REVISTA CIENTÍFICA
Ciencia y Método
ISSN 3103-1072

EDITORIAL GRUPO AEA

Artículo Científico

Evolución del derecho penal económico frente a los delitos financieros digitales

Developments in economic criminal law vis-à-vis digital financial crimes

Mina-Bone, Santos Geovanny [1]
https://orcid.org/0000-0002-2526-3988
santos.mina@utelvt.edu.ec
Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador, Esmeraldas.

Autor de correspondencia [1]

DOI / URL: https://doi.org/10.55813/gaea/rcym/v2/n3/50

Resumen: El artículo analiza la evolución del derecho penal económico frente a los delitos financieros digitales, un fenómeno cada vez más presente debido a la digitalización de las transacciones financieras y el auge de las criptomonedas. Este estudio aborda cómo los marcos legales tradicionales se ven desbordados por las características transnacionales y tecnológicas de los delitos financieros digitales. Se empleó una metodología exploratoria mediante revisión bibliográfica, utilizando fuentes académicas, jurídicas y documentos normativos. Se destacan los nuevos tipos penales relacionados con los criptoactivos, la responsabilidad penal empresarial, y la necesidad de normas internacionales armonizadas. Asimismo, el artículo identifica los principales desafíos para la persecución penal de estos delitos, como el anonimato de los autores, los conflictos jurisdiccionales y las limitaciones técnicas en las investigaciones. En conclusión, la investigación propone una actualización de las normativas y el fortalecimiento de las capacidades investigativas, resaltando la importancia de la cooperación internacional en la lucha contra la criminalidad económica digital.

Palabras clave: derecho penal económico, delitos financieros digitales, criptomonedas, jurisdicción, persecución penal.

Check for updates

Received: 18/Ago/2024
Accepted: 08/Sep/2024
Published: 30/Sep/2024

Cita: Mina-Bone, S. G. (2024). Evolución del derecho penal económico frente a los delitos financieros digitales. *Revista Científica Ciencia Y Método*, *2*(3), 52-66. https://doi.org/10.55813/gaea/rcym/v2/n3/50

Revista Científica Ciencia y Método (RCyM)
https://revistacym.com
revistacym@editorialgrupo-aea.com
info@editoriagrupo-aea.com

Abstract:

The article analyzes the evolution of economic criminal law in the face of digital financial crimes, a phenomenon increasingly present due to the digitization of financial transactions and the rise of cryptocurrencies. This study addresses how traditional legal frameworks are overwhelmed by the transnational and technological characteristics of digital financial crimes. An exploratory methodology was employed through literature review, using academic, legal sources and regulatory documents. It highlights the new criminal types related to cryptoassets, corporate criminal liability, and the need for harmonized international standards. The article also identifies the main challenges for the criminal prosecution of these crimes, such as the anonymity of the perpetrators, jurisdictional conflicts and technical limitations in investigations. In conclusion, the research proposes an update of regulations and the strengthening of investigative capacities, highlighting the importance of international cooperation in the fight against digital economic crime.

Keywords: economic criminal law, digital financial crimes, cryptocurrencies, jurisdiction, criminal prosecution.

1. Introducción

La evolución del derecho penal económico ha experimentado profundas transformaciones ante el auge de los delitos financieros digitales, que se han convertido en una amenaza creciente para la estabilidad económica y la confianza social. En las últimas décadas, la digitalización de las transacciones financieras, la expansión de las criptomonedas y la proliferación de plataformas electrónicas han propiciado la aparición de nuevas modalidades delictivas que superan los marcos normativos tradicionales (Zhao, 2021). Este fenómeno plantea un desafío jurídico de gran envergadura, puesto que las tipologías delictivas vinculadas con el ciberespacio se caracterizan por su transnacionalidad, volatilidad tecnológica y elevada capacidad de daño patrimonial. Tales características revelan lagunas sustantivas y procesales que dificultan la adecuada persecución penal, especialmente en contextos en los que los activos digitales se ocultan o transfieren mediante complejos mecanismos de anonimización (Maras, 2020).

Uno de los factores determinantes que agravan este problema radica en la insuficiencia de los sistemas de control y supervisión financiera. Si bien la regulación clásica se centraba en delitos como el fraude bancario, el blanqueo de capitales y la evasión fiscal, hoy se constata que las prácticas criminales en entornos virtuales implican patrones dinámicos y cambiantes que desbordan los límites de la jurisdicción penal tradicional (Mackenzie et al., 2020). La ausencia de marcos normativos uniformes y la disparidad de criterios interpretativos entre sistemas jurídicos contribuyen a la impunidad de los autores, quienes se aprovechan de las brechas

regulatorias. Además, la sofisticación tecnológica con la que se perpetran estos delitos requiere capacidades investigativas especializadas que no todos los Estados poseen, lo cual incrementa la vulnerabilidad institucional frente a redes criminales de gran alcance (Broadhurst et al., 2014).

