

UNIVERSIDAD DE ESPECIALIDADES ESPÍRITU SANTO

FACULTAD DE DERECHO, POLÍTICA Y DESARROLLO

TÍTULO:

FRAUDE PATRIMONIAL MEDIANTE CRIPTOACTIVOS: VACÍOS DE TIPICIDAD EN LA LEGISLACIÓN PENAL ECUATORIANA

TRABAJO DE TITULACIÓN QUE SE PRESENTA COMO REQUISITO PREVIO A OPTAR EL GRADO DE ABOGADO DE LOS TRIBUNALES Y JUZGADOS DE LA REPÚBLICA

NOMBRE DEL ESTUDIANTE:

JAIME EDUARDO ALVEAR FRANCO

NOMBRE DEL TUTOR:

Msc. JOSE CRISTHIAN CASTRO VELASTEGUI

SAMBORONDÓN, MAYO, 2026

CARTA DE APROBACIÓN DEL TUTOR

En mi calidad de tutor de Jaime Eduardo Alvear Franco, estudiante de la Facultad de Derecho, Política y Desarrollo de la Universidad de Especialidades Espíritu Santo,

CERTIFICO

Que, una vez analizado el trabajo de titulación titulado "Fraude patrimonial mediante criptoactivos: vacíos de tipicidad en la legislación penal ecuatoriana", presentado como requisito previo a obtener el grado de abogado, el mismo cumple con los requisitos y méritos académicos, razón por la cual lo APRUEBO en su totalidad.

Msc. JOSE CRISTHIAN CASTRO VELASTEGUI

TUTOR

INFORMACIÓN DEL AUTOR

Apellidos y nombres: Alvear Franco, Jaime Eduardo.

Título académico: Estudiante de Derecho, Facultad de Derecho, Política y Desarrollo.

Filiación institucional: Universidad de Especialidades Espíritu Santo (UEES), Ecuador.

Correo institucional: jealvear@uess.edu.ec.

Dirección de correspondencia: Facultad de Derecho, Edificio P, Universidad Espíritu Santo, Km. 2.5 Vía Puntilla, Samborondón.

DEDICATORIA

A ti, abuelita querida a la que extraño muchísimo, Rosario de los Ángeles Jaramillo de Franco, que pusiste en mis manos mi primer libro, que me enseñaste el amor por la lectura y que el amor más sincero es el que se da sin esperar nada a cambio. En cada página de este trabajo está algo de lo que me diste sin saberlo: la paciencia para ir paso a paso, la humildad para reconocer lo que no sé y las ganas de seguir adelante, aunque el camino se ponga difícil. Ojalá pudiera mostrarte esto en persona. Sé que desde donde estás, lo ves.

A mi madre, Dra. Rosario Franco Jaramillo, abogada, doctora en Jurisprudencia, exfiscal, expresidenta de la Corte Provincial de Justicia de Santa Elena, primera mujer en ostentar esa dignidad en la Corte de Justicia de Santa Elena, actual jueza provincial de la Sala Especializada de lo Penal, Penal Militar, Penal Policial y Tránsito de la Corte Provincial de Justicia del Guayas, magíster en derecho constitucional, penal y digital, estudiante de la Maestría en Inteligencia Artificial aplicada a la *Legaltech* en la Universidad de Salamanca, mujer de ley en el sentido más completo de la palabra. Crecí viendo cómo defiendes la justicia no como una idea abstracta, sino como una obligación diaria, con rigor, con ética y con una convicción que nunca cedió ante la comodidad. Que hayas seguido estudiando y especializándote mientras ejercías tu cargo, me enseñó que siempre hay algo más que aprender, y que eso no es debilidad, sino fortaleza. Este trabajo nació en parte de lo que aprendí al verte trabajar y esforzarte, como ocurre con todo lo que haces.

A mi padre, Dr. Jaime Eduardo Alvear Flores, expresidente y actual presidente de la Corte Provincial de Justicia de Imbabura, catedrático universitario, conferencista nacional e internacional, formador y miembro activo del cuerpo docente de la Función Judicial del Ecuador.

De él aprendí que el conocimiento sólo adquiere verdadero valor cuando se comparte; que la toga no representa un privilegio.

Me enseñó también a cuestionar el porqué de las cosas, a no conformarme con respuestas superficiales y a comprender que el pensamiento crítico es la base del crecimiento intelectual.

En mi mente se repite constantemente la frase que siempre me inculcó: *scientia potentia est*, atribuida a Francis Bacon (1597): el conocimiento es poder. No como una manera de controlar, sino como la capacidad de entender, decidir y actuar con criterio, autonomía y, sobre todo, responsabilidad frente a las dificultades de la vida.

AGRADECIMIENTO

Al Msc. Jose Cristhian Castro Velastegui, tutor de este trabajo, por la orientación a lo largo de todo el trayecto, por la exigencia académica que empuja a hacer las cosas bien y por la disposición constante que tuvo para revisar, corregir y guiar. Un buen tutor hace notar no solo los errores, sino también enseña a pensar. Eso es lo que encontré en este proceso.

A la Facultad de Derecho, Política y Desarrollo de la Universidad de Especialidades Espíritu Santo, por la educación que he recibido. La experiencia del paso por las aulas no solo deja una marca en el conocimiento, sino también en cómo encarar los problemas, argumentar con rigor y asumir la responsabilidad que supone ejercer el derecho.

A los doctores Jaime Eduardo Alvear Flores y Rosario Franco Jaramillo, mis padres, por ser una referencia profesional constante además de ser familia. No todos tienen el privilegio de nacer y crecer en un hogar donde el derecho es vivido con vocación y seriedad. Cada charla de sobremesa acerca de procesos, sentencias y normas fue un componente de mi formación, sin que yo lo supiera en ese momento.

A todos aquellos que, de alguna manera, ayudaron a que este trabajo llegara a su término: maestros, colegas y todas las personas que, con una consulta, una recomendación o simplemente su presencia hicieron más llevadera la travesía.

RESUMEN Y PALABRAS CLAVE

En Ecuador, el Código Orgánico Integral Penal (Coip) está vigente desde el año 2014 y, hasta la fecha, no ha contemplado a los criptoactivos dentro de los objetos de los delitos patrimoniales. Esta omisión, que ha pasado inadvertida, hoy causa 3 tipos de problemas: definitorios, tipológicos y procesales. Ningún artículo indica si los activos virtuales se incluyen dentro del patrimonio penalmente protegido. Tampoco está claro cuándo un fraude con criptomonedas debe ser acusado como estafa (art. 186), como captación ilegal de dinero (art. 323) o como apropiación fraudulenta por medios electrónicos (art. 190). A esa indefinición se suma un detalle no menor: el Coip no manifiesta nada sobre la cadena de custodia digital ni sobre los estándares periciales que deberían aplicarse a la evidencia obtenida en *blockchain.*

De manera dogmática e interpretativa, se aborda el régimen jurídico de los criptoactivos, las modalidades más frecuentes de fraude patrimonial y los problemas prácticos que aparecen en su investigación. Como conclusión se determina que: el vacío definitorio se resuelve leyendo con cuidado el artículo 186, mientras que las otras lagunas piden una reforma legislativa clara, capaz de incorporar los activos virtuales y dotar de instrumentos técnicos serios a la prueba.

PALABRAS CLAVE: activos virtuales; derecho penal económico; fraude patrimonial; lagunas jurídicas; legislación penal; tipicidad penal.

