Vol.10 No.2 (2026): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR.2026.e255

Digital evidence as a means of proof in the crime of extortion

La prueba digital como medio probatorio dentro del delito de extorsión

Autores:

Abad-Quinteros, Wyatt Iván
UNIVERSIDAD CATÓLICA DE CUENCA
Estudiante de la Maestría de Derecho Procesal Penal y Litigación Oral
Cuenca-Ecuador

wyatt.abad2@est.ucacue.edu.ec

https://orcid.org/0009-0002-9302-007X

Durán-Ramírez, Andrea Lisseth
UNIVERSIDAD CATÓLICA DE CUENCA
Docente Tutora del área de Derecho Procesal Penal y Litigación Oral
Cuenca – Ecuador

aduranr@ucacue.edu.ec

https://orcid.org/0000-0002-8382-1335

Fechas de recepción: 06-MAR-2026 aceptación: 06-ABR-2026 publicación: 30-JUN-2026

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

El presente articulo analiza la relevancia de los medios de prueba digital como un elemento esencial en los procesos judiciales por el delito de extorsión dentro de la normativa ecuatoriana. El objetivo general consistió en evaluar la importancia que tiene la evidencia electrónica para garantizar su validez en el debido proceso del sistema penal. Para su desarrollo se utilizó una metodología cualitativa y bibliografía fundamentada en la revisión de normas nacionales e informes de organismos internacionales especializados en seguridad digital y criminalidad organizada. A pesar de que los actos delictivos digitales han ido en aumento, el sistema judicial ecuatoriano presenta limitaciones en la gestión de cadenas de custodia y en la capacitación técnica de los profesionales de justicia. Así mismo se constató que el incremento de los casos de extorsión cometidos a través de los medios electrónicos, superaron el 170% en los últimos años, dichos casos no se acompañaron con la normativa procesal adecuada que regule con precisión la preservación y autenticidad de los datos. Con este antecedente se determinó que es de suma importancia reformar los protocolos vigentes para evitar la impunidad y fortalecer la seguridad para garantizar una tutela judicial efectiva.

Palabras clave: Prueba digital; Tecnología; Extorsión; Cadena de custodia; COIP.

Abstract

This article analyzes the relevance of digital evidence as an essential element in judicial proceedings for the crime of extortion under Ecuadorian law. The general objective was to evaluate the importance of electronic evidence in guaranteeing its validity within the due process of the criminal justice system. A qualitative methodology and a literature review were used, based on national regulations and reports from international organizations specializing in digital security and organized crime. Despite the increase in digital crimes, the Ecuadorian judicial system presents limitations in the management of chains of custody and in the technical training of legal professionals. Furthermore, it was found that the increase in extortion cases committed through electronic means has exceeded 170% in recent years, and these cases have not been accompanied by adequate procedural regulations that precisely govern the preservation and authenticity of the data. Given this background, it was determined that it is of utmost importance to reform the current protocols to prevent impunity and strengthen security to guarantee effective judicial protection.

Keywords: Digital evidence; Technology; Extortion; Chain of custody; COIP.

Introducción

La transformación tecnológica propia del siglo XXI ha cambiado de manera directa las dinámicas sociales y económicas, pero también las formas en que se cometen los delitos. Actualmente, la transición hacia una sociedad cada vez mas conectada ha permitido que las organizaciones criminales encuentren en el ciberespacio un lugar adecuado para desarrollar sus actividades ilícitas, dejando como resultado una serie de rastros electrónicos que resultan fundamentales para la administración de justicia. Entre estas conductas, la extorsión se ha consolidado como uno de los delitos que mas ha evolucionado, utilizando herramientas digitales para presionar a las víctimas bajo el anonimato que ofrece la red. En este contexto, la prueba digital se convierte en un elemento central dentro de la investigación penal actual; sin embargo, su correcta aplicación en el sistema judicial ecuatoriano enfrenta obstáculos de tipo técnico y jurídico que ponen en duda su integridad y su verdadera eficacia probatoria

A nivel internacional, la importancia de los datos electrónicos es incuestionable. Organismos como la Comisión Europea y Europol han señalado que cerca del 80% de las investigaciones penales dependen actualmente de la obtención de evidencia digital (Europol, 2025). De acuerdo con el Informe de Evaluación de la Amenaza del Crimen Organizado en Internet (IOCTA), el tráfico y secuestro de información sensible se han posicionado como las principales amenazas de esta década (Europol, 2025). Este escenario criminal, comprende fraudes complejos hasta extorciones sistemáticas, ha avanzado con mayor rapidez que la capacidad de reacción de las instituciones judiciales, generando una brecha importante en la preservación de datos volátiles y en el acceso oportuno a información cifrada. Por esta razón, resulta necesario establecer marcos jurídicos que no solo reconozcan la prueba digital, sino que también la regulen conforme a los estándares internacionales.

En el caso ecuatoriano, la problemática adquiere una mayor complejidad. A pesar de los esfuerzos por modernizar la legislación, el país todavía no cuenta con una normativa especializada que detalle procedimientos claros para la recolección y el análisis de la evidencia informática. Si bien reformas recientes han permitido que los documentos electrónicos sean admitidos dentro del proceso judicial, aun existen vacíos relevantes en cuanto a las garantías necesarias para certificar que no se alterasen dichas pruebas (Buestan, 2025). Tanto el Código Orgánico Integral Penal (Asamblea Nacional, 2014) como el Código Orgánico General de Procesos (Asamblea Nacional, 2015) reconocen de manera formal la validez de estos medios probatorios; sin embargo, la falta de reglas específicas sobre la cadena de custodia electrónica afecta la capacidad para trazar su trayectoria y, en consecuencia, la confiabilidad del material presentado ante los tribunales

El trabajo forense se ve limitado por aspectos como el cifrado de extremo a extremo, la eliminación rápida de registros por parte de los proveedores de servicios y las dificultades que surgen cuando los hechos involucran distintas jurisdicciones. A esto se añade que, en el

caso ecuatoriano, los operadores de justicia con frecuencia no disponen de los recursos tecnológicos ni de la formación especializada en criminalística digital que se requiere para este tipo de desafíos. Esta debilidad institucional no solo afecta la eficiencia del proceso penal, sino que favorece un ambiente de impunidad que termina debilitando la confianza de la ciudadanía en el sistema de administración de justicia.

La urgencia de tratar este problema se evidencia en las cifras oficiales. Según datos del Ministerio del Interior del Ecuador (2025), las denuncias por extorsión pasaron de 8,399 en el año 2022 a 23,087 en 2024, lo que representa un aumento acumulado del 174.9%. En este contexto, la presente investigación tiene como objetivo analizar la eficacia de la prueba digital dentro del delito de extorsión, considerando tanto las capacidades técnicas como las normas vigentes, con el propósito de que la justicia pueda responder al alto crecimiento de complejidad en el crimen digital

Planteamiento del Problema y Pregunta Orientadora

El punto central de esta investigación consiste en determinar si la prueba digital resulta realmente efectiva en el tratamiento del delito de extorsión dentro del sistema penal ecuatoriano. Esta problemática no puede analizarse desde una sola perspectiva, sino que requiere ser observada desde diferentes aspectos críticos. En primer lugar, es necesario examinar el marco normativo actual, para verificar si los criterios de admisibilidad y pertinencia previstos en la legislación nacional son suficientes frente a la naturaleza volátil de los datos electrónicos. No es suficiente que una prueba sea aceptada formalmente; también debe cumplir con estándares de integridad que permitan sostenerla durante el proceso.

