22

CIBERDELITOS

COMO TIPO PENAL DENTRO DEL ORDENAMIENTO JURÍDICO PENAL ECUATORIANO

ISSN: 2631-2662

CIBERDELITOS

COMO TIPO PENAL DENTRO DEL ORDENAMIENTO JURÍDICO PENAL ECUATORIANO

CYBERCRIMES AS A CRIMINAL OFFENSE WITHIN THE ECUADORIAN CRIMINAL LEGAL SYSTEM

Homero Abel Ramírez-Cabrera[1]
E-mail: hramirez@umet.edu.ec
ORCID: https://orcid.org/0009-0009-8847-4211
[1] Universidad Metropolitana. Ecuador.

Cita sugerida (APA, séptima edición)

Ramírez-Cabrera, H. A. (2026). Ciberdelitos como tipo penal dentro del ordenamiento jurídico penal ecuatoriano. *Revista Metropolitana de Ciencias Aplicadas*, 9(2), 203-211.

Fecha de presentación: 11/11/2025 **Fecha de aceptación:** 16/01/2026 **Fecha de publicación:** 01/03/26

RESUMEN

Mundialmente el ciberdelito se ha consolidado como una actividad común de rápido crecimiento, representando uno de los desafíos más difíciles para los países en vías de desarrollo. La proliferación de actividades cotidianas en línea, desde el entretenimiento hasta las finanzas, ha propiciado un terreno para que se expanda el ciberdelito, lo que exige atención y una respuesta legal eficaz. La tecnología avanza más rápido que la capacidad del legislador para regular amenazas cibernéticas de forma rápida. El Código Orgánico Integral Penal contiene tipos penales relacionados a los ciberdelitos, no obstante, a través del análisis se deduce que se necesita una actualización para cubrir de una forma más amplia el tema. El presente artículo científico tiene como objetivo proporcionar un estudio doctrinal y empírico exhaustivo sobre la evolución de los ciberdelitos en el Ecuador, mediante el enfoque cualitativo de carácter descriptivo y analítico, se examinan los vacíos normativos, las dificultades probatorias, entre otras cosas.

Palabras clave

Derecho penal, ciberdelitos, sistemas.

ABSTRACT

Cybercrime has established itself as a rapidly growing, common activity worldwide, representing one of the most difficult challenges for developing countries. The proliferation of everyday online activities, from entertainment to finance, has provided a breeding ground for cybercrime, demanding attention and an effective legal response. Technology advances faster than legislators' ability to quickly regulate cyber threats. The National Code of Criminal Procedure contains criminal offenses related to cybercrimes; however, analysis suggests that an update is needed to cover the topic more broadly. This scientific article aims to provide a comprehensive doctrinal and empirical study on the evolution of cybercrime in Ecuador. This article uses a descriptive and analytical qualitative approach, examining regulatory gaps and evidentiary difficulties, among other aspects.

Keywords

Criminal law, cybercrime, systems.

INTRODUCCIÓN

En la actualidad, la sociedad se encuentra inmersa en un proceso constante de transformación digital, caracterizado por el uso masivo de tecnologías de la información y la comunicación en los ámbitos personal, social, económico e institucional. Este contexto ha propiciado el surgimiento y la expansión de nuevas modalidades delictivas cometidas a través de sistemas electrónicos o informáticos, conocidas como ciberdelitos, las cuales representan una amenaza creciente para la seguridad jurídica, la intimidad, el patrimonio económico de los ciudadanos y el adecuado funcionamiento de las instituciones públicas y privadas del Estado ecuatoriano. Frente a esta realidad, el ordenamiento jurídico ha debido adaptarse progresivamente a las nuevas formas de criminalidad, incorporando figuras penales específicas dentro del Código Orgánico Integral Penal (COIP), como respuesta legislativa a los desafíos derivados del entorno digital.

Sin embargo, pese a estos avances normativos, persisten importantes limitaciones en el tratamiento jurídico de los delitos informáticos. Aún existen vacíos legales, escasa sistematización normativa y una insuficiente construcción jurisprudencial por parte de la Corte Constitucional y la Corte Nacional de Justicia. Esta situación genera dificultades técnicas al momento de adecuar los tipos penales a los hechos concretos, lo que plantea interrogantes sobre la verdadera eficacia del Código Orgánico Integral Penal frente a la ciberdelincuencia. En este contexto, el presente artículo desarrolla un estudio doctrinal y empírico sobre la evolución de los ciberdelitos en el Ecuador, analizando su incorporación en la legislación, las reformas implementadas y los principales desafíos que enfrenta su aplicación. Para ello, se parte de una revisión crítica de la normativa vigente, contrastada con datos estadísticos provenientes de investigaciones académicas, con el fin de evaluar la coherencia entre su regulación formal y su aplicación real en el sistema penal (Espinoza Carvajal & Paredes Fuentes, 2025).

