea que estén o no registrados con licencia o tengan requisitos similares de la regla de viaje[602].

---

[599] *Ibid.,* p. 13.

[600] *Idem.*

[601] *Idem.*

[602] *Idem.*

En relación con el umbral, el informe refiere que las jurisdicciones pueden optar por adoptar un umbral mínimo para las transferencias de criptoactivos de 1000 USD/EUR. Incluso si las jurisdicciones que implementen dicho umbral, aún deben exigir que los proveedores, cuando realicen transferencias por debajo del monto, recopilen: a) el nombre del originador y el beneficiario, y b) la dirección de billetera para cada uno o un número de referencia de transacción único para transferencias. Además, si dicha transferencia de criptoactivos va por debajo del umbral y se tiene una sospecha de operación sospechosa por blanqueo, se debe verificar dicha información relacionada con el cliente[603].

En la Unión Europea actualmente se aplica el Reglamento (UE) 2015/847 del Parlamento Europeo y del Consejo, el cual se adoptó siguiendo los estándares propuestos por el GAFI para garantizar que los proveedores de servicios de transferencias electrónicas y de servicios de pago acompañen las transferencias de fondos con información sobre el ordenante y el beneficiario. Sin embargo, el Parlamento Europeo, mediante la *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la información que acompaña a las transferencias de fondos y determinados criptoactivos*, se ha decidido ampliar el *travel rule* e incluir a los criptoactivos, ya que los flujos de dinero ilícito a través de transferencias de fondos y criptoactivos pueden dañar la integridad, la estabilidad y la reputación del sector financiero y amenazar el mercado interior de la Unión Eurpea, así como el desarrollo internacional.

El acuerdo provisional interinstitucional considera que el blanqueo de capitales, la financiación del terrorismo y la delincuencia organizada siguen siendo problemas importantes que deben abordarse a nivel de la Unión. La solidez, integridad y estabilidad del sistema de transferencias de fondos y criptoactivos y la confianza en el sistema financiero en su conjunto podrían verse gravemente comprometidas por los esfuerzos de los delincuentes, y sus asociados para ocultar el origen de los ingresos delictivos o transferir fondos con criptoactivos para actividades delictivas o fines terroristas.

---

[603] *Ibid.*, p. 15.

El artículo 2 de la presente propuesta reglamento se aplicará a las transferencias de fondos, en cualquier moneda, que envíe o reciba un proveedor de servicios de pago o un proveedor de servicios de pago intermediario establecido en la Unión. También se aplicará a las transferencias de criptoactivos, incluidas las transferencias de criptoactivos ejecutadas por medio de cajeros automáticos de criptoactivos (criptoATM), cuando el servicio de criptoactivos proveedor del originador o del beneficiario esté establecido en la Unión.

III. IMPLEMENTACIÓN DE UN SISTEMA DE TRAZABILIDAD DE OPERACIONES EN CRIPTOACTIVOS PARA LA PREVENCIÓN DE LAVADO DE ACTIVOS

Como ya se ha hecho referencia, un modelo de prevención de lavado de activos debe cumplir con ciertos pilares clásicos que tienen como finalidad el eximir de responsabilidad penal a la persona jurídica y el mitigar los riesgos, para evitar futuras sanciones. Estos pilares que se aplican a cualquier modelo de prevención son los siguientes:

- Oficial de cumplimiento
- Manual de procedimientos
- Capacitación del oficial y del área de cumplimiento
- Herramientas tecnológicas
- Auditorías internas y externas
- Reportes de operaciones
- Evaluaciones de riesgo
- Procedimientos y flujos operativos (control de límites/montos).
- Registro de perfiles y datos transaccionales
- Debida diligencia de los clientes

Sin duda, al tratarse de personas jurídicas que funcionan mediante plataformas virtuales de alto contenido tecnológico, los procedimientos de control que se deben seguir dentro de este modelo de prevención deben contar con la más alta

tecnología para poder verificar de forma eficiente el denominado *on boarding* digital para la validación no presencial del cliente. Este procedimiento de *know your costumer* (kyc) o debida diligencia que comprende distintos procedimientos como la verificación por medio de un sistema de reconocimiento biométrico-facial, la verificación de documentos, correo electrónico, teléfono, antecedentes, y el *on going* que tiene que ver con el monitoreo y trazabilidad de los criptoactivos.

Al día de hoy, existen una diversidad de empresas que proporcionan un conjunto de soluciones forenses, como es el servicio de criptoanálisis, la realización de una debida diligencia y de investigaciones detalladas, con la finalidad de mitigar riesgos.

Para el rastreo de las transacciones existen empresas tecnológicas como es el caso de CipherTrace Inspector, el cual proporciona una interfaz poderosa que permite rastrear transacciones de *blockchain* y mejorar la diligencia debida para investigaciones financieras. Mediante esta tecnología se puede rastrear cadenas de bloques de *bitcoin*, etc., lo que permite a los analistas el poder establecer la fecha, hora e ID de cada transacción, para un mejor control frente al lavado de activos.

IV. LOS SUJETOS OBLIGADOS EN LAS OPERACIONES CON CRIPTOACTIVOS

En el caso del Perú, mediante la Ley N.º 27693 se creó la Unidad de Inteligencia Financiera denominada “UIF”, encargada de recibir, analizar, tratar, evaluar y transmitir información para la detección del lavado de activos y del financiamiento del terrorismo; y fue incorporada a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) como una unidad especializada, según lo dispuso la Ley N.º 29038, Ley que incorpora la UIF-Perú

a la SBS. Asimismo, mediante Decreto Supremo N.º 018-2006-JUS, se aprobó el Reglamento de la Ley N.º 27693.

En relación con la supervisión de criptoactivos la UIF, siguiendo lo dispuesto por el GAFI en su recomendación nº 15 —en razón del riesgo que implican el desarrollo de actividades comerciales con activos virtuales, estas deben sujetarse a obligaciones de cumplimiento—, presentó ante el Ministerio de Justicia el Proyecto Peruano de Decreto Supremo del 2021 para incorporar a los proveedores de servicios virtuales como sujetos obligados a informar a ante la UIF-PERÚ. Según el mismo tenor del artículo único, pretende incorporar a los proveedores de servicios activos virtuales (PSAV) que comprenden cualquier persona física o jurídica, domiciliadas o constituidas en el país y que no esté bajo la cobertura de la ninguna recomendación del GAFI y que realice las actividades u operaciones en representación de una persona física o jurídica.

El 27 de julio del 2023, mediante Decreto Supremo N.° 006-2023-JUS, se amplía la lista de sujetos obligados a proporcionar información a la UIF-PERU. Según esta nueva reforma legislativa, a partir de ahora se consideran transferencias sujetas a control todas aquellas operaciones realizadas en activos virtuales por parte de los PSAV en nombre de una persona física o jurídica que mueve un activo virtual de una dirección o cuenta de activo virtual a otra, por lo que las transferencias son consideradas como transferencias transfronterizas y no cubren la adquisición de bienes o servicios.

Artículo 1.- Incorporación de sujetos obligados
Incorpórese como sujetos obligados a informar a la UIF-Perú, conforme a lo previsto en el numeral 3.3 del artículo 3 de la Ley N.° 29038, a los Proveedores de Servicios de Activos Virtuales (PSAV) que comprenden cualquier persona física o jurídica, domiciliada o constituida en el país, que no esté cubierta en ninguna otra de las Recomendaciones del Grupo de Acción Financiera Internacional (GAFI) y que, como negocio, realiza una o más de las siguientes actividades u operaciones para o en nombre de otra persona física o jurídica:

i. Intercambio entre activos y moneda fíat o de curso legal;

ii. Intercambio entre una o más formas de activos virtuales;

iii. Transferencia de activos virtuales;

iv. Custodia y/o administración de activos virtuales; o instrumentos que permitan el control sobre activos virtuales y;

v. Participación y provisión de servicios financieros relacionados con la oferta de un emisor y/o venta de un activo virtual.

Bajo este nuevo alcance normativo, todas aquellas personas físicas o jurídicas nacionales o extranjeras que ofrezcan servicios vinculados con los criptoactivos serán sujetos obligados a informar operaciones sospechosas y deberán implementar un sistema de prevención de lavado de activos SPLATF, para poder realizar una debida identificación de sus clientes, así como una debida trazabilidad de las operaciones que se realizan mediante su intermediación. La norma en cuestión está circunscrita de forma amplia a cualquier tipo de criptoactivo o activo virtual que se pueda ofrecer en el mercado, es decir, todo tipo de criptoactivos como *tokens* transaccionales, monedas estables, token de seguridad, token de utilidad, *tokens* no fungibles (NFT), etc.

