Revista Ciencias Holguín Vol. 31 Núm. 4 (2025)

Los delitos informáticos en el COIP y su actualización frente a nuevas formas de ciberdelitos / Computer crimes in the COIP and their updating in the face of new forms of cybercrime

[1]Luz Selena León Barzallo, https://orcid.org/0000-0002-1357-4658, lleon12@utmachala.edu.ec
[2]Angeline N. Olmedo Reyes, https://orcid.org/0000-0002-0895-6328, aolmedo1@utmachala.edu.ec
[3]Armando Rogelio Durán Ocampo, http://orcid.org/0000-0002-9524-0538, aduran@utmachala.edu.ec
[1,2,3] Universidad Técnica de Machala

Resumen

La ciberdelincuencia constituye uno de los temas más relevantes y contemporáneos del Derecho Penal. En el presente estudio se realiza un análisis de la norma penal ecuatoriana y su correspondencia con los preceptos normativos del Convenio de Budapest, donde se dispone la adecuación de las normas sustantivas y procesales que deben contribuir a la persecución, procesamiento y juzgamiento de la criminalidad digital, a las reglas de colaboración internacional en este sentido y, consecuentemente, al enfrentamiento de la criminalidad trasnacional. Se analizan figuras delictivas que se han estado suscitando en las últimas décadas y que muchas veces quedaron en la impunidad por falta de previsibilidad legal y por contraponer los principios de legalidad sustantiva y procesal. Se analiza la forma en que la legislación ecuatoriana, pese a los avances que ha demostrado en la persecución de los ciberdelitos, aún presenta deficiencias en el ámbito sustantivo y procesal que resulta necesario resolver, tales como la tipificación de conductas no descritas en la norma y la definición de reglas procesales que cumplan con las exigencias del Convenio sobre la Ciberdelincuencia, además, se verifica la necesidad de establecer mecanismos de prevención general y especial que objetivamente contribuyan a la evitabilidad de estas conductas.

Palabras clave: ciberdelitos, delitos informáticos, delincuencia organizada, delincuencia trasnacional.

Summary:

This paper deals with one of the most relevant and contemporary issues in Criminal Law, cybercrimes. An analysis of Ecuadorian criminal law and its correspondence with the normative precepts of the Budapest Convention is carried out, which provides for a tempering of the substantive and procedural rules that must contribute to the prosecution, prosecution and prosecution of digital crime, to the rules of international collaboration in this regard and, consequently, to the confrontation of transnational crime. It analyzes criminal figures that have been arising in recent decades and that often remained in impunity due to lack of legal predictability and oppose the principle of substantive and procedural legality. It is studied how Ecuadorian legislation, despite the progress it has shown in the prosecution of cybercrimes, still has deficiencies in the substantive and procedural field that need to be resolved, such as the classification of behaviors not described in the norm and the definition of procedural rules that comply with the requirements of the Convention on Cybercrime. In addition, the need to establish general and special prevention mechanisms that objectively contribute to the avoidability of these behaviors is verified.

Keywords: cybercrimes, computer crimes, organized crime, transnational crime.

Introducción

Desde hace algunos años Ecuador viene implementando políticas penales en el esclarecimiento y persecución de los delitos denominados como informáticos y ciberdelitos, los cuales, sin lugar a dudas son, todavía, una nueva forma de infracción penal que suele tener lugar con mucha frecuencia y que es de difícil comprensión para los operadores del Derecho. En tal sentido, es importante esclarecer puntos de entendimiento que sean ilustrativos para aquellos que están obligados a perseguirlos, defenderlos o juzgarlos.

Aunque el tema de las infracciones informáticas sigue siendo considerado novedoso, incomprensible y de difícil comprobación, en realidad, no es algo sobre lo que se haya discutido tan recientemente pues, desde hace algunos años se han convenido acuerdos a nivel mundial que han establecido las pautas esenciales a tener en cuenta para su enfrentamiento y su configuración legal; tal es el caso de la Convención de Budapest o Convenio sobre la Ciberdelincuencia, como también se le conoce (Consejo de Europa, 2001) el cual fue ratificado por el Estado ecuatoriano en el año 2024 mediante Decreto Ejecutivo No. 332 (Noboa Azín, 2024).

Este instrumento jurídico, usado, reconocido y ratificado por un número considerable de países, proporciona una serie de definiciones que son importantes para poder entender la forma de operar de los ciberdelincuentes, quienes, sin lugar a dudas, son personas muy inteligentes y siempre están un paso delante de los que se proponen perseguirlos, lo que hace cada vez más compleja su detención, procesamiento y sanción penal. Entre las definiciones principales están: delitos informáticos, interceptación ilegal, acceso ilícito, interferencia de datos y de sistemas, fraude informático y falsificación informática, uso de dispositivos, entre otras (Consejo de Europa, 2001).

A partir de las primeras conductas delictivas relacionadas con la informática y el mundo de las comunicaciones, comenzaron a aparecer manifestaciones delictivas, que antes, eran comunes, pero que ahora están relacionadas con las tecnologías, además de las que, son claramente informáticas. Tal es el caso de infracciones contra la intimidad por medios informáticos, delitos sexuales que se cometen solo utilizando plataformas informáticas, la instigación al suicidio o lesiones, esta última es una conducta que se ha ejecutado mediante juegos y plataformas informáticas. En tal sentido existen, en las normas penales más contemporáneas, infracciones delictivas por medios electrónicos que tienen un título específico en la norma para ellas y otras que, sin ser precisamente delitos informáticos, están vinculadas por su utilización directa.