El incremento sostenido de los delitos cometidos mediante tecnologías digitales ha puesto en evidencia los límites estructurales del sistema penal ecuatoriano. Si bien el Código Orgánico Integral Penal contempla diversos tipos penales relacionados con los ciberdelitos, la dispersión normativa, la ausencia de una categoría explícita que los agrupe, el limitado conocimiento especializado en la función judicial y las barreras técnicas para la obtención y valoración de pruebas digitales dificultan el acceso efectivo a la justicia (Ponce, 2024). Estas debilidades afectan directamente la capacidad del Estado para investigar, sancionar y prevenir este tipo de conductas. Desde esta perspectiva, surge la necesidad de examinar si el marco legal vigente responde adecuadamente a las exigencias actuales de la ciberdelincuencia, tanto en el plano doctrinal como en el normativo y práctico.

El objetivo general de la presente investigación es analizar, desde una perspectiva académica, doctrinal y normativa, los ciberdelitos en el Ecuador, su evolución histórica y los principales retos que presentan en su tratamiento jurídico. El estudio se desarrolló bajo un enfoque cualitativo, utilizando métodos analítico-descriptivo, sistemático y hermenéutico, sustentados en el análisis del Código Orgánico Integral Penal, así como en fuentes doctrinales y académicas especializadas.

En cuanto a las variables de investigación, se considera como variable independiente la tipificación normativa de los ciberdelitos, y como variable dependiente la efectividad jurídica real de dicha tipificación. La justificación del estudio radica en la necesidad de fortalecer y perfeccionar el marco normativo ecuatoriano frente a los delitos informáticos, dado que estos no solo comprometen la seguridad digital, sino también derechos fundamentales reconocidos en la Constitución, como la privacidad, la libertad de expresión y la protección de datos personales.

En este sentido, el presente artículo tiene como finalidad examinar la evolución de la normativa vigente en materia de ciberdelitos, centrándose en su tipificación en el Código Orgánico Integral Penal desde un enfoque doctrinal y empírico, y evaluando su aplicación en la práctica judicial. La investigación resulta pertinente debido a la urgencia de adaptar los tipos penales a los nuevos escenarios delictivos derivados del uso de tecnologías emergentes. El tratamiento normativo de los ciberdelitos no debe limitarse a aspectos técnicos, sino que debe articularse con los principios fundamentales del derecho penal, garantizando una protección efectiva de los derechos constitucionales y contribuyendo al orden público.

Finalmente, este estudio destaca la creciente importancia de los ciberdelitos en el contexto ecuatoriano y la complejidad que implica su abordaje desde el Código Orgánico Integral Penal. Si bien la tipificación de diversas conductas constituye un avance significativo, la doctrina y la evidencia empírica revelan la necesidad de futuras reformas. En esta línea, Espinoza & Paredes (2025) señalan que la falta de precisión en ciertos tipos penales y la ausencia de regulación de nuevas modalidades delictivas, como el phishing, generan dificultades en la correcta aplicación de la ley y en la sanción efectiva de los delincuentes informáticos.

METODOLOGÍA

El presente artículo cientifico adopta un enfoque cualitativo de carácter descriptivo y analítico que se sustenta en dos dimensiones el análisis doctrinal normativo y la revisión empírica de datos de estudios de pregrado relacionados a los ciberdelitos en Ecuador.

Diseño metodológico

Se emplea una metodología documental para examinar la evolución de la norma en el tratamiento de los ciberdelitos

en el ordenamiento jurídico ecuatoriano, se incluye una revisión sistemática del Código Orgánico Integral Penal, las reformas pertinentes, leyes conexas como la Ley de Protección de Datos Personales y diferentes documentos académicos. Paralelamente, se utilizó un enfoque empírico descriptivo a través de la recopilación de información estadística relacionadas con ciberdelitos. Para lograr aquello, se consultaron documentos oficiales de la Fiscalía General del Estado con la finalidad de identificar una tendencia y precedentes judiciales.

Técnicas de investigación

- **Análisis de contenido normativo del Código Orgánico Integral Penal:** Se estudió el articulado del Código Orgánico Integral Penal y su evolución en materia de ciberdelitos, con especial atención a la sección de Delitos contra la seguridad de los activos de los sistemas de información y comunicación.
- **Revisión doctrinal**: Se consultaron artículos científicos publicados en revistas e investigaciones de pregrado especializadas en derecho penal, tecnología y ciberseguridad.
- **Análisis estadístico básico**: Se sistematizaron datos proporcionados por la Fiscalía General del Estado y de otras investigaciones.