El artículo 5° del Decreto Legislativo N° 1106, sanciona al que *"*incumpliendo sus obligaciones funcionales o profesionales, omite comunicar a la autoridad competente, las transacciones u operaciones sospechosas que hubiere detectado, según las leyes y normas reglamentarias, será reprimido con pena privativa de la libertad no menor de cuatro ni mayor de ocho años, con ciento veinte a doscientos cincuenta días multa e inhabilitación no menor de cuatro ni mayor de seis años, de conformidad con los incisos 1), 2) y 4) del artículo 36 del Código Penal. La omisión por culpa de la comunicación de transacciones u operaciones sospechosas será reprimida con pena de multa de ochenta a ciento cincuenta días multa e inhabilitación de uno a tres años, de conformidad con los incisos 1), 2) y 4) del artículo 36 del Código Penal. La comisión por culpa de la comunicación de transacción u operación o sospechosa será reprimida con pena de multa de ochenta y ciento cincuenta días, multa e inhabilitación de uno a tres años, de conformidad con los incisos 1), 2) y 4) del artículo 36 del Código Penal*".*

Sin bien bajo el marco legal actual existe un vacío legal en materia de regularización de criptoactivos, no debemos perder perspectiva que el medio mediante el cual se adquieren los mismos es a través de transacciones convencionales mediante el sistema financiero. Esta situación permite realizar el control sobre cualquier operación que se considere sospechosa por parte de quien está ofreciendo el servicio para la compra o venta de criptoactivos. Más aún ahora con la regulación establecida en el Decreto Supremo N.° 006-2023-JUS. Sin embargo, la mayor problemática se suscita cuando esta realiza una operación de forma directa dentro de un protocolo específico, ya que, dado el alto contenido tecnológico de la transacción, hace muy difícil el poder ejercer algún control por parte de un tercero que funja de oficial de cumplimiento, pues el mismo protocolo no lo permitiría.

CAPÍTULO V
PROPUESTA *DE LEGE FERENDA*

Dada la trascendencia del tema objeto de investigación y la proyección al futuro que tienen lo criptoactivos, es que considero de vital importancia el elaborar una propuesta reflexiva legislativa normativa de *lege ferenda*, en la que se modifique el Decreto Legislativo N.° 1106, tomando en cuenta todos los pronunciamientos *soft law* emitido por el GAFI. Asimismo, debemos tener en consideración la gran aceptación que van teniendo los criptoactivos en el mercado nacional, así como la comercialización de estos por parte de distintas personas jurídicas y naturales. Situación que si bien va a la par con la innovación tecnológica del cambio, no es menos cierto que este nuevo escenario genera un espacio muy propicio para delinquir mediante la instrumentalización de criptoactivos. Por lo tanto, urge que el legislador adecue la normativa vigente contra el lavado de activos en el Perú y criminalice las tipologías actuales configuradas contra el lavado incorporando a los criptoactivos dentro del objeto material como un elemento de las mismas.

I. DECRETO LEGISLATIVO N.° 1106

Consideramos importante que se realice las reformas de los artículos 1, 2, 3, 4, 5 y 6 vigentes en el Decreto Legislativo N.° 1106, de la siguiente manera:

Artículo 1.- Actos de conversión y transferencia

El que convierte o transfiere dinero, bienes, **criptoactivos**, efectos o ganancias cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa.

Artículo 2.- Actos de ocultamiento y tenencia

El que adquiere, utiliza, guarda, administra, custodia, recibe, oculta o mantiene en su poder dinero, bienes, **criptoactivos**, efectos o ganancias, cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa.

Artículo 3.- Transporte, traslado, ingreso o salida por territorio nacional de dinero, **criptoactivos** o títulos valores de origen ilícito

El que transporta o traslada dentro del territorio nacional dinero, **criptoactivos** o títulos valores cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso; o hace ingresar o salir del país tales bienes con igual finalidad, será reprimido con pena privativa de libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa.

Artículo 4.- Circunstancias agravantes y atenuantes

La pena será privativa de la libertad no menor de diez ni mayor de veinte años y trescientos sesenta y cinco a setecientos treinta días multa, cuando:

1. El agente utilice o se sirva de su condición de funcionario público o de agente del sector inmobiliario, financiero, bancario o bursátil o **proveedor de servicios de criptoactivos o custodia de monederos electrónicos**

2. El agente cometa el delito en calidad de integrante de una organización criminal.

3. El valor del dinero, bienes, **criptoactivos,** efectos o ganancias involucrados sea superior al equivalente a quinientas (500) Unidades Impositivas Tributarias.

La pena será privativa de la libertad no menor de veinticinco años cuando el dinero, bienes, **criptoactivos**, efectos o ganancias provienen de la minería

ilegal, tráfico ilícito de drogas, terrorismo, secuestro, extorsión o trata de personas.

La pena será privativa de la libertad no menor de cuatro ni mayor de seis años y de ochenta a ciento diez días multa, cuando el valor del dinero, bienes, efectos o ganancias involucrados no sea superior al equivalente a cinco (5) Unidades Impositivas Tributarias. La misma pena se aplicará a quien proporcione a las autoridades información eficaz para evitar la consumación del delito, identificar y capturar a sus autores o partícipes, así como detectar o incautar los activos objeto de los actos descritos en los artículos 1, 2 y 3 del presente Decreto

CONCLUSIONES

1. El proceso de innovación tecnológica no ha sido ajeno a la criminalidad organizada, ya que su reciente evolución ha supuesto un cambio que le está permitiendo desafiar el orden estatal a través del proceso de globalización tecnológica, el cual está posibilitando nuevas formas de delincuencia mediante el uso de la informática y las telecomunicaciones. En la actualidad, las organizaciones criminales dedicadas al narcotráfico, trata de personas, blanqueo de capitales, se vienen instrumentalizando de diversas tecnologías en la red, que generan muchas dificultades en al ámbito de la persecución penal.

2. El ciberespacio se ha convertido en el quinto espacio estratégico más importante del planeta, después de la tierra, el mar, el aire y el espacio. Todas las nuevas tecnologías funcionan en el ciberespacio, razón de su importancia en este nuevo escenario criminógeno.

3. La transnacionalidad es uno de los principios más connotados del ciberespacio y se manifiesta en la posibilidad que permite la red a sus usuarios: el poder acceder desde cualquier parte del mundo a cualquier sitio web que se encuentre localizado en un servidor concreto. Sin embargo, este principio supone un tipo de obstaculización al momento de iniciar acciones penales por la comisión de ciberdelitos, ya que se requiere de la cooperación judicial internacional para poder realizar una persecución penal.

4. Esta problemática que plantea la transnacionalidad ha sido abordada por la normativa supranacional en materia de criminalidad organizada transnacional, en el Convenio sobre Ciberdelincuencia, celebrado en Budapest, el cual reconoce el interés de intensificar la cooperación judicial entre los Estados parte, tomando como punto de partida la digitalización, la convergencia y la globalización continuas de las redes informáticas, por el riesgo de que estas

puedan ser utilizadas para la comisión de ilícitos, y que la prueba de estos actos delictivos sean guardadas y transmitidas por dichas redes.

5. En materia estrictamente punitiva, en lo que se refiere a la aplicación espacial de la ley penal, el principio de territorialidad de forma taxativa determina que la ley penal se aplica a todo el que comete un hecho punible en el territorio de la República, salvo determinadas excepciones contenidas en el derecho internacional. Sin embargo, en el ciberespacio ocurre todo lo opuesto: si bien este nos transmite la sensación de que se encontraría en todos lados, lo cierto y concreto es que físicamente no se encuentra en ningún sitio, como para poder establecer una ubicación en relación con un suceso específico acontecido dentro de este espacio virtual, que permita ejercer algún tipo reacción por parte del Estado.

6. En el caso específico del delito de lavado de activos, su ejecución va muy entrelazada con el sistema financiero, me refiero a un conjunto de operaciones complejas y muy sofisticadas que permiten la colocación e integración de activos o capitales sucios en el orden económico, para posteriormente puedan ser maculados. En este escenario el fenómeno de las nuevas tecnologías se viene posicionado en el sistema financiero, por lo que poco a poco se van desplazando los pagos con dinero en efectivo, por medios de pago virtuales como es el caso de los criptoactivos.

7. Han aparecido nuevas formas de macular activos sucios, mediante la utilización del ciberespacio, aprovechando todo el componente tecnológico, para poder camuflar todas las ganancias ilícitas obtenidas. En este nuevo escenario delictivo, los criptoactivos también han obtenido un rol protagónico, justamente por dotar a las mismas de cierto anonimato, virtualidad y transnacionalidad.

8. El Grupo de Acción Financiera Internacional, desde el año 2014 al 2022, ha venido emitiendo distintos informes sobre las monedas virtuales y sus riesgos

potenciales de LA/FT, en el que se hacía especial referencia al poder cambiario de las monedas virtuales convertibles, y cómo estas pueden ser canjeadas por dinero real o por otras monedas virtuales y son potencialmente vulnerables a abusos para el blanqueo de dinero y financiación del terrorismo.

9. Un sector minoritario de la doctrina empieza a desarrollar una nueva forma de lavado de activos, conocida como el ciberlavado de activos, construcción conceptual que tiene su origen en la unión de dos palabras, ciberespacio (o *cyberespace*) y blanqueo.

10. Se define al ciberlavado como aquella conducta delictiva que utiliza medios tecnológicos a través del ciberespacio para dotar de una apariencia legítima a todas aquellas ganancias ilícitas que tiene su origen en una actividad criminal previa.