En las últimas décadas, el mundo entero se ha beneficiado de las transformaciones tecnológicas, esto ha generado una dependencia de ellas a niveles insospechados y hoy en día, prácticamente todo ha adquirido una forma tecnológica, el dinero, los servicios, los bienes, etcétera. Pero, no todo es bueno en este sentido, a su vez, se han generado nuevas formas de delincuencia y los Estados han enfrentado muchas dificultades en su esclarecimiento y persecución. El Código Orgánico Integral Penal (Ecuador. Asamblea Nacional, 2014), norma penal sustantiva y procesal del Ecuador que fuera promulgada desde el año 2014 estableció una serie

de conductas relacionadas con estos delitos y que denominó delitos informáticos, lo cual refuerza el esfuerzo continuo por adaptarse a las nuevas realidades tecnológicas.

El problema de las tecnologías de la información, es que son indetenibles y, si bien en la mayoría de los casos, proporcionan cosas positivas para la sociedad, también generan fenómenos negativos que evolucionan y cambian a diario, como lo es, el delito. Por ejemplo, ya hay modalidades delictivas que superan las tradicionales, tal es el caso de la modalidad de delito denominada como “Ransomware” (Kosinski, 2024), este delito consiste en que por medio de un programa informático se extorsiona a las personas a cambio de que se le devuelvan sus datos personales, puesto que, en principio, estos han sido retenidos y son amenazados con su divulgación, venta o uso inadecuado.

Otra modalidad ciberdelictiva frecuente es el “Phishing e ingeniería social” (Loya Lasluisa, 2024), el cual consiste en una serie de técnicas de engaño por medios electrónicos como: emails, redes sociales, llamadas telefónicas, etcétera y que se usan para la obtención de usuarios y credenciales de personas, lo que constituye una modalidad de fraude informático. También está el ataque denominado “*Cryptojacking*” (Castillo Reyes, 2019), también llamado como *Criptosecuestro*, es otra forma de cometer infracciones informáticas que, en este caso, consiste en el secuestro de un dispositivo electrónico a fin de utilizar sus criptomonedas.

Estos, son solo algunos de los *modus operandi* que se utilizan y que ya tienen nombre en el mundo de los ciberdelitos, sin embargo, el fenómeno del delito informático apenas inicia y, a consideración de muchos de sus estudiosos, es un mundo enteramente desconocido para los juristas y para los persecutores penales. El tema de la especialización en estas materias es tan complejo como, prácticamente, inexistente e incluso, los peritos informáticos que tienen la responsabilidad de investigar, cómo, cuándo y dónde se han cometido las infracciones penales, lo tienen sumamente complicado para llevarlo a juicio y ser ilustrativos en su informe pericial.

La importancia de la presente investigación radica en el impacto que representan estos delitos en los derechos de la sociedad y del Estado, atacando bienes jurídicos que merecen una especial protección, en muchos casos, con absoluta impunidad, tales como: su patrimonio, la privacidad, la seguridad informática y la seguridad pública. Aunque existe previsibilidad normativa en el Ecuador con los denominados delitos informáticos, su evolución representa retos significativos para el legislador, pues las nuevas modalidades delictivas pueden, incluso, ir contra el principio de legalidad y, por tanto, la perjudicial conducta quedaría en la absoluta impunidad.

Por ello es importante preguntarse ¿en qué medida el Código Orgánico Integral Penal resulta una norma efectiva ante las nuevas modalidades de ciberdelitos? Consecuentemente, como objetivo de esta investigación es válido analizar la regulación jurídica actual sobre los ciberdelitos en el Código Orgánico Integral Penal y verificar su capacidad de eficacia y adaptación frente a las nuevas modalidades de delitos informáticos. Como objetivos específicos se presentan: examinar los conceptos esenciales sobre los ciberdelitos que hasta el

momento han sido desarrollados y usados en el contexto ecuatoriano, definir el marco normativo que resulta aplicable según lo establecido en el Código Orgánico Integral Penal respecto a los delitos informáticos y proponer soluciones jurídicas frente a las insuficiencias identificadas.

La metodología que se emplea en la investigación es de tipo cualitativa con un profundo análisis documentológico, lo que ha permitido el estudio crítico de legislaciones de carácter nacional, instrumentos jurídicos internacionales relacionados con los delitos informáticos, en particular la Convención de Budapest. Con este enfoque se analizarán los conceptos claves, los elementos normativos sistemáticos que regulan la ciberdelincuencia y las reglas de interpretación jurídica para que se pueda comprender la tipicidad delictiva y las consecuencias jurídicas de estas clases de infracciones. Se realiza una evaluación de la efectividad del Código Orgánico Integral Penal frente a las nuevas conductas delictivas informáticas, lo que implica un estudio jurisprudencial, el análisis histórico y lógico de tales infracciones y lo que ha manifestado la doctrina especializada en este sentido.

Materiales y Métodos

La investigación se desarrolló bajo un enfoque cualitativo, orientado al análisis crítico y descriptivo de la normativa penal ecuatoriana en materia de delitos informáticos y su correspondencia con los estándares internacionales, especialmente el Convenio de Budapest sobre la Ciberdelincuencia.