Adicionalmente, se aplicaron los siguientes métodos científicos:

- **Método hermenéutico:** Propio de las ciencias jurídicas, se estudió la comprensión e interpretación de las normas relativas a los ciberdelitos tipificados en el Código Orgánico Integral Penal.
- **Método analítico-sintético:** Se lo utilizó para descomponer el fenómeno delictivo digital en diferentes variables y luego integrarlos de forma generalizada como parte de un problema.
- **Método sistémico:** Permitió comprender al ciberdelito como parte de un sistema globalizado, que sucede a nivel mundial y que, además está interconectado con factores sociales, tecnológicos y legislativos.

Criterios de selección

Las fuentes normativas y doctrinales antes mencionadas y detalladas en el apartado de referencias bibliográficas se seleccionaron con base en su relevancia, actualidad y pertinencia académica. En cuanto a las fuentes empíricas, se priorizó el acceso a documentos oficiales y para garantizar validez y confiabilidad.

DESARROLLO

Los ciberdelitos o delitos informáticos son las conductas ilícitas que de cometen por medio del uso de las Tecnologías de la Información y Comunicación, más reconocidas como TICS o también son las que tienen como objetivo principal los sistemas, redes o datos informáticos (Pons Gamón, 2017). Desde el punto de vista de Brenner (2010), los ciberdelitos se podrían calificar en dos grupos: el primero tiene delitos en los que el sistema informático es su objetivo principal como el hacking y el segundo grupo son los delitos en los que el sistema es el medio para la comisión de otros delitos como la distribución de pornografía infantil. En esta misma línea, la Oficina de las Naciones Unidas contra la Droga y el Delito (2013), la principal dificultad para abordar los ciberdelitos es la constante evolución tecnológica que vivimos, la transnacionalidad de sus consecuencias y la dificultad para obtener pruebas digitales; lo que exige que se desarrolle un marco legal especializado.

Evolución normativa referente a los ciberdelitos en el Ecuador

Actualmente, el internet y los teléfonos móviles son el principal medio de comunicación entre la mayor parte de la población a nivel mundial, no solo entre personas sino también los usan las organizaciones en diversos ámbitos. Desde el punto de vista de Quezada et al. (2022), los llamados “nativos digitales” emplean herramientas tecnológicas tanto en el trabajo como en momentos de recreación. Bajo este ángulo, tenemos también a las redes sociales que permiten la interacción entre usuarios, es decir, nosotros, que tenemos acceso inmediato a todo tipo de información de otras personas. No obstante, conforme nos vamos desarrollando en el ciberespacio y las tecnologías emergentes, asimismo, va incrementando el cibercrimen, transformando las formas típicas en las que cometían los delitos.

En Ecuador los ciberdelitos se han ido incorporando de forma gradual a nuestra legislación penal. La Fiscalía General del Estado (2023) en su Revista Científica de Ciencias Jurídicas, Criminología y Seguridad nos manifiesta que, al finalizar los años 90 se debatió sobre el comercio electrónico, y en el año del 2002 se expidió la Ley de comercio electrónico, mensajes de datos y firmas electrónicas con Registro Oficial No. 557 del 17 abr. 2002, que introdujo los delitos informáticos en el Código Penal de esa época. Dicha normativa regulaba los mensajes de datos, firmas electrónicas y protección de usuarios, incorporando tipos penales como la interceptación de datos o alteración de sistemas. La aprobación del Código Orgánico Integral Penal (Ecuador. Asamblea Nacional, 2014) representó un avance cualitativo porque por primera vez se sistematizó en un solo cuerpo penal todas las conductas penales cibernéticas relevantes.

Actualmente, el Código Orgánico Integral Penal contiene tipos penales propios de los delitos informáticos, incorporándolos al procedimiento penal y a la política penitenciaria nacional. Años después, se desarrollaron actualizaciones relevantes como la Ley Orgánica de Protección de Datos Personales del año 2021, la cual estableció un marco para proteger la privacidad en el tratamiento de datos (Ordóñez, 2024). A su vez, con el paso del tiempo

el Ministerio de Telecomunicaciones y de la Sociedad de la Información (2022) desarrolló la Estrategia Nacional de Ciberseguridad, en donde se ideó un espacio cibernético, en el que los ciudadanos puedan acceder a servicios virtuales con mayor seguridad. Dicho esto, se puede decir que, el Ecuador ha ido evolucionando desde un vacío legal hasta la inclusión de los ciberdelitos en la creación de planes estratégicos para evitar los llamados ciberdelitos.

El derecho penal clásico se construyó en base a las conductas físicas de las personas y las evidencias tangibles de las mismas; sin embargo, los delitos cometidos en sistemas digitales implican retos técnicos, jurisdiccionales porque en ocasiones el delito se comete de un país a otro, y procesales.

En el caso de Ecuador, Ordoñez (2024) manifiesta que el Código Orgánico Integral Penal emitido en el año 2014, ha ido incorporando de forma progresiva las figuras penales vinculadas a delitos informáticos, que incluyen el acceso no permitido ni consentido a sistemas, revelación ilegal de bases de datos, la suplantación de identidad, entre otros. No obstante, esto ha sido criticado por Tixi et al. (2022) expresando que, esto genera falta se sistematicidad y hace que se le dificulte al operador de justicia interpretar la norma.