11. En el caso del ciberlavado, su misma construcción terminológica indica que se requiere, para la ejecución de actos de conversión, transferencia u ocultamiento, que las ganancias ilícitas hayan sido obtenidas en actividades criminales vinculadas al ciberespacio virtual.

12. En la Unión Europea es donde se pueden apreciar los avances más significativos en materia de regulación de criptoactivos, tanto de forma jurídica general como desde una respuesta penal preventiva-punitiva. En esa línea tenemos la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, que es en la actualidad el mayor instrumento jurídico en prevención de utilización de criptoactivos para el blanqueo de capitales. Por último, tenemos la propuesta MICA, la cual tiene como finalidad regular las monedas estables o *stablecoins*.

13. Los criptoactivos como objeto material del delito se pueden subsumir mediante un juicio de tipicidad dentro de los elementos normativos de las topologías descritas en los artículos 1 y 2 del Decreto N.º 1106, y a partir de ello

efectuarse actos propios del blanqueo, como son actos de conversión, transferencia, tenencia y ocultamiento.

14. El delito lavado de activos está compuesto de tres etapas o fases operativas conocidas como la *colocación*, *ensombrecimiento* e *integración,* en las que se produce lo que se conoce como el ciclo del blanqueo o lavado. Bajo este esquema, los criptoactivos pueden perfectamente ser instrumentalizados como una herramienta útil en el proceso de blanqueo de fondos de origen ilícito.

15. Los criptoactivos son un tipo de activo que puede ser instrumentalizado en la configuración típica de las tipologías previstas en la sistemática de los artículos 1, 2 y 3 del Decreto Legislativo N.º 1106, los criptoactivos sí pueden ser objeto del delito de blanqueo de capitales, por ende también son susceptibles de aplicárseles medidas coerción reales, para su aseguramiento, así como lo es la consecuencia accesoria del decomiso, en el entendido de que estos activos virtuales se han bienes, efectos o ganancias del delito o cualquier transformación que estos hayan podido experimentar.

16. Hasta el cierre de esta tesis doctoral, no existe en el Perú ninguna propuesta legislativa normativa en materia de criptoactivos, para su uso como moneda de curso legal, ni a nivel preventivo represivo para fines vinculados al lavado de activos.

BIBLIOGRAFÍA

ABEL SOUTO, Miguel, "Blanqueo, innovaciones tecnológicas, amnistía fiscal de 2012 y reforma penal", en *Revista Electrónica de Ciencia Penal y Criminología,* n.º 14-14, 2012. Disponible en: <http://criminet.ugr.es/recpc/14/recpc14-14.pdf>.

ABOSO, Gustavo y ZAPATA, Florencia. *Cibercriminalidad y derecho penal*, Buenos Aires: B de F, 2006.

ADELL, Jordi, "Redes y Educación", en J. DE PABLOS, J. y J. JIMÉNEZ (eds.), *Nuevas tecnologías, comunicación audiovisual y educación,* Barcelona: Ed. Cedecs, 1998, pp. 10 y 11. Disponible en: <https://elbonia.cent.uji.es/jordi/wp-content/uploads/docs/Adell_redesyeducacion.pdf>.

ALEJANDRO VADELL, Gabriel, "Las Finanzas Descentralizadas (Defi) ¿La evolución de las cuentas off shore?", en *Centro de Estudios de Administración Tributaria CIAT*, 2021.

ÁLVAREZ LARRONDO, Federico, *Entendiendo al bitcoin y sus desafíos jurídicos y sociales*, Buenos Aires: Thomson Reuters Aranzandi, 2022.

ÁLVAREZ LÓPEZ, Carlos y CARRASCO PERERA, Ángel, "¿Qué es un metaverso?", en *Gomez-Acebo & Pombo*, febrero del 2022. Disponible en: <https://www.ga-p.com/publicaciones/que-es-el-metaverso/>.

ANZOLA, Ayelén, "Ciberblanqueo de capitales: El especial caso de los activos virtuales old wine in new bottles", en *Desafíos contra la lucha contra la corrupción: Gestión de riesgos y paradigmas globales*, Coruña: Colex, 2023.

ANZOLA, Ayelén, "La ejecución de las resoluciones de decomiso de activos virtuales en España", en *Revista Procesal,* n.° 57, 2022,

ARÁNGUEZ SÁNCHEZ, Carlos, “El bitcoin como instrumento y objeto de delitos”, en *Cuadernos de Política Criminal,* n.° 131, segunda época, septiembre del 2020, pp. 75-103.

ARÁNGUEZ SÁNCHEZ, Carlos, “El bitcoin como instrumento y objeto de delitos”, en *Cuadernos de Política Criminal,* n.° 131, segunda época, septiembre del 2020.

ARBULÚ RAMÍREZ, José Antonio, *El delito de lavado de activos*, Lima: Editorial Pacífico, 2018.

ARROYO GUARDEÑO, David, DÍAZ VICO, Jesús y HERNÁNDEZ ENCINAS, Luis, *¿Qué sabemos de Blockchain?*, Madrid: Catarata, 2019.

ASMAKOV Andrew, “Víctimas del Esquema Ponzi Bitconnect Recibirán $17 Millones en Compensaciones” en *Decrypt*, 13 de enero del 2023. Disponible en: <https://decrypt.co/es/119171/victimas-del-esquema-ponzi-bitconnect-recibiran-14-millones-en-compensaciones>.

ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES, *Políticas TIC: Manual para principiantes,* Chris NICOL (ed.), Montevideo, 2005. Disponible en: <https://www.apc.org/sites/default/files/ICT_Policy_Handbook_ES.pdf>.

AUER, Raphael y CLAESSENS, Stijin, “Regulación de las criptomonedas: evaluación de reacciones del mercado”, en *Informe Trimestral del BPI*, septiembre del 2018.

BACIGALUPO Enrique, *Manual de derecho penal*, Bogotá: Temis, 1989.

BALMACEDA QUIRÓS, Justo, *Delitos conexos y subsiguientes*, Barcelona: Atelier, 2014.

BALLESTEROS SÁNCHEZ, Julio, *Exigencias político criminales y operativas en la lucha contra la criminalidad organizada transnacional en instrumentos jurídicos*

y operativos en la lucha contra el tráfico internacional de drogas, Pamplona: Thomson Reuters Aranzandi, 2015.

BANCO CENTRAL DE RESERVA DEL PERÚ, *Glosario de términos económicos*. Disponible en: <http://www.bcrp.gob.pe/publicaciones/glosario/d.html>.

BANCO CENTRAL DE RESERVA DEL PERÚ, "Monedas digitales de bancos centrales", en *Moneda*, n.º 178, junio del 2019, p. 5. Disponible en: <https://www.bcrp.gob.pe/docs/Publicaciones/Revista-Moneda/moneda-178/moneda-178.pdf>.

BANCO CENTRAL DE RESERVA DE PERÚ, *Reporte de estabilidad financiera*, Lima: noviembre del 2021.

BANCO CENTRAL DE RESERVA DEL PERÚ, "Riesgos de las criptomonedas". Disponible en: <https://www.bcrp.gob.pe/sistema-de-pagos/articulos/riesgos-de-las-criptomonedas.html>.

BANCO DE ESPAÑA y CNMV, "Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión", 9 de febrero del 2021. Disponible en: <https://www.cnmv.es/Portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D>.

BANK FOR INTERNATIONAL SETTLEMENTS, "V. Criptomonedas: más allá del fenómeno de moda", en *Informe Económico Anual 2018 del BPI*.

BARRERA, José, "Chivo Wallet registra un promedio de 6,000 transacciones por día, según experto argentino", en *Diario el Mundo*, de fecha 24 de noviembre del 2021. Disponible en: <https://diario.elmundo.sv/economia/chivo-wallet-registra-un-promedio-de-6000-transacciones-por-dia-segun-experto-argentino>.

BARRIA HUIDOBRO, Cristian, "La dimensión del ciberespacio: Una propuesta de ciberseguridad", en *Cuaderno de Trabajo,* n.° 01-2019, Chile: CIEE, 2019.

BARRIO ANDRÉS, Moisés, “Concepto y clases de criptoactivos”, en *Criptoactivos. Retos y desafíos normativos*, Madrid: Wolters Kluwer, 2021.

BELLOCH ORTÍ, Consuelo. *Las tecnologías de la información y la comunicación (TIC),* Unidad Tecnología Educativa, Universidad de Valencia. Disponible en: <https://www.uv.es/~bellochc/pdf/pwtic1.pdf>.

BLANCO, Hernán, *Lavado de activos por sujetos obligados*, Buenos Aires: Abeledo Perrot, 2011.

BLANCO CORDERO, Isidoro, *El delito de blanqueo de capitales*, Pamplona: Aranzandi, 2012.

BELÉN LINARES, María, “Criptomoneda como herramienta para lavar activos criminales”, en *Ciberdelito nuevas tecnologías y derecho penal*, Ciudad de México: Editorial Flores, 2002.

BELÉN LINARES, María, “El uso de bitcoins para lavar activos. Aproximación a una técnica delictiva”, en *Sistema Penal e informática* n.º 02, Buenos Aires: Hammurabi, 2019.