Se empleó la revisión documental como principal técnica, lo que implicó la recopilación y el estudio sistemático de fuentes primarias y secundarias relevantes. Entre los materiales analizados se incluyeron textos legales, tratados internacionales, jurisprudencia, doctrina especializada y literatura científica, así como informes oficiales de organismos nacionales e internacionales.

Procedimiento:

El proceso metodológico se estructuró en las siguientes etapas:

1. **Identificación y selección de fuentes:** Textos legales, tratados internacionales, sentencias y publicaciones académicas sobre delitos informáticos en Ecuador y a nivel internacional.
2. **Análisis normativo y doctrinal:** Examen crítico de la normativa ecuatoriana vigente, identificando vacíos legales y desafíos procesales frente a nuevas modalidades de ciberdelitos.
3. **Comparación jurídica:** Contraste de las disposiciones del COIP con los lineamientos del Convenio de Budapest.
4. **Revisión jurisprudencial:** Análisis de fallos relevantes sobre la aplicación de normas de delitos informáticos.

5. **Síntesis y propuesta:** Elaboración de propuestas para la actualización y mejora del marco normativo nacional.

Limitaciones:

La investigación se basó exclusivamente en fuentes documentales. El análisis se centró en la legislación y doctrina hasta el año 2024 (Tabla 1).

Tabla 1. Principales materiales documentales analizados

Tipo de material	Fuente o referencia principal	Descripción y uso en la investigación
Legislación nacional	Código Orgánico Integral Penal (COIP)	Análisis de la tipificación de delitos informáticos y reformas
Tratados internacionales	Convenio de Budapest sobre la Ciberdelincuencia	Comparación de estándares internacionales y nacionales
Jurisprudencia	Sentencias de cortes nacionales e internacionales	Ejemplos de aplicación práctica de la normativa
Doctrina especializada	Artículos y libros sobre derecho penal y ciberdelitos	Fundamentación teórica y conceptual
Informes oficiales	Documentos de organismos nacionales e internacionales	Estadísticas y contexto sobre la criminalidad informática

Fuente. Elaboración propia

Desarrollo

En los últimos años, el desarrollo tecnológico ha generado transformaciones muy significativas, sobre todo, para las viejas generaciones. El adaptarse a usar las tecnologías de la información y la comunicación ha sido un desafío para jueces, fiscales y abogados, sobre todo, para los que más experiencia tenían en la administración de justicia, lo que, a su vez, ha sido una ventaja aprovechada por los jóvenes y por los delincuentes tecnológicos. La revolución digital lo ha venido a cambiar prácticamente todo y, sin lugar a dudas, ello ha constituido una forma de optimización de procesos para el desarrollo del ser humano, no obstante, también ha dado lugar a que se cometan conductas perjudiciales socialmente y, a su vez, desconocidas, las que, obviamente, no estaban tipificadas como infracción penal y que desafían las categorías clásicas del Derecho Penal.

En el caso del Estado ecuatoriano, el Código Orgánico Integral Penal alberga, entre sus postulados, una sección específica que ha sido dedicada a los delitos informáticos y que ha sido denominada como: “Delitos contra la seguridad de los activos de los sistemas de información y comunicación” (Asamblea Nacional, 2014, pág. 80). En virtud de ello, han sido incorporadas figuras delictivas tales como: “Revelación ilegal de base de datos” en el artículo 229; “Interceptación ilegal de datos” en el artículo 230, “Transferencia electrónica de activo patrimonial” en el 231, “Ataque a la integridad de sistemas informáticos”, en el artículo 232 (Asamblea Nacional, 2014, pág. 81) y, así sucesivamente, una serie más de infracciones penalmente relevantes específicas como forma de ciberdelitos de la norma penal.

Además, hay otras infracciones penales que son tradicionales y que conservan su regulación en este sentido, pero que con motivo de las transformaciones digitales, han surgido nuevas formas de comisión y por ello, el legislador se ha visto obligado a tipificar su realización por vías tecnológicas, un ejemplo podría ser la instigación al suicidio, que si bien es un delito que en la doctrina ha sido ejecutado mediante la manipulación de la víctima para que se autolesione y muera, en la actualidad, han existido manifestaciones de esta manipulación utilizando medios digitales. Asimismo, se han introducido instituciones procesales y técnicas especiales de investigación criminal que también buscan enfrentar el delito informático, utilizando mecanismos digitales para su enfrentamiento, a los que se hará referencia más adelante (Asamblea Nacional, 2014).

Pese a todo este avance, a que el legislador ha sido oportuno y ha pretendido definir una serie de conductas típicas para su posterior sanción en caso de que procesalmente se demuestre la culpabilidad, el fenómeno de la trasnacionalidad delictiva, el dinamismo de los ciberdelitos, la aparición constante de nuevas manifestaciones de delitos informáticos y la mutación de los existentes, tales como el ransomware, el phishing, el robo de identidad, pone día a día a prueba la capacidad de respuesta de los órganos de investigación criminal y del sistema judicial penal para poder juzgar y sancionar sin que se vulnere la legalidad, la seguridad jurídica y el derecho a la defensa de los presuntos infractores. En tal sentido, se estará desarrollando un informe donde se cuestione críticamente la configuración penal de los delitos informáticos, de modo que se identifiquen los vacíos legales y se reflexione acerca de la necesidad y fundamentos para la inclusión o modificación de determinadas figuras delictivas.