Nuestro Código Orgánico Integral Penal (COIP) contiene varios artículos donde se tipifican los principales ciberdelitos en el país, a continuación, se detallan:

- Art. 229 – Revelación ilegal de bases de datos: Se sanciona a la persona que revele información contenida en archivos o bases de datos electrónicas, "materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas"; sea para su propio beneficio o de un tercero. La pena dispuesta es de 1 a 3 años de prisión, sin embargo, si quién comete el delito goza de un cargo público, trabaja de forma interna en una entidad bancaria o en instituciones de la economía popular y solidaria que sean mediadores financieros, que actúen como intermediarios o también los contratistas serán sancionados con 3 a 5 años de prisión, por lo que se agrava la pena porque estos actores tienen mayor acceso a información delicada y personalísima, lo que hace más grave el delito.
- Art. 230 – Interceptación ilegal de datos: Se configura cuando una persona accede, copia o manipula información sin una debida autorización judicial para obtener un beneficio propio. Se sanciona con 3 a 5 años de pena privativa de libertad a quienes inciden en las siguientes conductas:
- Quién "intercepte, escuche, desvíe, grabe u observe" datos informáticos en tránsito, sea desde donde su punto de origen, destino o en el interior de un sistema informático, con la finalidad de obtener la información almacenada o disponible.
- Se refiere al delito de phishing que consiste en diseñar, desarrollar, vender, ejecutar, programar o enviar mensajes electrónicos con enlaces que redirijan a los usuarios a páginas de web fraudulentas o ventanas que modifiquen el dominio de la misma. Su objetivo es engañar a las personas para que accedan a estos sitios web maliciosos haciéndoles creer que son legítimos.
- Se sancionará a las personas que se encarguen de copiar, clonar o comercializar la información de las tarjetas electrónicas de débito, crédito y similares.
- También se sanciona a la persona que "produzca, fabrique, distribuya, posea o facilite" los materiales o los dispositivos electrónicos para comisión de la conducta del inciso anterior.
- Art. 231 – Transferencia electrónica de activo patrimonial: Se sancionará con pena privativa de libertad de 3 a 5 años para quien se lucre, alterando, manipulando o modificando el funcionamiento del sistema informático, es decir el uso fraudulento de sistemas digitales para apropiarse de forma no consentida del activo patrimonial de otra persona. Igualmente, se sancionará a la persona que facilite los datos de su cuenta bancaria para captar un activo patrimonial de forma ilegitima a través de transferencia bancaria ya sea para sí mismo o para un tercero.
- Art. 232 – Ataque a la integridad de sistemas informáticos: Se sanciona con pena privativa de libertad de 3 a 5 años a la persona que destruya, dañe, borre o cause el mal rendimiento de un sistema informático o de telecomunicaciones. Adicionalmente, se sanciona de forma expresa la creación o distribución de virus o troyanos, también llamados "malware". Si la acción afecta a los servicios públicos o los que están vinculados a la seguridad de la ciudadanía, la pena se agrava de 5 a 7 años.
- Art. 233 – Delitos contra la información pública reservada legalmente: Se priva de la libertad de 5 a 7 años a quien se encargue de destruir o inutilizar información pública de carácter reservada. Por otro lado, si se trata de un servidor público que obtiene de forma indebida esta información se lo sancionará con 3 a 5 años de pena privativa de libertad. Si se revela la información y se compromete la seguridad del Estado ecuatoriano, se sancionará a la persona con 7 a 10 años de pena privativa de libertad.
- Art. 234 – Acceso no consentido a un sistema informático, telemático o de telecomunicaciones: Quién acceda de forma total o parcial a un sistema informático o red de telecomunicaciones sin autorización previa y se mantenga en el mismo contra la voluntad del dueño o titular, sea para explotar de manera ilegal el acceso o para desviar su uso, será sancionado con pena privativa de libertad de 3 a 5 años.
- Art. 235 – Suplantación de identidad: Se prevé 1 a 3 años de pena privativa de libertad para quien "suplante la identidad de otra" persona con la finalidad de obtener algún beneficio ilícito, en este caso, este tipo penal se ajusta al robo de identidad digital o hasta la

creación de perfiles falsos de alguien más buscando algún beneficio.

- Art. 186, num. 1 y 2 – Estafa agravada: Dentro del tipo penal de estafa, en los numerales la pena se agrava a 7 años a quien defraude a alguien más a través de tarjetas de crédito o debito clonadas o también dispositivos electrónicos que alteren datos financieros.
- Art. 190 – Apropiación fraudulenta por medios electrónicos: El tipo penal se ajusta a la (s) persona (s) que a través de sistemas informáticos se apropie de bienes ajenos, incluyendo la manipulación de sistemas de métodos de pago o claves secretas en medios digitales como las aplicaciones. A su vez, se prevé la pena privativa de libertad de 1 a 3 años.