BIAGOSCH, A. ZENÓN, “Los paraísos fiscales y el lavado de activos”, en *Tratado de lavado de activos y financiación del terrorismo,* t. I, Buenos Aires: La Ley, 2012.

BIT2ME ACADEMY, “¿Qué es Bitcoin Core?”, 2 de enero del 2020. Disponible en: <https://academy.bit2me.com/que-es-bitcoin-core/>.

BIT2ME ACADEMY, “¿Qué es decentraland (MANA)?”, 15 de junio del 2021. Disponible en: <https://academy.bit2me.com/que-es-decentraland-mana/>.

BIT2ME ACADEMY, "¿Qué es el SHA-256?", 23 de julio del 2018. Disponible en: <https://academy.bit2me.com/sha256-algoritmo-bitcoin/>.

BIT2ME ACADEMY, "¿Qué son las *cold wallets*?", 14 de febrero del 2020. Disponible en: <https://academy.bit2me.com/que-son-cold-wallets/>.

BIT2ME ACADEMY, "¿Qué son las *hot wallets*?", 11 de febrero del 2020. Disponible en: <https://academy.bit2me.com/que-son-hot-wallets/>.

BOAR, Andrei, *Descubriendo el bitcoin*, España: Profit Editorial, 2018.

BODOQUE AGREDANO, Ángel y Orduna LANAU, Alberto, *Guía de investigación en el lavado de activos mediante criptodivisas*, Madrid: El PAcCTO, 2022.

BONILLA EGIDO, Antonio y MELER PLAYAN, Javier, "Aplicaciones Distribuidas P2P (Seminaris de Caso)". Disponible en: <http://docencia.ac.upc.es/FIB/CASO/seminaris/2q0304/M9.pdf>.

BORJA JIMÉNEZ, Emiliano, *Curso de política criminal,* Valencia: Tirant lo Blanch, 2003.

BUNDESANSTALT FÜR FINANZDIENSTLEISTUNGSAUFSICHT, "Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer", 19 de diciembre del 2013. Disponible en: <https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html>.

BUTERIN, Vitalik, "Ethereum white paper: A Next-Generation Smart Contract and Decentralized Application Platform", en *First versión,* vol. 53, 2014

CALLEGARI, André Luis. *El delito de blanqueo de capitales en España y Brasil*, Bogotá: Universidad Externado de Colombia, 2003.

CARMONA BORJAS, Juan Cristóbal, *Mundo jurídico de las criptomonedas*, Caracas: Juan Cristóbal Carmona, 2019.

CARO CORIA, Carlos, "La regulación de los criptoactivos en Latinoamérica", en *Criptoactivos. Retos y desafíos normativos*, Madrid: Wolters Kluwer, 2021.

CARREÑO DUEÑAS, Dalia, "El Derecho en la era de la Virtualidad. Nuevas Realidad Nuevo Derecho Virtual", en *Ars Boni et Aequi*, vol. 8, n.º 2, 2012.

CASTILLO ALVA, José Luis, "La necesidad de determinación del 'delito previo' en el delito de lavado de activos, una propuesta constitucional", en *Gaceta Penal & Procesal Penal*, n.º 4, Lima, octubre 2009.

CHÁVEZ, O. A., "Análisis jurisprudencial del Bitcóin", en *Giuristi: Revista de Derecho Corporativo,* vol. 2, n.º 3, 2021, p. 7. Disponible en: <https://doi.org/10.46631/Giuristi.2021.v2n3.02>.

CHIVO WALLET, "Términos y condiciones". Disponible en: <https://chivowallet.com/terminos-y-condiciones.html>.

CECCARELLI, Cristina, "Criptoactivos en el punto de mira de los blanqueadores de capitales: España e Italia", en *Revista Electrónica de Estudios Penales y de Seguridad*, n.º 7, Sevilla, 2021 p. 5. Disponible en: <https://www.ejc-reeps.com/Cecarelli.pdf>.

CNN, *Washington es el primer estado en aprobar una ley para proteger la neutralidad de la red*, 2018. Disponible: <https://cnnespanol.cnn.com/2018/03/06/neutralidad-red-estados-unidos-washington-ley-hb2282/>.

COGHLAN, Jesse, “El Banco Mundial no apoyará el centro de criptomonedas Sango de la República Centroafricana”, en *Cointelegrah*, 26 de mayo del 2022. Disponible en: <https://es.cointelegraph.com/news/world-bank-won-t-support-central-african-republic-s-sango-crypto-hub>.

COINBASE, “What is *proof of work*" or "*proof of stake*?”. Disponible en: <https://www.coinbase.com/es/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake>.

COINTELEGRAPH, “Cajeros automáticos de Bitcoin: Guía para principiantes sobre los cajeros de Bitcoin”. Disponible en: <https://es.cointelegraph.com/bitcoin-for-beginners/bitcoin-atms-a-beginners-guide-to-bitcoin-teller-machines>.

COMITÉ DE BASILEA DE SUPERVISIÓN BANCARIA, *Documento consultivo. Tratamiento prudencial de las exposiciones a criptoactivos*, junio del 2021

CÓRDOBA, Fernando J., *Delito de lavado de dinero*, Buenos Aires: Hammurabi, 2015.

D’ALBORA, Francisco J., *Lavado de Dinero*, Buenos Aires: Ad-Hoc, 2006.

DECRYPT, “¿Cuáles son los Diferentes Tipos de Nodos de Bitcoin? Conoce Cómo se Mantiene la Red Bitcoin”, 31 de julio del 2022. Disponible en: <https://decrypt.co/es/resources/cuales-son-los-diferentes-tipos-de-nodos-de-bitcoin-conoce-como-se-mantiene-la-red-bitcoin>.

DEL CARPIO DELGADO, Juana, “Breves comentarios sobre la reforma del 2016 del delito de lavado de activos”, en *Actualidad Penal,* n.° 32, febrero del 2017.

DOMÍNGUEZ GÓMEZ, Javier, “Criptografía: Función SHA-25”, 2018. Disponible en: <https://docplayer.es/169481186-Criptografia-funcion-sha-256.html>.

DOMINGO, CARLOS, Todo *lo que querías saber sobre bitcoin, criptomonedas y blockchain y no te atrevías a preguntar*, Barcelona: Editorial Planeta, 2018.

DRUG ENFORCEMENT ADMINISTRATION, *2020 National Drug Threat Assessment*, marzo del 2021.

DURRIE FIGUEROA, Roberto, *La ganancia económica el delito*, Madrid: Marcial Pons, 2017.

ÉCIJA BERNAL, Álvaro. *El ciberespacio un mundo sin ley*, Madrid: Editorial Wolters Luwer, 2017.

ELBITCOIN.ORG, *Bitcoin: La moneda del futuro. Qué es, cómo funciona y por qué cambiará el mundo*, 2013.

EL ECONOMISTA, "El Salvador compra 500 bitcoines aprovechando baja en su previo", 9 de mayo del 2022. Disponible en: <https://www.eleconomista.com.mx/internacionales/El-Salvador-compra-500-bitcoines-aprovechando-baja-en-su-precio-20220509-0078.html>.

ENRIQUE GONZÁLES, Carlos, "Estrategias internacionales para el ciberespacio" en MINISTERIO DE DEFENSA, INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (eds.), *El ciberespacio. Nuevo escenario de confrontación*, España, 2012.

ESPARZA, Marco y NICASTRO, Maximiliano, *Blockchain is Life,* Lima: Saxo, 2018.

ETHEREUM.ORG, "Guía de Ethereum". Disponible en: <https://ethereum.org/es/whitepaper/#notes>.

FABIÁN CAPARRÓS, Eduardo, *El delito de blanqueo de capitales*, Madrid: Editorial Colex, 1998.

EUROPEAN CENTRAL BANK, *Virtual Currency Schemes*, Frankfurt am Main, octubre del 2012, p. 13. Disponible en: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>.

FABIÁN CAPARRÓS, Eduardo, *Combate del lavado de activos desde el sistema judicial*, Washington DC: Fimart, 2006.

FATF REPORT, "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing", París, 14 de setiembre del 2020.

FERNÁNDEZ BERMEJO, Daniel y MARTÍNEZ ATIENZA, Gorgonio, *Ciberseguridad, ciberespacio y ciberdelincuencia*, Pamplona: Editorial Aranzandi, 2018.

FERNÁNDEZ BERMEJO, Daniel, "El marco jurídico del delito de blanqueo de capitales", en *Blanqueo de capitales y TIC: Marco jurídico y europeo, modus operandi y criptomonedas,* Pamplona: Editorial Aranzandi, 2019.

FERNÁNDEZ BURGUEÑO, Pablo, "Doce cosas que deberías saber antes de usar bitcoins (La ley y el bitcoin)", 31 de agosto del 2014. Disponible en: <https://www.abanlex.com/2013/11/12-cosas-que-deberias-saber-antes-de-usar-bitcoins/>.

FERNÁNDEZ MARTÍNEZ, Juan Carlos, "Evasión de impuestos y ciberblanqueo", en Abel GONZÁLEZ y Daniel FERNÁNDEZ (dirs.), *El blanqueo de capitales y su relación con la cibercriminalidad*, Pamplona: Editorial Aranzandi, 2019.