Conceptualización y marco jurídico regulatorio de los ciberdelitos

Según el (Consejo de Europa, 2001) en el Convenio sobre la Ciberdelincuencia, se consideran delitos informáticos aquel conjunto de conductas dañosas para la sociedad y el Estado que son cometidas en contra de los sistemas informáticos o utilizando medios informáticos, bases de datos, instrumentos digitales o mediante cualquier entorno electrónico. No obstante, según (Hernández Díaz, 2009) en sus inicios, los delitos informáticos se relacionaban con conductas contra los derechos patrimoniales y más, específicamente, con los delitos meramente económicos.

(Hernández Díaz, 2009) plantea que *Bequai*, en el año 1978 realizó un análisis sobre los delitos informáticos y dispuso que, si bien históricamente estas infracciones habían sido tratadas como una manifestación más de los delitos contra los derechos patrimoniales, el acento debía dejar de estar sobre la economía o la propiedad y situarse sobre los ordenadores. En su obra "*computer crimes*" hace referencia a delitos como los sabotajes informáticos, el robo de información previamente digitalizada y robo de programas informáticos, espionaje industrial, robo de mercancías por medio de manipulación de datos informáticos y fraudes financieros.

A partir de ello, varios autores comenzaron a investigar y a proporcionar información viable sobre los denominados delitos informáticos, reflexionando concretamente, sobre cómo se podían cometer otros múltiples delitos por medio de computadoras o, al menos, habiendo sido involucrados los ordenadores en su *modus operandi*, teniendo en cuenta esta cuestión, se ha concluido que debía considerarse delito informático toda infracción penal donde la computadora hubiera sido utilizada como medio o como objeto de la conducta punible. Luego de varios análisis, se les ha concedido a estos delitos una definición más amplia e inclusiva teniendo en cuenta que, si bien hay delitos informáticos concretos, hay otros, que también pueden ser cometidos desde o con un ordenador, por eso se decide nombrarles como: "criminalidad informática", "delincuencia informática" y "delitos informáticos" (Hernández Díaz, 2009).

El problema de los ciberdelitos, delitos informáticos o criminalidad informática con el Derecho Penal radica, fundamentalmente, en la concreción de las conductas en la norma penal. El principio de legalidad exige una subsunción exacta de la conducta en la norma penal, con lo cual, se podría configurar la conducta punible y consecuentemente, una vez que se demuestre su comisión exacta y concreta, se pueda sancionar. La falta de previsibilidad de las conductas, la inadecuada tipicidad de los actos concretos, los vacíos legales que en este sentido puedan existir, son consecuencia directa de la impunidad que se genera por delincuencia informática. A todo ello, súmese, la falta de preparación de los operadores del Derecho o de los investigadores.

Tabla 2. Conceptualización de los principales términos relacionados con los ciberdelitos

TÉRMINO	DEFINICIÓN	FUENTE O REFERENCIA PRINCIPAL
DELITOS INFORMÁTICOS	Conjunto de conductas dañinas para la sociedad y el Estado cometidas contra sistemas informáticos o utilizando medios informáticos y electrónicos.	Convenio de Budapest (2001), COIP
CIBERDELITOS	Infracciones penales que se cometen a través de tecnologías de la información y	Convenio de Budapest, doctrina

	comunicación, afectando bienes jurídicos como privacidad y patrimonio.	
ACCESO ILÍCITO	Entrada no autorizada a todo o parte de un sistema informático.	Convenio de Budapest, COIP art. 230
INTERCEPTACIÓN ILEGAL	Captación, grabación o monitoreo no autorizado de datos informáticos en tránsito o almacenados.	Convenio de Budapest, COIP art. 230
INTERFERENCIA DE DATOS	Alteración, daño, supresión o deterioro de datos informáticos sin autorización.	Convenio de Budapest, COIP art. 232
INTERFERENCIA DE SISTEMAS	Obstaculización grave del funcionamiento de un sistema informático mediante la introducción, transmisión, daño o supresión de datos.	Convenio de Budapest, COIP art. 232
FRAUDE INFORMÁTICO	Obtención ilícita de beneficios patrimoniales mediante manipulación o uso indebido de sistemas o datos informáticos.	Convenio de Budapest, COIP art. 231
FALSIFICACIÓN INFORMÁTICA	Introducción, alteración o supresión de datos informáticos con el fin de que sean tomados como auténticos.	Convenio de Budapest
RANSOMWARE	Software malicioso que restringe el acceso a datos o sistemas y exige un pago para su liberación.	Doctrina especializada
PHISHING	Técnica de engaño para obtener información confidencial (usuarios, contraseñas) a través de medios electrónicos fraudulentos.	Doctrina especializada
CRYPTOJACKING	Uso no autorizado de dispositivos informáticos de terceros para minar criptomonedas.	Doctrina especializada

Fuente. Elaboración propia

El Convenio sobre la Ciberdelincuencia como herramienta legislativa aplicable

El Convenio de Budapest o Convenio Sobre la Ciberdelincuencia del año 2001, (Consejo de Europa, 2001), ha sido considerado como el primer instrumento que en el ámbito internacional se ha suscrito para enfrentar la delincuencia informática concretamente, sobre todo, se suscribe como una necesidad de enfrentar

aquellas conductas que trascendían las fronteras nacionales con motivo de la aparición del internet y con el uso de ordenadores y a partir de sistemas informáticos. Por tal razón, resultó necesario para los Estados armonizar el Derecho Penal sustantivo, la colaboración en la investigación trasnacional y establecer métodos y técnicas en los procedimientos penales de investigación que estuvieran especializados en este tipo de conductas.

