

UNIVERSIDAD DE ESPECIALIDADES ESPÍRITU SANTO

FACULTAD DE DERECHO, POLÍTICA Y DESARROLLO

TÍTULO: LA EXTORSIÓN DIGITAL EN EL COIP Y LOS VACÍOS EN SU PERSECUCIÓN PROCESAL EN ECUADOR

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

NOMBRE DEL ESTUDIANTE:

JUAN FRANCISCO SEGURA PALMA

NOMBRE DEL TUTOR:

AB. ENRIQUE EFRAÍN ARGÜELLO ARELLANO, MSC.

SAMBORONDÓN, MAYO, 2026

LA EXTORSIÓN DIGITAL EN EL COIP Y LOS VACÍOS EN SU PERSECUCIÓN PROCESAL EN ECUADOR

CARTA DE APROBACIÓN DEL TUTOR

En mi calidad de tutor de **JUAN FRANCISCO SEGURA PALMA**, estudiante de la Facultad de Derecho, Política y Desarrollo de la Universidad de Especialidades Espíritu Santo,

CERTIFICO

Que, una vez analizado el trabajo de titulación titulado **"LA EXTORSIÓN DIGITAL EN EL COIP Y LOS VACÍOS EN SU PERSECUCIÓN PROCESAL EN ECUADOR"**, presentado como requisito previo a obtener el grado de Abogado, el mismo cumple con los requisitos y méritos académicos, razón por la cual lo **APRUEBO** en su totalidad.

AB. ENRIQUE EFRAÍN ARGÜELLO ARELLANO, MSC.

TUTOR

LA EXTORSIÓN DIGITAL EN EL COIP Y LOS VACÍOS EN SU PERSECUCIÓN PROCESAL EN ECUADOR

INFORMACIÓN DEL AUTOR

Apellidos y nombres: Segura Palma, Juan Francisco

Universidad de Especialidades Espíritu Santo – Ecuador (UESS)

Correo institucional: juanfransegura@uees.edu.ec

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

DEDICATORIA

El presente trabajo está dedicado a mi familia, quienes han sido el soporte fundamental en cada etapa de mi formación académica y personal. A mis padres, por su esfuerzo constante, sacrificio y apoyo incondicional. A quienes creyeron en mí incluso en los momentos de mayor dificultad. Este logro representa no solo una meta profesional, sino también el resultado del respaldo emocional y moral que siempre me brindaron.

JUAN FRANCISCO SEGURA PALMA

AGRADECIMIENTOS

Expreso mi sincero agradecimiento a la Universidad de Especialidades Espíritu Santo y a la Facultad de Derecho, Política y Desarrollo, por la formación académica impartida durante estos años. A mi tutor, MGS Efraín Arguello Arellano, por su orientación técnica y acompañamiento constante en el desarrollo de esta investigación. Asimismo, agradezco a todos los docentes que contribuyeron a fortalecer mi criterio jurídico.

JUAN FRANCISCO SEGURA PALMA

LA EXTORSIÓN DIGITAL EN EL COIP Y LOS VACÍOS EN SU PERSECUCIÓN PROCESAL EN ECUADOR

Resumen

La extorsión digital se ha consolidado como amenaza creciente, aprovechando el anonimato, la rápida circulación de datos y la capacidad transfronteriza de internet para coaccionar, manipular o explotar a las víctimas. La presente investigación se ha propuesto analizar el marco procesal penal ecuatoriano para la eficaz persecución del delito de extorsión digital. El enfoque utilizado es cualitativo; se emplearon los métodos de análisis-síntesis, exegético y comparativo, con apoyo en la técnica de revisión documental para todos ellos. Se advierte que Ecuador ha actualizado parcialmente la norma sustantiva, pero continúa aplicando estructuras procesales tradicionales a fenómenos tecnológicos complejos, con lo cual se limita la persecución efectiva de la extorsión digital. Destaca positivamente la adopción del Convenio de Budapest que abre espacio para varias figuras en materia de cooperación internacional. En esencia, se concluye que es necesaria una reforma puntual del COIP que incorpore los estándares de conservación urgente de los datos, los protocolos de extracción forense y el incremento de mecanismos colaborativos bilaterales e internacionales.

Palabras clave: Extorsión digital, persecución penal, cooperación internacional, evidencia digital.

LA EXTORSIÓN DIGITAL EN EL COIP Y LOS VACÍOS EN SU PERSECUCIÓN PROCESAL EN ECUADOR

Abstract

Digital extortion has consolidated itself as a growing threat, exploiting anonymity, the rapid circulation of data, and the cross-border capacity of the internet to coerce, manipulate, or exploit victims. This research set out to analyze the Ecuadorian criminal procedural framework for the effective prosecution of the crime of digital extortion. A qualitative approach was used; the methods of analysis–synthesis, exegetical interpretation, and comparative analysis were applied, all supported by documentary review techniques. The study shows that Ecuador has partially updated its substantive criminal law but continues to apply traditional procedural structures to technologically complex phenomena, thereby limiting the effective prosecution of digital extortion. A positive development is the adoption of the Budapest Convention, which opens the door to several mechanisms of international cooperation. In essence, the research concludes that a targeted reform of the COIP is necessary, one that incorporates urgent data-preservation standards, forensic extraction protocols, and enhanced bilateral and international cooperation mechanisms.

Keywords: Digital extortion, criminal prosecution, international cooperation, digital evidence.