FERNÁNDEZ, Yúbal, "Cómo entrar en la Deep Web: guía 2023 para entrar en TOR, ZeroNet, Freenet e I2P", en *Xataka,* 23 de marzo del 2023. Disponible en: <https://www.xataka.com/basics/como-entrar-deep-web-guia-2020-para-entrar-tor-zeronet-freenet-e-i2p>.

FINANCIAL ACTION TASK FORCE, “Report of new payment methods”, 13 de octubre del 2006. Disponible en: <http://www.fatf-gafi.org>.

FINANCIAL CONDUCT AUTORITY, “FCA warns consumers of the risks of investments advertising high returns based on cryptoassets”, enero del 2021. Disponible en: <https://www.fca.org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets>.

FINCEN GUIDANCE, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies”, 2009.

FINTECH MÉXICO, “¿Qué es FinTech?”. Disponible en: <https://www.fintechmexico.org/qu-es-fintech>.

FONDO MONETARIO INTERNACIONAL, “Comunicado de Prensa No. 22/13: El Directorio Ejecutivo del FMI concluye la Consulta del artículo IV con El Salvador correspondiente a 2021”, 25 de enero del 2022. Disponible en: <https://www.imf.org/es/News/Articles/2022/01/25/pr2213-el-salvador-imf-executive-board-concludes-2021-article-iv-consultation>.

FUENTES REQUENA, Ramon y GONZÁLES GARCÍA Abel, *Modus operandi* en el ciberblanqueo. Experimento práctico, en Abel GONZÁLEZ; Daniel FERNÁNDEZ (dirs.) *El blanqueo de capitales y su relación con la cibercriminalidad*, Pamplona: Editorial Aranzandi, 2019.

GRUPO DE ACCIÓN FINANCIERA DE LATINOAMÉRICA, *Ejercicio Bienal de Tipologías Regionales: Casos y tipologías regionales 2017-2018,* Quito, p. 3. Disponible en: <https://pplaft.cnbs.gob.hn/wp-content/uploads/2015/05/Informe-Tipologias-Regionales-GAFILAT-2018.pdf>.

GRUPO DE ACCIÓN FINANCIERA DE LATINOAMÉRICA, “Glosario de términos”. Disponible en: <https://www.gafilat.org/index.php/es/glosario-de-definiciones>.

GRUPO DE ACCIÓN FINANCIERA DE LATINOAMÉRICA, *Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales*, Buenos Aires, diciembre del 2021.

GRUPO DE ACCIÓN FINANCIERA DEL CARIBE, "Nota Interpretativa de la Recomendación N.° 15". Disponible en: <https://www.cfatf-gafic.org/index.php/es/documentos/gafi40-recomendaciones/421-fatf-recomendacion-15-nuevas-tecnologias>.

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Actualización dirigida en Implementación de Estándares del GAFI sobre Activos Virtuales y Proveedores de Servicios de Activos Virtuales*, París, 2022.

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Guía actualizada: EBR a los Activos Virtuales y Proveedores de Servicios de Activos Virtual,* París 2021.

GALLARDO, Ignacio, BAZÁN, Patricia y VENOSA, Paula, "Análisis del anonimato aplicado a criptomonedas", en XXV Congreso Argentino de Ciencias de la Computación, Río Cuarto, 2019.

GARCÍA CAVERO, P., "El decomiso de bienes relacionados con el delito en la legislación penal peruana", en *Derecho PUCP*, n.º 1, 2018, pp. 113-146.

GARCÍA CAVERO, Percy, *El delito de lavado de activos*, Lima: Jurista Editores, 2015.

GARCÍA DEL POYO, Rafael, "Algunos casos de uso", en *Criptoactivos. Retos y desafíos normativos,* Madrid: Wolters Kluwer, 2021.

GÁLVEZ VILLEGAS, Tomas, *El delito de lavado de activos*, Lima: Editorial Pacífico, 2014.

GÁLVEZ VILLEGAS, Tomas, “Autonomía del delito de lavado de activos y la prueba del delito previo”, en *Diálogo con la Jurisprudencia*, n.º 213, junio del 2016, pp. 17-37.

GALINDO, German, “Las senadoras de EE. UU. Kirsten Gillibrand y Cynthia Lummis presentan proyecto de ley sobre criptomonedas en Criptotendencias”, en *Criptotendencias.com*, 7 de junio del 2022. Disponible en: <https://www.criptotendencias.com/actualidad/las-senadoras-de-eeuu-kirsten-gillibrand-y-cynthia-lummis-presentan-proyecto-de-ley-sobre-criptomonedas/>.

GENDLER, Martín, “¿Qué es la neutralidad de la red? Peligros y potencialidades”, en *Hipertextos*, vol. 2, n.° 4, Buenos Aires, julio/diciembre del 2015, p. 11. Disponible en: <http://revistahipertextos.org/wp-content/uploads/2015/12/Qu%C3%A9-es-la-Neutralidad-de-la-Red-Mart%C3%ADn-Gendler.pdf>.

GOMA GARCÉS, Ignacio, *¿Qué es realmente Bitcoin?*, Madrid: Editorial Rasche, 2018.

GÓMEZ DE ÁGREDA, Ángel, “El Ciberespacio como Escenario de Conflictos, Identificación de las Amenazas”, en MINISTERIO DE DEFENSA e INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (eds.), *El ciberespacio. Nuevo escenario de confrontación*, España, 2012.

GÓMEZ ECHAVARRÍA, Cristina, “Todo lo que tienes que saber sobre Ross Ulbricht y Silk Road”, en *Vice*. Disponible en: <https://www.vice.com/es_co/article/qbqax5/todo-lo-que-tienes-que-saber-sobre-ross-ulbricht-y-el-silk-road>.

GÓMEZ INIESTA, Diego, “Utilización de las nuevas tecnologías en la comisión del blanqueo de dinero”, en *Revista Virtual USMP*, 2018, p. 5. Disponible: <https://derecho.usmp.edu.pe/cedp/revista/articulos/internacional/terrorismo.pdf>.

GÓMEZ LA TORRE, Rafael, “Estafas con bonos y criptoactivos dejan pérdidas de $254 millones en Reino Unido”, en *Criptonoticias*, 7 de febrero del 2019. Disponible en: <https://www.criptonoticias.com/seguridad-bitcoin/estafas-bonos-criptoactivos-reino-unido/>.

GONZALES BRIONES, Alfonso, “Fundamentos de programación e introducción a la tecnología blockchain*”* en *Economía digital y criptoactivos*, DoinGlobal y Fundación General de Universidad de Salamanca.

GONZÁLES GARCÍA, Abel y SANZ SIERRA, Javier, “Financiación del terrorismo y ciberblanqueo”, en Abel GONZÁLEZ y Daniel FERNÁNDEZ (dirs.), *El blanqueo de capitales y su relación con la cibercriminalidad*, Pamplona: Editorial Aranzandi, 2019.

GONZÁLES SÁNCHEZ, Margarita y HERNÁNDEZ SERRANO, María José, “Interpretación de la virtualidad. El conocimiento mediado por espacio de interacción social”, en *Apertura,* vol. 8, n.º 9, diciembre del 2008. Disponible en: <http://www.redalyc.org/articulo.oa?id=68811230001>.

GUTIÉRREZ, Omar y MORENO, Abraham, *El bitcoin: consideraciones financieras y legales sobre su naturaleza y propuesta de enfoque para su regulación*, Lima: Esan Ediciones, 2018.

GRANADOS ROMERO, Sonia, “La influencia de las nuevas tecnologías en el crimen organizado”, en *Propuestas Penales Nuevos Retos y Modernas Tecnologías. Memorias del IV Congreso de Jóvenes Investigadores de Ciencias Penales*, Salamanca: Ed. Universidad de Salamanca, 2016.

GRANGE, Jeremy, “Quiénes eran los *phreakers*, los extraordinarios personajes que hackeaban las redes telefónicas cuando no había computadores”, *BBC,* 1 de abril del 2017. Disponible en: <https://www.bbc.com/mundo/noticias-39433955>.

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Directrices para un Enfoque Basada en Riesgo. Monedas Virtuales*, junio del 2015.

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, "Informe Sobre Nuevos Métodos de Pago: Tarjetas Prepagas, Pagos por Telefonía Móvil y Pagos por Internet", Unión Europea, 2013

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, *Monedas virtuales: Definiciones claves y riesgos potenciales de LA/FT,* Unión Europea, 2014.

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL, "Virtual Currencies Key Definitions and Potential AML/CFT Risks", junio del 2014.

GRUPO EGMONT DE UNIDADES DE INTELIGENCIA FINANCIERA, *Proceso de apoyo y cumplimiento*, junio del 2014. Disponible en: <https://egmontgroup.org/wp-content/uploads/2021/09/Egmont_Group_of_Financial_Intelligence_Units_Support_and_Compliance_Process_Spanish.pdf>.

GUAITA, Martínez, J., "El fenómeno de las criptomonedas", en *Las criptomonedas: Digitalización del dinero 2.0*, Pamplona: Editorial Aranzandi, 2019.

