Polo del Conocimiento

Pol. Con. (Edición núm. 107) Vol. 10, No 6
Junio 2025, pp. 2342-2350
ISSN: 2550 - 682X
DOI: https://doi.org/10.23857/pc.v10i6.9817

Criminalidad en el ciberespacio: tipificación de delitos informáticos y desafíos probatorios en Ecuador

Cybercrime: Classification of computer crimes and evidentiary challenges in Ecuador

Cibercrime: Classificação de crimes informáticos e desafios probatórios no Equador

Elvis Guillermo Fuentes-Tenorio [I]
elvis.fuentest@ug.edu.ec
https://orcid.org/0009-0009-4536-4928

Correspondencia: elvis.fuentest@ug.edu.ec

Ciencias Sociales y Políticas
Artículo de Investigación

*** Recibido:** 05 de abril de 2025 ***Aceptado:** 11 de mayo de 2025 *** Publicado:** 27 de junio de 2025

I. Abogado, Magister, Docente de la Universidad de Guayaquil UG, Ecuador.

Resumen

La criminalidad en el ciberespacio se ha convertido en una de las amenazas más complejas del siglo XXI, especialmente en países en desarrollo como Ecuador, donde el marco normativo se encuentra en constante evolución. Este artículo analiza la tipificación de los delitos informáticos dentro del Código Orgánico Integral Penal (COIP) ecuatoriano, explorando los desafíos probatorios que enfrentan fiscales y jueces al momento de sustentar casos con evidencia digital. A partir de un enfoque doctrinario y jurisprudencial, se examinan experiencias internacionales en la persecución penal de ciberdelitos y se contrasta con la práctica ecuatoriana, identificando vacíos legales y dificultades operativas. El trabajo incluye análisis de casos relevantes y propone mejoras normativas y técnicas para garantizar una respuesta eficaz del sistema judicial. Se concluye que la capacitación especializada, la cooperación internacional y la adecuación legal son fundamentales para enfrentar los retos que plantea la criminalidad digital.

Palabras clave: ciberdelito; evidencia digital; COIP; tipificación penal; tecnología; delitos informáticos; justicia digital.

Abstract

Cybercrime has become one of the most complex threats of the 21st century, especially in developing countries like Ecuador, where the regulatory framework is constantly evolving. This article analyzes the classification of cybercrimes within the Ecuadorian Comprehensive Organic Criminal Code (COIP), exploring the evidentiary challenges faced by prosecutors and judges when supporting cases with digital evidence. Using a doctrinal and jurisprudential approach, it examines international experiences in the criminal prosecution of cybercrimes and compares them with Ecuadorian practice, identifying legal gaps and operational difficulties. The article includes analyses of relevant cases and proposes regulatory and technical improvements to ensure an effective response from the judicial system. It concludes that specialized training, international cooperation, and legal adaptation are essential to address the challenges posed by digital crime.

Keywords: cybercrime; digital evidence; COIP; criminal classification; technology; cybercrime; digital justice.

Resumo

O crime cibernético tornou-se uma das ameaças mais complexas do século XXI, especialmente em países em desenvolvimento como o Equador, onde o arcabouço regulatório está em constante evolução. Este artigo analisa a classificação dos crimes cibernéticos no Código Penal Orgânico Integral (COIP) equatoriano, explorando os desafios probatórios enfrentados por promotores e juízes ao fundamentar casos com provas digitais. Utilizando uma abordagem doutrinária e jurisprudencial, examina experiências internacionais na persecução penal de crimes cibernéticos e as compara com a prática equatoriana, identificando lacunas legais e dificuldades operacionais. O artigo inclui análises de casos relevantes e propõe melhorias regulatórias e técnicas para garantir uma resposta eficaz do sistema judicial. Conclui que treinamento especializado, cooperação internacional e adaptação jurídica são essenciais para enfrentar os desafios impostos pelo crime digital.

Palavras-chave: crime cibernético; provas digitais; COIP; classificação criminal; tecnologia; crime cibernético; justiça digital.

Introducción

En las últimas décadas, el avance tecnológico ha transformado radicalmente la forma en que las personas se comunican, realizan transacciones y almacenan información. Esta evolución, sin embargo, también ha dado lugar a un nuevo escenario para la comisión de delitos: el ciberespacio. Las actividades delictivas han migrado a plataformas digitales, generando un desafío inédito para los sistemas jurídicos tradicionales (González, 2021, p. 44).