La creciente incidencia de delitos financieros digitales impacta de manera directa en la confianza ciudadana en el sistema económico y en la percepción de la legitimidad del derecho penal económico. Desde una perspectiva macroeconómica, la multiplicación de esquemas fraudulentos, como las estafas de inversión en criptomonedas, ha derivado en perjuicios millonarios para particulares y empresas (Vinelli, 2021). A nivel micro, los afectados suelen enfrentar obstáculos para obtener resarcimiento efectivo debido a la opacidad de las operaciones y la dispersión internacional de los activos. Estos efectos negativos subrayan la necesidad de repensar el alcance y la eficacia de los instrumentos de prevención, detección y sanción de la criminalidad económica en el entorno digital.

La justificación de este estudio se fundamenta en la relevancia que tiene el fortalecimiento del derecho penal económico para preservar la estabilidad del orden jurídico-financiero. El abordaje de estas problemáticas desde una perspectiva comparada permite identificar buenas prácticas regulatorias y avances doctrinales que podrían inspirar reformas legislativas en distintos países. A su vez, la revisión sistemática de la literatura especializada facilita comprender los retos que plantea la incorporación de tecnologías disruptivas como la cadena de bloques (blockchain) y los criptoactivos en la actividad probatoria y en la definición típica de las conductas delictivas (Irwin & Milad, 2016). La viabilidad de la investigación radica en el acceso a fuentes doctrinales, jurisprudenciales y normativas actualizadas, así como en la disponibilidad de bases de datos internacionales que documentan el impacto de estos delitos y las respuestas estatales.

El objetivo principal de este artículo consiste en examinar la evolución del derecho penal económico frente a los delitos financieros digitales, mediante un análisis crítico de la literatura científica, la normativa comparada y las experiencias internacionales de persecución penal (Samaniego-Quiguiri, 2023). Este propósito persigue aportar elementos que contribuyan a la delimitación de conceptos, la identificación de tendencias regulatorias y la formulación de propuestas de mejora legislativa orientadas a optimizar la eficacia de la tutela penal de los bienes jurídicos económicos. En definitiva, la transformación acelerada del ecosistema financiero exige un replanteamiento profundo de los fundamentos, límites y técnicas del derecho penal económico, que garantice su capacidad de respuesta ante amenazas complejas y transversales.

2. Materiales y métodos

La metodología empleada en el presente artículo se fundamenta en un enfoque exploratorio de revisión bibliográfica, orientado a examinar de manera sistemática la evolución del derecho penal económico frente a los delitos financieros digitales. Este enfoque resulta adecuado debido a la naturaleza emergente y dinámica del objeto de estudio, que requiere un análisis crítico y comparado de la literatura especializada, la normativa vigente y los informes de organismos internacionales. Para ello, se realizó una búsqueda exhaustiva de fuentes primarias y secundarias en bases de datos académicas de alta relevancia, tales como Scopus, Web of Science, JSTOR y HeinOnline, así como en repositorios institucionales de organizaciones internacionales dedicadas a la prevención de la criminalidad económica y cibernética.

La selección de la bibliografía se efectuó con base en criterios de actualidad, pertinencia temática y rigor científico. Se incluyeron principalmente artículos de revisión, estudios empíricos, monografías jurídicas y documentos normativos publicados en los últimos quince años, priorizando aquellos que abordaran de manera específica el impacto de la digitalización en la criminalidad económica, la regulación penal de las criptomonedas, la tipificación de nuevas modalidades de fraude financiero y las estrategias de cooperación internacional en la persecución penal. Para optimizar la organización de la información recopilada, se elaboraron matrices de análisis en las que se clasificaron las fuentes según su enfoque conceptual, jurídico y operativo, facilitando así la identificación de tendencias regulatorias, vacíos normativos y propuestas de mejora legislativa.

El procedimiento de revisión contempló varias etapas. Inicialmente, se definieron las palabras clave y descriptores temáticos que orientaron las búsquedas, tales como “derecho penal económico”, “delitos financieros digitales”, “criptomonedas”, “cibercriminalidad financiera” y “responsabilidad penal”. Posteriormente, se procedió a la lectura crítica de los textos preseleccionados, con el fin de extraer las principales aportaciones doctrinales y los puntos de convergencia y divergencia entre los autores. La información relevante se integró en un esquema de categorías analíticas que permitieron estructurar los hallazgos de manera coherente y facilitar su interpretación comparativa.

Asimismo, se revisaron documentos normativos internacionales y regionales, como directivas de la Unión Europea, informes del Grupo de Acción Financiera Internacional y resoluciones de organismos especializados en la materia. Este proceso permitió incorporar una dimensión comparada que enriquece la discusión y proporciona un panorama más amplio sobre las respuestas jurídicas frente a la criminalidad económica digital. Finalmente, se consolidó un corpus documental que sirvió como base para el desarrollo de los apartados de resultados y discusión, con el propósito de ofrecer un análisis integral, ordenado y crítico que aporte elementos de reflexión y posibles líneas de actuación legislativa en este ámbito.