HAJDARBEGOVIC, Nermin "Tecnología de Cadena de Bloques Explicada: Impulsando Bitcon", Disponible en: <https://www.toptal.com/bitcoin/tecnologia-de-cadena-de-bloques-explicada-impulsando-bitcoin>.

HERENCIA ANTÓN, Jesús, "Fundamentos tecnológicos de los criptoactivos", en *Criptoactivos. Retos y desafíos normativos*, Madrid: Walter Kluwers, 2021.

HERNÁNDEZ QUINTERO, Hernando, *El lavado de activos*, Medellín: Jurídicas Gustavo Ibáñez, 2002.

HIJAS CID, Eduardo, “Bitcoins: algunas cuestiones jurídicas”. Disponible en: <https://www.elnotario.es/index.php/hemeroteca/revista-66/6525-bitcoins-algunas-cuestiones-juridicas>.

HURTADO POZO, José, *Manual de derecho penal. Parte general I,* 3.º ed., Lima: Editorial Grijley, 2005.

HERRERA, Jesús, “3000 cajeros automáticos en España añaden compra bitcoin”, en *Criptonoticias*, 15 de septiembre del 2022. Disponible en: <https://www.criptonoticias.com/comunidad/espana-3000-cajeros-automaticos-funcionan-bitcoin/>.

HERRERA, Diego y VADILLO, Sonia, *Sandbox regulatorio en América Latina y el Caribe para el ecosistema FinTech y el sistema financiero,* Banco Interamericano de Desarrollo, marzo del 2018, p. 5

IBÁÑEZ JIMÉNEZ, Javier, “Emisión, representación y gestión de criptoactivos”, en *Criptoactivos. Retos y desafíos normativos*, Madrid: Wolters Kluwer, 2021.

IGUAL, David, *Fintech: Lo que la tecnología hace por las finanzas*, Barcelona: Profit Editorial, 2016.

INTERNATIONAL CRIMINAL POLICE ORGANIZATION, “Cryptojacking makes Money for Criminals”, INTERPOL General Secretariat, Lyon, 2020, p. 1.

JESÚS VELASCO, Juan, “Breve historia de la criptografía”, en *Diario.es*, 20 de mayo del 2014. Disponible en: <https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html>.

JIMÉNEZ, Félix, *Elementos de teoría y políticas macroeconómicas para una economía abierta,* Lima: Fondo Editorial - Pontificia Universidad Católica del Perú, 2012.

JIMÉNEZ HERRERA, Juan Carlos, *Manual de derecho penal informático*, Lima: Jurista Editores, 2017.

JOFFRE CALASICH, Fabio, "Cripto criminalidad. NFT's, DEX's, *cross chain bridges*, nuevos datos e innovaciones en la tecnología blockchain de uso criminal", en *Ilícitos económicos y evidencia digital*, Argentina: Editores Fondo Editorial, 2022.

JONSHTON, David, ONAT YILMAZ, Sam, KANDAH, Jeremy, BENTENITIS, Nikos, HASHEMI, Farzad, GROSS, Ron, WILKINSON, Shanw y MASON, Steve, *The General Theory of Decentralized Applications, DApps*, enero del 2015. Disponible en: <http://cryptochainuni.com/wp-content/uploads/The-General-Theory-of-Decentralized-Applications-DApps.pdf>.

Jorge, GUILLERMO, "Políticas de Control del Lavado de Dinero", en *Tratado de lavado de activos y financiación al terrorismo*, t. I, Buenos Aires: La Ley, 2012,

KESSLER, Sam, "La fusión de Ethereum ya es un hecho y abre una nueva era para la segunda blockchain más grande", en *CoinDesk*, del 15 setiembre del 2022. Disponible en: <https://www.coindesk.com/tech/2022/09/15/la-fusion-de-ethereum-ya-es-un-hecho-y-abre-una-nueva-era-para-la-segunda-blockchain-mas-grande/>.

KIAYIAS, Aggelos, RUSSELL, Alexander, DAVID, Bernardo y OLIYNYKOV, Roman, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol", 21 de agosto del 2017. Disponible en: <https://app.box.com/s/eui5ayv98rw5m9ysvtnkrirlm5wpm7og>.

KOŁODZIEJCZYK, Hanna y JARNO Claudia, "Stablecoin - the stable cryptocurrency", *en Studia BAS*, vol. 3, n.º 63, 2020, pp. 155-170.

KNIFFKI, Johannes, "Transnacionalidad y Comunidad: un enfoque construccionista y discursivo", en *Espacios transnacionales: revista latinoamericana-europea de pensamiento y acción social,* año 1, n.º 1, 2013.

LA CAPITAL, “EE. UU. deroga la ley de Obama que aseguraba la neutralidad de la red”, 15 de diciembre del 2017. Disponible en: <https://www.lacapital.com.ar/el-mundo/eeuu-deroga-la-ley-obama-que-aseguraba-la-neutralidad-la-red-n1524319.html>.

Las tecnologías wifi y wimax, p. 15. Disponible en: <http://www.dip badajoz.es/agenda/tablon/jornadawifi/doc/tecnologias_wifi_wmax.pdf>.

LAMAS PUCCIO, Luis, *Lavado de activos y operaciones sospechosas*, Lima: Pacifico Editores, 2016, p. 53.

LAMAS SUÁREZ, Gerardo, *Cibercrimen, bitcoins y el lavado de activos*, Lima: Estación la Cultura, 2019.

LAMAS SUÁREZ, Gerardo, “Criptomonedas y el lavado de activos”, en *Ciberseguridad, cibercrimen y nuevas tecnologías - Riesgos y respuestas jurídicas*, Lima: Derecho Global, 2022.

LAMAS SUÁREZ Gerardo, *El delito previo en el tipo penal de lavado de activos*, Lima: Instituto Pacifico, 2017, p. 92.

LAMAS SUÁREZ, Gerardo, “El derecho penal y procesal penal en la nueva sociedad digital en el Perú”, en *Peruweek.pe*, Lima: 2020. Disponible en: <https://www.peruweek.pe/tag/gerardo-luis-lamas-suarez/>.

LESSIG Lawrence, “Las leyes del ciberespacio”, en *THEMIS: Revista de Derecho* n.º 44, pp. 171-179. Disponible en: <http://revistas.pucp.edu.pe/index.php/themis/article/view/10069/10504>.

LINS RIBEIRO, “La condición de la transnacionalidad”, en *Maguaré,* n.º 14, 1999.

LÓPEZ BISCAYART, Javier y LINARES, María, “Lavado de Dinero: Responsabilidad Judicial en el Marco de los Compromisos Internacionales asumidos en la materia”, en *Tratado de lavado de activos y financiación al terrorismo,* t. I, Buenos Aires: La Ley, Fondo Editorial de Derecho y Economía, 2012.

MANSO PORTO, Teresa, “El blanqueo de capitales entre la dogmática y la política criminal internacional: resultados desde una perspectiva de derecho comparado”, en *El delito de lavado de activos,* t. I., Lima: Editorial Grijley, 2017.

MARTÍN ENRÍQUEZ, Álvaro, NAVARRO GIMENO, M.ª Ángeles, RODRÍGUEZ FERNÁNDEZ, Esther y ONTIVEROS BAEZA, Emilio, *Las TIC y el sector financiero del futuro*, Madrid: Editorial Ariel, 2011.

MARTÍN RAMALLAL, Pablo, SABATER-WASALDÚA, Jesús y RUIZ-MONDAZA, Mercedes, “Metaversos y mundos virtuales, una alternativa a la transferencia del conocimiento: El Caso OFFF-2020”, en *Fonseca, Journal of Communication*, n.º 24, junio del 2022, pp. 87-107. Disponible en: <https://revistas.usal.es/cuatro/index.php/2172-9077/article/view/28287/27840>.

MARTÍNEZ HERNÁNDEZ, Luis Manuel, CECEÑAS TORRERO, Paula Elvira, ONTIVEROS HERNÁNDEZ, Verónica Clementina, “Qué es el ciberespacio”, en Luis MARTÍNEZ, PAULA CECEÑAS, Verónica ONTIVEROS (coords.), *Virtualidad, ciberespacio y comunidades virtuales,* México: Red Durango de Investigaciones Educativas, 2014, p. 48. Disponible en: <http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf>.

MARTÍNEZ MERCHÁN, Mary Luz, “Regulación de los criptoactivos en Colombia”, en *BDO,* 22 febrero de 2022. Disponible en: <https://www.bdo.com.co/es-co/publicaciones/boletines-audit/regulacion-de-los-criptoactivos-en-colombia>.

MARTÍNEZ, Matilde S., “Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil”, en *Cibercrimen y delitos informáticos Los nuevos tipos penales en la era del internet,* Buenos Aires: Erreius, 2018.

MENDOZA LLAMACPONCCA, Fidel, *El delito de lavado de activos. Aspectos sustantivos y procesales del tipo base de lavado de activos como delito autónomo,* Lima: Editorial Pacifico, 2017.