El Convenio de Budapest, regula una serie de definiciones que deben ser observadas por los Estados miembros y, a partir de ello, establecer conductas propias en cada uno de los países miembros, pero de un modo coherente y que parta de tales postulados. Tal es el caso de concepto como:

Artículo 1 -Definiciones A los efectos del presente Convenio:

a. por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa., y

b. por "datos informáticos" se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

c. por "proveedor de servicios" se entenderá:

i. toda entidad pública o privada que brinde a los usuarios de sus servicios la posibilidad de comunicarse entre sí por medio de un sistema informático, y

ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio, y

d. por "datos sobre el tráfico" se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente (Consejo de Europa, 2001, pág. 4).

Teniendo en cuenta tales definiciones, los Estados miembros de la Convención estarían obligados, por ella, a la regulación concreta de algunas cuestiones relacionadas con la ciberdelincuencia, debiéndose incorporar en la parte sustantiva de la ley, según lo dispuesto por la "Sección 1 -Derecho penal sustantivo", como mínimo, cinco títulos a la legislación penal de cada país y estos son:

Título 1 -Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (Consejo de Europa, 2001, pág. 4). Título 2 -Delitos informáticos (Consejo de Europa, 2001, pág. 6); Título 3 – Delitos relacionados con el contenido (Consejo de Europa, 2001, pág. 6) Título 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (Consejo de Europa, 2001, pág. 7) Título 5 – Otras formas de responsabilidad y de sanciones (Consejo de Europa, 2001, pág. 8).

En cuanto a la parte procesal de la norma de cada Estado miembro, se acuerda la “Sección 2 - Derecho procesal” (Consejo de Europa, 2001, pág. 9). donde debe regularse, preceptivamente, lo siguiente:

Título 1 “Disposiciones comunes” (Consejo de Europa, 2001, pág. 9), dentro de este título, dispone algunas reglas de carácter general que deberán ser observadas por los miembros y regula, por ejemplo, en el artículo 14 los ámbitos de aplicación de las disposiciones sobre el procedimiento. En el Título 2 “Conservación rápida de datos informáticos almacenados” (Consejo de Europa, 2001, pág. 11) tiene dos artículos uno para la conservación rápida de datos informáticos almacenados y el otro para la conservación y revelación parcial y rápida de datos sobre el tráfico. En el Título 3 “Orden de presentación” (Consejo de Europa, 2001, pág. 11) se regula cómo los Estados miembros deberán establecer los mecanismos para que cualquier persona o entidad estén obligados a entregar a la autoridad investigativa, los dispositivos o los sistemas informáticos donde consten almacenados los datos informáticos (Consejo de Europa, 2001).

En el Título 4 “Registro y confiscación de datos informáticos almacenados” (Consejo de Europa, 2001, pág. 11) se dispone que la autoridad legislativa ha de aprobar aquellas normas procesales que legitimen el registro a todo sistema informático o parte de los mismos y que resulten necesarios para la obtención de datos informáticos. El Título 5 “Obtención en tiempo de datos informáticos” (Consejo de Europa, 2001, pág. 12) encaminado, con el mismo propósito investigativo de ciberdelitos a legislar para garantizar la legitimidad procesal de grabaciones y la obtención en tiempo real de datos informáticos, relacionados con el tráfico de datos y asociados a las comunicaciones trasmitidas en cada territorio, relacionado con ello también está lo regulado por el artículo 20 “Obtención en tiempo real de datos sobre el tráfico” y el artículo 21 “Interceptación de datos sobre el contenido” (Consejo de Europa, 2001, pág. 12)

Respecto a las cuestiones procesales, también es importante hacer referencia a lo regulado en el convenio en la Sección 3 “Jurisdicción” (Consejo de Europa, 2001, pág. 14). Respecto a este punto, la convención establece que:

1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido:

a. en su territorio, o
b. a bordo de un buque que enarbole el pabellón de dicha Parte, o
c. a bordo de una aeronave matriculada según las leyes de dicha Parte, o

d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo (Consejo de Europa, 2001, pág. 14).

Ello implica que, desde el punto de vista territorial, los Estados que no lo hubieran establecido hasta el momento de su suscripción, deberán regular una serie de reglas relacionadas con el alcance de aplicación de la norma para la persecución y sanción de los delitos de esta naturaleza, de modo que, con independencia de que otro estado pueda ser competente para su procesamiento y juzgamiento, exista siempre una posibilidad real de hacerlo. Asimismo, en caso de conflictos sobre la jurisdicción, el último apartado del artículo 22 dispone que deberá resolverse mediante consulta para que se decida sobre cuál es el Estado más adecuado para la investigación y resolución del caso. Dentro de las reglas de cooperación internacional dispuestas por la convención están las pautas necesarias para los procesos de extradición en el artículo 24, los principios relativos a la asistencia mutua entre los Estados del artículo 25, la información espontánea, etcétera (Consejo de Europa, 2001).

Esta norma internacional, no es que resulte absolutamente inaplicable de manera directa en la resolución de un caso dentro de la sociedad ecuatoriana, pero, teniendo en cuenta la forma en que ha sido prevista, sus postulados no son más que mandatos que están encaminados a precisar a los Estados para que legislen o modifiquen sus normas penales sustantivas y procesales con el propósito de que resulte coherente y, sobre todo, legal, el procesamiento, persecución y sanción por los ciberdelitos nacionales y trasnacionales que tengan lugar. Por lo tanto, deberá, en el caso del Ecuador, ser atemperado el Código Orgánico Integral Penal con tales postulados, para que sea también legítimo y coherente con la comunidad internacional en los procesos que se siguen por este tipo de delincuencia.