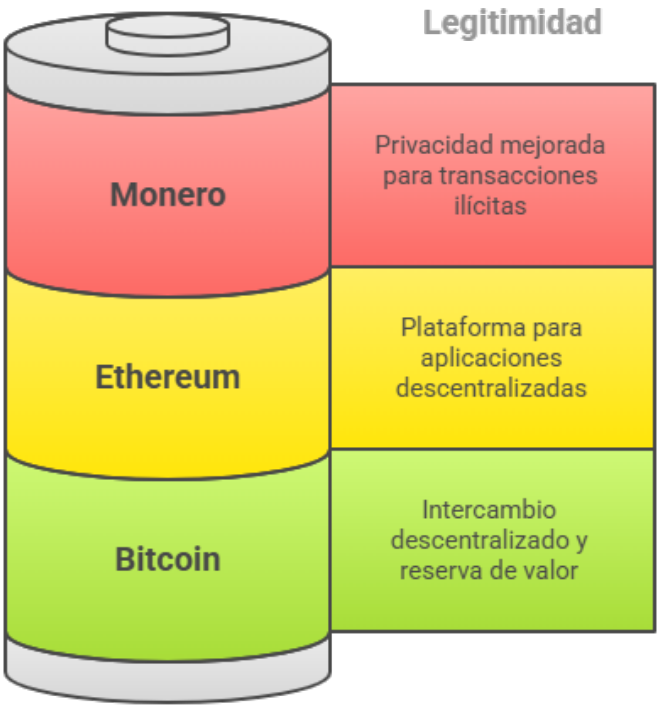
3. Resultados

3.1. Transformaciones normativas

3.1.1. Nuevos tipos penales sobre criptoactivos

El surgimiento de los criptoactivos ha generado un proceso de expansión conceptual del derecho penal económico, obligando a los legisladores y la doctrina a repensar las categorías tradicionales de bien jurídico protegido y objeto material del delito. La adopción generalizada de criptomonedas como Bitcoin, Ethereum o Monero ha evidenciado su potencial no solo como instrumentos lícitos de intercambio o reserva de valor, sino también como vehículos privilegiados de operaciones ilícitas, desde fraudes piramidales hasta el blanqueo de capitales de procedencia criminal (Zhao, 2021), en la figura 1 la imagen ilustra cómo las criptomonedas varían en su aplicabilidad, desde usos legítimos, como el intercambio descentralizado y las aplicaciones descentralizadas, hasta aplicaciones ilícitas, que incluyen el uso de monedas como Monero para transacciones no rastreables.

Figura 1
"Criptomonedas: Del uso legítimo al uso ilícito"



Nota: Las criptomonedas ofrecen diversas funciones que pueden ser aprovechadas para transacciones legítimas, pero también presentan riesgos debido a su uso en actividades ilícitas (Autores, 2024).

La doctrina penal contemporánea destaca que el anonimato técnico y la descentralización inherentes a estos activos dificultan la atribución de la titularidad y la trazabilidad de las operaciones, erosionando los sistemas clásicos de control financiero (Irwin & Milad, 2016). En respuesta, diversas jurisdicciones han incorporado tipos penales que tipifican conductas específicas vinculadas a la captación de fondos mediante criptomonedas sin registro, la comercialización de activos digitales con información fraudulenta y el ocultamiento patrimonial mediante plataformas de

intercambio. A título ilustrativo, el Código Penal español ha incluido reformas que permiten perseguir el blanqueo de capitales a través de monedas virtuales (Nieto Martín, 2020), mientras que legislaciones latinoamericanas, como la de México, incorporan obligaciones de identificación para operaciones de compraventa que superen determinados umbrales económicos.

Este desarrollo ha sido acompañado por pronunciamientos jurisprudenciales que reconocen el carácter patrimonial de los criptoactivos y su asimilación funcional a los medios tradicionales de pago. Tal reconocimiento contribuye a la consolidación de un paradigma normativo que configura los activos digitales como objeto material de múltiples conductas punibles: apropiación indebida, estafa agravada, delitos fiscales y financiación del terrorismo (Barzola-Plúas, 2022).

3.1.2. Responsabilidad penal empresarial

La transformación digital del sistema financiero ha acentuado la necesidad de dotar al derecho penal económico de mecanismos eficaces para exigir responsabilidad a las personas jurídicas. En este sentido, la atribución de responsabilidad penal empresarial por delitos cometidos mediante criptoactivos se fundamenta en la omisión de los deberes de supervisión, control y adopción de medidas razonables de compliance que permitan prevenir o detectar operaciones ilícitas (Nieto Martín, 2020).

La normativa comparada ha evolucionado en un sentido convergente: las empresas que prestan servicios de custodia, intercambio o emisión de criptoactivos están sujetas a obligaciones reforzadas de diligencia debida, reporte de operaciones sospechosas y verificación de la identidad de sus usuarios. El incumplimiento de estas obligaciones puede generar la responsabilidad penal autónoma de la persona jurídica, que se suma a la eventual responsabilidad individual de los órganos de administración o dirección.

Asimismo, se ha consolidado un modelo sancionador de carácter preventivo que no solo contempla sanciones pecuniarias significativas, sino también medidas accesorias como la disolución de la persona jurídica, la suspensión de actividades o la clausura temporal de establecimientos. Esta tendencia refleja la creciente relevancia del compliance penal como instrumento normativo indispensable para enfrentar la criminalidad económica en entornos digitales (Zetzsche et al., 2020).