MENDOZA LLAMACPONCCA, Fidel, *Lavado de activos y criminalidad empresarial*, Lima: Jurista Editores, 2022.

MENÉNDEZ PASTORELLI, Paola, "NFTS (not fungible tokens) desde una perspectiva jurídica", en *Biblioteca Nacional del Congreso de Chile - Asesoría Técnica Parlamentaria*, julio del 2022.

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL, "Informe sobre supervisión en España de normativa europea en materia de acceso a una internet abierta (Neutralidad de la red)", 2019, p. 8. Disponible: <https://avancedigital.mineco.gob.es/banda-ancha/Informesneutralidadred/NN_informe_ESPANA_2019_28_07_20.pdf>.

MIRÓ LLINARES, Fernando, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid: Marcial Pons, 2012.

MIRÓ LLINARES, Fernando, *Cibercrimen, cibercriminales y cibervíctimas,* Universitat Oberta de Catalunya, 2013. Recuperado de <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/70006/4/Delincuencia%20y%20TICs_M%C3%B3dulo%202_Cibercrimen%2C%20cibercriminales%20y%20ciberv%C3%ADctimas.pdf>.

MORA ASTABURUAGA, Aitor, "Smart Contracts. Reflexiones sobre su concepto, naturaleza y problemática en el derecho contractual", en *Revista de Derecho Uned*, n.º 27, 2021.

MORALES GARCÍA, Oscar, "Riesgos penales de la posesión, adquisición, venta e intercambio de criptoactivos", en *Criptoactivos retos y desafíos normativos*, Madrid: Wolter Klawuers, 2021.

MUÑOZ CONDE, Francisco, *Derecho penal. Parte general*, Valencia: Tirant lo Blanch, 2004.

NAKAMOTO, Satoshie, "Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario", 2008. Disponible en: <https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf>.

NARRALO BOLARTE, Enrique, "Incidencia de las nuevas tecnologías en el sistema penal: Aproximación al derecho penal en la sociedad de la información", en *Derecho y Conocimiento,* vol. 1, Universidad de Huelva: 2001, pp. 191-257.

NAVAS BLÁNQUEZ, JUAN JOSÉ, "Embargo y decomiso de criptomonedas en el Espacio Judicial Europeo", en *Revista de Estudios Europeos*, n.º extraordinario monográfico 1, Ediciones Universidad de Valladolid, 2023, pp. 349-383.

NAVARRO CARDOSO, Fernando, "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", en *Revista Electrónica de Ciencia Penal y Criminología*, n.º 21, 2019. Disponible en: <http://criminet.ugr.es/recpc>.

NIETO MARTÍN, Adam y GARCÍA MORENO, Beatriz, "Criptomonedas y derecho penal: más allá del blanqueo de capitales", en *Revista Electrónica de Ciencia Penal y Criminología*, n.º 23-17, 2021, pp. 1-31. Disponible en: <http://criminet.ugr.es/recpc/23/recpc23-17.pdf>.

NIST - COMPUTER SECURITY RESOURCE CENTER, "Cyberspace". Disponible en: <https://csrc.nist.gov/glossary/term/cyberspace#:~:text=Definition(s)%3A,and%20embedded%20processors%20and%20controllers>.

NOVELLA GONZÁLES DEL CASTILLO, Eduardo, "Hacia una nueva regulación europea: El Digital Finance Package", en *Criptoactivos. Retos y desafíos normativos*, Madrid: Wolters Kluwer, 2021.

NOVELLA GONZÁLES DEL CASTILLO, Eduardo, *El futuro reglamento europeo para de criptoactivos (propuesta mica)*, Madrid: Wolters Kluwer, 2021.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO, *Compendio de ciberdelincuencia organizada*, Viena, febrero del 2022, p. 8. Disponible en: <https://www.unodc.org/documents/Cybercrime/tools-and-resources/Compendio_de_delincuencia_organizada_ES.pdf>.

OPSITEL, "Neutralidad de red". Disponible en: <https://www.osiptel.gob.pe/portal-de-operadoras/regulacion/neutralidad-de-red/>.

ORGANIZACIÓN DE LAS NACIONES UNIDAS, "Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético", 12.° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador (Brasil), 12 a 19 abril del 2010, p. 4. Disponible en: <https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf>.

PACHECO JIMÉNEZ, María, "De La Tecnología Blockchain a La Economía Del Token", en *Derecho PUCP*, n.º 83, 2019, p. 64. Disponible en: <https://revistas.pucp.edu.pe/index.php/derechopucp/article/view/21468>.

PASTRÁN, Rosa María, "Athena Bitcóin provee la red de cajeros Chivo al gobierno", en *El Economista,* 18 de noviembre del 2021. Disponible en: <https://www.eleconomista.net/economia/Athena-Bitcoin-provee-la-red-de-cajeros-Chivo-al-gobierno-20211118-0008.html>.

PALOMINO MARTÍN, José María, *Derecho penal y nuevas tecnologías*, Valencia: Editorial Tirant lo Blanch, 2016.

PÉREZ BES, Francisco, *Código de derecho de la ciberseguirdad*, Madrid: Inicibe, 2021.

PÉREZ CORTÉS, Manuel, “Tecnologías para la defensa en el ciberespacio”, en MINISTERIO DE DEFENSA e INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (eds.), *El ciberespacio. Nuevo escenario de confrontación*, España, 2012.

PÉREZ LÓPEZ, Xesús, “Las criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento para el blanqueo de capitales en la Unión Europea y España”, en *Revista de Derecho Penal y Criminología*, 3.° época, n.° 18, 2017, pp. 141-187.

PÉREZ-SOLÀ, Cristina y HERRERA-JOANCOMARTÍ, Jordi, “Bitcoins y el problema de los generales bizantinos”, Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información (RECSI XIII), Universidad de Alicante, 2-5 de septiembre del 2014, p. 241. Disponible en: <https://web.ua.es/en/recsi2014/documentos/papers/bitcoins-y-el-problema-de-los-generales-bizantinos.pdf>.

PICÓN GONZÁLES, Jorge, *Paraísos fiscales: Rompiendo mitos: Evolución, uso y medidas antiparaísos,* Lima: Dogma Ediciones, 2020.

PLAZA, Nickolas, “Cártel de México lavó dinero a través de Binance usando bitcoin, reveló Forbes”, en *Criptonoticias,* 21 de diciembre del 2022. Disponible en: <https://www.criptonoticias.com/seguridad-bitcoin/cartel-mexico-lavo-dinero-binance-usando-bitcoin-revelo-forbes/>.

PRADO SALDARRIAGA, Víctor, *Criminalidad organizada. Parte especial*, Lima: Pacífico Editores, 2016.

PRADO SALDARRIAGA, Víctor, “Lavado de Activos en el Perú: problemas y alternativas”, en *Lex: Revista de la Facultad de Derecho y Ciencia Política de la Universidad Alas Peruanas*, vol. 17, n.º 24, 2019, pp. 161-178. Disponible en: <https://revistas.uap.edu.pe/ojs/index.php/LEX/article/view/1815/1983>.

PRADO SALDARRIAGA, Víctor, *Lavado de activos y financiación del terrorismo*, Lima: Editora Jurídica Grijley, 2007.

QUARMBY Brian, “El proyecto de ley Lummis-Gillibrand sobre criptomonedas probablemente se aplace hasta el año que viene”, en *Cointelegraph*, 20 de julio del 2022. Disponible en: <https://es.cointelegraph.com/news/lummis-gillibrand-crypto-bill-likely-deferred-to-next-year>.

RAMÍREZ MORÁN, David, “Riesgos y regulación de las divisas virtuales” en *Instituto Español de Estudios Estratégicos*, 19 de marzo del 2014, p. 5. Disponible en: <http://www.ieee.es/Galerias/fichero/docs_analisis/2014/DIEEEA182014_ImplicacionesFuturoDivisasElectronicas_DRM.pdf>.

REÁTEGUI SÁNCHEZ, James y REÁTEGUI LOZANO, Rolando, *El delito de lavado de activos y de crimen organizado,* Lima: A&C Ediciones, 2017.

REYES ECHANDÍA, Alfonso, *La tipicidad*, Bogotá: Temis, 1989.

RIVERA JIMÉNEZ, Adriana, DE LA MORA MONDRAGÓN, Maritza, GISHOLT AVILÉS, Pamela y CAMACHO HERNÁNDEZ, Salvador, *Los NFT en la propiedad intelectual,* en blog *AMPPI,* n.° 45, junio-julio del 2021. Disponible en: <https://amppi.org.mx/wp-content/uploads/2021/07/45Blg_7aArtCmtTICS-NFTs_JunJul2021.pdf>.

RODRÍGUEZ GÓMEZ, Cristina. “Bitcoin: problemas reales”, en *Derecho y TIC. Vertientes actuales*, México: UNAM, 2016. Disponible en: <https://archivos.juridicas.unam.mx/www/bjv/libros/9/4065/18.pdf >.

