Verdad y Derecho
Revista Arbitrada de Ciencias Jurídicas y Sociales
Vol. 5(especial7), 1-11, 2026
https://doi.org/10.62574/6c6ns745

Sustento jurídico de los ciberdelitos en el derecho penal ecuatoriano

Legal basis of cybercrimes in Ecuadorian criminal law

Holguer Fabricio Niauñay-Llanga
holguernl19@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Riobamba, Ecuador
https://orcid.org/0009-0006-4175-9015

Mauro Leodan Padilla-Rodríguez
mauropr52@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Riobamba, Ecuador
https://orcid.org/0009-0008-5958-8503

Julio Juvenal Aldana-Zavala
ur.julioaz41@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Riobamba, Ecuador
https://orcid.org/0000-0002-7934-9103

RESUMEN

La expansión de las tecnologías digitales ha dado lugar a nuevas formas delictivas que desafían las categorías tradicionales del derecho penal y exigen respuestas normativas actualizadas. Es así que el estudio se planteó como objetivo central analizar el sustento jurídico de los ciberdelitos en el derecho penal ecuatoriano. En este sentido se empleó un enfoque cualitativo, de tipo jurídico-documental, con análisis de contenido de 11 obras y artículos académicos y cuatro instrumentos normativos nacionales e internacionales. Entre los resultados se obtuvo que el Código Orgánico Integral Penal tipifica conductas como el acceso no consentido a sistemas, la interceptación ilegal de datos y la apropiación fraudulenta por medios electrónicos, aunque presenta vacíos frente a modalidades como el phishing, la sextorsión y el ciberacoso, y limitaciones en la cooperación internacional y la prueba digital. Entre las conclusiones se estableció que su fortalecimiento exige actualización normativa y capacidades técnicas de investigación.

Descriptores: delito informático; derecho penal; seguridad informática; cooperación internacional; tecnología de la información. (Fuente: Tesauro UNESCO).

ABSTRACT

The expansion of digital technologies has given rise to new forms of crime that challenge the traditional categories of criminal law and require updated normative responses. The study set out to analyse the legal basis of cybercrimes in Ecuadorian criminal law. A qualitative, legal-documentary approach was used, with content analysis of 11 academic works and articles and four national and international legal instruments. The results show that the Comprehensive Organic Criminal Code criminalises conduct such as unauthorised access to systems, illegal interception of data and fraudulent appropriation by electronic means, although it has gaps regarding modalities such as phishing, sextortion and cyberbullying, and limitations in international cooperation and digital evidence. It is concluded that strengthening it requires legislative updating and technical investigative capacities.

Descriptors: computer crime; criminal law; computer security; international cooperation; information technology. (Source: UNESCO Thesaurus).

Recibido: 02/09/2026. Revisado: 23/09/2026. Aprobado: 14/10/2026. Publicado: 28/10/2026.

Sección artículos de investigación

INTRODUCCIÓN

El impacto de la tecnología digital en la sociedad contemporánea ha sido profundo, por cuanto las interacciones económicas, sociales y personales se desarrollan cada vez más en entornos virtuales donde circulan datos, dinero e información sensible. Este desplazamiento ha generado nuevas oportunidades para la comisión de delitos, de allí que conductas como el acceso no autorizado a sistemas, el fraude electrónico, la suplantación de identidad o la difusión no consentida de contenido íntimo se hayan convertido en preocupaciones centrales de la política criminal.

Partiendo de lo expuesto, el Ecuador incorporó en el Código Orgánico Integral Penal un conjunto de tipos penales vinculados con las tecnologías de la información, entre ellos la apropiación fraudulenta por medios electrónicos, el acceso no consentido a un sistema informático, la interceptación ilegal de datos y la revelación ilegal de bases de datos (Asamblea Nacional, 2014, arts. 190 y 229 a 234). Lo anterior supone un avance respecto de la legislación anterior, en la que estas conductas se encontraban dispersas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Congreso Nacional, 2002).