3.1.3. Normas internacionales armonizadas

La dimensión transnacional de los delitos financieros digitales ha puesto de relieve la insuficiencia de respuestas estrictamente nacionales y ha impulsado la necesidad de normas internacionales armonizadas. El Grupo de Acción Financiera Internacional (GAFI) ha desempeñado un papel esencial en la definición de estándares globales sobre activos virtuales, promoviendo la adopción del enfoque conocido como “Travel Rule”, que obliga a los proveedores de servicios de criptoactivos a compartir información identificativa de los usuarios en las transferencias (Bonilla-Morejón, 2023).

En el ámbito europeo, la Directiva (UE) 2018/843 ha modificado de forma sustancial la normativa antilavado al ampliar su alcance a plataformas de intercambio y proveedores de carteras digitales, incorporando la obligación de registro ante autoridades competentes y la implementación de programas de monitoreo de operaciones inusuales. Estas disposiciones buscan reducir las asimetrías regulatorias que generan oportunidades de arbitraje normativo y reforzar la capacidad de los Estados para cooperar en investigaciones internacionales (Barzola-Plúas, 2022).

La evolución de estos instrumentos refleja un consenso progresivo sobre la necesidad de mecanismos uniformes que conjuguen la protección del mercado financiero, la prevención de riesgos sistémicos y la eficacia de la persecución penal. La armonización normativa no solo facilita la cooperación judicial y policial, sino que otorga certeza jurídica a los operadores económicos que actúan en el ecosistema digital (Zhao, 2021).

3.1.4. Regulación específica de tokens digitales

El auge de los tokens digitales, particularmente en el contexto de las Initial Coin Offerings (ICOs), ha precipitado reformas que delimitan con precisión su naturaleza jurídica y su régimen de emisión, comercialización y control.

MiCA distingue entre distintos tipos de tokens —tokens de utilidad, tokens referenciados a activos y e-money tokens— y define las condiciones de autorización, obligaciones de transparencia e información que deben cumplir los emisores. Este marco dota a las autoridades competentes de potestades de supervisión que facilitan la identificación de prácticas fraudulentas y el aseguramiento de activos vinculados a investigaciones penales (Samaniego-Quiguiri, 2023).

Algunos ordenamientos nacionales, como el alemán, han incorporado previsiones específicas sobre la calificación penal de conductas que impliquen la emisión de tokens sin registro, la omisión de información esencial para los inversores o el uso de estos instrumentos como vehículo de fraude (Zetzsche et al., 2020). Estas medidas son consistentes con el enfoque preventivo del derecho penal económico contemporáneo y con la exigencia de proteger la confianza pública en los mercados digitales.

3.2. Desafíos en la persecución

3.2.1. Anonimato de autores

Uno de los principales obstáculos en la persecución de los delitos financieros digitales es el anonimato de los autores, facilitado por las características inherentes a muchas criptomonedas y tecnologías relacionadas. Las criptomonedas como Bitcoin, Monero, y ZCash, entre otras, permiten a los usuarios realizar transacciones sin revelar su identidad, lo que complica significativamente la tarea de rastrear a los delincuentes (Chan et al., 2020). Mientras que Bitcoin utiliza un sistema pseudónimo en el que las direcciones de los monederos están asociadas a códigos alfanuméricos,

criptomonedas como Monero emplean protocolos de privacidad más robustos que ocultan tanto las direcciones de envío como de recepción, así como los montos de las transacciones, lo que las convierte en herramientas particularmente eficaces para actividades ilegales (Lorenz et al., 2020). Esto es problemático porque las autoridades dependen de la trazabilidad para vincular los crímenes con los individuos responsables.

Aunque las agencias de aplicación de la ley han adoptado tecnologías de análisis forense para estudiar las transacciones en blockchain, estas herramientas no siempre son efectivas, especialmente en redes que priorizan la privacidad (Irwin & Milad, 2016). La incapacidad de rastrear las transacciones de forma efectiva genera una grave brecha en las capacidades investigativas, ya que las transacciones pueden realizarse de manera oculta, dificultando la identificación de los responsables. Además, el uso de servicios de mezcla (mixers) y otras herramientas diseñadas para aumentar el anonimato, como las redes privadas virtuales (VPN) o las redes de anonimato como Tor, complican aún más el proceso de seguimiento de los flujos de fondos. En este contexto, la dificultad para identificar de manera efectiva a los autores del delito no solo ralentiza las investigaciones, sino que en muchos casos contribuye a la impunidad.

3.2.2. Conflictos de jurisdicción

La globalización de la economía digital ha dado lugar a un aumento de los delitos cibernéticos transnacionales, lo que crea importantes conflictos jurisdiccionales en la persecución de los delitos financieros digitales. A diferencia de los delitos tradicionales, que suelen estar confinados dentro de los límites territoriales de un Estado, los delitos financieros digitales, como el fraude, el blanqueo de capitales y el robo de criptomonedas, pueden involucrar a múltiples actores en diferentes jurisdicciones. Esto hace que las autoridades competentes de cada país se enfrenten a dificultades en términos de determinación de la jurisdicción adecuada para investigar y procesar el delito (Arrazola Ruiz, 2018). Un caso típico podría involucrar un servidor ubicado en un país, el beneficiario del delito en otro y la víctima en una tercera nación, lo que genera disputas sobre cuál es el Estado que tiene la competencia exclusiva para procesar el caso.