LA EXTORSIÓN DIGITAL EN EL COIP Y LOS VACÍOS EN SU PERSECUCIÓN PROCESAL EN ECUADOR

Índice

Introducción 8

1. La extorsión digital en el COIP: análisis del tipo penal 11

2. El problema de la aplicación territorial de la ley penal frente a la extorsión digital 14

3. Otras dificultades procesales en la persecución de la extorsión digital 17

3.1. La cadena de custodia y la extracción de la evidencia digital 18

3.2. Anonimato tecnológico 19

3.3. Transnacionalidad y barreras de cooperación internacional 21

Conclusiones 22

Recomendaciones 24

Bibliografía 26

LA EXTORSIÓN DIGITAL EN EL COIP Y LOS VACÍOS EN SU PERSECUCIÓN PROCESAL EN ECUADOR

Introducción

La expansión acelerada de las tecnologías digitales ha reconfigurado profundamente la manera en que interactúan las personas, las empresas y las instituciones públicas. Hoy, una porción esencial de las actividades humanas – desde la comunicación interpersonal y las operaciones financieras hasta la gestión documental y los trámites administrativos, por solo citar algunas – se realiza en entornos conectados[1]. Sin embargo, esta misma infraestructura digital también genera condiciones para la aparición de modalidades delictivas más sofisticadas. Dentro de este contexto, la extorsión digital se ha consolidado como amenaza creciente, aprovechando el anonimato, la rápida circulación de datos y la capacidad transfronteriza de internet para coaccionar, manipular o explotar a las víctimas[2]. Tradicionalmente este delito se concebía como una conducta en la cual el agresor ejercía violencia o intimidación de manera directa sobre la víctima, generalmente mediante amenazas físicas o presenciales con la finalidad de obtener un beneficio económico[3]. En la actualidad, esa lógica se ha trasladado al espacio digital, donde la intimidación se produce mediante correos electrónicos, plataformas de mensajería instantánea, redes sociales, accesos ilícitos a bases de datos, cifrado malicioso de información o amenazas de divulgación de contenido privado[4].

---

[1] BATALLAN, Ana Belén et al., "Gobernanza en la era meta: retos y desafíos para el sector público" en BONIFACIO, José Alberto (comp.) y SAGALSKY, Ruth Sofía (comp.), *El Estado y la Administración Pública en debate: encrucijadas y desafíos para el desarrollo. Memorias del IV Congreso Nacional de Estudios de Administración Pública*, vol. 2, 2024.

[2] LOZANO DOMÍNGUEZ, Valle, "Ciberterrorismo en el siglo XXI" en *CEU Universidad San Pablo*, 2025, URL https://dspace.ceu.es/server/api/core/bitstreams/6997d195-a853-413d-b847-af7dd49c52e0/content consultado 05/05/2026.

[3] Art. 185 Código Orgánico Integral Penal, 28 de enero de 2014 (Registro Oficial Suplemento No. 180, de 10 de febrero de 2014) (COIP).

[4] HERRERA SEGUEL, Marta y ORTIZ PULGAR, Ymay, *Criminalidad informática y ciberdelincuencia*, 2024.

Esta nueva realidad ha obligado a los ordenamientos jurídicos a replantear sus categorías tradicionales. En el caso ecuatoriano, la reforma de marzo de 2023 al artículo 185 del Código Orgánico Integral Penal (en adelante, COIP) constituyó un avance relevante, al reconocer expresamente que la violencia o intimidación pueden ejercerse por cualquier medio, incluidos los digitales y electrónicos[5]. Esta modificación resolvió parcialmente la discusión doctrinal sobre la adecuación típica de la extorsión cometida en entornos virtuales.

No obstante, configurar una infracción penal no garantiza *per se* la eficacia persecutoria. El problema no reside únicamente en la tipicidad, sino en la insuficiencia del marco procesal para investigar, preservar, autenticar y judicializar evidencia digital[6], además del eventual obstáculo de la territorialidad en la aplicación de la ley, que se complica por el carácter transfronterizo que puede adoptar la extorsión digital[7]. Es por ello que se plantea como hipótesis que Ecuador ha actualizado parcialmente la norma sustantiva, pero continúa aplicando estructuras procesales tradicionales a fenómenos tecnológicos complejos, con lo cual se limita la persecución efectiva de la extorsión digital.

En consecuencia, surge una interrogante central: ¿es suficiente el marco procesal ecuatoriano para enfrentar de manera efectiva la extorsión digital, o persisten vacíos normativos que generan impunidad? La presente investigación sostiene

[5] Art. 43 Ley Orgánica Reformatoria a Varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral, 7 de marzo de 2023 (Registro Oficial Suplemento No. 279, 29 de marzo de 2023) (LORVCL).

[6] ORTIZ NIVELA, Milza Naomi et al., "Insuficiente regulación de la prueba digital y su valoración en el proceso penal" en *593 Digital Publisher CEIT*, vol. 10, No. 4, 2025, DOI https://doi.org/10.33386/593dp.2025.4.3399 consultado 05/05/2026.

[7] QUEZADA QUIZHPE, Alex Benjamín y GENDE RUPERTI, Carla Guadalupe, "Delito de Ciberextorsicion: Un Análisis Jurídico, y Comparativo en País de Latinoamérica, Perú, Colombia y Ecuador" en *593 Digital Publisher CEIT*, vol. 10, No. 1, 2025, DOI https://doi.org/10.33386/593dp.2025.1.2893 consultado 05/05/2026.

que, si bien la reforma al artículo 185 del COIP fue necesaria, la falta de regulación especializada en materia probatoria, tecnológica, además de la multidimensionalidad en la comprensión del fenómeno, limita severamente la capacidad del sistema penal para responder ante esta modalidad delictiva.

El objetivo general de este trabajo es: analizar el marco procesal penal ecuatoriano para la eficaz persecución del delito de extorsión digital. Para alcanzarlo, se han trazado los siguientes objetivos específicos: 1) describir los elementos del tipo penal de la extorsión digital en el COIP; 2) determinar los límites de la aplicación territorial de la ley penal en relación con el delito de extorsión digital; 3) establecer las dificultades procesales actuales para la persecución efectiva de las modalidades de extorsión digital; y 4) proponer los fundamentos de una reforma normativa procesal integral para la perseguibilidad del delito de extorsión digital.

El estudio exige un enfoque cualitativo porque el problema no se reconduce hacia la medición de la frecuencia del delito u otras tendencias, sino a comprender la estructura jurídico-procesal que limita su persecución efectiva. La hipótesis requiere un análisis profundo de los significados normativos, de las interpretaciones doctrinales y de las prácticas procesales, razón por la cual el método de análisis-síntesis es eficaz para descomponer dichas aristas del problema e integrarlas luego en una comprensión sistemática del asunto procedimental.