El Código Orgánico Integral Penal y su atemperamiento reglamentario con los postulados del Convenio de Budapest

Pese a que todavía existen muchas cuestiones por resolver en el Código Orgánico Integral Penal respecto a los delitos informáticos, pues, recientemente ha sido ratificado el Convenio sobre la Ciberdelincuencia como una de las estrategias contra la delincuencia trasnacional que aboga la política del presidente del Ecuador Daniel Noboa, mediante el Decreto Ejecutivo 332 de fecha 12 de julio de 2024 (Noboa Azín, 2024) , existen algunos avances que fueron introducidos mediante la Ley Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos del año 2021 (Asamblea Nacional, Ecuador, 2021) y mediante la Ley Orgánica Reformatoria a Varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral del año 2023 (Asamblea Nacional, Ecuador, 2023).

Modificaciones introducidas por la Ley Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha Contra los Delitos Informáticos.

La Ley Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha Contra los Delitos Informáticos del año 2021 (Asamblea Nacional, Ecuador, 2021) introdujo en el Código Orgánico Integral Penal figuras sustitutivas como el caso del artículo 230, el cual se tipificó como: "Interceptación ilegal de datos" (Asamblea Nacional, 2014, pág. 81), asimismo, el artículo 232, que definió como: "Ataque a la integridad de sistemas informáticos" (Asamblea Nacional, 2014, pág. 81), como artículo sustituido también estuvo el 234 que se denomina "Acceso no consentido a un sistema informático, telemático o de telecomunicaciones".

Como artículos agregados introdujo la referida norma figuras delictivas nuevas, tales como: el artículo 234.1 "Falsificación informática", (Asamblea Nacional, 2014, pág. 82) en el artículo 234.2 una regla de adecuación de la sanción que opera solo en caso de la comisión de los delitos del 232, 234 y 234 numeral 1 y donde se tenga como resultado la perturbación "de forma grave o duradera a un sistema informático que apoye una actividad destinada a asegurar funciones sociales críticas, como cadenas de abastecimiento, salud, seguridad y bienestar económico de las personas, o funcionamiento regular de los servicios públicos" (Asamblea Nacional, 2014, pág. 82).

En el artículo 234.4 del Código Orgánico Integral Penal la misma ley, introdujo definiciones coincidentes con la de la Convención de Budapest, referentes y específicamente relacionadas con los delitos informáticos, a fin de establecer las aclaraciones pertinentes y necesarias para la interpretación normativa sustantiva en este sentido. Concretamente introdujo conceptos claros sobre lo que se debe entender por "Contenido Digital", "Datos de tráfico", "Proveedores de servicios" y "Sistema informático" (Asamblea Nacional, 2014, pág. 82).

También introdujo modificaciones para el tratamiento de otros delitos que, sin ser necesariamente considerados como delitos informáticos también son una manifestación de la ciberdelincuencia puesto que se cometen con la utilización de ordenadores como, por ejemplo, la sustitución introducida por el inciso primero del artículo 103 "Pornografía con utilización de niñas, niños o adolescentes" (Asamblea Nacional, 2014, pág. 38), el delito de "Hostigamiento" (Asamblea Nacional, 2014, pág. 51) previsto en el artículo 154.2 del Código Orgánico Integral Penal y que, aunque por su naturaleza de antaño, es una conducta perturbadora de la tranquilidad emocional de las personas en la interacción con otras personas de forma física, actualmente, es cometido por cualquier persona mediante herramientas informáticas y aplicaciones, por tanto, puede tener manifestaciones de ciberdelito.

En el mismo sentido, la referida ley reformatoria introdujo la figura contravencional que denominó como: "Contravenciones de acoso escolar y académico" (Asamblea Nacional, 2014, pág. 53), la cual, similar a lo que ocurre con las anteriores, puede ser cometida por medios tecnológicos de información y comunicación. Modificó el delito de "Violencia psicológica contra la mujer o miembros del núcleo familiar" (Asamblea Nacional, 2014, pág. 54), el "Delito de acoso sexual" sustituyó el delito de "Corrupción de niños niñas y adolescentes el de "Abuso sexual" y el de "Violación" agregó el delito de "Extorsión sexual" entre otras modificaciones que, tienen

como propósito proteger a las personas de la comisión de tales infracciones con la utilización de medios informáticos, donde, por falta legislativa, antes se podía producir impunidad (Asamblea Nacional, 2014).

Modificaciones introducidas por la Ley Orgánica Reformatoria a Varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral

La Ley Orgánica Reformatoria a Varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral (Asamblea Nacional, Ecuador, 2023), al igual que la anterior, introdujo al Código Orgánico Integral Penal numerosos cambios, algunos de ellos relacionados, específicamente, con la ciberdelincuencia o, cuando sin ser figuras específicas de delitos informáticos, constituyen una forma de criminalidad digital. Por ejemplo, se introdujo una modificación al clásico delito de "Extorsión" (Asamblea Nacional, 2014, pág. 64) donde se plantea que este puede ser cometido, "inclusive a través de medios digitales, electrónicos o el uso de panfletos," lo cual, constituye una manifestación de la ciberdelincuencia.