Las dificultades de jurisdicción se ven amplificadas por la falta de acuerdos internacionales que definan claramente cómo debe abordarse la cooperación judicial en casos de delitos cibernéticos. Si bien existen instrumentos como la Convención de Budapest sobre Ciberdelincuencia, ratificada por una serie de países, la aplicación práctica de este tratado sigue siendo limitada y se enfrenta a obstáculos debido a la diversidad de normativas nacionales y la falta de un sistema global de resolución de disputas (Cejuela et al., 2015). Esta disparidad normativa genera vacíos legales y permite que los delincuentes exploten las lagunas jurisdiccionales, eligiendo operar desde países con legislaciones más laxas o sin acuerdos de cooperación. El reto de la jurisdicción también se ve exacerbado por la velocidad a la que las transacciones

digitales pueden cruzar fronteras, lo que requiere una respuesta ágil y coordinada entre países para evitar que los perpetradores escapen de la justicia.

3.2.3. Limitaciones técnicas de investigación

Las limitaciones técnicas en la investigación de delitos financieros digitales son uno de los desafíos más persistentes para las autoridades encargadas de hacer cumplir la ley. La rápida evolución de las tecnologías utilizadas en la comisión de estos delitos ha superado las capacidades de muchos de los sistemas tradicionales de forensia digital, dejando a los investigadores con herramientas insuficientes para afrontar los retos que presenta el ecosistema digital actual. Un aspecto particularmente problemático es el uso generalizado de criptografía de extremo a extremo y otras tecnologías de cifrado, que protegen la privacidad de las transacciones y dificultan su análisis (Samaniego-Quiguiri et al., 2024). Aunque existen herramientas de análisis de blockchain, como Chainalysis y CipherTrace, estas están diseñadas principalmente para analizar redes públicas y no son eficaces en redes privadas o cifradas, como las que utiliza Monero (Lorenz et al., 2020).

Otra limitación importante es la dependencia de los investigadores de información proveniente de plataformas centralizadas, como exchanges de criptomonedas, que, aunque pueden tener registros de transacciones, no siempre están dispuestos a cooperar con las autoridades debido a las diferencias regulatorias entre países (Mendoza-Armijos et al., 2023). Además, la gran cantidad de datos generados por los delitos financieros digitales y su complejidad técnica requiere de expertos altamente capacitados en áreas como la ciberseguridad, la criptografía y el análisis de blockchain, algo que no está disponible de manera generalizada en todas las agencias de aplicación de la ley (Irwin & Milad, 2016).

Finalmente, las limitaciones de recursos en términos de personal y financiamiento también afectan la capacidad de las autoridades para implementar las tecnologías más avanzadas. La lucha contra los delitos financieros digitales exige inversiones sustanciales en capacitación y en el desarrollo de capacidades tecnológicas especializadas, que no siempre son viables en los marcos presupuestarios de las instituciones públicas.

4. Discusión

En la presente discusión se aborda la complejidad inherente a la evolución del derecho penal económico frente a los delitos financieros digitales, un campo en el que los marcos normativos y las capacidades investigativas tradicionales se ven desbordadas por las características dinámicas y transnacionales del cibercrimen. La digitalización de las finanzas ha generado una serie de retos que obligan a una reconfiguración de las estrategias tanto normativas como procesales, pues la criminalidad económica digital no solo trasciende las fronteras geográficas, sino que también se apoya en tecnologías disruptivas que desafían las estructuras legales tradicionales (Irwin &

Milad, 2016). Estos desafíos requieren una reflexión crítica sobre la capacidad de las autoridades para abordar los delitos cometidos mediante criptomonedas y otras herramientas digitales.

Uno de los obstáculos más significativos radica en el anonimato de los autores de los delitos. Las criptomonedas, con su promesa de descentralización y privacidad, proporcionan un terreno fértil para actividades ilícitas, ya que permiten a los delincuentes operar sin dejar rastros fácilmente identificables (Zhao, 2021). A pesar de los esfuerzos por parte de las agencias de control para incorporar tecnologías de análisis forense de blockchain, estas herramientas son insuficientes cuando se trata de redes altamente privadas o de transacciones complejas que emplean criptografía avanzada (Lorenz et al., 2020). La naturaleza pseudónima de monedas como Bitcoin y el anonimato total que ofrecen plataformas como Monero hacen que el rastreo de los fondos sea extremadamente complejo. Este fenómeno subraya la necesidad urgente de perfeccionar las capacidades forenses, no solo para el seguimiento de criptomonedas, sino también para la identificación de los actores detrás de las transacciones, lo cual sigue siendo una de las principales limitaciones en la persecución penal de estos delitos (Samaniego-Quiguiri, 2023).