Por consiguiente, la relevancia del tema radica en que la evolución tecnológica avanza con mayor rapidez que la legislación, habida cuenta de que Gamón (2017) describió internet como una nueva era del delito, con fenómenos como el ciberterrorismo y la delincuencia organizada en red, y Mayer Lux (2018) advierte que la comprensión criminológica de estos delitos es necesaria para su adecuado tratamiento penal. De ello se sigue la necesidad de evaluar la suficiencia del sustento jurídico de los ciberdelitos en el Ecuador.

Pero, ¿cuál es el sustento jurídico de los ciberdelitos en el derecho penal ecuatoriano y qué vacíos presenta? A partir de lo planteado, la investigación tiene por objetivo central analizar el sustento jurídico de los ciberdelitos en el derecho penal ecuatoriano, con la finalidad de identificar sus fortalezas, sus vacíos y criterios para su actualización.

Referencial teórico

En cuanto al concepto, Wall (2007) caracterizó el cibercrimen como una transformación del delito propia de la sociedad de la información, distinguiendo entre los delitos contra la integridad de los sistemas, los delitos asistidos por computadora y los delitos de contenido. En consonancia con ello, Miró Llinares (2012) analizó la fenomenología y la criminología de la delincuencia en el ciberespacio, destacando que este espacio modifica las variables de oportunidad, distancia y anonimato. Esto implica que el ciberdelito constituye un fenómeno con características propias, que excede al delito tradicional cometido con nuevos medios.

Desde la dogmática penal, Mayer Lux (2017) examinó el bien jurídico protegido en los delitos informáticos, proponiendo distinguir entre la funcionalidad de los sistemas informáticos y los bienes jurídicos tradicionales afectados por medios informáticos, y Romeo Casabona (2006) reunió los principales retos jurídico-penales y político-criminales que plantea el cibercrimen. Al hilo de ello, la tipificación debe definir con precisión las conductas para respetar el principio de legalidad sin quedar desactualizada por la evolución tecnológica. De allí se desprende la tensión entre taxatividad y flexibilidad que caracteriza a esta materia.

En función de lo planteado, el Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como Convenio de Budapest, constituye el principal instrumento internacional en la materia, toda vez que armoniza las

definiciones de los delitos, establece facultades procesales para la obtención de pruebas electrónicas y regula la cooperación internacional (Consejo de Europa, 2001). Tal instrumento revela que la eficacia de la persecución depende de la coordinación entre Estados, por cuanto los ciberdelitos suelen tener carácter transnacional.

Con base en lo expuesto, la investigación de estos delitos plantea tensiones con los derechos fundamentales, ya que Sarmiento Vallejo (2022) y Alfonso Rodríguez (2024) analizan las garantías que deben acompañar la interceptación de comunicaciones, y Álvarez Robles (2022) examina la protección de los derechos en y desde la red. Por añadidura, la Ley Orgánica de Protección de Datos Personales establece un régimen que interactúa con la tutela penal de la información (Asamblea Nacional, 2021).

Desde el estudio del fenómeno, Holt y Bossler (2014) evaluaron el estado de la investigación sobre cibercrimen y advirtieron la escasez de datos confiables sobre su prevalencia, mientras que Punín et al. (2024) documentan la percepción de periodistas ecuatorianas sobre ciberseguridad y violencia digital. Semejante evidencia supone que los ciberdelitos afectan de manera diferenciada a ciertos grupos, como las mujeres que ejercen una actividad pública.

MÉTODO

La investigación se desarrolló con enfoque cualitativo, de tipo jurídico-documental, orientada a examinar los tipos penales vinculados con las tecnologías de la información en el ordenamiento ecuatoriano y su correspondencia con los estándares doctrinarios e internacionales.