En segundo lugar, la eficacia de la prueba digital depende en gran medida del factor humano y técnico. Se observa una brecha en la capacitación especializada de los operadores de justicia, es decir, fiscales, jueces y peritos, cuya preparación en el análisis de evidencia informática no siempre es igual. Esta falta de recursos y de formación técnica no solo reduce la capacidad de respuesta del Estado frente a los casos de extorsión, sino que incluso puede ocasionar la nulidad de procesos por errores cometidos en la cadena de custodia

Además, la evolución constante de las Tecnologías de la Información y la Comunicación (TIC) plantea nuevos desafíos. La rapidez con la que los grupos criminales adoptan sistemas de anonimato y cifrado obliga a las instituciones a adaptarse constantemente. Finalmente, no puede dejarse de lado el gran problema social, en el que la percepción de ineficacia técnica del sistema judicial desmotiva a las víctimas a denunciar, incrementando la llamada “cifra negra” de la extorsión, ya que muchas personas prefieren ceder ante el extorsionador antes que iniciar un proceso judicial que consideran poco efectivo o incluso revictimizante, más allá del gasto económico que les podría conllevar

En última instancia, la falta de protocolos técnicos no representa solo un problema administrativo, sino que se convierte en un factor que favorece la impunidad. La incapacidad

del Estado para garantizar la mismidad de la evidencia digital permite que las defensas técnicas logren la exclusión probatoria de elementos incriminatorios reales, lo que termina vulnerando el derecho a la tutela judicial efectiva de las víctimas y debilitando la credibilidad del sistema penal en contra del crimen organizado.

Marco teórico

El impacto de la revolución digital en la criminalidad actual

El marco teórico de esta investigación no se limita a reunir conceptos, sino que se presenta como el soporte necesario para comprender la transformación del delito en la sociedad actual. La nacionalizad masiva ha reducido las fronteras físicas del crimen y ha obligado a replantear el funcionamiento de las instituciones del Derecho Penal. El paso de lo analógico a lo digital ha provocado un cambio en las formas de obtención, custodia y valoración de la prueba, lo que exige una relación constante entre el derecho y la ingeniería informática.

En el caso ecuatoriano, la extorsión ha dejado de ser un delito vinculado exclusivamente físico entre autor y víctima, para convertirse en una práctica transnacional e inmaterial. Esta transformación demuestra que la prueba digital ya no puede considerarse un elemento secundario, sino que constituye el eje principal para garantizar la justicia y el debido proceso. Por ello, resulta necesario analizar los antecedentes normativos que regulan esta materia, asegurando que el tratamiento de la evidencia electrónica sea adecuado tanto desde el punto de vista técnico como jurídico.

Dentro de este contexto, resulta necesario señalar que la evidencia digital posee rasgos propios como la volatibilidad y la fragilidad, que la diferencian de manera clara de las pruebas físicas tradicionales. De acuerdo con lo dispuesto por la Asamblea Nacional (2014) en el Código Orgánico Integral Penal, la legalidad de la prueba depende de que esta sea obtenida de forma licita y conservada sin alteraciones; sin embargo, la experiencia judicial demuestra que, sin protocolos técnicos adecuados de cadena de custodia digital (hash, sellado de tiempo, entre otros), la aplicación de la norma terminaría siendo más teórica que real.

Antecedentes y Evolución de la Prueba Digital en el Contexto Ecuatoriano

Durante las últimas décadas, el Estado ecuatoriano ha promovido la modernización de sus procedimientos mediante el uso de herramientas digitales, con el objetivo de mejorar la gestión pública y, responder a las exigencias de una sociedad cada vez más conectada. Esta transición hacia lo digital ha impactado distintos ámbitos, desde la administración pública hasta el sistema judicial, permitiendo que los registros electrónicos dejen de ser simples apoyos y pasen a ocupar un lugar central en la verdad procesal.

La necesidad de adecuar el sistema judicial a los estándares internacionales en materia de ciberseguridad y derecho informático dio lugar a un momento clave: la expedición del Código Orgánico Integral Penal) COIP) en 2014 y, posteriormente, la entrada en vigencia

del Código Orgánico General de Procesos (COGEP) (Asamblea Nacional, 2014, 2015). Estas normas representaron un punto de quiebre, ya que por primera vez ofrecieron un respaldo legal para incorporar documentos electrónicos y meta datos como medios probatorios que sean validos dentro del proceso penal.

Desafíos Normativos y la Brecha Técnica

La doctrina actual y diversos estudios recientes coinciden en que no basta con admitir la prueba digital si no existen reglas especializadas que regulen de forma estricta la cadena de custodia electrónica. Según Buestan (2025), la falta de protocolos técnicos estandarizados para la obtención, conservación y análisis de la evidencia genera un escenario de inseguridad jurídica. Cuando no se cuenta con una metodología clara que asegure que los datos no han sido modificados, el proceso penal pierde fuerza, lo que facilita impugnaciones que terminan favoreciendo la impunidad.

A nivel internacional, organismos como Europol (2025) han advertido que, considerando que más del 85% de las investigaciones criminales actuales incluyen algún componente digital, los sistemas judiciales que no logren reducir la distancia entre la ley escrita y la capacidad técnica quedaran apartados frente al avance del crimen organizado. Esta problemática se vuelve aún más visible en los casos de extorsión, donde las aplicaciones de mensajería cifrada y las redes sociales se han convertido en el principal foco del delito (Europol, 2025)

El Marco Normativo del COIP y el Delito de Extorsión

El Código Orgánico Integral Penal (COIP) es el eje principal del sistema punitivo ecuatoriano. Su estructura no solo está orientada a sancionar las conductas delictivas, sino también a proteger los derechos fundamentales y garantizar el debido proceso. En este sentido, el COIP ha debido adaptarse a nuevas realidades, como la responsabilidad penal de las personas jurídicas y las formas actuales de criminalidad organizada, lo que evidencia una tendencia moderna que reconoce que el delito ya no se desarrolla exclusivamente en el ámbito físico

En lo referente al delito de extorsión, el COIP (Asamblea Nacional, 2014) y sus reformas hasta el año 2025 establecen un marco sustantivo que reconoce la gravedad de esta conducta cuando se ejecutan a través de los medios de comunicación. La normativa actual contempla agravantes específicas cuando el victimario utiliza sistemas electrónicos o redes digitales para coaccionar a la víctima. Este incremento en las sanciones es una respuesta directa al incremento de daños por el medio digital, el cual permite al delincuente amplificar el daño, actuar bajo el anonimato y atacar la estabilidad psíquica y económica de las personas con mayor facilidad