En función de lo expuesto, el método exegético es indispensable para interpretar el alcance del artículo 185 del COIP, las reglas de aplicación territorial de la ley penal y las normas procesales relativas a las evidencias digitales. De esa forma, se pueden identificar tensiones, vacíos y contradicciones relevantes. El carácter

complejo del delito de extorsión digital justifica también el empleo del método comparativo para examinar cómo otros sistemas jurídicos han abordado el fenómeno y, en especial, problemas como la cadena de custodia digital, la cooperación internacional, la autenticación de datos electrónicos, entre otros.

La combinación de tales métodos no busca cuantificar diferencias, sino interpretar cómo tales hallazgos pueden asimilarse en el ordenamiento penal ecuatoriano. Al sintetizar las ideas, podrán abordarse los fundamentos de una reforma normativa procesal integral para la perseguibilidad del delito de extorsión digital. En todo este contexto, la técnica de revisión documental es la idónea para garantizar la revisión contextualizada de normas, doctrina y otros criterios relacionados con el objetivo central de la investigación.

1. La extorsión digital en el COIP: análisis del tipo penal

La reforma del artículo 185 del COIP introdujo una diferenciación explícita entre la extorsión tradicional y la digital. Mientras la extorsión clásica se estructura sobre la coacción directa a través de amenazas físicas, patrimoniales o reputacionales, la extorsión digital introduce medios tecnológicos como canales para ejercer la ilícita presión sobre la víctima[8]. Esta separación normativa obedece a la creciente sofisticación de los ciberdelitos y a la necesidad de adaptar el derecho penal a un entorno donde el potencial anonimato, la velocidad de difusión y la internacionalización del internet amplifican la capacidad lesiva del comisor.

Retomando la extorsión en su modalidad tradicional, el núcleo del injusto aquí es el uso de la violencia o intimidación para compeler a la víctima a que haga u

[8] CORDOVA SAINT-PERE, Jilmar Moises, "Análisis de la situación actual del delito de extorsión y los medios digitales en la legislación peruana" en *Fides Et Ratio*, vol. 31, 2026, DOI https://doi.org/10.55739/fer.187 consultado 05/05/2026.

omita un acto que derive en un perjuicio patrimonial para sí o para otro. Se recurre a la instrumentalización del miedo como mecanismo para doblegar la voluntad ajena. Suele haber una relación interpersonal más o menos directa en la que el agresor presiona mediante la inminencia de un daño que es generalmente verificable y se localiza en un espacio concreto[9].

Ahora bien, las incorporaciones al COIP en el 2023 sobre la extorsión digital sugiere que no se agota en una variante comisiva adicional a las tradicionales, sino que tiene elementos propios que le son intrínsecos. En principio, el tipo penal incorpora la utilización de medios electrónicos, informáticos, telemáticos o de naturaleza similar como instrumentos para ejecutar la amenaza, lo que supone nuevas formas de la coacción. Entre estas, proliferan la posible difusión de imágenes íntimas, la manipulación de datos, el acceso no autorizado a cuentas bancarias o en redes sociales, la suplantación de identidad, entre otras[10]. La doctrina comparada sostiene que la extorsión digital opera en un ecosistema donde la asimetría de la información y la capacidad de daño a la reputación son exponencialmente mayores que en la extorsión clásica[11].

Una diferencia estructural significativa entre ambas modalidades es el anonimato del comisor en ciertos casos. Mientras la extorsión tradicional suele implicar un agresor físicamente localizable, el extorsionista digital puede ocultar su identidad mediante red privada virtual (VPN, por sus siglas en inglés), cuentas falsas o

[9] NÁJERA GONZÁLEZ, Xavier, "Breve estudio dogmático del delito de extorsión en el Código Penal del Estado de Puebla, México" en *Nuevo Foro Penal*, No. 100, 2023, DOI https://doi.org/10.17230/nfp19.100.1 consultado 05/05/2026.

[10] GRAHAM, Roderick S. y SMITH, Shawn K., *Cybercrime and Digital Deviance*, 2da ed., 2024, URL https://dokumen.pub/download/cybercrime-and-digital-deviance-9781032254524-9781032249193-9781003283256.html consultado 05/05/2026.

[11] LINDSAY, Jon R., "Stuxnet and the Limits of Cyber Warfare" en *Security Studies*, vol. 22, No. 3, 2013, DOI https://doi.org/10.1080/09636412.2013.816122 consultado 05/05/2026.

servidores ubicados en otros países. Esta característica altera la dinámica del delito, pues la víctima no solo enfrenta la amenaza, sino la incertidumbre sobre quién la formula.

En su variante relacionada con la amenaza de divulgar actos, imágenes u otras informaciones relacionadas con el ámbito de la sexualidad de la víctima si no se cumple con la entrega de dinero o bienes, o realiza o se abstiene de realizar determinado acto, la doctrina comparada ha reconocido que el anonimato que puede rodear al responsable dificulta la imputación penal y exige técnicas de investigación especializadas[12]. Esta figura está incorporada implícitamente en el artículo 185 del COIP, a diferencia del delito de extorsión sexual, que se refiere a la incitación o coacción para que la víctima ejecute conductas de exhibicionismo sexual a cambio de un provecho personal para el agente extorsivo o para otro[13].

El artículo 185 del COIP también supone la posibilidad de que la extorsión digital pueda adoptar un carácter transfronterizo, pues agrava la medida de la pena cuando el delito "… se comete total o parcialmente desde el extranjero[14]". Así, la amenaza puede originarse en otro país, circular por servidores foráneos o involucrar plataformas globales[15]. Esta modalidad genera problemas competencia territorial, como se analizará en el apartado 2 más adelante. Si bien la reforma adoptada reconoce esa realidad, no desarrolló mecanismos procesales específicos para enfrentarla, lo que limita la eficacia del tipo penal.

No escapa tampoco a la configuración de la extorsión en su modalidad digital que

[12] ALONSO RUIDO, Patricia et al., "Sextorsión: una estrategia de violencia sexual online en el estudiantado universitario" en *Pedagogía Social*, No. 45, 2024, URL http://recyt.fecyt.es/index.php/PSRI/ consultado 05/05/2026.
[13] Art. 172.1. COIP.
[14] Art. 185, inciso tercero, numeral 4 COIP.
[15] GRAHAM & SMITH, *Cybercrime and Digital Deviance*, p. 7.

puede confluir con otras conductas relacionadas con el cibercrimen, como el acceso no autorizado a bases de datos o la violación de la privacidad de otros datos personales. Estas dudas interpretativas se acentúan cuando se aprecia la concurrencia de dichas figuras, de manera que en ocasiones hay que resolver si la conducta es de medio a fin, o si está incluida entre los elementos del mismo delito, o si hay simplemente concurso real[16].