RODRÍGUEZ MIRANDA, Carla y VANINI CARBONI, Ornella, “Neutralidad de la red, un debate pendiente en Argentina”, en *Revista Oficios Terrestres*, n.º 8, México: UNAM, 2016. Disponible en: <https://perio.unlp.edu.ar/ojs/index.php/oficiosterrestres/article/view/1587/1428>

ROSEMBUJ, Tulio. *Bitcoin*, Barcelona: Editorial el Fisco, 2015

ROSAS CASTAÑEDA, Juan Antonio, *La prueba en el delito de lavado de activos*, Lima: Gaceta Jurídica, 2015.

ROXIN, Claus, *Teoría del tipo penal: Tipos abiertos y elementos jurídicos del deber*, Buenos Aires: Depalma, 1979.

RUIZ RODRÍGUEZ, Luis y GONZÁLES AGUDELO, Gloria, "El factor tecnológico en la expansión del crimen organizado", en *Centro de Investigación Interdisciplinaria en Derecho Penal Económico*, 2014. Disponible en: <https://rodin.uca.es/bitstream/handle/10498/23069/EL-FACTOR-TECNOLOGICO-EN-LA-EXPANSION-DEL-CRIMEN-ORGANIZADO.pdf?sequence=1&isAllowed=y>.

RUIZ-CLAVIJO GARCÍA, Teresa, "Recursos para la prevención de delitos relacionados con el blanqueo de capitales y cibercriminalidad", en Abel GONZÁLEZ y Daniel FERNÁNDEZ (coords.), *El blanqueo de capitales y su relación con la cibercriminalidad*, Pamplona, Editorial Aranzandi, 2019.

SAIN, Gustavo, *La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal en cibercriminal y delitos informáticos*, Buenos Aires: Erreius, 2018.

SALAS BETETA, Christian, "El delito de lavado de activos y su dificultad probatoria en el CPP de 2004. Comentarios al Decreto Legislativo N.° 1106", en *Gaceta Penal & Procesal Penal*, n.º 35, mayo del 2012, Lima.

SALDAÑA TABOADA, Patricia, "¿Por qué las organizaciones criminales utilizan criptomonedas? Los bitcoins en el crimen organizado", en *El Criminalista Digital. Papeles de Criminología*, n.º 6, 2017.

SÁNCHEZ, Óscar, *Bitcoin: Qué son las criptomonedas y como ganar dinero fácil con ellas*, San Bernardino CA, 2017.

SANTIAGO, Raúl y NAVARIDAS, Fermín, “La web 2.0 en escena”, en *Píxel-Bit. Revista de Medios y Educación,* n.º 41, julio del 2012, pp. 19-30. Disponible en: <http://www.redalyc.org/pdf/368/36828247002.pdf>.

SANTÍN GONZALES, Abel, “Peer to Peer. Sistemas Operativos Distribuidos”. Disponible en: <http://www.dit.upm.es/~joaquin/so/p2p/p2p.pdf>.

SECURITIES AND EXCHANGE COMMISSION, Release No. 81207/25, julio de 2017. Disponible en: <https://www.sec.gov/files/litigation/investreport/34-81207.pdf>.

SILVA, Magaly, “El acelerado crecimiento de las fintech y los desafíos para su regulación”, en *Moneda*, n.º 171, 2017, pp. 42-26.

SILVA SÁNCHEZ, Jesús María, *La expansión del derecho penal: Aspectos de la política criminal y las sociedades postindustriales*, Buenos Aires: Edisofer, 2011,

SIRVIERA MARTINS, Amaury, *El derecho y las nuevas tecnologías en ciberdelitos*, Ciudad de México: Nuevas Tecnologías y Derecho Penal, 2022.

SOLÍS UMAÑA, Mario, “Libertarismo y justicia social: La libertad como valor político”, en *Revista Humanidades*, vol. 1, n.º 1, 2011, p. 2. Disponible en: <file:///C:/Users/Estudio%20Lamas%20Puccio/Downloads/Dialnet-LibertarismoYJusticiaSocial-4920531.pdf>.

STANG, Gerald, “Bienes comunes globales: Entre la cooperación y la competencia”, *Issue Brief,* n.º 17, Instituto de Estudios de Seguridad de la Unión Europea, 2013.

SUPERINTENDENCIA DEL MERCADO DE VALORES, “Advertencia sobre la adquisición de monedas virtuales o criptomonedas y la participación en esquemas de financiamiento mediante el uso de unidades de valor denominadas tokens”, Lima, 2020. Disponible en: <https://www.smv.gob.pe/Uploads/COMUNICADO_Criptomoneda_ICO_Logo.pdf>.

SUPERINTENDENCIA DE MERCADO DE VALORES, “Comunicado advertencia sobre la adquisición de monedas virtuales o criptomonedas y la participación en esquemas conocidos como ICOs”. Disponible en: <https://www.smv.gob.pe/uploads/COMUNICADO%20ICOS%2021_11_2.pdf>.

SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP, “Activos virtuales y proveedores de servicios de activos virtuales: Diagnóstico situacional, legislación comparada y exposición a los riesgos de LA/FT en el Perú”, 2009, p. 22.

SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP, Oficio N.º 05294-2022-SBS, 9 de febrero del 2022.

SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP, Resolución SBS N.º 1201-2018, 28 de marzo de 2018

SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP, “Sergio Espinosa: además de las normas de la UIF, se requiere una regulación más amplia para las criptomonedas”, en *Prevención de lavado de activos y financiamiento del terrorismo,* p. 9, 2022.

SUPERINTENDENCIA NACIONAL DE ADUANAS Y DE ADMINISTRACIÓN TRIBUTARIA, Informe N.º 057-2017-SUNAT/5D0000. Disponible en: <https://www.sunat.gob.pe/legislacion/oficios/2017/informe-oficios/i057-2017.pdf>.

SUEIRO, CARLOS, *El derecho penal en la era digital*, Lima: A&C Ediciones, 2018.

SWISS FINANCIAL MARKET SUPERVISORY AUTHORITY, “FINMA makes an unfavorable prognosis for Bitcoin Suisse AG licensing produce”, marzo del 2021. Disponible en: <https://www.finma.ch/en/news/2021/03/20210317-mm-btcs/>.

TAPSCOTT, Don y TAPSCOTT, Alex, *La revolución Blockchain*, Bogotá: Editorial Planeta, 2017.

TEMPERINI, Marcelo, “Delitos Informáticos y Cibercrimen: Alcances, conceptos y características”, en *Cibercriminal y delitos informáticos*, Buenos Aires: Erreius, 2018.

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM, *Decentralised Finance (DeFi)*, 2022.

THE WHITE HOUSE, “FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets”, setiembre del 2022. Disponible en: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/>.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *El ciberdelito: Guía para los países en desarrollo,* abril del 2012. Disponible en: <https://www.itu.int/dms_pub/itu-d/oth/01/0b/d010b0000073301pdfs.pdf>.

UNITED NATIONS OFFICE ON DRUGS AND CRIME, *United States of America v. Ross William Ulbricht*, No. 15-1815-cr (2d Cir. May 31, 2017). Disponible en: <https://sherloc.unodc.org/cld/en/case-law-doc/cybercrimecrimetype/usa/2017/united_states_of_america_v._ross_william_ulbricht_no._15-1815-cr_2d_cir._may_31_2017.html>.

U.S. SECURITE AND EXHCHANGE COMMISSION, “Investor Alert: Bitcoin and other virtual currency - releated investments”, mayo del 2014. Disponible en: <https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html>.

VEGA AGUILAR, Alberto y ARÉVALO MINCHOLA, Maguín, *Ciberdelitos. Análisis del sistema penal,* Lima: Editorial Iustitas, 2022.

VILLALPANDO, Waldo, *Crimen organizado transnacional*, Buenos Aires: Astres, 2014.

VILLAVICENCIO TERREROS, Felipe, “Delitos Informáticos”, en *IUS ET VERITAS,* vol. 24, n.º 49, 2014, pp. 284-304. Disponible en: <https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630>.

WEIGEND Thomas y JECHECK, Hans, *Tratado de derecho penal. Parte general*, Granada: Comares, 2003.

WHARTON BLOCKCHAIN AND DIGITAL ASSET PROJECT Y WORLD ECONOMIC FORUM, “Defi Beyond the Hype. The Emerging World of Decentralized Finance”, mayo del 2021.

ZAMORA SÁNCHEZ, Pedro, *Marco jurídico del lavado de dinero*, México: Editorial Mexicana, 2000.

ZOCARO MARCOS, “El marco regulatorio de las criptomonedas en Argentina. Comparativa con otros países”, en *Centro de Estudios de Administración Tributaria.*

ZÚÑIGA RODRÍGUEZ, Laura, *Criminalidad de empresa y criminalidad organizada*, Lima: Jurista Editores, 2013.

ZÚÑIGA RODRÍGUEZ, Laura, *Política criminal*, Madrid: Colex, 2001, p. 252.

ZÚÑIGA RODRÍGUEZ, Laura, *El concepto de criminalidad organizada transnacional: problemas y propuestas.* Nuevo Foro Penal, *[S. l.]*, v. 12, n. 86, p. 62–114, 2016. DOI: 10.17230/nfp.12.86.2. Disponible en: https://publicaciones.eafit.edu.co/index.php/nuevo-foro-penal/article/view/3646.