Conviene subrayar que, el Código Orgánico Integral Penal no solo contiene los delitos mencionados, sino que también abarca otros delitos que están vinculados más bien a las tecnologías, como las infracciones relacionadas a la integridad de terminales móviles que se encuentran en los artículos 191 hasta el 195. Al mismo tiempo, se toman en cuenta conductas consideradas "especiales" como el terrorismo informático que se desglosa dentro del delito de terrorismo en el artículo 366.

Tabla 1. Ciberdelitos tipificados en el Código Orgánico Integral Penal.

Ciberdelito	Artículo del COIP (si se menciona)	Sanción
Acceso Ilegal	234	3 a 5 años de prisión
Interceptación Ilegal	230.1	3 a 5 años de prisión
Interferencia de Información	232	3 a 5 años de prisión
Interferencia del Sistema	232	3 a 5 años de prisión
Falsificación Informática	234.1	3 a 5 años de prisión
Transferencia Electrónica de Activo Patrimonial	231	3 a 5 años de prisión
Pornografía Infantil (Producción/ Distribución)	103	13 a 16 años de prisión
Posesión de Pornografía Infantil	104	10 a 13 años de prisión
Grooming		1 a 3 años o 3 a 5 años de prisión
Oferta de Servicios Sexuales por Medios Electrónicos (a menores)	174	7 a 10 años de prisión
Ciberacoso	166	6 meses a 1 año (1 a 3 años si la víctima es menor)
Acoso Sexual Cibernético		1 a 5 años de prisión
Violación del Derecho a la Intimidad	178	1 a 3 años de prisión
Revelación de Secreto o Información Personal de Terceros		1 a 3 años de prisión
Apropiación Fraudulenta por Medios Electrónicos	190	1 a 3 años de prisión
Pharming	230.2	3 a 5 años de prisión
Phishing	230.2	3 a 5 años de prisión
Ataque a la Integridad de Sistemas Informáticos	232	3 a 5 años de prisión (5 a 7 años si afecta servicios públicos)
Suplantación de Identidad (con fines de estafa)	186	
Alteración Ilegal de Identidad	211	

Como se puede observar en la tabla, el Código Orgánico Integral Penal nos presenta una gran variedad de ciberdelitos, que se podrían clasificar en algunos grupos. Los ataques relacionados a los sistemas de información incluyen el acceso ilegal, la interceptación ilegal de información dirigida hacia, desde o dentro de un sistema informáticos, la interferencia de la misma que implica dañar, borrar, deteriorar, alterar o eliminar información. Los delitos relacionados con la pornografía infantil involucran varias acciones como producir, ofertar, distribuir, adquirir o poseer la misma, con una pena privativa de libertad entre los trece y dieciséis años. Derivado de este delito, tenemos el grooming, que es la captación de un menor de edad con una finalidad sexual a través de dispositivos electrónicos.

Ahora, otros ciberdelitos que contempla el Código Orgánico Integral Penal, tenemos el ciberacoso, que se da cuando una persona hostiga o amenaza a alguien más a través de las TICS, redes sociales, correos o cualquier espacio, causando daño a la dignidad de la persona y afectando su paz mental. Paralelamente, está el hostigamiento que se realiza a través de cualquier medio digital, molestando o perturbando a otra persona de forma reiterada, se sanciona con seis meses a un año de cárcel. Otros delitos expresados en el Código Orgánico Integral

Penal incluyen la reprogramación de información de equipos terminales móviles, el intercambio, comercialización y compra; y las lesiones a los derechos de autor.

A su vez, se penaliza la duplicación de información de tarjetas de débito y crédito y actividades relacionadas, el fraude informático, el ataque a la integridad de sistemas informáticos que incluye el diseño, venta o distribución de "malware" y la destrucción de infraestructura física, el acceso no autorizado a sistemas de información, la falsificación informática y el terrorismo cuando se utiliza tecnología para tomar el control de medios de transporte o plataformas marinas. Entonces, se puede decir que, las sanciones por los ciberdelitos varían considerablemente porque pueden ser desde meses hasta años de pena privativa de libertad dependiendo de la gravedad del delito, de agravantes, entre otras cosas.

Desarrollo de las leyes referente a la ciberdelincuencia en Ecuador

La función legislativa abordó los ciberdelitos en el Ecuador desde que promulgaron en el 2002 la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. El mencionado cuerpo legal fue el primer reconocimiento que surgió como necesidad de que regulen las actividades y transacciones que se realizaban en los medios informáticos o digitales, sentó las bases para los tipos penales informáticos. Luego, con la modernización del derecho penal a través del Código Orgánico Integral Penal (COIP), que incluyó dentro de sus libros diversas disposiciones relacionas con los ciberdelitos (Bolaños, 2022).