La criminalidad informática, también denominada ciberdelincuencia, engloba conductas ilícitas que afectan bienes jurídicos protegidos a través del uso de tecnologías de la información. Entre los delitos más comunes se encuentran el acceso no autorizado a sistemas, la interceptación de datos, el fraude informático, la suplantación de identidad y la distribución de malware (Vásquez & Herrera, 2022, p. 61).

En Ecuador, la necesidad de adaptar la legislación penal a estos nuevos delitos se evidenció en la inclusión de un capítulo específico sobre delitos informáticos dentro del Código Orgánico Integral Penal (COIP), promulgado en 2014. No obstante, la práctica judicial aún enfrenta dificultades

significativas en materia de recolección, preservación y valoración de evidencia digital (López, 2023, p. 89).

Uno de los principales retos radica en el carácter volátil y replicable de la información digital. La evidencia electrónica, como correos, metadatos, registros de navegación o archivos comprimidos, puede ser fácilmente manipulada o eliminada si no se manejan protocolos adecuados (Valverde, 2021, p. 34).

Asimismo, el principio de territorialidad del derecho penal entra en tensión cuando los delitos informáticos se cometen desde otros países. Esta extraterritorialidad de la conducta delictiva requiere la cooperación jurídica internacional, algo que aún es incipiente en la región andina (Morales, 2020, p. 112).

La debilidad institucional y la limitada formación técnica de muchos operadores de justicia dificultan aún más el procesamiento adecuado de los ciberdelitos. Las fiscalías, por ejemplo, suelen carecer de peritos especializados en informática forense, lo que afecta la cadena de custodia y la validez probatoria (Rivadeneira, 2023, p. 52).

Por otra parte, el marco legal ecuatoriano aún presenta vacíos en cuanto a la regulación de delitos emergentes, como el ransomware, la minería no autorizada de criptomonedas, o la explotación sexual en línea, los cuales requieren respuestas penales más actualizadas (Romero & Paredes, 2022, p. 76).

La jurisprudencia nacional en esta materia es aún limitada. Pocas sentencias abordan con profundidad los aspectos técnicos del delito informático, y la mayoría se resuelven por faltas de pruebas suficientes o errores en la calificación jurídica (Corte Nacional de Justicia, 2022, p. 5).

Desde un enfoque de política criminal, resulta fundamental comprender que la lucha contra la criminalidad digital no puede sustentarse exclusivamente en la represión. Es necesario un enfoque preventivo que integre educación digital, seguridad informática y marcos legales eficaces (Delgado, 2021, p. 99).

Además, el tratamiento de la evidencia digital exige el respeto de las garantías procesales y derechos fundamentales, como el debido proceso, la cadena de custodia y la presunción de inocencia. De lo contrario, se corre el riesgo de obtener condenas basadas en pruebas vulnerables o ilícitas (Pazmiño, 2023, p. 40).

En este contexto, el presente artículo tiene como objetivo analizar la tipificación de los delitos informáticos en el Ecuador, los principales desafíos probatorios para su sanción judicial y la necesidad de fortalecer el marco institucional y legal frente a la criminalidad digital.

El estudio se desarrolla mediante un enfoque doctrinario, comparado y jurisprudencial, abarcando no solo la legislación ecuatoriana, sino también experiencias internacionales relevantes que puedan aportar buenas prácticas a la realidad nacional.

Estado del arte

Diversas investigaciones han abordado el fenómeno delictivo en el ciberespacio desde perspectivas jurídicas, técnicas y sociales. La obra de Clough (2015, p. 102) resalta la necesidad de una comprensión multidisciplinaria de los delitos informáticos, advirtiendo que la tecnología evoluciona con mayor rapidez que la legislación. En el contexto latinoamericano, autores como Rodríguez (2019, p. 78) destacan el rezago normativo frente al dinamismo de los ciberataques y la falta de cooperación entre Estados.

En Ecuador, estudios recientes han analizado las limitaciones de la legislación penal frente a delitos como el hacking, el phishing y la pornografía infantil digital. Cevallos (2021, p. 33) sostiene que, aunque el COIP tipifica varias conductas, persisten lagunas jurídicas sobre ciberdelitos transnacionales o sobre la responsabilidad penal de las personas jurídicas. De igual manera, Villamarín (2020, p. 85) plantea que las instituciones judiciales carecen de herramientas técnicas adecuadas para procesar evidencia digital.