En cuanto al corpus, se seleccionaron intencionalmente 11 obras y artículos académicos publicados entre 2006 y 2024 y cuatro instrumentos

normativos, esto es, el Código Orgánico Integral Penal, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la Ley Orgánica de Protección de Datos Personales y el Convenio de Budapest. Se excluyeron tesis, revistas incluidas en listados de calidad dudosa y documentos de procedencia no verificable, esto con la finalidad de sostener el análisis en fuentes confiables.

En este sentido se empleó el análisis de contenido por dimensiones, esto es, tipificación, bien jurídico, prueba digital y cooperación internacional, construyéndose categorías emergentes por inducción. Como limitación, el estudio no analiza estadísticas de denuncias ni sentencias por ciberdelitos, por lo que sus conclusiones se apoyan en la literatura y en el marco normativo revisado.

RESULTADOS

El análisis permitió identificar los tipos penales del Código Orgánico Integral Penal vinculados con las tecnologías de la información y las modalidades que la literatura señala como no cubiertas de manera específica, tal como se presenta en la tabla 1.

Tabla 1. *Ciberdelitos en el Código Orgánico Integral Penal y modalidades emergentes.*

Tipo o modalidad	Regulación	Observación
Apropiación fraudulenta por medios electrónicos	COIP, art. 190	Cubre transferencias no consentidas mediante manipulación de sistemas.
Acceso no consentido a un sistema informático	COIP, art. 234	Protege la integridad y confidencialidad de los sistemas.
Interceptación ilegal de datos	COIP, art. 230	Exige delimitar su relación con la interceptación judicial autorizada.
Ataque a la integridad de sistemas	COIP, art. 232	Sanciona la destrucción o alteración de datos y programas.
Phishing y suplantación de identidad	Sin tipo específico	Se reconduce a estafa o apropiación, con dificultades probatorias (Mayer Lux, 2018).
Sextorsión y difusión no consentida de contenido íntimo	Tipificación parcial	Respuesta fragmentada frente a la violencia digital (Punín et al., 2024).

Nota. Elaboración propia (2026) a partir del Código Orgánico Integral Penal (Asamblea Nacional, 2014) y del corpus analizado.

De la tabla 1 se desprende que el Código Orgánico Integral Penal ofrece un sustento jurídico para los ciberdelitos que afectan la integridad de los sistemas y el patrimonio, empero presenta vacíos frente a modalidades que combinan el engaño, la manipulación psicológica y la violencia digital, por cuanto estas conductas deben reconducirse a tipos tradicionales que no capturan su especificidad. Esto indica que la legislación responde mejor a los ataques técnicos que a los delitos de contenido y de ingeniería social.

En función de lo anterior, los hallazgos se agruparon en categorías emergentes sobre el sustento jurídico de los ciberdelitos, tal como se observa en la tabla 2.

Tabla 2. *Categorías emergentes sobre el sustento jurídico de los ciberdelitos.*

Categoría	Definición	Fuentes
Tensión entre taxatividad y evolución tecnológica	Riesgo de obsolescencia de los tipos penales.	Mayer Lux (2017); Romeo Casabona (2006)
Especificidad criminológica	Características propias del delito en el ciberespacio.	Wall (2007); Miró Llinares (2012)
Déficit de cooperación internacional	Limitaciones para obtener prueba transfronteriza.	Consejo de Europa (2001); Gamón (2017)
Garantías en la investigación digital	Equilibrio entre persecución y privacidad.	Sarmiento Vallejo (2022); Alfonso Rodríguez (2024)

Nota. Elaboración propia (2026).

En cuanto a la tensión entre taxatividad y evolución tecnológica, los estudios coinciden en que la redacción de los tipos penales debe ser lo bastante precisa para respetar el principio de legalidad y lo bastante amplia para abarcar nuevas técnicas, de allí que Mayer Lux (2017) proponga definir los delitos a partir del bien jurídico afectado y no de la herramienta utilizada.