En similar sentido se sustituyó el artículo 366 que regula la configuración jurídica del "Terrorismo" (Asamblea Nacional, 2014, pág. 122), figura que entre sus conductas plantea la comunicación o difusión de información que ponga en peligro la seguridad del trasporte terrestre, marítimo o aéreo. Esta norma jurídica introdujo como regla procesal importantísima un artículo que denominó como "Denuncia con reserva de identidad" la que, relacionado con el uso de plataformas informáticas, garantiza la reserva de la identidad de las personas que pongan en conocimiento de las autoridades la presunta comisión de delitos como "peculado, enriquecimiento ilícito, concusión, cohecho, tráfico de influencias, oferta de realizar tráfico de influencias, y testaferrismo; obstrucción de la justicia, sobreprecios en contratación pública, actos de corrupción en el sector privado" (Asamblea Nacional, 2014, pág. 140) entre otros; lo cual se realiza, o debe realizarse, en la mayoría de casos por medios informáticos o telemáticos que se implementen a tal fin, según el propio artículo 430 numeral 1 del Código Orgánico Integral Penal.

Introdujo modificaciones también en el artículo 417 del Código Orgánico Integral Penal al regular los "Registros relacionados con un hecho constitutivo de infracción" (Asamblea Nacional, 2014, pág. 153), donde se hace especial referencia a las grabaciones, fotografías y demás datos captados por un medio digital o tecnológico, lo que servirá como evidencia procesal en el esclarecimiento de los hechos objeto de imputación y prueba.

El Código Orgánico Integral Penal, dedica a partir de esta modificación una sección solo al tratamiento de los contenidos digitales, a la que denominó "Actuaciones especiales relativas a contenido digital" (Asamblea Nacional, 2014, pág. 158) y que se encuentra regulada en el artículo 477 numeral 1 y siguientes de la referida norma, entre ellas están las reglas para el aseguramiento de datos, lo que se relaciona con las disposiciones que se supone se deben regular a partir de lo convenido por el Convenio de Budapest. Asimismo, el contenido de la orden de prestación para la obtención obligada de los datos informáticos; se regula la en el 477.3 la "Búsqueda, registro, acceso y secuestro de datos informáticos" (Asamblea Nacional, 2014, pág. 158) y las reglas

para la cooperación internacional en relación con los ciberdelitos y se establecen las “Reglas para la preservación y divulgación expedita de contenido digital en la cooperación internacional" (Asamblea Nacional, 2014, pág. 159), entre otras cuestiones procesales para la investigación, persecución y sanción efectiva de la delincuencia informática.

Tabla 1. Diferencias relevantes entre el Convenio de Budapest y el Código Orgánico Integral Penal

Parámetro de comparación	Convenio de Budapest	Código Orgánico Integral Penal
Ámbito de aplicación de la norma:	Tiene un espectro de aplicabilidad en el ámbito internacional e implica que debe existir colaboración trasfronteriza.	Tiene un ámbito de aplicación nacional, con determinadas excepciones específicas dispuestas en la propia ley.
Delitos tipificados:	Ataques a sistemas informáticos, fraude informático, contenido ilícito, delitos contra la propiedad intelectual.	Regula un conjunto de infracciones enfocadas en el fraude digital, el acceso no autorizado a bases de datos e información, sabotaje por medios digitales y protección de datos estatales.
Reglas procesales para los ciberdelitos:	Establece reglas relacionadas con la conservación de datos y la regulación para su acceso, la interceptación y el registro de dichos datos.	Regula la búsqueda de datos y el secuestro de los mismos, los puntos de contacto y su interceptación.
Protección de datos personales:	Regula la protección de la integridad de datos con carácter personal pero no tiene un capítulo o sección específica para ello.	Penaliza concretamente el uso de información reservada.
Enfoque preventivo:	Promueve la colaboración, la capacitación técnica de los ciberdelitos y la armonización de estos delitos.	Se limita a la regulación normativa de las infracciones y los procedimientos.

Fuente. Elaboración propia.

Pese a que no se había ratificado hasta julio de 2024 del Convenio de Budapest para la tipificación de conductas específicas relacionadas con la ciberdelincuencia, el Código Orgánico Integral Penal ya había ido incorporando una serie de infracciones que, específicamente cumplían con sus mandatos, o sea, conductas y reglas procesales que se introdujeron mediante leyes reformatorias de los años 2021 y 2023. Estas, en alguna medida no tenían como fin específico regular los delitos informáticos, sino más bien, enfrentar la delincuencia

organizada y tipificar conductas no descritas anteriormente y que se estaban suscitando, sin embargo, fueron incluyendo y cumpliendo con los mandatos del Convenio de Budapest.

Conclusiones

1. El análisis realizado evidencia que, si bien el Código Orgánico Integral Penal (COIP) ha incorporado avances importantes en la tipificación de los delitos informáticos, persisten vacíos legales frente a nuevas formas de ciberdelitos que surgen con el desarrollo tecnológico. Esta situación limita la capacidad de respuesta del sistema penal ante conductas que aún no están claramente descritas en la norma. Por tanto, es fundamental una actualización constante de la legislación para garantizar la protección efectiva de los derechos y bienes jurídicos afectados por la criminalidad digital.