En síntesis, los elementos del tipo penal con sus peculiaridades son los siguientes: a) el sujeto activo puede ser cualquier persona, sin cualidad especial; b) el sujeto pasivo es aquella persona cuya libertad de autodeterminación y cuyo patrimonio resultan afectados por la amenaza; c) es pluriofensivo porque ataca simultáneamente el patrimonio y la libertad individual[17]; d) la conducta consiste en exigir u obligar con violencia o intimidación a una persona para obtener un beneficio económico o de otro tipo; e) el núcleo del injusto es la amenaza, que debe ser idónea y seria, capaz de generar coacción en la víctima; f) el elemento subjetivo es de dolo directo; g) el medio comisivo es de naturaleza digital (sistemas informáticos, redes sociales, mensajería electrónica, etc.); h) es de consumación anticipada, pues no requiere la entrega efectiva del beneficio injustamente solicitado por el agresor.

2. El problema de la aplicación territorial de la ley penal frente a la extorsión digital

El COIP establece el principio de territorialidad como regla general, de modo que

[16] POSADA MAYA, Ricardo, "El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual" en *Nuevo Foro Penal*, vol. 13, No. 88, 2017, URL https://dialnet.unirioja.es/descarga/articulo/6074006.pdf consultado 05/05/2026.

[17] FERNÁNDEZ CHOLOQUINGA, Luis Miguel y MONTALVO RAMOS, Fernández Andrés, "Análisis jurídico de las formas y medios de extorsión en el Ecuador", *Polo del Conocimiento (Edición núm. 117*), vol. 11, No. 4, 2026, DOI https://doi.org/10.23857/pc.v11i4.11475 consultado 05/05/2026.

la ley penal ecuatoriana se aplica a los delitos cometidos en el territorio nacional[18]. Sin embargo, la extorsión digital que se configura a partir del artículo 185 del propio Código introduce un desafío de aplicación, pues el delito puede involucrar servidores informáticos en el extranjero y/o el agresor puede hallarse fuera del Ecuador. La doctrina advierte que los ciberdelitos, en general, erosionan el criterio de perseguibilidad del lugar de la comisión y obligan a los sistemas penales a reinterpretar la territorialidad para no generar espacios de impunidad[19]. El COIP también prevé su aplicación cuando la infracción, aun cometida fuera del país, produce efectos en él o en los lugares sometidos a su jurisdicción[20]. Esta previsión es muy importante para el delito de extorsión digital, pues aunque el agresor no se encuentre en Ecuador físicamente, la amenaza se materializa donde esté la víctima, además del daño reputacional y/o los efectos patrimoniales para ella. Comenta VELASCO NÚÑEZ que, en la jurisprudencia española, los delitos cometidos a través de medios informáticos otorgan competencia al juzgador "… en todos y cada uno de los sitios donde se manifiestan sus efectos, lo que incluye tanto el lugar de la acción como el del resultado[21]". Este criterio parece replicarse favorablemente en el artículo citado.

De esta forma, basta que uno de los elementos del *iter criminis* ocurra en Ecuador para que la jurisdicción territorial se active frente al delito de extorsión digital. Se amplía la noción de ejecutividad del ilícito más allá de la frontera, siempre que la

[18] Art. 14.1. COIP.
[19] HILDEBRANDT, Mireille, *Law for Computer Scientists and Other Folk*, 2020.
[20] Art. 14.2. a) COIP.
[21] VELASCO NÚÑEZ, Eloy, *Aspectos procesales de la investigación y de la defensa de los delitos informáticos*, 2021, URL https://web.icam.es/bucket/Aspectos%20Procesales%20de%20la%20Investigacion%20y%20Defensa%20Delitos%20Informaticos.pdf consultado 06/05/2026.

víctima sí se encuentre en territorio nacional. No obstante la doctrina y la jurisprudencia no son pacíficas en cuanto a la competencia territorial en cuanto a los delitos cometidos a través de internet o por medios digitales. En otras jurisdicciones, como la española, a veces se ha utilizado la teoría de la actividad para determinar la competencia en función del lugar donde se ejecutan los actos que originan el núcleo de la conducta típica; sin embargo, en otros casos se atiende a la teoría del resultado[22], que es más afín al artículo 14.2. a) del COIP. Sin embargo, cuando el agente comisor se encuentra en el extranjero, mucho dependerá la legislación del otro país para asegurar que se cumpla con el juzgamiento en Ecuador. Esto no solo depende de la necesidad de activar un proceso de extradición, sino de la posibilidad real que el otro país considere que es el competente para incoar la causa porque prevalece el criterio de la actividad en lugar del de resultado. Ese supuesto bien pudiera resolverse con la alternativa que plantea el artículo 14.2. b) del COIP, que condiciona la aplicación de la ley penal ecuatoriana a este tipo de conductas si la infracción no haya sido juzgada en el país donde se cometió[23].

El precepto anterior puede generar contradicciones insalvables. Por ejemplo, la falta de activación oportuna de los mecanismos de investigación penal en el extranjero o la dilación en su desarrollo pueden provocar la prescripción de la acción en Ecuador. También la decisión judicial en el exterior puede conducir a un sobreseimiento que, aunque parezca injusto, es improbable que pueda activar

[22] ORTIZ PRADILLO, Juan Carlos, "Determinación de la jurisdicción y competencia para la investigación y enjuiciamiento de los daños informáticos", en *Centro de Estudios Jurídicos del Ministerio de Justicia*, 2016, URL https://www.cej-mjusticia.es/sede/publicaciones/ver/11317 consultado 06/05/2026.
[23] Art. 14.2. b) COIP.

la jurisdicción ecuatoriana en virtud del principio constitucional de *non bis in idem*[24].