ABSTRACT AND KEYWORDS

In Ecuador, the Comprehensive Organic Criminal Code (Coip) has been in effect since 2014 and, to date, has not included crypto assets among the objects of property crimes. This omission, which has gone largely unnoticed, now causes three types of problems: definitional, typological, and procedural. No article indicates whether virtual assets are included within criminally protected assets. It is also unclear when cryptocurrency fraud should be charged as fraud (Art. 186), as illegal fundraising (Art. 323), or as fraudulent appropriation by electronic means (Art. 190). Adding to this lack of definition is another significant detail: the Coip makes no mention of the digital chain of custody or the expert standards that should be applied to evidence obtained from *blockchain*.

This article addresses, from both a dogmatic and interpretative perspective, the legal framework for crypto assets, the most frequent forms of property fraud, and the practical problems that arise in their investigation. In conclusion, it is determined that: the definitional gap is resolved by carefully reading article 186, while the other gaps call for a clear legislative reform, capable of incorporating virtual assets and providing serious technical instruments for the proof.

KEYWORDS: criminal legislation; criminal typicity; economic criminal law; legal gaps; property fraud; cryptoassets; digital evidence.

ÍNDICE

CARTA DE APROBACIÓN DEL TUTOR 1

INFORMACIÓN DEL AUTOR 2

DEDICATORIA 3

AGRADECIMIENTO 5

RESUMEN Y PALABRAS CLAVE 6

ABSTRACT AND KEYWORDS 7

ÍNDICE 8

Introducción 10

Objetivo general 10

Objetivos específicos 10

Pregunta del problema jurídico 11

1. FUNDAMENTOS DOGMÁTICOS DEL DERECHO PENAL 11

2. CRIPTOACTIVOS EN ECUADOR: ESTATUS JURÍDICO, MODALIDADES DE FRAUDE Y OBSTÁCULOS PARA LA TUTELA PENAL 12

2.1 Los criptoactivos como bienes lícitos 12

2.2 Modalidades de fraude, tipos penales aplicables y sus límites 13

2.3 Los obstáculos concretos para la tutela penal 15

3. BASE JURÍDICA DEL PATRIMONIO Y EL DELITO DE ESTAFA 16

3.1 Los tipos penales patrimoniales del Coip frente a los criptoactivos 16

3.2 El alcance del patrimonio protegido frente a los criptoactivos 18

4. JURISPRUDENCIA COMPARADA Y LECCIONES PARA EL ECUADOR 19

5. PROPUESTA NORMATIVA DE DESARROLLO CONSTITUCIONAL 21

5.1 Propuesta para el artículo 186 del Coip (estafa) 21

5.2 Propuesta para el artículo 190 del Coip (apropiación fraudulenta) 22

5.3 Propuesta para el artículo 323 del Coip (captación ilegal) 22

Conclusiones 23

Recomendaciones 25

Bibliografía 30

1. Normativa 30

2. Jurisprudencia 30

3. Pronunciamientos regulatorios y organismos internacionales 31

4. Doctrina 32

Introducción

En Ecuador, miles de personas están comprando, vendiendo e invirtiendo en criptoactivos con una naturalidad que contrasta con el silencio de la regulación jurídica. El Coip fue redactado en 2014, cuando los criptoactivos eran un fenómeno marginal; esa marginalidad ha desaparecido, pero la norma no ha sido objeto de actualización. El resultado es una acumulación de vacíos en tres planos: definitorio, tipológico y probatorio. La pregunta que recorre este trabajo es si esa ausencia normativa impide o dificulta la persecución penal del fraude con criptoactivos. La hipótesis es que sí: algunas lagunas pueden colmarse con interpretación sistemática, otras requieren reforma expresa.

La metodología es dogmático-interpretativa y sistemática. Se analizan las normas del ordenamiento ecuatoriano, la jurisprudencia comparada y la doctrina especializada, con el objeto de ofrecer criterios directamente aplicables por los operadores de justicia.

Objetivo general

Identificar los vacíos de tipicidad del Coip en relación con el fraude patrimonial mediante criptoactivos, distinguir los que pueden colmarse con las normas vigentes de los que requieren modificación legislativa y proponer criterios concretos para esta última.

Objetivos específicos

1. Determinar el estatus jurídico de los criptoactivos y su relación con el patrimonio penalmente protegido.
2. Identificar las modalidades de fraude y los tipos penales del Coip aplicables.
3. Analizar los vacíos que obstaculizan la persecución penal.
4. Proponer criterios de reforma legislativa.

Pregunta del problema jurídico

¿Las lagunas de tipicidad del Coip impiden una adecuada persecución penal del fraude patrimonial mediante criptoactivos en el Ecuador?

1. FUNDAMENTOS DOGMÁTICOS DEL DERECHO PENAL

El derecho penal, como mecanismo de control social de *última ratio*, opera bajo el principio de legalidad: ninguna conducta puede ser sancionada si no ha sido previamente definida por la ley (*nullum crimen sine lege*)[1]. Este principio garantiza seguridad jurídica y prohíbe la analogía en perjuicio del procesado[2]. La tipicidad describe los elementos objetivos y subjetivos de la conducta penalmente relevante[3]; el bien jurídico es el interés que el derecho penal resguarda con cada tipo[4]; la antijuridicidad exige que la conducta lesione ese bien sin justa causa[5]; y la culpabilidad requiere un juicio de reproche personal al autor fundado en su capacidad de comprender la ilicitud de su acción[6].

Aplicados al problema de los criptoactivos, estos presupuestos revelan el nudo central: si el patrimonio penalmente protegido no incluye expresamente los activos digitales, el fiscal que intenta encuadrar un fraude en el artículo 186 del Coip debe construir un argumento interpretativo que no todos los operadores están dispuestos a aceptar. La tipicidad estricta, en

[1]ROXIN, Claus, Derecho Penal. Parte General, t. I, Madrid: Civitas, 1997, pp. 137-180. Véase también FERRAJOLI, Luigi, Derecho y razón. Teoría del garantismo penal, Madrid: Trotta, 1995, pp. 374-379.

[2]FERRAJOLI, Derecho y razón, op. cit., pp. 380-385. En la jurisprudencia ecuatoriana, vid. Corte Constitucional del Ecuador, Sentencia N.º 1364-17-EP/23, caso N.º 1364-17-EP, ponente: Daniela Salazar Marín, sobre las dimensiones formal y material del principio de legalidad penal.

[3]MIR PUIG, Santiago, Derecho Penal. Parte General, 10.ª ed., Barcelona: Reppertor, 2016, pp. 153-160; MUÑOZ CONDE, Francisco; GARCÍA ARÁN, Mercedes, Derecho Penal. Parte General, 10.ª ed., Valencia: Tirant lo Blanch, 2019, pp. 247-260.

[4]ROXIN, Derecho Penal. Parte General, op. cit., pp. 51-56; MIR PUIG, Derecho Penal. Parte General, op. cit., pp. 117-125.

[5]JAKOBS, Günther, Derecho Penal. Parte General. Fundamentos y teoría de la imputación, Madrid: Marcial Pons, 1997, pp. 419-425.

[6]ROXIN, Derecho Penal. Parte General, op. cit., pp. 791-800; ZAFFARONI, Eugenio Raúl; ALAGIA, Alejandro; SLOKAR, Alejandro, Derecho Penal. Parte General, 2.ª ed., Buenos Aires: Ediar, 2002, pp. 649-680.

lugar de ser garantía, se convierte en obstáculo cuando la norma fue redactada antes de que el objeto del delito existiera[7].

2. CRIPTOACTIVOS EN ECUADOR: ESTATUS JURÍDICO, MODALIDADES DE FRAUDE Y OBSTÁCULOS PARA LA TUTELA PENAL

2.1 Los criptoactivos como bienes lícitos: lo que el ordenamiento ecuatoriano prohíbe y lo que no

Criptoactivos es un término más amplio que criptomonedas: comprende cualquier representación digital de valor transferible mediante tecnología de registro distribuido[8], e incluye *tokens* de acceso a plataformas, los que representan derechos sobre activos subyacentes, *stablecoins* y los no fungibles. Para efectos del análisis penal, lo relevante no es la clasificación técnica del activo, sino si tiene valor económico verificable en el tráfico jurídico.