Para el sistema procesal, la prueba digital es hoy el mecanismo principal para la reconstrucción de la verdad material. El COIP reconoce la validez de:

- Registros y bitácoras electrónicas.
- Capturas de pantalla y volcados de datos certificados.
- Comunicaciones interceptadas mediante orden judicial.
- Análisis de los trazados de ubicación para su localización

Siempre que estos elementos probatorios se obtengan respetando las garantías constitucionales y se conserve su integridad, se convierten en una herramienta clave para identificar a los responsables y eliminar las redes de extorsión digital que operan en el país

El Código Orgánico General de Procesos (COGEP) y la Eficacia de lo Digital

Mientras el COIP determina qué conductas constituyen delito, el Código Orgánico General de Procesos (COGEP) es el cuerpo normativo que fija las reglas para la práctica de la prueba dentro del sistema judicial ecuatoriano. La entrada en vigencia del COGEP significó un cambio hacia un modelo por audiencias, basado en la oralidad, la celeridad y la transparencia. En relación con la evidencia digital, este código resulta esencial, ya que deja de depender exclusivamente del soporte en papel y adopta los entornos virtuales, garantizando que el derecho al debido proceso se mantenga en medio de la complejidad técnica de la era informática (Asamblea Nacional, 2015).

Uno de los aportes más relevantes del COGEP se encuentra en sus artículos 117, 196 y 202, donde se regula la admisibilidad de los documentos electrónicos. La legislación ecuatoriana acoge el "Principio de Equivalencia Funcional", conforme al cual un documento digital tiene la misma validez y eficacia probatoria que un documento físico, siempre que pueda comprobarse su origen y que su contenido no haya sido alterado. Este principio adquiere especial importancia en los casos de extorsión, en donde la prueba principal suele consistir en un mensaje de WhatsApp, un correo electrónico o una transferencia bancaria.

De forma concreta, el artículo 202 del COGEP establece la presunción de originalidad para los documentos generados de manera electrónica. Esto implica que cualquier archivo digital, junto con sus anexos y meta datos, se considera original para efectos legales. Dicha disposición constituye una herramienta relevante tanto para la fiscalía como para la defensa, pues permite que las copias digitalizadas incorporadas al expediente tengan el mismo valor jurídico que las pruebas físicas tradicionales, siempre que se observen los protocolos adecuados de preservación

Normativa Complementaria y el Resguardo de Derechos Fundamentales

La administración de la prueba digital en el Ecuador no se limita a los códigos penales o procesales, sino que exige un marco normativo que lo complemente y que proporcione claridad técnica en protección de derechos. En este contexto, la Ley Orgánica de Protección de Datos Personales (LOPDP) de 2021 cumple una función esencial (Asamblea Nacional, 2021). Durante la investigación de delitos de extorsión, con frecuencia se accede a información privada y sensible; por ello, esta normativa establece limites precisos para

asegurar que la obtención de la evidencia no vulnere derechos como la intimidad o el habeas data

Este marco regulatorio garantiza que el acceso y la conservación de los datos electrónicos por parte del Estado se realice bajo condiciones estrictas de legalidad. De esta manera, la normativa complementaria no solo cubre los vacíos técnicos del COIP, sino que funciona como un mecanismo de protección de garantías constitucionales de los ciudadanos, evitando que la persecución del delito termine convirtiéndose en una vulneración de la libertad

Naturaleza y Pilares de la Evidencia Digital

Para que la información almacenada o transmitida por medios digitales pueda ser considerada como evidencia digital dentro de un proceso judicial, debe cumplir con una serie de requisitos básicos:

- Autenticidad: La capacidad de demostrar de forma clara que la prueba procede de la fuente indicada y que la identidad del autor es real. En la extorsión digital implicaría vincular un perfil o número telefónico con una persona real.
- Integridad: La garantía de que el dato no ha sufrido modificaciones (accidentales o intencionadas) desde el momento de su hallazgo hasta su presentación en juicio. Esto se logra mediante herramientas forenses como el cálculo de funciones hash.
- Relevancia: La pertinencia de la prueba para demostrar el cometimiento del delito o la responsabilidad del procesado.

La evidencia digital, por su propia naturaleza, es volátil y frágil. A diferencia de un objeto físico, como un arma, un registro de servidor o un mensaje de texto pueden desaparecer en cuestión de segundos. Por ello, la criminalística digital aplica procedimientos específicos de recolección y análisis que permiten asegurar la trazabilidad de la información. Solo a través de una cadena de custodia electrónica continua se puede garantizar que los datos obtenidos de dispositivos como teléfonos móviles, servidores en la nube o redes sociales sean aceptados por un juez como una representación fiel de los hechos investigados.

Conceptualización y Dimensiones de la Evidencia Digital

Dentro del contexto de la justicia contemporánea, la evidencia digital supera la idea limitada de un simple “archivo informático”. Se entiende como el conjunto de información con valor probatorio que es almacenada, procesada o transmitida en formato binario, y que puede ser recuperada para su valoración dentro de un proceso judicial (OECD, 2024). En el ámbito de la ciberdelincuencia, esta evidencia se presenta en diversas formas, como correos electrónicos, registros de mensajería, meta datos ocultos, historiales de navegación y datos de geolocalización

En el caso particular del delito de extorsión, la prueba digital no solo constituye un elemento secundario para el delito, sino que se convierte en el medio mismo de la coacción. A través

de ella, los investigadores pueden establecer el vínculo entre la amenaza emitida y el daño económico o psicológico sufrido por la víctima, permitiendo reconstruir con mayor precisión la secuencia de los hechos que, de otro modo, quedarían ocultos en el anonimato de la red.

El Pilar de la Autenticidad

La autenticidad es el primer requisito esencial que debe superar cualquier elemento digital para ser admitido como prueba en juicio. No basta con presentar un dato; es necesario demostrar, mediante criterios técnicos y jurídicos, que la información es verdadera, que proviene de la fuente declarada y que no ha sido manipulada o suplantada (Buestan, 2025)

Dado que el entorno digital facilita prácticas como la suplantación de identidad, la autenticidad se garantiza a través de la combinación de varias herramientas, entre ellas:

- Análisis forense de meta datos: Permite identificar la fecha de creación del archivo, el dispositivo desde el cual fue generado y las posibles modificaciones realizadas por su autor.
- Sellos de Tiempo Criptográficos: Aseguran que el dato existía en un momento determinado y que no haya sido alterado a posteriori.
- Certificaciones Periciales: La validación por parte de un experto acreditado que dote de fe técnica el hallazgo, vinculando la actividad digital con un sujeto procesal específico.