Además, el conflicto de jurisdicción es otro de los puntos álgidos en la persecución de delitos financieros digitales. La globalización de las transacciones digitales ha originado un escenario donde las actividades ilícitas pueden ser perpetradas en un país y tener efectos devastadores en otro, complicando la determinación de cuál es el Estado competente para ejercer la jurisdicción. A menudo, el delincuente elige operar desde una nación con regulaciones laxas, aprovechándose de las lagunas jurídicas y de las disparidades en la legislación internacional (Cejuela et al., 2015). Si bien existen acuerdos y convenios internacionales, como la Convención de Budapest sobre Ciberdelincuencia, la implementación de estos acuerdos sigue siendo inconsistente y la cooperación entre Estados puede verse afectada por intereses políticos y económicos. La falta de un marco normativo globalmente armonizado en el ámbito del derecho penal económico digital genera incertidumbre y puede conducir a una impunidad jurídica que, en muchos casos, elude la justicia.

Por otro lado, las limitaciones técnicas de las investigaciones se presentan como otro desafío relevante. Las autoridades encargadas de investigar delitos financieros digitales a menudo carecen de los recursos y las capacidades técnicas necesarias para enfrentar la complejidad de las herramientas utilizadas por los delincuentes. A pesar del avance en el desarrollo de software especializado en análisis de blockchain, la velocidad a la que evolucionan las tecnologías digitales y la complejidad de los crímenes cibernéticos requieren una capacitación continua y un fortalecimiento de las capacidades institucionales (Samaniego-Quiguiri et al., 2024). El uso de tecnologías avanzadas como la criptografía de extremo a extremo y las redes de anonimato como Tor complican enormemente la tarea de los investigadores, quienes, a menudo, no cuentan con la formación ni el acceso a las herramientas más avanzadas necesarias para rastrear de manera efectiva las transacciones ilícitas (Lorenz et al., 2020). Esta

brecha técnica no solo retrasa las investigaciones, sino que también incrementa la posibilidad de que los delincuentes escapen de la justicia debido a las deficiencias en la recopilación de pruebas electrónicas y la capacidad de vincular a los autores con sus actividades ilegales.

La combinación de anonimato, conflictos jurisdiccionales y limitaciones técnicas plantea un panorama complicado para la evolución del derecho penal económico en el ámbito digital. Estos retos exigen un enfoque holístico que no solo implique la creación de marcos normativos más adaptados a las nuevas tecnologías, sino también el fortalecimiento de las capacidades investigativas, con especial énfasis en la cooperación internacional. Sin embargo, la creación de marcos jurídicos eficaces que aborden estos desafíos es un proceso complejo y requiere un enfoque multidisciplinario que involucre no solo a juristas y legisladores, sino también a expertos en tecnología, criptografía y ciberseguridad (Bonilla-Morejón, 2023).

Por otro lado, es relevante destacar que la investigación de estos delitos debe contar con la implementación de políticas que fomenten una mayor cooperación internacional en la ejecución de medidas legales y de vigilancia. La existencia de entidades como el Grupo de Acción Financiera Internacional (GAFI) ha sido fundamental para establecer directrices internacionales, como las que abordan la regulación de criptoactivos y el blanqueo de capitales (Bonilla-Morejón, 2023). Sin embargo, para que estas medidas sean realmente eficaces, es imprescindible que los países ajusten sus legislaciones nacionales y sus capacidades operativas para cumplir con los estándares internacionales, lo que requiere un esfuerzo coordinado a nivel global.

En conclusión, la persecución de delitos financieros digitales plantea una serie de desafíos que requieren una respuesta integral que combine la innovación tecnológica con la evolución normativa y una cooperación internacional más robusta. La adaptación del derecho penal económico al entorno digital es un proceso continuo que debe involucrar tanto la actualización de la legislación como el fortalecimiento de las capacidades investigativas, lo cual es esencial para garantizar una respuesta efectiva frente a los delitos cibernéticos que afectan tanto a individuos como a sistemas económicos a nivel global.

5. Conclusiones

Las transformaciones en el derecho penal económico frente a los delitos financieros digitales revelan la necesidad de una evolución normativa que logre adaptarse a las características dinámicas y globales del entorno digital. La emergencia de nuevas tecnologías como las criptomonedas y los tokens digitales ha generado un reto significativo para los marcos jurídicos existentes, los cuales, aunque continúan siendo útiles para regular actividades tradicionales, se ven insuficientes para abordar de manera eficaz las amenazas que surgen en el ciberespacio. La adopción generalizada de criptomonedas ha dado lugar a nuevos tipos penales, permitiendo a las autoridades

regular las transacciones ilícitas en blockchain, pero al mismo tiempo ha facilitado el anonimato de los delincuentes, lo que ha dificultado la tarea de identificarlos y responsabilizarlos.

El anonimato, inherente a muchas de las tecnologías utilizadas en el crimen financiero digital, es uno de los mayores desafíos en la persecución de estos delitos. Las criptomonedas como Monero, que permiten transacciones completamente privadas, representan un obstáculo significativo para las investigaciones, ya que hacen imposible la trazabilidad de los fondos involucrados en actividades ilícitas. A pesar de los esfuerzos por parte de las autoridades para implementar herramientas de análisis forense más avanzadas, el anonimato total de ciertos criptoactivos continúa siendo una barrera considerable que impide la identificación efectiva de los responsables.