La posición del Ecuador frente a los criptoactivos se articula en tres planos. El primero es la ausencia regulatoria: no existe marco normativo específico, ninguna superintendencia ejerce supervisión y no hay protección institucional para el inversor. El segundo es la prohibición parcial como medio de pago: el artículo 94 del Código Orgánico Monetario y Financiero establece al dólar como moneda de curso legal[9] y el artículo 98 prohíbe medios de pago no autorizados[10]; los criptoactivos no figuran entre los instrumentos aprobados por la

[7]BACIGALUPO, Enrique, Derecho Penal. Parte General, Buenos Aires: Hammurabi, 1999, pp. 105-115. Sobre los retos específicos del delito informático frente a la dogmática clásica, vid. HERNÁNDEZ BASUALDO, Héctor, "Problemas de política criminal y dogmática penal frente al delito informático", Revista de Derecho (Valdivia), vol. XIV, 2003, pp. 77-101.

[8]GAFI, Orientaciones sobre el enfoque basado en el riesgo para activos virtuales y proveedores de servicios de activos virtuales, París: GAFI, 2021, párr. 23-30; WERBACH, Kevin; CORNELL, Nicolas, "Contracts Ex Machina", Duke Law Journal, vol. 67, n.º 2, 2017, pp. 318-325.

[9]Ecuador, Código Orgánico Monetario y Financiero, art. 94, Registro Oficial Suplemento N.º 332, de 12 de septiembre de 2014.

[10]COMF, art. 98.

Junta de Política y Regulación Monetaria[11], lo que veda su uso como instrumento de pago dentro del sistema financiero. El tercer plano es el de la licitud patrimonial privada: la tenencia, compra, venta e intercambio de criptoactivos entre particulares no está prohibida.

Dos novedades normativas recientes reflejan un reconocimiento implícito. La Ley *Fintech*, vigente desde diciembre de 2022, reguló actividades tecnológicas relacionadas con *blockchain*[12]. La reforma tributaria de 2024 incluyó los rendimientos del *trading* de activos digitales en la declaración de renta[13]. Ninguna define qué son los criptoactivos ni establece protección penal, pero ambas evidencian que el reconocimiento avanzó del lado financiero sin llegar al campo penal.

Esta triple realidad tiene una consecuencia directa para el análisis penal: los fraudes con criptoactivos ocurren en la zona lícita de la inversión y la tenencia, no en la zona prohibida del pago. La víctima que pierde *bitcoin* en una plataforma fraudulenta está siendo despojada de un activo con valor económico verificable[14]. El propio Estado reconoce ese valor al gravar sus rendimientos con el impuesto a la renta[15]; no puede recaudar sobre ese valor y negarlo cuando se trata de proteger a quien lo pierde en un fraude.

2.2 Modalidades de fraude, tipos penales aplicables y sus límites

Lo que hace difícil perseguir penalmente el fraude con criptoactivos no es la conducta en sí misma. El engaño, la promesa falsa y el aprovechamiento de la confianza ajena son tan viejos

[11]Junta de Política y Regulación Monetaria del Ecuador, Resolución N.º JPRM-2023-014-M, de 7 de agosto de 2023, sobre clasificación de medios de pago.

[12]Ecuador, Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos, Registro Oficial Suplemento N.º 215, Segundo Suplemento, de 22 de diciembre de 2022.

[13]Ecuador, Reforma a la Ley Orgánica de Régimen Tributario Interno, Registro Oficial Suplemento N.º 525, de 25 de marzo de 2024.

[14]MAYER LUX, Laura, "El uso de criptomonedas en el lavado de activos: desafíos regulatorios y penales", Revista de Derecho Penal y Criminología, n.º 25, 2021, pp. 50-58; ARTEAGA, Pablo, "Criptomonedas en Ecuador: ¿Realmente el BCE puede prohibir o criminalizar su uso?", Lexis.ec, 22 de agosto de 2024, https://www.lexis.com.ec, consultado el 29/04/26.

[15]Reforma a la LORTI, op. cit.

como el comercio. Lo que cambia es el soporte tecnológico y, con él, la pregunta de qué tipo penal se aplica con precisión. En el Ecuador se repiten cuatro modalidades que no se encuadran todas en el mismo artículo del Coip, y confundirlas tiene consecuencias procesales reales.

La primera es la plataforma de inversión fraudulenta. Una empresa, o quien aparenta serlo, ofrece rendimientos garantizados sobre inversiones en criptoactivos y desaparece una vez recibido el capital. Si lo entregado fue dinero *fiat* con promesa de rendimientos en criptoactivos, aplica el artículo 323[16]; si lo aportado directamente fueron criptoactivos, el tipo correcto es el artículo 186[17], porque el objeto de la disposición patrimonial viciada por el engaño es el propio activo digital.

La segunda modalidad es el esquema piramidal con envoltorio digital: el rendimiento prometido proviene del dinero de nuevos inversores[18], no de operaciones reales. La tercera es la venta de *tokens* inexistentes: la víctima adquiere participación en un proyecto *blockchain* que nunca existió o que no tenía valor. El tipo aplicable en ambos casos es el artículo 186.

La cuarta modalidad tiene una estructura completamente distinta: el fraude por acceso no autorizado o *phishing*. Mediante mensajes que simulan ser de plataformas legítimas, el autor obtiene las claves privadas de la *wallet* de la víctima y transfiere los fondos sin que exista ningún acto de disposición voluntario. El tipo penal aplicable no es la estafa del artículo 186, sino la apropiación fraudulenta por medios electrónicos del artículo 190 del Coip [19].

La distinción entre el artículo 186 y el artículo 190 no es un tecnicismo menor[20]. Afecta la calificación del hecho, la pena aplicable y la estrategia procesal. En la estafa del 186, el

---

[16]Coip ,art. 323.

[17]Coip , art. 186.

[18]MOISEIENKO, Anton, "Money Laundering through Cryptocurrencies: Risks and Regulatory Responses", Journal of Money Laundering Control, vol. 24, n.° 2, 2021, pp. 387-397; ALAGNA, Flavia; TRUCCO, Luca, "Cryptocurrency Fraud and Criminal Liability: A Comparative Analysis", Computer Law & Security Review, vol. 47, 2022, DOI: 10.1016/j.clsr.2022.105743.

[19]Coip, art. 190.

[20]Sobre la diferenciación dogmática entre estafa y apropiación por medios informáticos, vid. MATA Y MARTÍN, Ricardo M., "Estafa convencional, estafa informática y robo en el ámbito de internet", Revista Penal, n.° 6, 2000,

elemento central es el engaño que produce un error que determina una disposición patrimonial voluntaria, aunque viciada. En la apropiación del 190, no hay disposición voluntaria[21]: la víctima no entrega nada; le sustraen. Un tribunal que confunda estos elementos puede declarar la nulidad del proceso por error en la calificación jurídica.

2.3 Los obstáculos concretos para la tutela penal

Saber qué tipo penal aplica es necesario, pero no suficiente. Quienes han intentado perseguir estos casos en Ecuador han chocado con obstáculos que no son todos normativos. Algunos son técnicos, otros son institucionales. Todos son reales.

El primero es la falta de reconocimiento legal expreso de los criptoactivos como parte del patrimonio protegido. No hay norma que señale que "los criptoactivos son bienes en el sentido del artículo 186 del Coip", y esa ausencia genera incertidumbre al formular cargos. El artículo 186 no tiene referencia expresa al activo digital, lo que no significa que no se aplique, sino que su aplicación requiere un argumento jurídico que el operador de justicia debe construir, y no todos lo hacen.