Por su parte, el déficit de cooperación internacional aparece como el principal obstáculo para la persecución, ya que los autores, los servidores y las víctimas suelen encontrarse en distintos países, y el Ecuador no ha completado su incorporación al marco del Convenio de Budapest (Consejo de Europa, 2001). Semejante hallazgo supone que la eficacia de la ley penal nacional se ve limitada sin mecanismos ágiles de obtención de prueba electrónica en el extranjero.

En lo que respecta a las garantías en la investigación, los resultados indican que la obtención de prueba digital exige autorizaciones judiciales y protocolos de cadena de custodia que protejan la privacidad de las personas investigadas, toda vez que Sarmiento Vallejo (2022) y Alfonso Rodríguez (2024) advierten sobre los riesgos de interceptaciones sin control suficiente. De ello se sigue que la persecución de los ciberdelitos no puede justificar la vulneración de la intimidad.

DISCUSIÓN

Los resultados confirman que el derecho penal ecuatoriano cuenta con un sustento jurídico básico para los ciberdelitos, en consonancia con la clasificación de Wall (2007) sobre delitos contra la integridad de los sistemas y delitos asistidos por computadora. Sin embargo, la literatura revisada permite advertir que la tipificación vigente no cubre de manera adecuada los delitos de contenido y las modalidades basadas en la ingeniería social, que hoy constituyen una parte relevante de la ciberdelincuencia.

En el plano dogmático, la propuesta de Mayer Lux (2017) de diferenciar el bien jurídico informático de los bienes tradicionales permite comprender por qué el phishing o la sextorsión no encajan plenamente en los tipos existentes, ya que combinan la afectación del patrimonio o de la intimidad con el uso abusivo de los sistemas. Esto invita a reflexionar sobre la conveniencia de reformas que tipifiquen estas conductas con precisión, en lugar de forzar su encuadramiento en figuras tradicionales.

Comoquiera que la persecución depende de la cooperación transfronteriza, la adhesión plena al Convenio de Budapest (Consejo de Europa, 2001) permitiría al Ecuador acceder a mecanismos de asistencia mutua y de conservación rápida de datos. Es ingenuo pensar que la reforma de los tipos penales, por sí sola, resolverá el problema de la impunidad; de ahí un reto intrínseco para la Fiscalía General del Estado, que consiste en desarrollar unidades especializadas con capacidad técnica de análisis forense digital.

Otro aspecto que debe ser revisado es la relación entre la tutela penal y la protección de datos, toda vez que la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional, 2021) establece obligaciones de seguridad para los responsables del tratamiento cuya inobservancia facilita la

comisión de ciberdelitos. A tenor de lo que plantea Miró Llinares (2012), la prevención situacional en el ciberespacio, mediante medidas técnicas y organizativas, resulta tan relevante como la sanción penal.

En virtud de lo abordado, el sustento jurídico de los ciberdelitos en el Ecuador puede comprenderse como un marco en construcción, adecuado para los ataques técnicos e insuficiente para las nuevas modalidades de engaño y violencia digital. Como limitación, el estudio no analiza sentencias por ciberdelitos, por lo que se recomienda que investigaciones futuras examinen la aplicación judicial de los artículos 190 y 229 a 234 del Código Orgánico Integral Penal.

CONCLUSIONES

El Código Orgánico Integral Penal ofrece un sustento jurídico para los ciberdelitos al tipificar la apropiación fraudulenta por medios electrónicos, el acceso no consentido a sistemas, la interceptación ilegal de datos, la revelación ilegal de bases de datos y los ataques a la integridad de los sistemas informáticos.

Este marco presenta vacíos frente a modalidades como el phishing, la suplantación de identidad, la sextorsión y otras formas de violencia digital, así como limitaciones derivadas de la falta de incorporación plena al Convenio de Budapest, de la escasa capacidad técnica de investigación y de la necesidad de equilibrar la obtención de prueba digital con la protección de la privacidad.