Otro desafío importante que se presenta en la persecución de los delitos financieros digitales es el conflicto de jurisdicción. La transnacionalidad de estos delitos genera situaciones donde diferentes países pueden reclamar la competencia para juzgar los actos delictivos, lo que genera un laberinto legal que impide una cooperación judicial eficiente y provoca que algunos delincuentes se beneficien de las lagunas jurídicas entre naciones. Aunque existen esfuerzos internacionales para armonizar las normativas, las diferencias entre los sistemas legales de los países dificultan la acción coordinada y la resolución rápida de casos transnacionales.

Las limitaciones técnicas también son una barrera significativa en la investigación de estos delitos. A medida que las tecnologías cambian y se sofisticaron, las herramientas de investigación tradicionales se quedan atrás, dificultando el rastreo de datos, la identificación de actores y la obtención de pruebas. El uso de tecnologías de encriptación y redes anónimas complica aún más la recolección de pruebas digitales que podrían vincular a los delincuentes con los delitos cometidos. Estas limitaciones subrayan la necesidad urgente de actualizar las capacidades técnicas de las agencias de investigación y de aumentar la cooperación entre los diferentes actores internacionales.

En conclusión, los delitos financieros digitales presentan una serie de retos complejos que requieren una respuesta multifacética, que combine la actualización de las normas jurídicas con el fortalecimiento de las capacidades técnicas y la cooperación internacional. La evolución del derecho penal económico debe ir de la mano con la creación de marcos regulatorios más específicos que aborden las características particulares del cibercrimen, sin perder de vista la importancia de la cooperación transnacional. Solo mediante un esfuerzo conjunto y una actualización constante de las herramientas y normativas se podrá garantizar la efectividad de la persecución penal frente a los delitos financieros digitales en el futuro.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.

Referencias Bibliográficas

Arcos-Chaparro, I. A., & Epia-Silva, M. A. (2024). La transverzalización del debido proceso en las relaciones laborales particulares. *Journal of Economic and Social Science Research*, *4*(2), 17–43. https://doi.org/10.55813/gaea/jessr/v4/n2/100

Arrazola Ruiz, D. (2018). *La ciberjurisdicción y los conflictos derivados de los delitos en internet: Retos y soluciones*. Editorial Dykinson.

Barzola-Plúas, Y. G. (2022). Reformas Constitucionales en Ecuador: Impacto y Perspectivas. Revista Científica Zambos, 1(1), 86-101. https://doi.org/10.69484/rcz/v1/n1/23

Barzola-Plúas, Y. G. (2022). Reformas Constitucionales en Ecuador: Impacto y Perspectivas. *Revista Científica Zambos*, *1*(1), 86-101. https://doi.org/10.69484/rcz/v1/n1/23

Bonilla-Morejón, D. M. (2023). Derecho Penal y Políticas de Seguridad en Ecuador: Análisis de la Eficacia. Revista Científica Zambos, 2(3), 59-74. https://doi.org/10.69484/rcz/v2/n3/50

Bonilla-Morejon, D. M., Bonilla-Morejón, J. S., Guano-Fogacho, J. E., Meléndez-Carrasco, P. V., Murillo-Ramos, F. R., Peña-Chauvín, S. M., Samaniego-Quiguiri, D. P., Solis-Miranda, D. F., Vásquez-Quinatoa, L. H., & Núñez-Ribadeneyra, R. A. (2023). *Los gritos silenciosos de las víctimas de violencia de género: Un enfoque desde la perspectiva pre procesal y procesal penal en el Ecuador.* Editorial Grupo AEA. Retrieved from. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.41

Bonilla-Morejón, D. M., Samaniego-Quiguiri, D. P., & Paredes-Fierro, E. J. (2023). Los Derechos Humanos y su enfoque en las poblaciones vulnerables. In *Sinergia Científica: Integrando las Ciencias desde una Perspectiva Multidisciplinaria* (pp. 15–48). Editorial Grupo AEA. https://doi.org/10.55813/egaea.cl.2022.21

Bravo-Bravo, I. F., & Herrera-Sánchez, M. J. (2023). Tendencias Globales del Liderazgo Transformacional en Empresas Modernas. *Horizon Nexus Journal, 1*(2), 14-31. https://doi.org/10.70881/hnj/v1/n2/15

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). *An analysis of the nature of groups engaged in cyber crime*. *International Journal of Cyber Criminology, 8*(1), 1–20. https://ssrn.com/abstract=2461983

Casanova-Villalba, C. I., Herrera-Sánchez, M. J., Bravo-Bravo, I. F., & Barba-Mosquera, A. E. (2024). Transformación de universidades incubadoras a creadoras directas de empresas Spin-Off. *Revista De Ciencias Sociales*, *30*(2), 305-319. https://doi.org/10.31876/rcs.v30i2.41911

Cejuela, I., González, M., & Núñez, M. (2015). *Delitos cibernéticos y la cooperación judicial internacional en el ámbito penal*. Editorial Tirant lo Blanch.

Chan, T., Biedermann, R., & Hammond, J. (2020). Cryptocurrency laundering: A framework for investigation. *Journal of Financial Crime, 27*(2), 471-485.