El segundo es la identificación del autor. Las transacciones en *blockchain* ocurren entre direcciones alfanuméricas sin nombre[22]. Vincular una dirección a una persona física requiere información adicional que no siempre está disponible, y cuando la plataforma opera desde el exterior sin presencia jurídica en Ecuador, obtenerla depende de cooperación internacional, que es lenta y con frecuencia infructuosa.

---

pp. 51-63; GALÁN MUÑOZ, Alfonso, El fraude y la estafa mediante sistemas informáticos. Análisis del art. 248.2 CP, Valencia: Tirant lo Blanch, 2005, pp. 241-260.

[21]GALÁN MUÑOZ, El fraude y la estafa mediante sistemas informáticos, op. cit., pp. 285-301.

[22]CANO MARTÍNEZ, Jeimy José, Computación forense. Descubriendo los rastros informáticos, 2.ª ed., Bogotá: Alfaomega, 2015, pp. 412-428; RIQUERT, Marcelo Alfredo, Ciberdelitos. Régimen penal de las nuevas tecnologías, Buenos Aires: Hammurabi, 2019, pp. 187-205.

El tercero es la valoración probatoria. El Coip regula la evidencia digital en términos genéricos en el artículo 460[23], pero no prevé protocolos específicos para activos virtuales ni estándares para peritajes de *blockchain*. Un *hash* de transacción o un análisis de trazabilidad son instrumentos que el proceso penal ecuatoriano no ha integrado con procedimientos claros.

El cuarto es la jurisdicción. La mayoría de las plataformas fraudulentas no tienen domicilio en Ecuador y sus responsables pueden estar en cualquier parte del mundo. El principio de territorialidad del artículo 14 del Coip funda la competencia de los tribunales ecuatorianos cuando el perjuicio ocurre en el país[24], pero esto no resuelve el problema práctico: notificar a un imputado en el exterior, ejecutar medidas cautelares sobre *wallets* o recuperar activos en múltiples jurisdicciones requiere instrumentos que Ecuador no tiene todavía.

El quinto es más difícil de cuantificar: muchas víctimas no denuncian por creer que la actividad era cuasilegal o por desconfianza en el sistema[25]. La consecuencia es una cifra negra que impide dimensionar el problema y priva a los tribunales de los casos que generarían los precedentes necesarios.

3. BASE JURÍDICA DEL PATRIMONIO Y EL DELITO DE ESTAFA FRENTE A LOS CRIPTOACTIVOS EN EL ECUADOR

3.1 Los tipos penales patrimoniales del Coip frente a los criptoactivos: artículos 186, 323 y 190

El artículo 186 del Coip construye la estafa sobre cuatro elementos sucesivos[26]: un engaño idóneo para inducir a error, el error efectivamente provocado en la víctima, un acto de

[23]Coip, art. 460.

[24]Coip, art. 14.

[25]MIRÓ LLINARES, Fernando, "La oportunidad criminal en el ciberespacio. Aplicación de la Teoría de las Actividades Cotidianas para la prevención del cibercrimen", Revista Electrónica de Ciencia Penal y Criminología (RECPC), n.º 13-07, 2011, http://criminet.ugr.es/recpc/13/recpc13-07.pdf, consultado el 29/04/26.

[26]CHOCLÁN MONTALVO, José Antonio, El delito de estafa, 2.ª ed., Barcelona: Bosch, 2009, pp. 75-92; PASTOR MUÑOZ, Nuria, La determinación del engaño típico en el delito de estafa, Madrid: Marcial Pons, 2004,

disposición patrimonial derivado de ese error y un perjuicio económico verificable. Sin embargo, la norma no precisa qué debe entenderse por "patrimonio" ni qué bienes integran su objeto material, lo que abre una zona interpretativa especialmente sensible cuando lo disputado no es dinero convencional ni un bien corporal, sino una representación digital de valor como los criptoactivos.

El artículo 323, por regla general, no resulta aplicable a estos supuestos. Sanciona la captación habitual y masiva de recursos del público sin autorización de la autoridad competente[27], dentro de la lógica del sistema financiero regulado, y protege el orden socioeconómico antes que el patrimonio individual. En los conflictos típicos con criptoactivos, desarrollados entre particulares, no concurren la habitualidad, la masividad ni la oferta pública de rendimientos que exige el tipo, pues no existe intermediación financiera en sentido estricto, sino intercambios privados sobre activos digitales. Solo de manera excepcional podrá invocarse cuando el caso adopte la estructura de un esquema piramidal o de captación masiva mediante criptoactivos.

Cabe recordar que, en Ecuador, las criptomonedas no están prohibidas, pero tampoco integran el sistema financiero regulado; por ello, quien solicita fondos para "invertir en criptomonedas" no realiza gestión financiera en sentido estricto, sino una relación entre particulares. En consecuencia, el artículo 323 queda fuera no por la licitud de las criptomonedas, sino porque el problema no es financiero-regulatorio, sino patrimonial.

---

pp. 103-128; PÉREZ MANZANO, Mercedes, "El tipo objetivo de la estafa: reflexiones sobre la teoría de la imputación objetiva", Anuario de Derecho Penal y Ciencias Penales, vol. XLVI, fasc. III, 1993, pp. 1023-1063. En la jurisprudencia nacional, vid. Corte Nacional de Justicia, Sala Especializada de lo Penal, Penal Militar, Penal Policial y Tránsito, Resolución R: 151-2017, Juicio J: 042-2016-SSI, Gaceta Judicial, Serie XIX, N.º 2, Quito: CNJ, 2019, p. 851, disponible en https://www.cortenacional.gob.ec/cnj/images/Produccion_CNJ/Gaceta/Gaceta-Judicial-II-serie-XIX.pdf, consultado el 30/04/26.

[27]BAJO FERNÁNDEZ, Miguel; BACIGALUPO SAGGESE, Silvina, Derecho Penal Económico, 2.ª ed., Madrid: Centro de Estudios Ramón Areces, 2010, pp. 412-428.

El artículo 190, por su parte, tampoco ofrece una respuesta general para estos conflictos. La norma no castiga cualquier apropiación o incumplimiento vinculado a bienes digitales[28], sino únicamente la utilización fraudulenta de sistemas informáticos, redes electrónicas o de telecomunicaciones, acompañada de la alteración, manipulación o modificación de su funcionamiento, para facilitar la apropiación de un bien ajeno o procurar una transferencia no consentida de bienes, valores o derechos. Cuando el conflicto se reduce a un engaño entre particulares, a una falsa promesa de inversión o a un posterior incumplimiento en la devolución de lo entregado, no concurre la manipulación técnica del sistema que exige el tipo, sino un fraude patrimonial clásico que escapa de su ámbito. Por lo tanto, el artículo 190 solo se aplicará cuando haya una intervención indebida en el sistema informático (como acceder sin autorización a billeteras digitales, manipular plataformas de intercambio o modificar credenciales y claves) que posibilite la obtención o transferencia del criptoactivo.

La trilogía normativa de los artículos 186, 323 y 190 establece una protección patrimonial en tres niveles distintos: la intrusión tecnológica, el engaño entre personas y la captación financiera irregular. Sin embargo, los tres tienen una misma área ciega: no aclaran si el patrimonio penalmente protegido incluye los activos digitales, lo que genera incertidumbre a la hora de interpretar los criptoactivos.