En consecuencia, el fortalecimiento del sustento jurídico de los ciberdelitos exige reformas que tipifiquen con precisión las nuevas modalidades, la adhesión al Convenio de Budapest, la creación de unidades fiscales

especializadas en análisis forense digital y la articulación de la tutela penal con el régimen de protección de datos personales.

FINANCIAMIENTO

No monetario.

CONFLICTO DE INTERÉS

No existe conflicto de interés con personas o instituciones ligadas a la investigación.

AGRADECIMIENTOS

A la Universidad Regional Autónoma de los Andes (UNIANDES), por el apoyo brindado al desarrollo de esta investigación.

REFERENCIAS

Alfonso Rodríguez, A. J. (2024). Interceptación de comunicaciones telefónicas, seguridad(es) y garantías procesales [Telephone interception, security and procedural guarantees]. *Ciencia Policial*, (182), 97–144. https://doi.org/10.14201/cp.31812

Álvarez Robles, T. (2022). Las garantías de los derechos fundamentales en y desde la red: El contexto español [Guarantees of fundamental rights on and from the internet: The Spanish context]. *Revista Chilena de Derecho y Tecnología*, *11*(1), 5–40. https://doi.org/10.5354/0719-2584.2022.60197

Asamblea Nacional. (2014). *Código Orgánico Integral Penal* [Comprehensive Organic Criminal Code]. Registro Oficial Suplemento 180, 10 de febrero de 2014.

Asamblea Nacional. (2021). *Ley Orgánica de Protección de Datos Personales* [Organic Law on Personal Data Protection]. Registro Oficial Quinto Suplemento 459, 26 de mayo de 2021.

Congreso Nacional. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos* [Law on Electronic Commerce, Electronic Signatures and Data Messages]. Registro Oficial Suplemento 557, 17 de abril de 2002.

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia* [Convention on Cybercrime] (Serie de Tratados Europeos n.º 185). Budapest, 23 de noviembre de 2001.

Gamón, V. P. (2017). Internet, la nueva era del delito: Ciberdelito, ciberterrorismo, legislación y ciberseguridad [Internet, the new era of crime: Cybercrime,

cyberterrorism, legislation and cybersecurity]. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, (20), 80–93. https://doi.org/10.17141/urvio.20.2017.2775

Holt, T. J., y Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos [The legal interest protected in computer crimes]. *Revista Chilena de Derecho*, *44*(1), 235–260. https://doi.org/10.4067/S0718-34372017000100011

Mayer Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos [Criminological elements for the criminal-law analysis of computer crimes]. *Ius et Praxis*, *24*(1), 159–206. https://doi.org/10.4067/S0718-00122018000100159

Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio* [Cybercrime: Phenomenology and criminology of crime in cyberspace]. Marcial Pons.

Punín, M. I., Ordóñez, K., Suing, A., Rivera Salas, P. E., Gonzálvez Vallés, J. E., y Mariscal Vega, S. (2024). Ciberseguridad y violencia digital, percepción de periodistas ecuatorianas [Cybersecurity and digital violence: Perceptions of Ecuadorian women journalists]. En *Perspectivas transversales: Cultura, educación y género* (pp. 317–328). Marcial Pons. https://doi.org/10.2307/jj.27976077.32

Romeo Casabona, C. M. (Coord.). (2006). *El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales* [Cybercrime: New criminal-law challenges, new criminal-policy responses]. Comares.

Sarmiento Vallejo, G. H. (2022). El derecho a la privacidad y a la intimidad en el contexto de la interceptación de las comunicaciones en el Ecuador [Privacy in the context of communications interception in Ecuador]. *Serie Científica de la Universidad de las Ciencias Informáticas*, *15*(7), 242–261.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Derechos de autor: 2026 Por los autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones de la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0)
https://creativecommons.org/licenses/by-nc-sa/4.0/