Integridad y el Uso de Funciones Hash

Si la autenticidad permite responder al "quién", la integridad se relaciona con el "qué", ya que garantiza que la prueba no haya sido modificada desde el momento de su recolección hasta su análisis final (Banegas & Andrade, 2022). Debido a que los datos digitales son altamente volátiles y pueden ser alterados sin dejar una señal evidente, la criminalística informática se apoya en herramientas propias de la criptografía.

Para proteger esta integridad se emplean algoritmos de reducción conocidos como funciones hash, tales como SHA-256 o, en contextos menos sensibles, MD5. Estos mecanismos producen una especie de "huella digital" única para cada archivo. Si se modifica, aunque sea un solo bit del documento original, el valor hash cambia por completo, lo que permite detectar de inmediato una posible alteración. La conservación de esta huella es lo que permite al órgano jurisdiccional tener la certeza de que la evidencia presentada en audiencia es exactamente la misma que fue obtenida del dispositivo del sospechoso.

La Cadena de Custodia Digital

La cadena de custodia digital no debe ser entendida como una simple serie de trámites administrativos, sino como un protocolo integral y debidamente documentado que asegura la integridad de la prueba tanto desde el plano forense como jurídico. Este proceso comienza con la identificación y el aseguramiento del entorno digital. En esta fase, el investigador no

solo ubica los dispositivos, sino que también debe aplicar medidas para proteger el entorno, evitando la perdida de datos volátiles almacenados en la memoria RAM, los cuales pueden contener claves de cifrado o sesiones activas de aplicaciones de mensajería usadas para cometer la extorsión. Los errores cometidos en esta etapa inicial suelen ser una de las principales causas de la nulidad probatoria en los tribunales ecuatorianos.

Una vez asegurado el entorno, se pasa a la fase de recolección y adquisición técnica, donde el nivel de rigor debe ser máximo. En este punto se utilizan bloqueadores de escritura (write blockers) para impedir que, al conectar el dispositivo a la estación forense, se modifique siquiera un bit del contenido original. El objetivo es obtener una imagen forense, es decir, una copia bit a bit del soporte, que permita realizar los análisis sin comprometer la evidencia matriz.

Dentro de la metodología actual, resulta indispensable incorporar la informática forense en la nube (Cloud Forensics). Hoy en día, muchos extorsionadores emplean servicios como Google Drive o iCloud, lo que coloca al investigador frente a una infraestructura cambiante. Aqui surge un problema de carácter jurisdiccional: determinar si un fiscal ecuatoriano puede autorizar el acceso a un servidor que físicamente se encuentra en otro país, dando la posibilidad de acceder a los datos desde territorio nacional.

Posteriormente, la etapa de preservación asegura que la prueba sea almacenada bajo condiciones controladas, registrando cada intervención humana sobre el objeto para evitar contaminaciones o manipulaciones indebidas. El proceso continua con el análisis forense, donde peritos especializados emplean herramientas para recuperar archivos eliminados y reconstruir conversaciones cifradas. Esta fase constituye el núcleo de la investigación, pues convierte la información en prueba con valor jurídico. Finalmente, el procedimiento culmina con la presentación en audiencia, momento en el cual el perito debe demostrar que la cadena de custodia se mantuvo sin interrupciones, permitiendo que el juzgador valore la evidencia con plena confianza en su autenticidad.

Es necesario profundizar en que la cadena de custodia no se limita a ser un simple registro de nombres y fechas, sino que constituye una garantía de inalterabilidad sustentada en la ciencia informática. En este sentido, el empleo de algoritmos de reducción hash (como SHA-256 o MD5) funciona como el “ADN” de la evidencia digital. Si durante el desarrollo del proceso penal el hash de la prueba presentada en juicio no coincide de forma exacta con el hash generado al momento de la incautación, la prueba pierde toda su credibilidad, ya que desde un punto de vista matemático se demuestra que ha sido alterada, aunque sea con un solo bit.

Este nivel de rigor técnico debe analizarse desde la perspectiva de la llamada “mismidad”. La mismidad garantiza que aquello que se examina en el laboratorio y lo que se valora en el tribunal sea exactamente lo mismo que se recolecto en la escena del crimen digital. En casos de extorsión, donde los archivos suelen ser capturas de tráfico de red o volcados de bases de

datos, cualquier descuido en la custodia, como el uso de memorias USB en el que la falta de sellado electromagnético, puede dar lugar a impugnaciones exitosas por parte de la defensa, dejando al Estado sin su principal elemento de convicción

El Principio de Equivalencia Funcional y el Documento Electrónico en el COGEP

La integración del Principio de Equivalencia Funcional dentro del Código Orgánico General de Procesos (COGEP) representa un avance en la historia del derecho procesal ecuatoriano. Este principio no es simplemente una regla de admisión; es una declaración de validez jurídica que otorga al documento digital mensajes de texto, correos electrónicos, registros de bases de datos el mismo valor probatorio que posee un documento físico tradicional firmado de forma manuscrita. No obstante, su aplicación en los casos de extorsión resulta compleja, pues la equivalencia funcional exige que se pueda asegurar tanto la accesibilidad para su consulta posterior como la preservación de la integridad del contenido desde el momento en que fue generado

En este contexto, el artículo 202 del COGEP dispone que los documentos producidos de manera electrónica se consideran originales. Esta presunción legal busca agilizar la administración de justicia, pero al mismo tiempo impone una carga probatoria técnica importante. En los procesos penales por extorsión, la defensa suele cuestionar la validez de las capturas de pantalla o de las impresiones de correos electrónicos, alegando que se trata de representaciones gráficas fácilmente alterables. Por ello, el discurso jurídico debe ampliarse para explicar que la equivalencia funcional no protege la simple “imagen” de la conversación, sino el archivo digital subyacente junto con sus meta datos. Si el Estado ecuatoriano pretende fortalecer la seguridad jurídica, debe avanzar desde la mera aceptación del documento electrónico hacia una verificación técnica obligatoria que certifique que el mensaje analizado cuenta con firma electrónica o con un sello de tiempo que garantice que su contenido no fue manipulado después de la amenaza extorsiva.

La Ley Orgánica de Protección de Datos Personales (LOPDP) y el Límite al Poder Punitivo

No es posible examinar la prueba digital en los delitos de extorsión sin entender que los datos contenidos en un dispositivo como mensajes, fotografías o registros de ubicación constituyen extensiones de la personalidad y se encuentran protegidos por el derecho al Habeas Data. En este punto, resulta indispensable analizar la tensión existente entre el artículo 66 de la Constitución, que garantiza la inviolabilidad de las comunicaciones, y la facultad del Estado para investigar hechos delictivos

La LOPDP establece que el tratamiento de datos personales es licito cuando resulta necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de potestades públicas, sin embargo, esto no puede entenderse como un cheque en blanco para intervenir sin límites en la esfera privada de las personas

En la práctica judicial, esto implica que la Fiscalía debe observar el Principio de Minimización de Datos. Al investigar una extorsión, el perito informático tiene la obligación ética y legal de extraer únicamente la información que sea estrictamente necesaria para probar el acto ilícito. Si durante un peritaje se extraen datos sensibles del investigado que no guardan relación con la extorsión (como su historial clínico o sus inclinaciones políticas), se podría estar vulnerando la LOPDP, lo que generaría una responsabilidad administrativa para el Estado y, potencialmente, la exclusión de la prueba. Por lo tanto, el marco normativo ecuatoriano debe evolucionar hacia la creación de " protocolos de búsqueda selectiva", donde el juez de garantías penales actúe como un filtro para que el determine qué carpetas digitales pueden ser abiertas y cuáles deben permanecer bajo la privacidad del ciudadano.