Luego, es notorio que, si bien el artículo 14 del COIP permite afirmar la jurisdicción en Ecuador cuando el comisor se encuentra en el extranjero, basado en el criterio del resultado, la persecución efectiva dependerá de la cooperación internacional para obtener las evidencias digitales, identificar al agresor y acceder a registros de la información en terceros países, como se verá en el apartado siguiente. En general, el criterio de aplicación territorial de la ley penal debe ser flexible en estos casos, para poder lograr la eficaz protección de los derechos de las víctimas de este tipo de delitos.

3. Otras dificultades procesales en la persecución de la extorsión digital

La persecución procesal de la extorsión digital enfrenta un conjunto de obstáculos estructurales que derivan de las limitaciones que impone el sistema jurídico para operar en entornos tecnológicos complejos y cambiantes. La volatilidad de la evidencia digital, la ausencia de protocolos especializados de extracción y preservación, el anonimato tecnológico y financiero que caracteriza a los agresores y la transnacionalidad como rasgo distintivo eventualmente, configuran escenarios de dificultad práctica. Estos factores, combinados con la fragmentación normativa internacional y la lentitud de los mecanismos tradicionales de cooperación, revelan que la eficacia del artículo 185 del COIP depende menos de su formulación sustantiva y más de la capacidad del Estado para adaptar sus herramientas procesales a la dinámica propia de los delitos cometidos en el ciberespacio.

[24] Art. 76.7. i) Constitución de la República del Ecuador (Registro Oficial No. 449 de 20 de octubre de 2008) (CRE).

3.1. La cadena de custodia y la extracción de la evidencia digital

El COIP tiene una lógica probatoria mayormente analógica, lo que es especialmente apreciable en el artículo 456 sobre la cadena de custodia. Esta viene diseñada para objetos físicos (armas, documentos, materiales, etc.)[25], pero la evidencia digital, en cambio, se compone de datos volátiles, replicables y fácilmente alterables, cuya integridad depende de metadatos y de procedimientos forenses especializados[26].

Al no existir una regulación específica para la recolección, preservación y/o autenticación de la evidencia digital se genera un vacío crítico. Los fiscales carecen de un marco normativo que establezca cómo debe actuarse desde el primer momento, o sea, cuando reciben la *notitia criminis*. Esta brecha ha sido expuesta por la propia Fiscalía General del Estado en informes técnicos, donde se advierte que la falta de protocolos estandarizados provoca exclusiones probatorias frecuentes[27].

En la práctica, se suelen excluir capturas de pantallas, impresiones de chats o archivos extraídos sin el debido peritaje forense. Ello se debe a que en su materialización se carecen de garantías de autenticidad. La evidencia digital debe cumplir estándares de integridad y trazabilidad. Las reformas introducidas en el año 2023, si bien incorporaron actuaciones especiales relativas al contenido digital[28], no cerraron todas las brechas existentes al respecto.

---

[25] Art. 456 COIP.

[26] OCHOA ARÉVALO, Paúl A., "El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación" en *Economía y Política*, No. 28, 2018, DOI https://doi.org/10.25097/rep.n28.2018.03 consultado 06/05/2026.

[27] SALAZAR MÉNDEZ, Diana, "El rol de la administración de justicia y la cooperación internacional en la lucha contra la ciberdelincuencia", *Revista Perfil Criminológico*, 2021, URL https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf consultado 06/05/2026.

[28] Art. 66 LORVCL.

En realidad, el procedimiento de extracción de evidencia digital es complejo: a) requiere de imagen forense o adquisición *bit* a *bit* porque no se trabaja con el dispositivo original, sino una copia exacta clonada con bloqueadores de escritura; b) cálculo de *hash* o establecimiento de la huella digital única del dispositivo original y su copia a través de algoritmos criptográficos; c) preservación de *logs* o registros automáticos de actividades en los sistemas; d) extracción de metadatos, que implica el análisis de la información oculta para la contextualización del archivo y verificación de trazabilidad; y, e) documentación detallada de cada manipulación hasta llegar a la fase final[29]. En Colombia, por ejemplo, estos protocolos se aplican con rigidez y existen laboratorios forenses especializados a ese fin[30].

3.2. Anonimato tecnológico

Otra gran barrera procesal es la incapacidad del sistema penal para romper el anonimato tecnológico. Sucede que los extorsionadores utilizan VPN, redes de código abierto, correos cifrados y hasta servidores *offshore* para ocultar su dirección IP y ubicación real. Las herramientas tradicionales de investigación como el rastreo de las comunicaciones son inútiles frente a estas sofisticadas formas de ejecución. La doctrina forense más aceptada en el ámbito anglosajón plantea que los sistemas penales deben incorporar técnicas avanzadas de trazabilidad digitales y nuevas facultades judiciales para la intervención

[29] Fundación Panamericana para el Desarrollo, *Guía técnica sobre análisis forense y evidencia digital. Proyecto de creación de capacidades del sector judicial ecuatoriano para combatir la delincuencia transnacional y el narcotráfico*, 2026, URL https://oeco.padf.org/wp-content/uploads/2026/01/6.-GUIA-TECNICA-SOBRE-ANALISIS-FORENSE-Y-EVIDENCIA-DIGITAL.pdf consultado 06/05/2026.

[30] BELTRÁN HERNÁNDEZ, César Ramiro y PERDOMO MÉNDEZ, Juan Sebastián, *Diseño e implementación de un Piloto de Laboratorio Forense Especializado en Respuesta a Incidentes de ciberseguridad para una Entidad Pública del Distrito de Bogotá*, 2024.

telemática[31].

Más complejo aún resulta cuando la intervención debe hacerse a través los servidores en la nube, las redes sociales o las plataformas de mensajería cifrada[32]. La complejidad aquí se acentúa por la combinación de barreras técnicas con los marcos legales transnacionales. Por ejemplo, los proveedores de servicios de mensajería cifrada (*Whatsapp*, *Telegram*, etc.) a menudo no pueden entregar el contenido de los mensajes porque no tienen acceso a las claves de cifrado de los usuarios de punto a punto; asimismo, los datos almacenados en servidores en la nube (*Google*, *Microsoft*, etc.) suelen estar físicamente disponibles en un tercer país ajeno al conflicto entre las partes del proceso penal, lo que complica la obtención de pruebas.