3.2 El alcance del patrimonio protegido frente a los criptoactivos

Al revisar con detenimiento los tipos penales analizados en el apartado anterior, se descubre que el verdadero nudo del problema no está en que falten normas para sancionar conductas fraudulentas o abusivas. Las hay, y con elementos típicos razonablemente amplios. La dificultad real aparece un paso antes: ninguna de esas disposiciones define qué abarca

[28]GALÁN MUÑOZ, El fraude y la estafa mediante sistemas informáticos, op. cit., pp. 285-301; ROMEO CASABONA, Carlos María, "Los delitos de daños en el ámbito informático", en ROMEO CASABONA, Carlos María (dir.), El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales, Granada: Comares, 2006, pp. 250-260.

exactamente el patrimonio que dicen proteger. Mientras esa ausencia regulatoria no generaba mayores complicaciones tratándose de dinero en efectivo, vehículos o inmuebles, la irrupción de los criptoactivos puso al descubierto una zona gris que el legislador ecuatoriano todavía no ha resuelto.

Ante esa indeterminación, la doctrina penal ha recorrido dos vías de interpretación que es preferible diferenciar con precisión. Algunos abogan por una interpretación de tipo económico-funcional del patrimonio, la cual sostiene que lo fundamental no es la manera en que un bien se presenta o el soporte en el que se encuentra, sino su capacidad real de representar valor y de ser objeto de apropiación. Desde este punto de vista, un *token* no fungible o un *bitcoin* deberían recibir la misma protección penal que una transferencia bancaria, ya que en la práctica llevan a cabo una función económica similar. Frente a esta postura, hay otra variante formalista que estima que la tutela penal exige una determinada previsión normativa previa a la intervención penal. Entonces, si el ordenamiento jurídico no ha declarado explícitamente que los criptoactivos son bienes o que se integran al patrimonio, el operador de justicia no puede ampliar el alcance de un tipo penal por medio de la analogía, sobre todo en lo que hace referencia a lo criminal, donde el principio de legalidad estricta plantea auténticas barreras infranqueables.

La realidad es que este debate va más allá del ámbito exclusivamente académico. La respuesta que puede ofrecer el sistema penal oscilando entre una legalidad sin penalidad por atipicidad y la sanción efectivamente impuesta al culpable según el enfoque que decida un juez en el momento de la resolución de un caso determinado o un fiscal cuando formule los cargos. Esta oscilación no es un problema irrelevante, sino que manifiesta una debilidad estructural del ordenamiento ecuatoriano frente a las modalidades delictivas que operan exclusivamente en el ámbito de lo digital.

4. JURISPRUDENCIA COMPARADA Y LECCIONES PARA EL ECUADOR

Lo ocurrido en otros ordenamientos no resuelve el problema ecuatoriano, pero sí ofrece criterios definidos. Dos decisiones recientes resultan relevantes.

La primera corresponde al caso *D'Aloia* contra Personas Desconocidas, que fue resuelto por el Tribunal Superior de Inglaterra y Gales en el año 2024. El tribunal reconoció que los *tokens* USDT pueden ser objeto de Derechos de propiedad en sentido jurídico aun independientemente de qué tengan o no el reconocimiento de moneda de curso legal, bastando con que solamente posea valor económico comprobable en el tráfico. Precisamente ese es el criterio que este trabajo propone para el artículo 186 del Coip. El fallo también rechazó parte de las reclamaciones por la razón de que la pericia no cumplía con los estándares metodológicos que se exigían, ya que la trazabilidad *blockchain* por sí sola no sirve de nada si la pericia no es consistente o reproducible. Para Ecuador, esta segunda línea del fallo constata que el vacío procesal en materia de peritaje *blockchain* no es un mero problema normativo y ha costado ya a víctimas reales el haber quedado sin la posibilidad de obtener la reparación.

La segunda decisión es el caso *Arbistar,* resuelto por la Audiencia Nacional de España en primera instancia en septiembre de 2025 y confirmado en apelación en marzo de 2026[29]. Arbistar captó fondos prometiendo rendimientos en criptomonedas que nunca se materializaron y fue condenado por estafa masiva, con un universo aproximado de 32.000 inversores afectados, de los cuales 9.494 ejercieron acusación particular y un quebranto patrimonial estimado en 200 millones de euros. Lo más relevante para el Ecuador: el tribunal reconoció que los *bitcoins* entregados constituían el perjuicio patrimonial del tipo penal sin necesidad de reconocimiento expreso como moneda de curso legal[30]. El tipo aplicado, la estafa, tiene una estructura similar al artículo 186 del Coip: engaño, error inducido, disposición patrimonial y

[29]Audiencia Nacional (España), Sala de lo Penal, Sección Tercera, Sentencia de 17 de septiembre de 2025, Caso Arbistar (Santiago Fuentes Jover y Diego Felipe Fernández Nojarova), confirmada y agravada por la Sala de Apelación de la Audiencia Nacional, Sentencia de 11 de marzo de 2026, que duplicó las penas (de 8 a 16,5 años y de 6 a 11,5 años, respectivamente) e introdujo el delito de organización criminal.

[30]AN, Sentencia Caso Arbistar, op. cit.

perjuicio. Lo que Ecuador aún no tiene es la certeza normativa ni el protocolo pericial para llegar a ese resultado de forma sistemática, sin depender del criterio individual del fiscal o del juez que conozca el caso.

Ambas decisiones refuerzan la tesis central: el artículo 186 del Coip puede alcanzar los fraudes con criptoactivos si se interpreta sistemáticamente y el sistema probatorio adopta los estándares internacionales.

5. PROPUESTA NORMATIVA DE DESARROLLO CONSTITUCIONAL PARA RESOLVER LOS VACÍOS DE TIPICIDAD EN LOS ARTÍCULOS 186, 190 Y 323 DEL COIP

Partiendo del principio de legalidad penal (art. 76, numeral 3, de la Constitución de la República del Ecuador)[31], se propone una solución normativa que dote de certeza al objeto material de los delitos patrimoniales en entornos digitales. Consiste en una disposición general en el Título Preliminar del Coip [32], complementada con cláusulas interpretativas en los artículos 186, 190 y 323 que incluyan las representaciones digitales de valor y los activos virtuales. Así se garantiza seguridad jurídica y aplicación uniforme, sin expandir el *ius puniendi*.

5.1 Propuesta normativa para el artículo 186 del Coip (estafa)

Incorporar un inciso final o numeral interpretativo en el artículo 186:

Para efectos de este artículo, se entenderá por patrimonio el conjunto de bienes, derechos y valores susceptibles de apreciación económica, con independencia de su soporte material o digital. Se incluyen expresamente las representaciones digitales de valor, activos virtuales y criptoactivos, siempre que su valor sea verificable en el tráfico jurídico o económico.

[31] Ecuador, Constitución de la República del Ecuador, art. 76, numeral 3, Registro Oficial N.º 449, de 20 de octubre de 2008.

[32] Sobre la exigencia de normas previas, claras y públicas como fundamento del *ius puniendi* y la prohibición de analogía, vid. Corte Constitucional del Ecuador para el Período de Transición, Sentencia N.º 031-10-SEP-CC, caso N.º 0649-09-EP; y Corte Constitucional del Ecuador, Sentencia N.º 1364-17-EP/23, op. cit.

Esta incorporación no altera el verbo rector ni la estructura típica del engaño, sino que precisa el objeto material del delito, asegurando que el desplazamiento patrimonial pueda recaer sobre activos digitales sin necesidad de forzar la interpretación[33]. Con ello se respeta la reserva de ley y se cumple la exigencia de taxatividad del artículo 76, numeral 3, de la Constitución.

5.2 Propuesta normativa para el artículo 190 del Coip (apropiación fraudulenta por medios electrónicos)

Incorporar un inciso aclaratorio dentro del artículo 190:

Para la configuración de este delito, se entenderá que los bienes o valores objeto de apropiación comprenden tanto aquéllos de naturaleza material como las representaciones digitales de valor, incluidos activos virtuales y criptoactivos, cuando sean susceptibles de control, transferencia o disposición mediante sistemas electrónicos, informáticos o telemáticos.