La Extorsión Digital: Un Fenómeno Transnacional en Expansión

Según los reportes del Ministerio del Interior (2025), Ecuador ha experimentado un salto alarmante de 8,399 denuncias en 2022 a más de 23,000 en 2024. Este incremento del 174.9% pone de manifiesto que el sistema judicial ha sido sobrepasado por la velocidad de adaptación de las bandas criminales, que operan con estructuras jerarquizadas desde los centros de privación de libertad, utilizando la tecnología para intimidar a sectores productivos enteros sin necesidad de presencia física

Al contrastar esta realidad con el contexto regional, se observa que países como Colombia enfrentan desafíos similares, con un acumulado de más de 102,000 denuncias que han obligado a sus autoridades a crear unidades de élite especializadas en ciber-extorsión. En Perú, la situación es muy similar con reportes que indican que más de un millón y medio de ciudadanos han sido víctimas de alguna modalidad de extorsión digital solo en el primer trimestre de 2025. Asimismo, Guatemala refleja una tendencia al alza que confirma que el anonimato proporcionado por las redes sociales y las aplicaciones de mensajería instantánea es el motor principal de este delito a nivel continental. Esta comparativa internacional no solo sirve para ver la gravedad del problema en Ecuador, sino para justificar la necesidad urgente de adoptar protocolos de cooperación judicial que permitan rastrear el origen de las amenazas, muchas de las cuales provienen de servidores o redes fuera de la jurisdicción nacional.

País	Datos Estadísticos (2019-2025)	Fuente de Referencia
Ecuador	174.9% de incremento acumulado (23,087 casos en 2024)	Ministerio del Interior (2025)
Colombia	102,289 denuncias registradas	Radiografía de la Extorsión (2024)
Perú	1.7 millones de víctimas solo en el primer trimestre de 2025	Radiografía de la Extorsión (2024)
Guatemala	Crecimiento de 18,096 (2023) a 24,978 (2024)	Radiografía de la Extorsión (2024)

Nota: Cuadro hecho en base a los datos recopilados

Más allá de las frías estadísticas oficiales, resulta necesario analizar el fenómeno de la llamada “Cifra Negra” en la extorsión digital. Se calcula que por cada caso denunciado en el Ecuador existen al menos tres que permanecen ocultos, ya sea por el temor de las víctimas o por la desconfianza en la capacidad técnica de la policía para rastrear a los extorsionadores en la Deep Web. Este silencio termina distorsionando las políticas publicas y minimiza la verdadera gravedad de esta amenaza.

El impacto socioeconómico es devastador, las pequeñas y medianas empresas (PYMES) en ciudades como Guayaquil o Manta están destinando un porcentaje significativo de sus ingresos al pago de “vacunas digitales” para evitar el secuestro de sus datos o el desprestigio en redes sociales. Por ello, la prueba digital no solo cumple una función procesal, sino que se convierte en una herramienta esencial para recuperar la paz pública. Sin una capacidad real de judicialización que se base en evidencia técnica robusta, la extorsión digital continuará evolucionando hacia formas más agresivas, como el uso de deepfakes para coaccionar a figuras públicas y empresarios

El Fenómeno del "Going Dark" y el Cifrado de Extremo a Extremo

Uno de los obstáculos más críticos y contemporáneos que enfrenta la persecución penal de la extorsión es el fenómeno técnico-jurídico conocido como "Going Dark". Este concepto describe la creciente brecha entre la capacidad legal de las autoridades para ordenar la interceptación de comunicaciones y su capacidad técnica para acceder a los datos. La implementación masiva del cifrado de extremo a extremo (E2EE) por parte de proveedores globales como WhatsApp o Telegram significa que ni siquiera las propias empresas tecnológicas pueden descifrar los mensajes en tránsito. Esto crea un "agujero negro" informativo donde los extorsionadores operan con una impunidad técnica casi absoluta, dificultando que los fiscales obtengan la materialidad del delito en tiempo real.

Ante la imposibilidad de interceptar el flujo de datos, la investigación debe volcarse hacia la forense de dispositivos finales, lo que implica la incautación física de los teléfonos móviles para realizar extracciones de memoria directa antes de que los datos sean borrados o el dispositivo se bloquee. Además, este escenario justifica la necesidad de fortalecer la cooperación internacional con las empresas tecnológicas mediante el canal de "peticiones de emergencia”. La doctrina internacional sugiere que, para compensar la opacidad del cifrado, el marco normativo ecuatoriano debe evolucionar hacia la regulación de la extracción de datos en la nube (Cloud Forensics), permitiendo que, previa autorización judicial, se puedan recuperar respaldos de las comunicaciones que no siempre están protegidos por el cifrado de extremo a extremo, recuperando así el equilibrio entre el derecho a la privacidad y el deber del Estado de perseguir el crimen

El Estándar de Admisibilidad: Pertinencia, Utilidad y Conducencia

Para que un mensaje sea admitido dentro de un juicio penal, debe cumplir con la tríada de conducencia, pertinencia y utilidad. La conducencia se entiende como el propósito legal del medio; en la actualidad, un archivo digital es el soporte adecuado para demostrar una amenaza. La pertinencia exige que dicho archivo permita probar elementos concretos del tipo penal de extorsión, como la coacción económica. Sin embargo, en muchos casos las acusaciones fracasan por presentar una cantidad excesiva de datos que carecen de utilidad real para el juzgador.

Superado el filtro de admisibilidad, el juez debe proceder a la valoración conforme a la Sana Critica. Esto implica que el juzgador no se encuentra sujeto a una tarifa legal estricta, sino que debe aplicar las reglas de la lógica, la ciencia y la experiencia. Surge entonces un problema: ¿cómo puede un juez, sin una formación técnica, valorar la fiabilidad de un algoritmo hash sin incurrir en la arbitrariedad? Esta valoración exige un dialogo, en el cual el informe pericial no es asumido como una verdad absoluta, sino como una opinión técnica susceptible de contradicción. Resulta fundamental que el análisis judicial examine la persistencia de la prueba, si existen dudas sobre si los sellos de tiempo presentan inconsistencias, el juez debe disminuir su valor probatorio en aplicación del principio in dubio pro reo, garantizando la seguridad jurídica frente a posibles errores de manipulación forense.

En la investigación de los delitos de extorsión, suele aparecer la tentación de obtener información mediante accesos no autorizados a cuentas de correo o redes sociales bajo el argumento de la urgencia. No obstante, si la obtención inicial de los datos vulnera el derecho a la intimidad y no cuenta con una orden judicial previa y especifica, toda la evidencia derivada carecerá de validez jurídica.