La extorsión digital contemporánea también puede exigir el pago en criptomonedas (*Bitcoin*, etc.). Estas transacciones se realizan a través de las llamadas "billeteras frías" o direcciones no vinculadas a identidades verificadas (*non-KYC wallets*), por lo que su seguimiento requeriría mecanismos de rastreo que dependen de entes externos[33]. La combinación del anonimato financiero y el tecnológico es uno de los principales factores que dificulta la persecución de la extorsión digital en América Latina y Europa[34].

---

[31] KOOPS, Bert-Jaap y ROBINSON, Tessa, "Cybercrime Law. A European Perspective" en CASEY, Eoghan (Ed.), *Digital Evidence and Computer Crime*, 3ra ed., 2011.

[32] RODRÍGUEZ, Gladys Stella, "Privacidad y seguridad en la nube: algunas implicaciones jurídico-económicas desde el comercio electrónico transfronterizo" en *Lex – Revista de la Facultad de Derecho y Ciencias Políticas*, vol. 18, No. 25, 2020, https://doi.org/10.21503/lex.v18i25.2109 consultado 06/05/2026.

[33] MAIMAI, Lee, *No KYC Crypto Wallets: Privacy, Open-Source, and Self-Custody Explained*, 2025, URL https://onekey.so/blog/es/ecosystem/no-kyc-crypto-wallets-privacy-open-source-and-self-custody-explained/?srsltid=AfmBOooPKDR0I6YtQzJsEfHbT6a0TMMU6mLff6qdwf5RSrqPzK4Sg1od consultado 06/05/2026.

[34] LLAMAS COVARRUBIAS, Jersain Zadamig y MOLINÉ RODRÍGUEZ, César, "Ciberseguridad en América Latina y el Caribe: hacia una arquitectura legal y un marco común" en *EU Cyber Net*,

Es claro entonces que la prueba de la finalidad extorsiva depende de la reconstrucción del *iter criminis* digital. La extorsión usualmente adopta la forma de varios mensajes sucesivos, instrucciones de pago, enlaces a billeteras de criptomonedas u otras variantes que, sin protocolos de preservación de la evidencia digital, provoca su descarte como elemento probatorio. En especial, dentro del contexto analizado, la falta de trazabilidad afecta la tipicidad subjetiva y, por ende, la imputación concreta a una persona.

3.3. Transnacionalidad y barreras de cooperación internacional

Como ya se ha esbozado, la extorsión digital suele ejecutarse desde servidores ubicados en el extranjero, por lo que una investigación efectiva requiere de la cooperación de uno o más países más allá de aquel donde se investiga el delito de extorsión digital. Los mecanismos de cooperación penal internacional son generalmente lentos y burocráticos. En delitos cometidos a través de medios digitales, los datos pueden eliminarse en cuestión de horas, por lo que la evidencia es difícil de obtener.

El Convenio sobre la Ciberdelincuencia o Convenio de Budapest, adoptado por la Unión Europea en 2001[35], contiene mecanismos de cooperación rápida aplicables dentro de la región. Ecuador actualmente es parte activa, pues desde el 12 de diciembre de 2024 lo suscribió y depositó oficialmente el instrumento de adhesión, aprovechando esta posibilidad que dicho cuerpo de derecho internacional permitía[36]. Dicho Convenio regula detalladamente el registro de

2026, URL https://www.eucybernet.eu/wp-content/uploads/2026/01/ciberseguridad-en-america-latina-y-el-caribe.pdf consultado 06/05/2026.

[35] Consejo de Europa, Convenio sobre la Ciberdelincuencia, 23 de noviembre de 2001 (Serie de Tratados Europeos No. 185, 3 de diciembre de 2001) (Convenio de Budapest).

[36] Ministerio de Relaciones Exteriores y Movilidad Humana, "Depósito del instrumento de ratificación del Convenio de Budapest" en *Cancillería del Ecuador*, 2024, URL

dispositivos electrónicos, la intervención de comunicaciones telemáticas, la figura del agente encubierto informático, las órdenes para la conservación rápida de los datos y el acceso remoto, entre otras variantes dirigidas al aseguramiento de la información digital.

No es difícil percatarse que – con la salvedad de los suscriptores del Convenio de Budapest – cada país puede tener reglas distintas sobre retención de datos, privacidad, acceso a la información digital, entre otras. La falta de armonización normativa es, entonces, uno de los principales factores que puede atentar contra la perseguibilidad de la extorsión digital. Incluso, los proveedores de servicios digitales operan con sujeción a reglas diferentes en función del país donde cuenten con sus servidores o centros de gestión de servicios.

Asimismo, muchos países solo colaboran si la conducta investigada es un delito homologable en ambas jurisdicciones, pero la extorsión digital no siempre se tipifica igual y, además, posee una multiplicidad de formas de manifestarse. Esta disparidad puede provocar que las solicitudes de cooperación internacional sean rechazadas al no cumplir con el principio de la doble incriminación[37]. La falta de acuerdos bilaterales específicos es un obstáculo aun cuando se cuenta con tratados generales de asistencia penal debido a las peculiaridades de los delitos que involucran evidencias digitales.

Conclusiones

El estudio del artículo 185 del COIP demuestra que la extorsión digital posee elementos típicos propios. Destaca lo relativo al medio comisivo digital, la

https://www.cancilleria.gob.ec/2024/12/13/deposito-del-instrumento-de-ratificacion-del-convenio-de-budapest/ consultado 06/05/2026.

[37] GERCKE, Marco, *Understanding Cybercrime: A Guide for Developing Countries*, 2011, 2da ed.

idoneidad de la amenaza y la posibilidad de anonimato del agresor. El tipo penal es adecuado desde una perspectiva dogmática pues identifica con sus elementos esenciales a la conducta, protege bienes jurídicos relevantes y no limita la pluralidad de formas en las que puede darse la coacción digital. Sin embargo, la eficacia de la punición dependerá de la capacidad procesal para acreditar la amenaza, su origen y la finalidad extorsiva.