Estrada-Ayre, C. P., & Porras-Sarmiento, S. (2023). *Peculado Doloso y el Principio de Proporcionalidad de la Pena*. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.32

García Moreno, M., & Vargas Fonseca, A. D. (2023). Restitución de derechos territoriales y ordenamiento ambiental en territorios étnicos en Colombia. *Journal of Economic and Social Science Research*, *3*(3), 76–96. https://doi.org/10.55813/gaea/jessr/v3/n3/74

Guerrero-Velástegui, C. A. (2023). *Entorno Empresarial desde la Gestión del Derecho Laboral: Breves Apuntes desde una Perspectiva Académica. Editorial Grupo AEA.* https://doi.org/10.55813/egaea.l.2022.42

Herrera-Enríquez, G., Casanova-Villalba, C., Herrera-Sánchez, M., Navarrete-Zambrano, C., & Ruiz-López, S. (2021). Estructura del sistema de información para el análisis multidimensional de la resiliencia socioecológica a través de Fuzzy AHP. *Revista Ibérica de Sistemas e Tecnologias de Informacao*, (E39), 77-90.

Irwin, A.S.M., & Milad, G. (2016). The use of cryptocurrencies in funding violent jihad. *Journal of Money Laundering Control,* Vol. 19 No. 4, pp. 407-425. https://doi.org/10.1108/JMLC-01-2016-0003

Lorenz, S., McDonald, D., & Martinez, P. (2020). Blockchain analytics and cryptocurrency forensics: Challenges in the investigation of illicit financial flows. *Computer Law & Security Review, 40*, 105513.

Mackenzie, S., Hamilton-Smith, N., & Henry, A. (2020). The digital criminal: Cybercrime, social deviance and digital technologies. *British Journal of Criminology, 60*(6), 1485–1506.

Maras, M.-H. (2020). *Cybercriminology*. Oxford University Press.

Mendoza-Armijos, H. E., Camacho-Medina, B. M., & García-Segarra, H. G. (2023). Análisis de la justicia restaurativa como alternativa al sistema penal tradicional en América Latina. Revista Científica Ciencia Y Método, 1(3), 58-69. https://doi.org/10.55813/gaea/rcym/v1/n3/20

Nieto Martín, A. (2020). *Derecho penal económico y de la empresa* (2.ª ed.). Thomson Reuters Aranzadi.

Núñez-Ribadeneyra, R. A. (2023). Derechos Humanos y Justicia Social en el Contexto Ecuatoriano. *Revista Científica Zambos*, *2*(3), 42-58. https://doi.org/10.69484/rcz/v2/n3/49

Puyol-Cortez, J. L., Casanova-Villalba, C. I., Herrera-Sánchez, M. J., & Rivadeneira-Moreira, J. C. (2024). REVISIÓN METODOLÓGICA AG2C PARA LA ENSEÑANZA DEL ÁLGEBRA BÁSICA A ESTUDIANTES CON DISCALCULIA. *Perfiles*, *1*(32), 15-27. https://doi.org/10.47187/perf.v1i32.280

Samaniego Quiguiri, D. P., Bonilla-Morejón, D. M., Martínez-Tapia, J. D., Navarrete-Valladolid, M. I., Solis-Miranda, D. F., Zambrano-Villacrés, D. E., Bucheli-Cárdenas, C. M., Murillo-Ramos, F. R., Erazo-Zela, V. H., & Guala-Agualongo, C. J. (2023). *El derecho a ser padres: Rompiendo los paradigmas del derecho*

de familia, bajo una concepción legal o ilegal. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.51

Samaniego-Quiguiri, D. P. (2023). Acceso a la Justicia y Equidad en el Sistema Legal Ecuatoriano. Revista Científica Zambos, 2(2), 50-62. https://doi.org/10.69484/rcz/v2/n2/45

Samaniego-Quiguiri, D. P., Bonilla-Morejón, D. M., Pérez-Serrano, X. O., Salazar-Guerrero, R. J., Erazo-Domínguez, H. del R., Yánez-Erazo, T. F., Calles-Poveda, L. R., & Quiroz-Becerra, L. V. (2024). Revelando la Verdad: El Papel del Whistleblowing en la Preservación de la Integridad Estatal. Un Análisis de su Impacto en los ámbitos Penal, Administrativo y Financiero, explorando los desafíos y soluciones legales. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.75

Santander-Salmon, E. S., Herrera-Sánchez, M. J., & Bravo-Bravo, I. F. (2023). La importancia de la digitalización en la administración empresarial mediante un análisis bibliográfico actualizado. *Multidisciplinary Collaborative Journal, 1*(2), 39-51. https://doi.org/10.70881/mcj/v1/n2/15

Vargas-Fonseca, A. D., Borja-Cuadros, O. M., & Cristiano-Mendivelso, J. F. (2023). *Estructura Ecológica Principal de la Localidad de Engativá: Estudio desde una perspectiva de ordenamiento territorial y sus instrumentos jurídicos.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.38

Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius Et Praxis*, *53*(053), 95-110. https://doi.org/10.26439/iusetpraxis2021.n053.4995

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2020). Regulating Libra: The transformative potential of Facebook's cryptocurrency and possible regulatory responses. *Fordham Journal of Corporate & Financial Law, 25*(1), 159–200.

Zhao, J. (2021). Criminal law in the age of cryptocurrencies: Challenges and perspectives. *Computer Law & Security Review, 40*, 105513.