Esto conduce a la necesidad de aplicar el llamado “test de proporcionalidad” al momento de admitir la prueba digital, como un mecanismo de control que evite abusos y preserve los derechos fundamentales. El juez debe evaluar si la afectación al derecho a la privacidad del investigado es proporcional al fin perseguido, que es desarticular una red de extorsión. Además, se debe considerar la 'teoría del descubrimiento inevitable': si la fiscalía puede demostrar que habría llegado a esa evidencia digital de todas formas por medios legales, la prueba podría ser admitida. Este debate es fundamental para evitar que el exceso de tecnicismos se convierta en mecanismos de impunidad para delincuentes cibernéticos altamente capacitados

Además, el derecho a la contradicción exige que la fiscalía entregue a la defensa el acceso a la "copia espejo" de la evidencia para realizar una contra pericia. Sin esta verificación de los algoritmos hash, la prueba digital se volvería incuestionable, lo cual es peligroso ante la posibilidad de fallos técnicos o manipulaciones en el software de extracción.

Hacia un Modelo de Justicia Digital en Ecuador

Para revertir la falta de confianza pública y enfrentar con éxito la extorsión digital, Ecuador debe pasar de un modelo reactivo a uno proactivo y técnicamente sólido. Siguiendo las recomendaciones de la Comisión Europea (2025), es obligatorio que el país desarrolle un marco normativo integral que no solo nombre a la prueba digital, sino que regule minuciosamente su ciclo de vida.

Este fortalecimiento institucional requiere una visión interdisciplinaria que incluya:

- Estandarización de Protocolos: Realizar manuales para la recolección de evidencia en la nube y dispositivos móviles.
- Cooperación Judicial Internacional: Dado que la extorsión digital suele ignorar las fronteras, es vital fortalecer los tratados de asistencia legal mutua. Según la OECD (2024), el acceso oportuno a datos alojados en servidores extranjeros es el mayor obstáculo actual; por ello, la adhesión plena a instrumentos como el Convenio de Budapest es fundamental para superar las barreras jurisdiccionales

Metodología

La presente investigación se sustenta en un diseño metodológico solido que busca asegurar la validez y el rigor de los resultados obtenidos. El estudio adopta un enfoque cualitativo, lo que permite una aproximación más profunda a la doctrina y a la jurisprudencia, facilitando la comprensión de la prueba digital mas allá de su dimensión puramente técnica. El nivel de investigación es descriptivo y analítico, orientado a examinar las complejas normas y procesos que regulan la evidencia electrónica en los delitos de extorsión.

Fundamentación del Enfoque y Métodos de Investigación

La estructura metodológica de esta investigación ha sido concebida bajo un enfoque cualitativo de carácter descriptivo y analítico, lo que posibilita superar la simple recopilación de datos y ofrecer una interpretación critica de la realidad jurídica. La utilización del método inductivo-deductivo resulta esencial en este trabajo, ya que permite partir de la observación de casos concretos de extorsión dentro del sistema judicial ecuatoriano para derivar en principios generales que deben orientar a la prueba digital. Este tipo de razonamiento lógico asegura que las conclusiones alcanzadas no se queden en simples formulaciones teóricas, sino que puedan traducirse en soluciones prácticas aplicables a la labor cotidiana de fiscales y tribunales del país.

De igual manera, la aplicación del método comparativo se justifica por la necesidad de identificar modelos exitosos en ordenamientos jurídicos que han avanzado con mayor rapidez en el contexto de la era digital. Al contrastar de manera sistemática los marcos legales de España, Argentina, Estados Unidos y Colombia, se logra un análisis de "derecho proyectado", donde se evalúan qué instituciones jurídicas internacionales podrían integrarse

al COIP o al COGEP. Al analizar la Ley Orgánica de Protección de Datos Personales junto con el código penal, se pueden identificar los distintos enfoques de derechos que ocurren cuando el Estado intercepta comunicaciones privadas, permitiendo proponer un equilibrio que respete tanto la eficacia de la persecución penal como las garantías constitucionales de los ciudadanos.

Técnicas e Instrumentos de Recolección de Información

La técnica predominante fue la revisión bibliográfica en donde se utilizó el fichaje de contenido como instrumento principal para catalogar y analizar literatura especializada en revistas indexadas, tratados de derecho comparado y jurisprudencia de altas cortes.

El proceso de revisión se ejecutó bajo una estructura de cuatro fases:

1. Heurística: Localización y selección de fuentes primarias y secundarias con bases de datos científicas, priorizando la actualidad y el rigor académico.

2. Crítica: Evaluación de la pertinencia de los materiales respecto al fenómeno de la extorsión digital y la prueba pericial informática.

3. Análisis y Síntesis: Extracción de datos clave para integrar los hallazgos normativos con los reportes técnicos de organismos como Europol (2025) y el Ministerio del Interior (2025).

4. Formulación: Redacción de conclusiones y recomendaciones basadas en la evidencia contrastada durante el estudio.

Esta arquitectura metodológica permitió ver la problemática desde una visión completa, garantizando que las recomendaciones propuestas para el fortalecimiento del sistema judicial ecuatoriano tengan un sustento tanto teórico como práctico y comparativo.

Resultados

Análisis comparativo de la prueba digital en la legislación internacional

La Evolución del delito: De lo Físico a lo Bit

Históricamente, la extorsión era entendida como un delito de control territorial y coacción física, asociado a estructuras mafiosas tradicionales (Varese, 2010). Hoy, la extorsión se ejecuta a través de correos electrónicos, transferencias de criptoactivos y huellas digitales en redes sociales. Esta transformación exige que el Derecho Comparado sea la guía para actualizar nuestras leyes.

Modelos de Regulación Global

El presente análisis se estructura sobre tres ejes fundamentales para entender cómo el mundo está procesando la evidencia digital:

- El Modelo Europeo: Caracterizado por una armonización supranacional, que busca que la obtención de datos entre países de la Unión sea casi tan fluida como dentro de una misma frontera.
- El Sistema Anglo-Sajón (Estados Unidos): Enfocado en garantías constitucionales estrictas (como la Cuarta Enmienda) y una jurisprudencia muy desarrollada sobre la privacidad y la interceptación de comunicaciones.
- La Experiencia Latinoamericana: Donde países como Colombia y Argentina han liderado reformas específicas, pero aún luchan con su implementación y los recursos limitados.

Este enfoque multidisciplinario permitirá no solo identificar las debilidades de la legislación ecuatoriana, sino también proponer estrategias efectivas para la prevención y el control delictivo en el entorno tecnológico.

Delito y Evidencia: El Salto Cualitativo hacia la Virtualidad

Históricamente, la extorsión ha sido conceptualizada como un acto de coacción basado en la violencia física o en la amenaza directa de daño inminente, generalmente vinculado a estructuras o sistemas mafiosos que imponían tributos ilegales bajo una supuesta "protección" (Varese, 2010).