En este caso, la norma cumple una función de adecuación técnica entre el medio comisivo y el objeto material. No amplía el tipo penal, sino que evita interpretaciones restrictivas que excluyan injustificadamente los activos digitales, manteniendo coherencia con la lógica del propio artículo, que ya está diseñado para entornos tecnológicos.

5.3 Propuesta normativa para el artículo 323 del Coip (captación ilegal de dinero)

Aquí la técnica debe ser más cuidadosa, porque, como ya identificamos, el problema no es solo el objeto, sino la naturaleza de la intermediación.

Se propone incorporar un inciso final:

A efectos de la presente investigación, se definirá el término "dinero" o "recursos del público" como aquella clase de valor entregado por terceros en la expectativa de reembolso, o de un

[33]Sobre la dimensión constitucional del derecho a la propiedad y la obligación del Estado de garantizar su acceso y protección en todas sus formas, vid. Corte Constitucional del Ecuador, Sentencia N.º 176-14-EP/19, caso N.º 176-14-EP, ponentes: Wendy Molina Andrade, Tatiana Ordeñana Sierra y Manuel Viteri Olvera.

beneficio, lo que incluye medios de pago electrónicos, bienes virtuales o representaciones digitales del valor, siempre y cuando la actividad incluya un esquema habitual y masivo de captación, que sea análogo a la intermediación financiera.

Esta redacción tiene aquí una doble función: en primer lugar, evitar que la defensa sostenga que las criptomonedas no son dinero; en segundo lugar, establecer un criterio de equivalencia funcional, que permite diferenciar las operaciones simples con criptoactivos de las que son verdaderos mecanismos de captación ilegal.

Además, mantiene intacto el núcleo de tipo penal, que no es otro que la intermediación financiera no autorizada, evitando así una expansión ilegítima del derecho penal hacia conductas externas.

Las tres propuestas aportan una lógica común, no crean nuevos delitos ni modifican las penas, sino que redimensionan el objeto material desde una visión económica y funcional, de tal forma que permite a cualquier juez poder usar los tipos penales sin tener que recurrir a la analogía o a interpretaciones forzadas.

Conclusiones

Lo que este trabajo demuestra no es la falta de un marco legal que permita la persecución del fraude que involucre criptoactivos en Ecuador, sino más bien la ambigüedad existente de las normas jurídicas que tienen por objeto la regulación del uso de criptoactivos. Chainalysis (2023) estima que, entre junio de 2022 y julio de 2023, en Ecuador ingresó alrededor de USD 7.000 millones en criptoactivos, lo que supone un 5,8 % del PIB. Esa magnitud de patrimonio privado está expuesta si el sistema penal no plantea una respuesta previsible.

El primer obstáculo que se presenta es de definición. El Coip no deja claro si los criptoactivos son parte del patrimonio que protege el derecho penal. Esta falta de definición no

cierra la puerta de un modo automático, pero sí exige que cada juez y cada Fiscal plantee su propia respuesta, lo que el principio de legalidad prohíbe: la ley tiene que ser la que determine, no quien la aplica.

La calificación es el segundo de los problemas. El Coip ofrece tres encuadres potenciales para la misma conducta delictiva: captación ilícita (artículo 323), estafa (artículo 186) o apropiación por medios electrónicos (artículo 190). Un error en la elección no sería un error de tipo académico; sino que tarde o temprano desembocaría en una nulidad, en una absolución, o en que la parte víctima quede sin respuesta.

El tercero es un problema de prueba. El fiscal, aunque puede establecer qué artículo le corresponde, sigue sin demostrar el hecho. El Coip no incluye de qué modo proteger un activo digital, ni cuál es el modo de rastrearlo en una cadena de bloques, ni qué condiciones debería reunir la pericia sobre este tipo de prueba. Si la evidencia no sobrepasa el proceso judicial, una conducta puede ser evidentemente antijurídica y quedar impune.

Aclarando esto, el art. 186 establece una solución digna de ser resaltada. En caso de que sea analizado desde una perspectiva funcional-económica del patrimonio, podrá incluirse a los criptoactivos, previa prueba de su valor económico, sin necesidad de forzar el texto ni de vulnerar el principio de legalidad. No se trata de una visión aislada: en sentido similar se pronunció tanto la Audiencia Nacional en el caso *Arbistar* (2025, ratificado en 2026) como el tribunal inglés en D'Aloia v Persons Unknown (2024), acogiendo la idea de que los criptoactivos habían sufrido un daño patrimonial sin adquirir el reconocimiento como moneda.

Entonces, la hipótesis inicial se confirma. Ecuador cuenta con regulaciones que, si se comprenden y se saben aplicar, pueden dar respuesta a la problemática del fraude con criptoactivos, y el capítulo 5 ofrece sugerencias concretas para abordar los vacíos de regulación que se ha identificado. Pero, mientras no se lleven a cabo esas modificaciones en la regulación,

la situación será la misma: que el juez o el fiscal correspondiente será el que determine la protección de la víctima, dejando de lado lo que indica la ley.

Recomendaciones

A partir del análisis realizado, las siguientes recomendaciones pretenden cubrir las tres lagunas que han sido detectadas, pero ninguna de ellas presupone la creación de nuevos delitos ni la apertura del poder punitivo del estado, sino que se pretende precisar, más no expandir.

Primera recomendación: precisar el alcance del patrimonio protegido (técnica legislativa)

Lo que más urge es cerrar la indeterminación definitoria. El Coip carece de una norma que establezca qué comprende el patrimonio como bien jurídico protegido. La Sección Novena del Libro Primero, dedicada a los delitos contra el derecho a la propiedad, comienza directamente con el delito de extorsión sin ningún tipo de encuadre conceptual previo, y esa falta es la raíz del problema. En ausencia de una definición expresa, cualquier operador de justicia puede dudar de si los criptoactivos quedan fuera o no del patrimonio penalmente protegido.

Para cerrar esa laguna, se prevé la inclusión de un artículo innumerado al comienzo de la sección mencionada, justo antes del artículo 185.

Texto vigente:

> No hay. La Sección Novena: Los delitos contra el derecho a la propiedad (arts. 185-202) no incluyen ninguna norma que defina el bien jurídico patrimonial.

Texto con la reforma:

> ***Art. (...). Alcance del patrimonio protegido. Para efectos de los delitos previstos en esta sección, se definirá al patrimonio como el conjunto de bienes, derechos y valores que tienen un contenido económico, sin importar si son físicos o digitales.***

> ***Se incluyen específicamente los criptoactivos y otras representaciones digitales de valor que tienen la capacidad de aumentar su valor económico.***

A esa definición general deben sumarse precisiones dentro de los artículos 186, 190 y 323.

Artículo 186. Estafa

El tipo penal de estafa protege el patrimonio, pero no precisa que abarca este concepto frente a activos de naturaleza digital. Se propone incorporar un inciso final que despeje esa duda.

Texto vigente:

> Art. 186. Estafa. La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

Texto con la reforma:

> ***Art. 186. Estafa. La persona que, [...] Para efectos de este artículo, el patrimonio cuyo perjuicio se requiere para la configuración del tipo comprende los bienes, derechos y valores de cualquier naturaleza, incluyendo los activos y las representaciones digitales de valor susceptibles de apreciación económica.***

Artículo 190. Apropiación fraudulenta por medios electrónicos

Este tipo opera en entornos tecnológicos, pero no menciona activos digitales de forma expresa. Se propone un inciso final que cierre esa brecha.