A nivel internacional, se ha promovido la Convención de Budapest sobre Ciberdelincuencia como un estándar legal, aunque Ecuador no la ha ratificado. Según Jiménez (2022, p. 59), esta omisión limita la cooperación penal internacional. Mientras tanto, la Unión Europea ha avanzado en directivas para armonizar legislaciones nacionales y capacitar a los operadores de justicia.

Marco teórico

El ciberespacio constituye un nuevo ámbito de interacción social, económica y política que exige ser conceptualizado jurídicamente. Castells (2001, p. 151) lo define como una estructura social construida mediante redes digitales, donde emergen nuevos fenómenos de poder y control. En este

contexto, los delitos informáticos se entienden como aquellas conductas antijurídicas que se valen de tecnologías para afectar bienes jurídicos protegidos (Solís, 2021, p. 93).

Desde la dogmática penal, se discute si estas conductas deben clasificarse como delitos comunes cometidos mediante medios digitales, o si constituyen figuras autónomas. Silva (2020, p. 107) defiende una tipificación autónoma, dado que los elementos técnicos alteran el bien jurídico protegido y la estructura típica de la conducta. Además, la teoría del delito exige nuevos enfoques para abordar aspectos como el dolo digital o la culpabilidad algorítmica.

Por otro lado, el tratamiento procesal de la evidencia digital plantea desafíos a los principios del debido proceso. Conforme a López y Méndez (2023, p. 144), la evidencia digital debe ser obtenida con cadena de custodia técnica, mediante herramientas forenses que aseguren su integridad y autenticidad. La prueba informática demanda, por tanto, una interacción entre el derecho penal, el derecho procesal penal y la informática forense.

Estudios de caso y experiencias internacionales

Uno de los casos paradigmáticos en América Latina es el del "Banco de Brasil" (2018), donde un grupo de hackers transfirió millones de dólares mediante suplantación de identidad digital. La justicia brasileña logró sentencias firmes gracias a la recolección forense de metadatos, demostrando la eficacia de una normativa especializada y cuerpos técnicos capacitados.

En contraste, en Ecuador, el caso de la filtración de datos personales de más de 20 millones de registros en 2019, conocido como el "caso Novaestrat", evidenció la débil estructura de ciberseguridad y la inoperancia en el procesamiento de evidencia digital. El proceso penal avanzó lentamente y la responsabilidad penal no fue claramente determinada (Paredes, 2021, p. 68).

En Estonia, país pionero en gobernanza digital, se han desarrollado protocolos de ciberdefensa y legislación moderna que permite la sanción rápida de ciberdelitos. En ese país, la evidencia digital se presenta mediante firmas electrónicas y registros con trazabilidad en blockchain, lo que garantiza confiabilidad y eficacia judicial (Kaska, 2020, p. 21).

Normativa ecuatoriana sobre delitos informáticos

El Código Orgánico Integral Penal (COIP) ecuatoriano, en su Título IV, Capítulo II, tipifica los delitos contra los sistemas informáticos. Entre estos se encuentran: acceso no consentido a sistemas informáticos (art. 232), interceptación de datos (art. 233), ataque a la integridad de sistemas (art. 234), sabotaje informático (art. 235), fraude informático (art. 236) y otros.

Sin embargo, dicha normativa no contempla nuevas formas de ciberdelito, como la sextorsión, el acoso virtual ni el uso de deepfakes con fines delictivos. Además, el COIP carece de disposiciones específicas sobre obtención de evidencia digital, lo que afecta la legalidad y validez procesal de las pruebas obtenidas (CNJ, 2022, p. 4).

Metodología

Este trabajo aplica un enfoque cualitativo-descriptivo con base en tres métodos:

Método Descriptivo: Permite caracterizar las normas jurídicas ecuatorianas sobre delitos informáticos y los mecanismos procesales aplicables a la evidencia digital.

Método Bibliográfico: Se utiliza para analizar doctrina, artículos académicos, normativa nacional e internacional y jurisprudencia relevante sobre ciberdelitos.

Método Fenomenológico Jurídico: Se centra en la experiencia de operadores de justicia en casos reales, considerando su interpretación subjetiva sobre los vacíos legales y dificultades probatorias en la práctica judicial ecuatoriana.

Discusión y resultados

Definición: Los delitos informáticos son conductas típicas, antijurídicas y culpables cometidas mediante el uso de tecnologías digitales para vulnerar bienes jurídicos como la intimidad, el patrimonio o la seguridad informática (Solís, 2021, p. 95).