No obstante, la digitalización ha generado una transformación importante en el modus operandi; hoy en día, el autor del delito utiliza el anonimato que ofrece la red para intimidar sin necesidad de presencia física, ampliando el alcance de la conducta a nivel global y aumentando su complejidad técnica.

Dentro de este nuevo escenario, la prueba digital se convierte en el único medio capaz de romper esa barrera del anonimato. Elementos como los registros de transacciones en blockchain o billeteras digitales, los meta datos de las comunicaciones en aplicaciones de mensajería y los registros detallados de tráfico (logs) resultan esenciales para una correcta judicialización. De acuerdo con la OECD (2024) y Buestan (2025), este tipo de evidencias permite reducir la distancia entre autor y víctima, facilitando la reconstrucción del camino del delito y estableciendo la conexión delictiva necesariaa para una sentencia condenatoria.

El Modelo de la Unión Europea: Armonización y Cooperación Supranacional

A diferencia de otros sistemas, la UE procura que las fronteras nacionales no se conviertan en un obstaculo para la justicia penal. El eje central de esta politica es la reciente Hoja de Ruta para el Acceso Legal a los Datos (COM/2025/50 final), que fija un marco ténico - jurídico coordinado para la obtención y conservación de evidencias electrónicas en delitos transnacionales como la extorsión (Comisión Europea, 2025).

Este modelo se caracteriza por dos aspectos fundamentales:

- Reducción de la fricción jurisdiccional: Permite que una autoridad judicial de un Estado Miembro solicite pruebas directamente a un proveedor de servicios como una red social ubicado en otro Estado Miembro, sin recurrir a los lentos mecanismos tradicionales de cooperación internacional.
- Equilibrio garantista: El intercambio de información se rige por los principios de proporcionalidad y necesidad, de modo que la persecución penal no vulnere la privacidad de los ciudadanos ni las garantías procesales básicas.

El Modelo Estadounidense

La regulación de la prueba digital en los Estados Unidos está directamente condicionada por la Cuarta Enmienda, que protege a las personas frente a registros e incautaciones irrazonables (García, 2025).

En el modelo anglosajón, la obtención de evidencia digital exige de manera obligatoria una orden judicial (warrant) fundada en la llamada "causa probable". Esta orden no puede ser vaga ni general, debe detallar con precisión que datos se buscan y en que dispositivos se realizara la incautación. Este nivel de rigor cumple una doble función

1. Protección de la privacidad: Opera como un limite frente al poder punitivo del Estado.

2. Validez probatoria: Garantiza que la prueba sea solida dentro del juicio, reduciendo el riesgo de exclusión por violaciones a los derechos civiles.

No obstante, el sistema admite excepciones en situaciones de "peligro inminente", en las que la urgencia de salvar una vida o evitar la destrucción de la prueba autoriza la recolección sin orden previa, bajo un control judicial posterior estricto. Este modelo ha servido como referencia internacional para buscar un equilibrio entre la eficacia investigativa y el respeto a la libertad individual.

La Praxis Técnica en el Sistema Federal Estadounidense

En Estados Unidos, la jurisprudencia federal no se limita únicamente a exigir una orden judicial, sino que ha construido estándares técnicos complejos para la mantener la autenticidad de la evidencia. No es suficiente presentar un archivo digital; el Estado debe probar, mas allá de toda duda razonable, que la cadena de custodia no tuvo interrupciones y que la prueba representa de forma fiel la realidad digital existente en el momento que se realizó el hallazgo.

Este grado de exigencia implica que los agentes investigadores no actúen solo como policías, sino también como técnicos con certificaciones especializadas. Tal como expone García (2025), este modelo prioriza la protección del individuo frente a eventuales excesos del poder estatal, estableciendo que cualquier error en la documentación de la cadena de custodia puede dejar sin efecto meses de investigación.

El Modelo Colombiano: Control Judicial

Colombia se ha consolidado como un referente regional al desarrollar un esquema de controles judiciales tanto preventivos como posteriores. Su normativa no solo reconoce la importancia de la evidencia digital, sino que describe con precisión los procedimientos para la interceptación de comunicaciones y el acceso a meta datos, siempre bajo el filtro del principio de proporcionalidad.

La Corte Constitucional colombiana, en decisiones relevantes como la C-540/12, ha señalado que la vigilancia estatal en entornos digitales debe tener límites definidos para evitar abusos institucionales (Corte Constitucional de Colombia, 2012). Asimismo, Colombia fue pionera al promulgar la Ley 527 de 1999, que introdujo la noción de equivalencia y el uso de firmas digitales certificadas para garantizar la autenticidad e integridad de los documentos electrónicos, dándoles la misma fuerza jurídica que a las evidencias físicas.

Realidades Comparadas: Ecuador y Perú frente al Desafío Digital

En Ecuador, si bien el COIP (2014) y el COGEP (2015) establecen un marco legal para reconocer la prueba electrónica y exigen autorización judicial previa para su obtención, la práctica procesal evidencia una brecha preocupante. De acuerdo con Buestan (2025) y la Corte Constitucional del Ecuador (2020), el país no dispone de protocolos técnicos que unifiquen el análisis forense, lo que provoca una aplicación desigual de la ley según la capacidad técnica de cada unidad judicial.

En el caso peruano, el panorama es parecido. Los tribunales vienen aceptando de manera progresiva la validez de la prueba digital en los delitos informáticos, apoyándose en la autenticidad y en el respeto a las garantías procesales. No obstante, a diferencia de Colombia, Peru aun no cuenta con una regulación específica sobre la ciberextorsión dentro de su Código Penal, lo que obliga a los jueces a recurrir a tipos penales genéricos lo que ocasiona, en ciertos casos, vacíos en que la normativa lo debería considerar como delito o no

Hacia la Estandarización Internacional

La diversidad de enfoques normativos entre el garantismo estadounidense, la armonizacion europea y el control judicial colombiano representa un reto importante para la persecución de delitos transfronterizos. No obstante, también constituye una oportunidad para que países como Ecuador adopten estándares internacionales comunes. La creación de protocolos compartidos no solo facilitara la cooperación judicial, sino que permitirá que la lucha contra la extorsión digital se realice con respeto a los derechos humanos y a los principios del Estado de Derecho, evitando que la tecnología termine siendo un medio de impunidad o de opresión estatal.

Síntesis Comparativa y Perspectivas Globales

El estudio comparado muestra un abanico de respuestas frente a la ciberdelincuencia. Por un lado, la Unión Europea apuesta por un modelo de armonización que integra el soporte tecnológico con una coordinación jurídica sin precedentes (Comisión Europea, 2025). En contraste, el sistema anglosajón privilegia un garantismo constitucional, en el cual el control judicial funciona como resguardo de la privacidad (García, 2025).