El objetivo del Código Orgánico Integral Penal fue colocar un punto final a la dispersión normativa existente en materia penal con el anterior Código Penal, buscando establecer una mayor certeza de tipos penales. El legislador de ese entonces tomó en consideración las garantías constitucionales y la necesidad de que combatir el delito de manera eficiente. La promulgación del Código Orgánico Integral Penal fue un paso importante para la sociedad ecuatoriana porque el enfoque era unificado e integraba a los ciberdelitos dentro de un marco penal más amplio y estructurado.

Desde que el Código Orgánico Integral Penal entró en vigencia, ha experimentado algunos cambios o mejor llamadas reformas. Uno de los más importantes fue la Ley Orgánicas Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha Contra Delitos Informáticos (Ecuador. Asamblea Nacional, 2021), que reflejó una solución para adaptar el Código Orgánico Integral Penal a las amenazas cibernéticas especificas como la violencia sexual digital. La comunidad internacional ha influido en el desarrollo de la legislación sobre ciberdelitos en el Ecuador. El país ha tomado como bases instrumentos internacionales como el Convenio sobre la Ciberdelincuencia del Consejo de Europa y el Modelo Interamericano de Legislación sobre Delitos Informáticos desarrollado por la Organización de Estados Americanos.

Las estadísticas revelan un aumento creciente en los delitos cibernéticos con la apropiación fraudulenta por medios electrónicos como la más común (Maldonado, 2025). Dicho incremento, junto con la identificación grupos de atención vulnerable como lo son niños, niñas y adolescentes, destaca la urgencia de que fortalezca las medidas preventivas y la conciencia pública sobre los riesgos especio informático. Adicionalmente, Juca & Medina (2023) expresan que en el Ecuador el número de denuncias por ciberdelitos han aumentado e indica que la Fiscalía General del Estado registró 718 denuncias por ciberdelitos en el año 2019, 1030 denuncias en el 2020 que incrementaron a 1851 denuncias en el año 2021, esto deja en evidencia que durante la pandemia de COVID 19 hubo un incremento considerable.

La penalización de los ciberdelitos en el país ha sido de diversas formas y se basa en la protección de los bienes jurídicos básicos adaptados a la actual era digital que vivimos. Desde el punto de vista de Enríquez (2021) la ciberdelincuencia creció desde los años 80, manifiesta que la referencia principal de los ciberdelitos es la Convención de Budapest sobre la Ciberdelincuencia emitida el año 2001. Aunque Ecuador no ha ratificado dicho convenio se considera que los tipos penales del Código Orgánico Integral Penal se inspiran en las categorías de tal instrumento internacional. Así pues, el autor expresa que, desde la perspectiva clásica, este tipo de delitos se clasifican en tres grupos: delitos con el objetivo meramente informático, delitos que utilizan medios informáticos o tecnológicos como medio para la comisión de otros delitos y delitos que se relacionan al contenido que se difunde en redes sociales.

En esta misma línea, Robalino y Malo (2024) explican que, el primer grupo contiene los ciberdelitos más comunes como el fraude online, suplantación de identidad, estafa agravada o incluso falsificación de datos personales. El segundo grupo encierra delitos que se relacionan a vulneraciones a los Derechos Humanos, como la pornografía infantil, comercio ilícito de armas o animales exóticos, es decir que, el medio informático es un medio para que se cometan otros delitos. El tercer grupo incluye ataques que se dirigen a individuos, sistemas informáticos del Estado o de entidades privadas; las acciones se hacen a través de redes de dispositivos infectados, que propagan malware o virus para que se comprometan equipos sin que el dueño del dispositivo lo note o pueda prevenirlo.

Con base a Durbin (2023), los ciberdelitos que tienen una mayor incidencia en el Ecuador son la instalación de software malicioso o más conocido como malware que busca hackear claves, información personal, datos relacionados a las aplicaciones de los bancos e historial de navegación, los cuales tiene como fin ser explotados para

la comisión de otros delitos como robos financieros o suplantación de identidad. Otro delito común es la falsificación de documentos, delito en el que los datos que han sido robados se usan para crear pasaportes o licencias falsas, facilitando los robos de identidad e incluso la evasión fiscal. Asimismo, la extorsión es considerada como un ciberdelito porque cuando el ciberdelincuente tiene la información privada como fotos y mensajes, amenazan con hacerla pública a menos que se pague determinada cantidad de dinero y causa daño emocional y psicológico a las víctimas.