En general, el COIP cuenta con bases normativas suficientes para afirmar jurisdicción sobre casos de extorsión digital cuando los efectos del delito se producen en el país. No obstante, el carácter transnacional del fenómeno, la fragmentación normativa internacional y la dependencia de la cooperación extranjera pueden dificultar la aplicación efectiva de este criterio, pues las evidencias pueden estar alojadas en servidores, bases de datos o sistemas foráneos. La territorialidad formal es adecuada, pero su operatividad práctica se autolimita sin mecanismos ágiles de cooperación y protocolos claros de preservación de la evidencia digital.

Se han identificado dificultades procesales como la existencia de una cadena de custodia normalmente analógica y la falta de protocolos de extracción forense. Los problemas relacionados con el anonimato tecnológico y financiero del comisor, la volatilidad de la evidencia y la relativa lentitud de la cooperación internacional son barreras estructurales que impiden la persecución efectiva del delito investigado. Destaca, sin embargo, la adhesión plena de Ecuador al Convenio de Budapest, con lo cual la cooperación con países de la Unión Europea y demás signatarios externos se refuerza.

La eficacia de la persecución del delito de extorsión cometido a través de medios

digitales depende de herramientas procesales flexibles y actualizadas. Por ello, es indispensable proceder a una reforma puntual del COIP que incorpore los estándares de la evidencia digital, las facultades de investigación telemática, los mecanismos de conservación urgente de los datos, los protocolos de extracción forense y el incremento de la cooperación internacional. La acreditación de los elementos típicos del delito, la identificación del autor y la reconstrucción del *iter criminis* digital dependen de ello en la práctica.

Recomendaciones

A fin de lograr que los hallazgos de la investigación se traduzcan en una propuesta concreta, es necesario elaborar un proyecto de ley orgánica reformatoria que considere modificaciones integrales en cada ámbito donde se detectaron falencias. De modo sintético se presentan las bases sobre las cuales puede construirse dicho proyecto:

1) Añadir a las actuaciones especiales relativas al contenido digital del artículo 477.1. del COIP previsiones relacionadas con la cadena de custodia digital que incluyan las distintas etapas de la extracción forense, a saber: a) adquisición *bit* a *bit*, b) cálculo de *hash*, c) preservación de *logs*, d) extracción de metadatos y e) documentación detallada.

2) Incluir en las actuaciones especiales relativas al contenido digital del artículo 477.2. del COIP la posibilidad de ordenar, cuando el caso lo requiera, la intervención inmediata de un perito criminalista especializado para que la entrega o remisión de datos de contenido alojados en sistemas informáticos no padezca *a posteriori* vicios que provoquen su nulidad o exclusión probatoria.

3) Precisar en las actuaciones especiales relativas al contenido digital del artículo

477.3. del COIP la posibilidad de dictar la orden de conservación rápida de la evidencia con el congelamiento de acceso del titular de los datos para cualquier proveedor nacional o internacional con actividad en el país o que sea un ente cooperante.

4) Evaluar la viabilidad de la introducción de figuras derivadas del Convenio de Budapest como el agente encubierto informático, la creación de laboratorios forenses especializados, la red de cooperación rápida y constante, la creación de equipos conjuntos de trabajo para la investigación forense en casos complejos de extorsión digital transnacional, entre otras que aconseje la experiencia.

Bibliografía

Constitución de la República del Ecuador (Registro Oficial No. 449 de 20 de octubre de 2008).

Consejo de Europa, Convenio sobre la Ciberdelincuencia, 23 de noviembre de 2001 (Serie de Tratados Europeos No. 185, 3 de diciembre de 2001).

Código Orgánico Integral Penal, 28 de enero de 2014 (Registro Oficial Suplemento No. 180, de 10 de febrero de 2014).

Ley Orgánica Reformatoria a Varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral, 7 de marzo de 2023 (Registro Oficial Suplemento No. 279, 29 de marzo de 2023).

ALONSO RUIDO, Patricia, ESTÉVEZ, Iris, VARELA PORTELA, Cristina y SOTELINO LOSADA, Alexandre, "Sextorsión: una estrategia de violencia sexual online en el estudiantado universitario" en *Pedagogía Social*, No. 45, 2024, pp. 29-43, URL http://recyt.fecyt.es/index.php/PSRI/ consultado 05/05/2026.

BATALLAN, Ana Belén, BURGOS, Edna Natalia, POZYWILKO, Susana Marilyn y RODRÍGUEZ, Gustavo Alberto, "Gobernanza en la era meta: retos y desafíos para el sector público" en BONIFACIO, José Alberto (comp.) y SAGALSKY, Ruth Sofía (comp.), *El Estado y la Administración Pública en debate: encrucijadas y desafíos para el desarrollo. Memorias del IV Congreso Nacional de Estudios de Administración Pública*, vol. 2, Asociación Argentina de Estudios de Administración Pública, 2024, Buenos Aires, pp. 23-34.

BELTRÁN HERNÁNDEZ, César Ramiro y PERDOMO MÉNDEZ, Juan Sebastián, *Diseño e implementación de un Piloto de Laboratorio Forense Especializado en Respuesta a Incidentes de ciberseguridad para una Entidad Pública del Distrito de Bogotá*, Pontificia Universidad Javeriana, 2024, Bogotá.

CORDOVA SAINT-PERE, Jilmar Moises, "Análisis de la situación actual del delito de extorsión y los medios digitales en la legislación peruana" en *Fides Et Ratio*, vol. 31, 2026, pp. 167-192, DOI https://doi.org/10.55739/fer.187 consultado 05/05/2026.

FERNÁNDEZ CHOLOQUINGA, Luis Miguel y MONTALVO RAMOS, Fernández Andrés, "Análisis jurídico de las formas y medios de extorsión en el Ecuador", *Polo del Conocimiento (Edición núm. 117*), vol. 11, No. 4, 2026, pp. 1163-1181, DOI https://doi.org/10.23857/pc.v11i4.11475 consultado 05/05/2026.

Fundación Panamericana para el Desarrollo, *Guía técnica sobre análisis forense y evidencia digital. Proyecto de creación de capacidades del sector judicial*

ecuatoriano para combatir la delincuencia transnacional y el narcotráfico, PADF, 2026, URL https://oeco.padf.org/wp-content/uploads/2026/01/6.-GUIA-TECNICA-SOBRE-ANALISIS-FORENSE-Y-EVIDENCIA-DIGITAL.pdf consultado 06/05/2026.