2. La comparación entre la normativa ecuatoriana y los estándares internacionales, especialmente el Convenio de Budapest, revela la necesidad de fortalecer los mecanismos de cooperación internacional y de adaptar las reglas procesales nacionales a las exigencias del contexto global. La persecución y sanción de los ciberdelitos requiere no solo de normas sustantivas adecuadas, sino también de procedimientos ágiles y compatibles con la colaboración transnacional. Esto permitirá enfrentar de manera más eficiente la naturaleza trasnacional de estos delitos.

3. El estudio identificó la importancia de establecer mecanismos de prevención general y especial que contribuyan a reducir la incidencia de los ciberdelitos. La prevención debe incluir tanto la concienciación y capacitación de los operadores de justicia como la promoción de buenas prácticas en el uso de tecnologías de la información. Asimismo, es necesario fomentar la especialización técnica y jurídica para mejorar la investigación y el enjuiciamiento de estas conductas.

4. Finalmente, se concluye que la eficacia del COIP frente a los ciberdelitos depende de su capacidad de adaptación a las nuevas realidades tecnológicas y del fortalecimiento de la formación de los actores del sistema penal. La actualización normativa, la cooperación internacional y la prevención integral son elementos clave para enfrentar los retos que plantea la ciberdelincuencia en Ecuador. Solo así se podrá garantizar una respuesta penal adecuada y el respeto a los principios de legalidad y seguridad jurídica.

Bibliografía

Acurio Del Pino, S. (s.f.). *Delitos infomáticos generalidades.* Retrieved 16 de 06 de 2025, from PUCE: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Asamblea Nacional, Ecuador. (2014). *Código Orgánico Integral Penal.* Registro Oficial Suplemento 180. Retrieved 17 de 06 de 2025, from blob:https://app.lexis.com.ec/a488ad5c-bb19-44f6-b9d3-ee7a671b388c

Asamblea Nacional, Ecuador. (2021). *Ley Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha Contra los Delitos Informáticos.* Quito: Registro Oficial Suplemento No. 526. Retrieved 18 de 06 de 2025, from https://esilecstorage.s3.amazonaws.com/biblioteca_silec/REGOFORIGINAL/2021/55D6031574DF5DA0D4E2B078F890938218B200DE.pdf

Asamblea Nacional, Ecuador. (2023). *Ley Orgánica Reformatoria a varios cuerpos legales para el fortalecimiento de las capacidades institucionales y la seguridad integral.* Quito: Registro Oficial Suplemento No. 279. Retrieved 18 de 06 de 2025, from https://esilecstorage.s3.amazonaws.com/biblioteca_silec/REGOFORIGINAL/2023/CE728FB1F6DCECA170117254D0123F9046A7D133.pdf

Barranco Torres, C. (2014). *Ciberacoso: concepto y aspectos educativos.* Retrieved 20 de 06 de 2025, from Universidad de Granada, Facultad de Ciencias de la Eduación: https://digibug.ugr.es/bitstream/handle/10481/36357/BarrancoTorres_TFG.pdf?sequence=1&isAllowed=y

Castillo Reyes, A. (17 de 02 de 2019). *Ataques Informaticos.* Retrieved 16 de 06 de 2025, from https://www.paginaspersonales.unam.mx/app/webroot/files/5810/AtaquesInformaticos.pdf

Consejo de Europa. (23 de 11 de 2001). *Convenio sobre la Ciberdelincuencia.* Retrieved 16 de 06 de 2025, from https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Ecuador. Asamblea Nacional. (2014). *Código Orgánico Integral Penal.* Quito: Registro Oficial No. 180. Retrieved 16 de 06 de 2025, from https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Hernández Díaz, L. (2009). El delito informático. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología, 23*, 227-243. Retrieved 20 de 06 de 2025, from https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

Kosinski, M. (04 de 06 de 2024). *¿Qué es el ransomware?* Retrieved 16 de 06 de 2025, from IBM: https://www.ibm.com/mx-es/think/topics/ransomware#:~:text=a%20las%20v%C3%ADctimas.-,Pagos%20de%20rescate,con%20el%2070%20%25%20en%202020.&text=Los%20expertos%20apuntan%20a%20una,posible%20motor%20de%20este%20cambio.

Loya Lasluisa, J. (08 de 2024). *Explotación de ChatGPT para la generación de ataques de Phishing.* Retrieved 16 de 06 de 2025, from Repositorio Digital Escuela Politécnica Nacional del Ecuador : https://bibdigital.epn.edu.ec/bitstream/15000/26140/1/CD%2014400.pdf

Moreno Arellano, A. (2019). *Grooming en la adolescencia.* Retrieved 20 de 06 de 2025, from Universitat Abat Oliba CEU: https://dspace.ceu.es/server/api/core/bitstreams/fa36f568-5654-4381-8811-a69a66e6bed8/content

Noboa Azín, D. (07 de 12 de 2024). *Ecuador, Decreto Ejecutivo No. 332.* Presidencia de la República del Ecuador: https://strapi.lexis.com.ec/uploads/DE_332_20240612145331_1_6683002cc1.pdf

Como citar este artículo

León Barzallo, L. S., Olmedo Reyes, A. N., & Durán Ocampo, A. R. (2025). Los delitos informáticos en el COIP y su actualización frente a nuevas formas de ciberdelitos. Revista Ciencias Holguín, *31*(4), 162-179.

Fecha de envío a revisión: 10 de septiembre de 2025

Aprobado para publicar: 20 de noviembre de 2025