Los ciberdelitos presentan retos en su sanción, Guerrero (2021) argumenta que en nuestro ordenamiento jurídico, se identifican varios vacíos legales referentes a los ciberdelitos porque mientras las conductas delictivas en el mundo real son sancionadas, quienes están delinquiendo en el ciberespacio suelen ser personas que tienen habilidades informáticas avanzadas y por lo general, poseen conocimientos superiores en sistemas informáticos, lo que les permite la comisión exitosa del delito y con mucha más facilidad, y en ocasiones sin dejar rastro, por tal motivo el tiempo es clave en este tipo de delitos porque la evidencia es efímera y perecedera, por lo tanto, el enjuiciamiento de los actores de los delitos cibernéticos es más compleja.

Con base en Juca & Medina (2023) los delitos cibernéticos han incrementado en los últimos años, lo que los posiciona como una amenaza principal para la seguridad digital a nivel nacional. Por lo tanto, se revela la necesidad del gobierno en reforzar los mecanismos de respuesta y fomentar una mayor conciencia en la ciudadanía sobre la seguridad digital. Por consiguiente, se puede deducir a manera de analogía que, un archivo borrado desaparece con rapidez, por lo que se necesita un método o procedimiento más ágil que genere un efecto inmediato.

En la opinión de Cuenca (2022), en relación a la sanción considera que, hay un desconocimiento de los ciberdelitos por parte de nuestros legisladores al momento de tipificar las conductas como delitos y a su criterio, esto se puede dar debido a la falta de familiarización con la materia lo que lleva a una tipificación imprecisa de ciertos actos en variables como la acción delictiva y los sujetos involucrados en la comisión del delito. En cuanto a la definición legal, indica que, nuestras normas penales referentes a los delitos informáticos padecen de lagunas legales concordando con Guerrero (2021), piensa que cuando se aplican a casos específicos, los tipos penales pueden ser interpretados erróneamente por el juzgador, generando diversos problemas. Por una parte, quien es el denunciante puede obtener un resultado que no espera, por otra parte, el acusado estaría enfrentando una pena que no le corresponde al delito que cometió.

Concerniente a las penas, surge la duda sobre si la pena es proporcional al delito cometido. Las penas previstas en el Código Orgánico Integral Penal van desde 1 a 5 años en la mayoría de los casos, el agravante de algunos tipos penales es hasta 7 años, son relativamente moderadas o mínimas comparadas con la comisión del delito. Saltos et al. (2021) enfatizan en que nuestra legislación sobre los ciberdelitos es algo amplia, sin embargo, carece de la especificad necesaria. Por tal motivo, surge la idea de una reforma que detalle completamente y clasifique adecuadamente los diferentes tipos de estos delitos.

CONCLUSIONES

Se concluye que la evolución tecnológica ha transformado las dinámicas en las que nos desarrollamos, por lo tanto, han cambiado las formas delictivas, dando paso al surgimiento de nuevos tipos penales que no solo representan un desafío en el Ecuador, sino a nivel mundial. A pesar de que el Código Orgánico Integral Penal ha ido incorporando paulatinamente los ciberdelitos, aún así existen vacíos normativos, imprecisiones en la norma y barreras que limitan su aplicación a los hechos. A través del análisis doctrinal y empírico del presente artículo, se evidenció que la normativa actual no responde integralmente a los desafíos que surgen con la ciberdelincuencia.

Se observó el esfuerzo del legislador para incorporar los ciberdelitos que van desde la pornografía infantil hasta el fraude electrónico. No obstante, el análisis doctrinal estudiado, deja en claro que aún hay muchas cosas por mejorar, especialmente para las nuevas modalidades que cada día se van actualizando como el ciberacoso que con el pasar del tiempo tiene más variantes. Consideramos que es importante que el Código Orgánico Integral Penal debe estar armonizado con otras leyes como la Ley de Protección de Datos y Comercio Electrónico.

Luego de haber investigado de forma exhaustiva el tema podemos concluir que, el Código Orgánico Integral Penal contiene avances significativos en la tipificación de ciberdelitos en el país porque ha integrado un catálogo diverso de conductas ilícitas informáticas que van desde accesos a sistemas informáticos y fraudes digitales hasta ataques a sistemas privados o del Estado, y, ha desarrollado penas específicas para aquellos. El mencionado cuerpo legal junto con otras normas como la Ley de Datos Personales han hecho posible que se persigan penalmente las amenazas cibernéticas. No obstante, pudimos notas que la eficacia real de dichas normas aún está en vías de desarrollo.

Tal y como lo mencionaron diversos autores se necesitan reformas continuas, se debería elaborar una ley especial enfocada solamente en los ciberdelitos unificando todos sus aspectos, armonizando la misma a instrumentos internacionales y la misma, debe proveer guías procesales ágiles y eficaces. Relativo a lo académico, se concluye que el Código Orgánico Integral Penal cubre los delitos informáticos “básicos”, pero aún contiene brechas o vacíos para los nuevos delitos que se van configurando conforme pasa el tiempo como el ciberacoso. En este sentido,

también es importante mencionar que hay que capacitar a los legisladores para que al momento de desarrollar el tipo de penal no dejen vacíos legales, a los jueces para que sean capaces de subsumir correctamente el hecho al tipo penal y el Gobierno debe promover una cultura de ciberseguridad que involucre a la ciudadanía en general.