Texto vigente:

> Art. 190. Apropiación fraudulenta por medios electrónicos. La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o

> modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Texto con la reforma:

> ***Art. 190. Apropiación fraudulenta por medios electrónicos. La persona que utilice fraudulentamente [...] Para la configuración de este delito, se entenderán comprendidos dentro de los bienes, valores o derechos susceptibles de apropiación o transferencia no consentida, los activos y las representaciones digitales de valor, incluyendo los criptoactivos.***

Artículo 323. Captación ilegal de dinero

Este tipo fue diseñado para proteger el orden financiero del país frente a esquemas de captación masiva, no el patrimonio individual. Algunos operadores lo han aplicado a casos de fraude con criptoactivos que no tienen esa estructura, lo que desnaturaliza el tipo. Se propone un inciso final que delimite su alcance con precisión.

Texto vigente:

> Art. 323. Captación ilegal de dinero. La persona que organice, desarrolle y promocione de forma pública o clandestina, actividades de intermediación financiera sin autorización legal, destinadas a captar ilegalmente dinero del público en forma habitual y masiva, será sancionada con pena privativa de libertad de cinco a siete años. La persona que realice operaciones cambiarias o monetarias en forma habitual y masiva, sin autorización de la autoridad competente, será sancionada con pena privativa de libertad de tres a cinco años.

Texto con la reforma:

> ***Art. 323. Captación ilegal de dinero. La persona que organice, [...] Para los efectos de este artículo, la captación de criptoactivos o representaciones digitales***

> ***de valor quedará comprendida en el tipo únicamente cuando se realice de forma habitual, masiva y organizada bajo esquemas asimilables a intermediación financiera no autorizada. En los otros casos de fraude que incluyan estos activos, se aplicará el artículo 186 de este Código.***

Las tres precisiones tienen una lógica común: no crean nuevos delitos ni cambian las penas, sino que aclaran el objeto material de los tipos existentes para garantizar que la protección penal no dependa de cómo cada operador judicial lo interprete ese día.

Segunda recomendación: protocolos de evidencia digital

Si el sistema no tiene la capacidad de demostrar los hechos, la reforma normativa es inútil. El Coip, en su artículo 460, regula de manera general la evidencia digital, pero no incluye protocolos concretos para activos virtuales ni normas para los peritajes de trazabilidad en cadena de bloques. Ecuador requiere normas precisas para gestionar este tipo de pruebas: cómo se identifica y protege un criptoactivo, cómo se documenta su cadena de custodia y qué procedimiento tiene que seguir una pericia de trazabilidad en *blockchain* para ser reproducible y no ser descartado en audiencia. La mejor reforma normativa puede ser ineficaz sin esa regulación concreta, debido a la falta de una prueba admisible.

Tercera recomendación: cooperación internacional

La mayoría de las plataformas fraudulentas no tienen domicilio en Ecuador y sus responsables pueden estar en cualquier parte del mundo. El artículo 14 del Coip permite fundar la competencia de los tribunales ecuatorianos cuando el perjuicio ocurre en el país, pero eso no resuelve el problema práctico de notificar a alguien en el exterior, congelar activos en múltiples billeteras o recuperar fondos de jurisdicciones que no cooperan. Ecuador debería explorar la adhesión al Convenio de Budapest sobre la ciberdelincuencia (ETS N.º 185)[34], fortalecer los

[34]Consejo de Europa, Convenio sobre la ciberdelincuencia (ETS N.º 185), Budapest, 23 de noviembre de 2001.

mecanismos de intercambio de información financiera en el marco del GAFILAT[35] y desarrollar protocolos específicos para la persecución penal transfronteriza de fraudes con activos digitales. Sin instrumentos reales de cooperación internacional, la reforma interna queda incompleta.

Cuarta recomendación: capacitación especializada

Nada de lo anterior funciona si quienes tienen que aplicarlo no están preparados. Los fiscales necesitan saber cómo funciona una cadena de bloques. Los jueces necesitan entender qué significa un *hash* de transacción. Los peritos deben estar alineados con las normas internacionales en materia de trazabilidad. Eso necesita programas de capacitación continúa y actualizada, articulados institucionalmente desde la Fiscalía General del Estado y el Consejo de la Judicatura, tomando como modelo a las unidades especializadas en cibercrimen que han sido establecidas en países de la región, y no solo cursos ocasionales con un alcance limitado.

Quinta recomendación: coherencia entre el derecho penal, el financiero y la regulación tecnológica

El Estado ecuatoriano enfrenta una contradicción que debe solucionar. Hoy cobra impuesto a la renta sobre los rendimientos del trading de activos digitales y exige a los operadores del sector que reporten en sus controles antilavado. Sin embargo, si una persona pierde esos mismos activos a causa de un fraude, el sistema penal no le brinda una respuesta clara. Ese desajuste no es únicamente un asunto normativo, pone en peligro la protección real de la propiedad en los entornos digitales. Las tres ramas (la financiera, la penal y la de regulación tecnológica) deben avanzar en conjunto, ya que el resguardo del patrimonio digital no puede estar supeditado a cuál de ellas reconozca el valor del activo en ese momento.

[35]GAFILAT (Grupo de Acción Financiera de Latinoamérica), Documentos sobre intercambio de información financiera y cooperación regional, https://www.gafilat.org, consultado el 29/04/26.

Bibliografía

1. Normativa

Constitución de la República del Ecuador, Registro Oficial N.º 449, 20 de octubre de 2008.

Código Civil, Registro Oficial Suplemento N.º 46, 24 de junio de 2005.

Código Orgánico Integral Penal (Coip), Registro Oficial Suplemento N.º 180, 10 de febrero de 2014.

Código Orgánico Monetario y Financiero, Registro Oficial Suplemento N.º 332, 12 de septiembre de 2014.

Consejo de Europa, Convenio sobre la ciberdelincuencia (ETS N.º 185), Budapest, 23 de noviembre de 2001.

Ecuador, Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos, Registro Oficial Suplemento N.º 215, Segundo Suplemento, 22 de diciembre de 2022.

Ecuador, Reforma a la Ley Orgánica de Régimen Tributario Interno, Registro Oficial Suplemento N.º 525, 25 de marzo de 2024.

Ecuador, Ley Orgánica para la Mejora Recaudatoria a través del Combate al Lavado de Activos, Decreto Ejecutivo N.º 477, Registro Oficial N.º 700, Suplemento, 10 de diciembre de 2024.

Organización de las Naciones Unidas, Convención de las Naciones Unidas contra la ciberdelincuencia, Nueva York, 2024.

Unión Europea, Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (MiCA), Diario Oficial de la Unión Europea, L 150, 9 de junio de 2023, pp. 40-205. Aplicación plena desde el 30 de diciembre de 2024.

2. Jurisprudencia

Audiencia Nacional (España), Sala de lo Penal, Sección Tercera, Sentencia de 17 de septiembre de 2025, Caso *Arbistar* (Santiago Fuentes Jover y otro), estafa masiva continuada mediante plataforma de criptomonedas (200 millones de euros, 32.000 inversores afectados, 9.494 acusaciones particulares). Confirmada y agravada por la Sala de Apelación de la Audiencia Nacional, Sentencia de 11 de marzo de 2026. Nota de prensa oficial del Consejo General del Poder Judicial, disponible en www.poderjudicial.es.

Corte Constitucional del Ecuador, Sentencia N.º 176-14-EP/19, caso N.º 176-14-EP, dimensión constitucional del derecho a la propiedad en acciones de protección y obligación del Estado de garantizar el acceso y protección del derecho de propiedad en todas sus formas, ponentes: Wendy Molina Andrade, Tatiana Ordeñana Sierra y Manuel Viteri Olvera.

Corte Constitucional del Ecuador, Sentencia N.º 1364-17-EP/23, caso N.º 1364-17-EP, principio de legalidad penal (art. 76, numeral 3, CRE): dimensión formal (reserva de ley) y dimensión material (mandato de tipicidad), límites de la prohibición de analogía frente a la interpretación sistemática, ponente: Daniela Salazar Marín.