GERCKE, Marco, *Understanding Cybercrime: A Guide for Developing Countries*, ITU-D ICT Applications and Cybersecurity Division, 2011, 2da ed., Ginebra.

GRAHAM, Roderick S. y SMITH, Shawn K., *Cybercrime and Digital Deviance*, 2da ed., 2024, URL https://dokumen.pub/download/cybercrime-and-digital-deviance-9781032254524-9781032249193-9781003283256.html consultado 05/05/2026.

HERRERA SEGUEL, Marta y ORTIZ PULGAR, Ymay, *Criminalidad informática y ciberdelincuencia*, Academia Judicial de Chile, 2024, Santiago, URL https://academiajudicial.cl/wp-content/uploads/2025/06/MD-76-Criminalidad-informatica-y-ciberdelincuencia_web-1.pdf consultado 05/05/2026.

HILDEBRANDT, Mireille, *Law for Computer Scientists and Other Folk*, Oxford University Press, 2020, Oxford.

KOOPS, Bert-Jaap y ROBINSON, Tessa, "Cybercrime Law. A European Perspective" en CASEY, Eoghan (Ed.), *Digital Evidence and Computer Crime*, 3ra ed., Elsevier, 2011, pp. 123-185.

LINDSAY, Jon R., "Stuxnet and the Limits of Cyber Warfare" en *Security Studies*, vol. 22, No. 3, 2013, pp. 365-404, DOI https://doi.org/10.1080/09636412.2013.816122 consultado 05/05/2026.

LLAMAS COVARRUBIAS, Jersain Zadamig y MOLINÉ RODRÍGUEZ, César, "Ciberseguridad en América Latina y el Caribe: hacia una arquitectura legal y un marco común" en *EU Cyber Net*, 2026, URL https://www.eucybernet.eu/wp-content/uploads/2026/01/ciberseguridad-en-america-latina-y-el-caribe.pdf consultado 06/05/2026.

LOZANO DOMÍNGUEZ, Valle, "Ciberterrorismo en el siglo XXI" en *CEU Universidad San Pablo*, 2025, URL https://dspace.ceu.es/server/api/core/bitstreams/6997d195-a853-413d-b847-af7dd49c52e0/content consultado 05/05/2026.

MAIMAI, Lee, *No KYC Crypto Wallets: Privacy, Open-Source, and Self-Custody Explained*, 2025, URL https://onekey.so/blog/es/ecosystem/no-kyc-crypto-wallets-privacy-open-source-and-self-custody-explained/?srsltid=AfmBOooPKDR0I6YtQzJsEfHbT6a0TMMU6mLff6qdwf5RSrqPzK4Sg1od consultado 06/05/2026.

Ministerio de Relaciones Exteriores y Movilidad Humana, "Depósito del instrumento de ratificación del Convenio de Budapest" en *Cancillería del Ecuador*, 2024, URL https://www.cancilleria.gob.ec/2024/12/13/deposito-del-instrumento-de-ratificacion-del-convenio-de-budapest/ consultado 06/05/2026.

NÁJERA GONZÁLEZ, Xavier, "Breve estudio dogmático del delito de extorsión en el Código Penal del Estado de Puebla, México" en *Nuevo Foro Penal*, No. 100, 2023, pp. 11-33, DOI https://doi.org/10.17230/nfp19.100.1 consultado 05/05/2026.

OCHOA ARÉVALO, Paúl A., "El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación" en *Economía y Política*, No. 28, 2018, pp. 35-44, DOI https://doi.org/10.25097/rep.n28.2018.03 consultado 06/05/2026.

ORTIZ NIVELA, Milza Naomi, VEGA PILA, Luis Edwin y GARCÍA SEGARRA, Holger Geovanny, "Insuficiente regulación de la prueba digital y su valoración en el proceso penal" en *593 Digital Publisher CEIT*, vol. 10, No. 4, 2025, pp. 1057-1070, DOI https://doi.org/10.33386/593dp.2025.4.3399 consultado 05/05/2026.

ORTIZ PRADILLO, Juan Carlos, "Determinación de la jurisdicción y competencia para la investigación y enjuiciamiento de los daños informáticos", en *Centro de Estudios Jurídicos del Ministerio de Justicia*, 2016, URL https://www.cej-mjusticia.es/sede/publicaciones/ver/11317 consultado 06/05/2026.

POSADA MAYA, Ricardo, "El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual" en *Nuevo Foro Penal*, vol. 13, No. 88, 2017, pp. 72-112, URL https://dialnet.unirioja.es/descarga/articulo/6074006.pdf consultado 05/05/2026.

RODRÍGUEZ, Gladys Stella, "Privacidad y seguridad en la nube: algunas implicaciones jurídico-económicas desde el comercio electrónico transfronterizo" en *Lex – Revista de la Facultad de Derecho y Ciencias Políticas*, vol. 18, No. 25, 2020, https://doi.org/10.21503/lex.v18i25.2109 consultado 06/05/2026.

QUEZADA QUIZHPE, Alex Benjamín y GENDE RUPERTI, Carla Guadalupe, "Delito de Ciberextorsicion: Un Análisis Jurídico, y Comparativo en País de Latinoamérica, Perú, Colombia y Ecuador" en *593 Digital Publisher CEIT*, vol. 10, No. 1, 2025, pp. 546-556, DOI https://doi.org/10.33386/593dp.2025.1.2893 consultado 05/05/2026.

SALAZAR MÉNDEZ, Diana, "El rol de la administración de justicia y la cooperación internacional en la lucha contra la ciberdelincuencia", *Revista*

Perfil Criminológico, 2021, URL https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf consultado 06/05/2026.

VELASCO NÚÑEZ, Eloy, *Aspectos procesales de la investigación y de la defensa de los delitos informáticos*, 2021, URL https://web.icam.es/bucket/Aspectos%20Procesales%20de%20la%20Investigacion%20y%20Defensa%20Delitos%20Informaticos.pdf consultado 06/05/2026.