REFERENCIAS

Bolaños, L. (2022). ***Análisis histórico jurídico de la evolución del ciberacoso en la legislación penal ecuatoriana y sus incidencias*** [Tesis de maestría, Pontificia Universidad Católica del Ecuador].

Brenner, S. W. (2010). ***Cybercrime: Criminal threats from cyberspace***. https://ecommons.udayton.edu/cgi/viewcontent.cgi?article=1023&context=law_fac_pub

Durbin, S. (2023). Cuatro tendencias de riesgo cibernético para observar en 2023. ***Forbes Ecuador***. https://www.forbes.com.ec/innovacion/cuatro-tendencias-riesgo-cibernetico-observar-2023-n27981

Ecuador. Asamblea Nacional. (2014). ***Código Orgánico Integral Penal***. Registro Oficial 180. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Ecuador. Asamblea Nacional. (2021). ***Ley orgánica reformatoria al Código Orgánico Integral Penal***. Registro Oficial Suplemento No. 526. https://vlex.ec/vid/ley-organica-reformatoria-codigo-875227482

Espinoza Carvajal, G. G., & Paredes Fuentes, F. E. (2025). Los ciberdelitos y la protección de datos personales en el sistema penal ecuatoriano. ***Revista Lex, 8***(29), 559–572. https://doi.org/10.33996/revistalex.v9i28.302

Fiscalía General del Estado. (2023). ***Boletín de prensa: Sentencia por tentativa de acceso no consentido a sistemas informáticos***. https://www.fiscalia.gob.ec/accesibilidad/fiscalia-obtiene-sentencia-por-los-delitos-de-acceso-no-consentido-a-un-sistema-informatico-telematico-o-de-telecomunicaciones-y-revelacion-ilegal-de-base-de-datos/

Fuentes-Águila, M. R., Díaz-de Perales, A. V., Brito-Febles, O. P., Sarango-Aguirre, H., Castillo, F. J., & Ramírez-de Castillo, A. (2024). ***Perspectivas de la prevención como estrategia del control social en Ecuador.*** Editorial UMET.

Guerrero, D. (2021). ***Análisis del ciberdelincuente en el derecho penal ecuatoriano*** [Tesis de maestría, Universidad Regional Autónoma de los Andes].

Juca Maldonado, F., & Medina Peña, R. (2023). Ciberdelitos en Ecuador y su impacto social: Panorama actual y futuras perspectivas. ***Revista Portal de la Ciencia, 4***(3), 325–337. https://doi.org/10.51247/pdlc.v4i3.394

Maldonado Montenegro, C. D. (2024). Análisis sobre la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en el Ecuador: Desafíos y perspectivas. ***Revista Criminalidad, 66***(3), 27–44. https://doi.org/10.47741/17943108.660

Oficina de las Naciones Unidas contra la Droga y el Delito. (2013). ***Comprehensive study on cybercrime***. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

Ordóñez, L. (2024). El marco legal de los delitos cibernéticos en Ecuador. ***Reincisol, 5***(3), 1447–1469. https://doi.org/10.59282/reincisol.V3(5)1447-1469

Ponce, M. (2024). Delitos informáticos: Caso Ecuador. ***Revista San Gregorio, 1***(58), 119–123. https://doi.org/10.36097/rsan.v1i58.2667

Pons Gamon, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity. URVIO. Revista Latinoamericana De Estudios De Seguridad, (20), 80–93. https://doi.org/10.17141/urvio.20.2017.2563

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis conceptual del delito informático en Ecuador. ***Conrado, 17***(78), 343–351. https://www.scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343

Tixi-Janeta , S. G., Merizalde-Avilés , M. L., Romero-Fernández , A. J., & Jordán-Naranjo , G. V. (2023). Los delitos informáticos en el Código Orgánico Integral Penal ecuatoriano. IUSTITIA SOCIALIS, 8(1), 1610–1619. https://doi.org/10.35381/racji.v8i1.3339

Conflictos de interés:

El autor declara no tener conflictos de interés.

Contribución de los autores:

Homero Abel Ramírez-Cabrera: Conceptualización, curación de datos, análisis formal, investigación, metodología, supervisión, validación, visualización, redacción del borrador original y redacción, revisión y edición.

Declaración ética:

El estudio aborda temas relacionados con estudiantes/ personas vulnerables, pero se realizó únicamente mediante revisión documental, análisis de información secundaria o bases de datos públicas. No implicó la participación directa de seres humanos ni el manejo de información personal identificable.