Ejemplos de Implementación y Resultados: En Ecuador, el procesamiento exitoso de delitos informáticos ha sido escaso. Los casos juzgados tienden a archivarse por falta de pruebas, como ocurrió en la causa No. 17282-2021-00121 por fraude informático, donde la pericia digital fue desestimada por no respetar la cadena de custodia (CNJ, 2022, p. 3).

Cuestiones Éticas: El uso de inteligencia artificial para detectar delitos en redes plantea interrogantes sobre vigilancia estatal y protección de derechos fundamentales, como la privacidad y libertad de expresión (González, 2022, p. 117).

Conclusiones

Los delitos informáticos constituyen un fenómeno criminal creciente que desafía la capacidad de respuesta del sistema penal ecuatoriano. Pese a avances normativos, la legislación vigente presenta

limitaciones en la tipificación de conductas nuevas, la regulación de la evidencia digital y la cooperación internacional. La carencia de herramientas tecnológicas, personal capacitado y protocolos forenses impacta negativamente en la eficacia procesal y vulnera el principio de tutela judicial efectiva.

Frente a esta realidad, se impone la necesidad de adoptar una política criminal integral que contemple reformas legislativas, inversión en capacidades técnicas y promoción de buenas prácticas en la recolección de evidencia digital. Asimismo, la ratificación de tratados internacionales sobre ciberdelincuencia fortalecería la respuesta estatal ante fenómenos transfronterizos.

Recomendaciones

1. Reformar el COIP para incluir nuevas formas de ciberdelito y procedimientos especiales para la prueba digital.
2. Crear unidades especializadas en ciberdelincuencia dentro de la Fiscalía y Policía Nacional.
3. Capacitar a jueces y fiscales en informática forense y evidencia digital.
4. Establecer protocolos técnicos para la obtención, conservación y presentación de evidencia informática.
5. Promover la adhesión de Ecuador a la Convención de Budapest para fortalecer la cooperación internacional.

Referencias

1. Castells, M. (2001). La era de la información: economía, sociedad y cultura. Siglo XXI Editores.
2. Cevallos, M. (2021). Análisis de la legislación ecuatoriana sobre delitos informáticos. Revista Derecho y Sociedad, 34(2), 30–38.
3. Clough, J. (2015). Principles of Cybercrime. Cambridge University Press.
4. Corte Nacional de Justicia. (2022). Boletín jurídico sobre ciberdelincuencia. https://www.cortejusticia.gob.ec/ciberdelitos2022
5. Delgado, S. (2021). Política criminal y sociedad digital. Estudios Jurídicos, 19(1), 97–105.

6. González, P. (2021). Criminalidad digital en América Latina. Revista Iberoamericana de Derecho Penal, 15(3), 40–50.
7. Jiménez, F. (2022). Cibercriminalidad y cooperación penal internacional. Revista Latinoamericana de Derecho Penal, 20(1), 55–63.
8. Kaska, K. (2020). Estonia's Cyber Defense Strategy. Journal of Cybersecurity Studies, 4(2), 15–24.
9. López, C., & Méndez, T. (2023). Prueba digital y proceso penal. Cuadernos de Derecho Penal, 11(2), 140–150.
10. Morales, H. (2020). Derecho penal global y delitos informáticos. Estudios Jurídicos Comparados, 12(1), 110–122.
11. Paredes, A. (2021). El caso Novaestrat: vulnerabilidad digital en Ecuador. Revista Seguridad y Sociedad, 9(2), 65–71.
12. Pazmiño, R. (2023). Derechos fundamentales y prueba digital. Revista Constitucional Andina, 8(1), 38–45.
13. Rodríguez, L. (2019). Ciberdelincuencia y legislación penal. Derecho Penal y Tecnología, 6(1), 75–83.
14. Romero, J., & Paredes, M. (2022). Nuevos delitos digitales: un análisis crítico del COIP. Revista Jurídica del Ecuador, 10(1), 70–78.
15. Rivadeneira, V. (2023). Obstáculos judiciales en la persecución penal de delitos informáticos. Justicia y Proceso, 4(1), 50–56.
16. Silva, B. (2020). Ciberdelitos y estructura típica. Teoría del Delito Contemporáneo, 17(2), 105–115.
17. Solís, A. (2021). Delitos informáticos: teoría y práctica. Ediciones Jurídicas.
18. Valverde, J. (2021). Evidencia digital: un nuevo reto para el proceso penal. Revista Derecho Procesal, 7(3), 30–36.
19. Villamarín, E. (2020). Vulnerabilidades del sistema penal ecuatoriano frente a la ciberdelincuencia. Estudios Jurídicos Ecuatorianos, 5(2), 80–88.