Corte Constitucional del Ecuador para el Período de Transición, Sentencia N.º 031-10-SEP-CC, caso N.º 0649-09-EP, principio de legalidad penal y seguridad jurídica (arts. 76, numeral 3, y 82 de la CRE): exigencia de normas jurídicas previas, claras y públicas como fundamento del ius puniendi.

Corte Nacional de Justicia, Sala Especializada de lo Penal, Penal Militar, Penal Policial y Tránsito, Resolución R: 151-2017, Juicio J: 042-2016-SSI, "Delito de estafa: elementos constitutivos y engaño como elemento principal", Gaceta Judicial, Serie XIX, N.º 2, Quito: CNJ, 2019, p. 851, disponible en https://www.cortenacional.gob.ec/cnj/images/Produccion_CNJ/Gaceta/Gaceta-Judicial-II-serie-XIX.pdf, consultado el 30/04/26.

High Court of England and Wales, Chancery Division, D'Aloia v Persons Unknown, [2024] EWHC 2342 (Ch) (Deputy Judge Farnhill), resolución sobre reconocimiento de *tokens* USDT como propiedad y estándares de trazabilidad pericial en fraude con criptoactivos.

3. Pronunciamientos regulatorios y organismos internacionales

Banco Central del Ecuador, Comunicado oficial sobre *Bitcoin*, 8 de enero de 2018, disponible en www.bce.fin.ec.

Banco Central del Ecuador y Junta de Política y Regulación Monetaria, Comunicado oficial "Los criptoactivos no son una moneda de curso legal, ni un medio de pago autorizado en Ecuador", 13 de agosto de 2024, disponible en www.bce.fin.ec.

CHAINALYSIS, The 2023 Geography of Cryptocurrency Report, Nueva York: Chainalysis Inc., 2023, https://go.chainalysis.com/2023-geography-of-cryptocurrency-report.html, consultado el 30/04/26.

Ecuador, Junta de Política y Regulación Monetaria, Resolución N.º JPRM-2023-014-M, 7 de agosto de 2023, clasifica los medios de pago en físicos, electrónicos y billeteras electrónicas, y enumera taxativamente los medios de pago electrónicos autorizados en territorio nacional.

GAFI (Grupo de Acción Financiera Internacional), Orientaciones sobre el enfoque basado en el riesgo para activos virtuales y proveedores de servicios de activos virtuales, París: GAFI, 2021.

GAFILAT (Grupo de Acción Financiera de Latinoamérica), Documentos sobre intercambio de información financiera y cooperación regional, https://www.gafilat.org, consultado el 29/04/26.

INTERPOL, Informe sobre delitos financieros con criptoactivos, Lyon: INTERPOL, 2022.

4. Doctrina

ALAGNA, Flavia; TRUCCO, Luca, "Cryptocurrency Fraud and Criminal Liability: A Comparative Analysis", en *Computer Law & Security Review*, vol. 47, 2022, Elsevier, DOI: 10.1016/j.clsr.2022.105743.

ARTEAGA, Pablo, "Criptomonedas en Ecuador: ¿Realmente el BCE puede prohibir o criminalizar su uso?", en *Lexis.ec*, 22 de agosto de 2024, disponible en www.lexis.com.ec, consultado el 29/04/26.

BACIGALUPO, Enrique, *Derecho Penal. Parte General*, Buenos Aires: Hammurabi, 1999.

BAJO FERNÁNDEZ, Miguel; BACIGALUPO SAGGESE, Silvina, *Derecho Penal Económico*, 2.ª ed., Madrid: Centro de Estudios Ramón Areces, 2010.

CANO MARTÍNEZ, Jeimy José, *Computación forense. Descubriendo los rastros informáticos*, 2.ª ed., Bogotá: Alfaomega, 2015.

CHOCLÁN MONTALVO, José Antonio, *El delito de estafa*, 2.ª ed., Barcelona: Bosch, 2009.

FERRAJOLI, Luigi, *Derecho y razón. Teoría del garantismo penal*, Madrid: Trotta, 1995.

GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos. Análisis del art. 248.2 CP*, Valencia: Tirant lo Blanch, 2005.

HERNÁNDEZ BASUALDO, Héctor, "Problemas de política criminal y dogmática penal frente al delito informático", en *Revista de Derecho (Valdivia)*, vol. XIV, 2003, pp. 77-101, Universidad Austral de Chile.

JAKOBS, Günther, *Derecho Penal. Parte General. Fundamentos y teoría de la imputación*, Madrid: Marcial Pons, 1997.

MATA Y MARTÍN, Ricardo M., "Estafa convencional, estafa informática y robo en el ámbito de internet", en *Revista Penal*, n.º 6, 2000, pp. 51-63, La Ley.

MAYER LUX, Laura, "El uso de criptomonedas en el lavado de activos: desafíos regulatorios y penales", en *Revista de Derecho Penal y Criminología*, n.º 25, 2021, pp. 45-78, UNED Ediciones.

MIRÓ LLINARES, Fernando, "La oportunidad criminal en el ciberespacio. Aplicación de la Teoría de las Actividades Cotidianas para la prevención del cibercrimen", en *Revista Electrónica de Ciencia Penal y Criminología (RECPC)*, n.º 13-07, 2011, ISSN 1695-0194, disponible en http://criminet.ugr.es/recpc/13/recpc13-07.pdf, consultado el 29/04/26.

MIR PUIG, Santiago, *Derecho Penal. Parte General*, 10.ª ed., Barcelona: Reppertor, 2016.

MOISEIENKO, Anton, "Money Laundering through Cryptocurrencies: Risks and Regulatory Responses", en *Journal of Money Laundering Control*, vol. 24, n.º 2, 2021, pp. 387-397, Emerald, DOI: 10.1108/JMLC-08-2020-0090.

MUÑOZ CONDE, Francisco; GARCÍA ARÁN, Mercedes, *Derecho Penal. Parte General*, 10.ª ed., Valencia: Tirant lo Blanch, 2019.

PASTOR MUÑOZ, Nuria, *La determinación del engaño típico en el delito de estafa*, Madrid: Marcial Pons, 2004.

PÉREZ MANZANO, Mercedes, "El tipo objetivo de la estafa: reflexiones sobre la teoría de la imputación objetiva", en *Anuario de Derecho Penal y Ciencias Penales*, vol. XLVI, fasc. III, 1993, pp. 1023-1063, Madrid: BOE-CGPJ.

QUINTERO OLIVARES, Gonzalo, *Parte General del Derecho Penal*, 4.ª ed., Navarra: Aranzadi, 2010.

RIQUERT, Marcelo Alfredo, *Ciberdelitos. Régimen penal de las nuevas tecnologías*, Buenos Aires: Hammurabi, 2019.

ROMEO CASABONA, Carlos María, "Los delitos de daños en el ámbito informático", en ROMEO CASABONA, C. M. (dir.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada: Comares, 2006, pp. 235-289.

ROXIN, Claus, *Derecho Penal. Parte General*, t. I, Madrid: Civitas, 1997.

SILVA SÁNCHEZ, Jesús María, *La expansión del derecho penal. Aspectos de la política criminal en las sociedades postindustriales*, 3.ª ed., Madrid: Edisofer, 2011.

WERBACH, Kevin; CORNELL, Nicolas, "Contracts Ex Machina", en *Duke Law Journal*, vol. 67, n.º 2, 2017, pp. 313-382.

ZAFFARONI, Eugenio Raúl; ALAGIA, Alejandro; SLOKAR, Alejandro, *Derecho Penal. Parte General*, 2.ª ed., Buenos Aires: Ediar, 2002.