En America Latina se evidencia un avance normativo relevante, aunque limitado por problemas relacionados con la capacitación y la escasez de recursos técnicos. Para que Ecuador alcance una persecución efectiva de la extorsión digital, resulta indispensable que los instrumentos legales no solo existan, sino que se adapten a la volatilidad de la realidad actual mediante la cooperación internacional junto con el fortalecimiento de capacidades forenses de última generación (OECD, 2024).

El Modelo de la Cuarta Enmienda y la "Expectativa Razonable de Privacidad"

Al examinar el modelo de Estados Unidos como posible referente para Ecuador, es necesario profundizar en la doctrina de la "Expectativa Razonable de Privacidad", surgida del caso "Katz v. United States". Este criterio constitucional establece que la protección de la Cuarta Enmienda no se limita a espacios físicos, sino que acompaña a la persona. En materia de prueba digital, esto implica que el Estado no puede acceder a los datos de un teléfono móvil o a la ubicación GPS de un ciudadano sin una orden judicial basada en causa probable, aun cuando el dispositivo se encuentre en un lugar público. Esta garantía constituye un pilar que impide que la investigación de una extorsión se transforme en una "expedición de pesca", donde se vulnere la privacidad de miles de personas inocentes con el fin de buscar y encontrar un responsable.

En Estados Unidos, una orden judicial para registrar un dispositivo electrónico debe ser "particularizada"; es decir, debe indicar con precisión que archivos se buscan, en que carpetas y dentro de que rango de fechas. Si la policía excede estos límites, la prueba es excluida bajo la "Doctrina del Fruto del Árbol Ponzoñoso". Expandir este análisis permite argumentar que Ecuador necesita reformar su normativa para que las órdenes de interceptación y registro digital en casos de extorsión no sean "cheques en blanco", sino mandatos judiciales que protejan la intimidad del investigado en áreas que no guardan relación con el ilícito, asegurando así que la justicia sea tan técnica como respetuosa de los derechos humanos.

Cooperación Internacional y el Convenio de Budapest como Horizonte

Dado que el delito de extorsión digital suele ejecutarse a través de infraestructuras transnacionales como lo son los servidores en Estados Unidos, servicios de correo en Europa y cuentas bancarias en paraísos fiscales, la soberanía nacional de Ecuador se ve limitada. Aquí es donde el Convenio de Budapest sobre Ciberdelincuencia surge como el estándar que el país debe aspirar a implementar plenamente. Este tratado internacional no solo tipifica conductas, sino que establece mecanismos ágiles para la asistencia penal, permitiendo la

conservación rápida de datos informáticos que, de otro modo, serían borrados por el proveedor de servicios antes de que llegue un exhorto diplomático tradicional

La relevancia de este apartado se encuentra en el estudio de la jurisdicción y la competencia dentro del ciberespacio. ¿Quién tiene la facultad de investigar una extorsión cuando el delincuente se ubica en Quito, la víctima en Guayaquil y los mensajes se encuentran almacenados en un servidor situado en Dublin? La doctrina de la "ubicuidad" plantea que el delito se comete tanto en el lugar donde se origina la acción como en aquel donde se producen sus efectos. No obstante, en ausencia de convenios de cooperación vigentes, el fiscal ecuatoriano se enfrenta a una verdadera barrera burocrática al intentar solicitar información a empresas como Meta o Google. Por esta razón, fortalecer el marco normativo internacional no constituye un simple interés académico, sino una necesidad operativa, solo a través de la estandarización de las solicitudes de evidencia transfronteriza y de la creación de puntos de contacto permanentes las 24 horas del día, Ecuador podrá disminuir la impunidad en delitos que, por su propia naturaleza, desafían las fronteras físicas de los Estados.

Discusión

Propuesta de reforma normativa para el fortalecimiento de la justicia digital

La presente investigación no solo busca diagnosticar las falencias del sistema actual, sino proponer soluciones concretas que permitan al Estado ecuatoriano enfrentar la criminalidad organizada con herramientas jurídicas. Ante las vulnerabilidades identificadas en el sistema procesal penal y civil, se propone una reforma integral al Código Orgánico Integral Penal (COIP) y al Código Orgánico General de Procesos (COGEP) bajo las siguientes estrategias:

Creación e Institucionalización de la "Preservación Expedita de Datos" (Quick Freeze)

Uno de los mayores obstáculos en la persecución de la extorsión es que la información es muy volátil. Actualmente, mientras la Fiscalía solicita y obtiene una orden judicial de interceptación, los registros de conexión (logs) suelen ser borrados por los proveedores de servicios (ISP) debido a sus políticas internas de almacenamiento. Por ello, se propone la incorporación de un artículo en el COIP que faculte a los agentes fiscales a ordenar la conservación inmediata de datos de tráfico por un periodo inicial de 90 días.

Esta medida no implica el acceso al contenido de las comunicaciones (el cual seguiría requiriendo orden judicial), sino el "congelamiento" de la información técnica. La reforma debe especificar que el incumplimiento por parte de las operadoras de telecomunicaciones se establecerá como el delito de desobediencia a decisiones legítimas de autoridad competente. Con esta figura, se garantiza que la evidencia digital sea inmovilizada en el instante mismo de la noticia del crimen, evitando que el transcurso del tiempo se convierta en un aliado para el extorsionador.

Subespecialización y Certificación de Peritos en el Consejo de la Judicatura

El sistema de acreditación pericial vigente en Ecuador padece de un enfoque generalista que resulta insuficiente para la complejidad de la extorsión digital. La presente propuesta exige la creación de categorías de especialización obligatoria dentro del Reglamento del Sistema Pericial Integral. Es de carácter obligatorio que el Consejo de la Judicatura diferencie al perito informático tradicional del experto en "Informática Forense de Redes" y "Cloud Forensics"

La reforma propone que, para intervenir en casos de delitos informáticos, el perito deba poseer o acreditar certificaciones internacionales vigentes y demostrar conocimientos avanzados en la arquitectura de aplicaciones de mensajería con cifrado de extremo a extremo. Esto garantiza que el profesional no solo se limite a realizar capturas de pantalla, sino que sea capaz de extraer meta datos, analizar los protocolos de red y sustentar la integridad del hash ante un tribunal. La parte técnica del cuerpo pericial reducirá los errores en la cadena de custodia y elevará la calidad de la prueba presentada, otorgando al juzgador elementos de convicción científica imposibles de objetar

Protocolo de Cooperación Directa y Canales Digitales Certificados con Big Tech

La soberanía digital de Ecuador se ve desafiada cuando la evidencia reside en servidores de empresas extranjeras como Meta, Google o X (antes Twitter) El procedimiento actual de asistencia penal internacional resulta anacrónico y excesivamente lento. Por ello, se plantea la necesidad de crear un marco legal interno que permita simplificar la solicitud de información no contenida, como los meta datos de registro y los logs de IP, a través de la creación de una Oficina de Enlace de Cooperación Tecnológica

Este esquema normativo haría posible que las solicitudes de datos de suscriptores se gestionen mediante canales digitales certificados y puntos de contacto permanentes para todo momento, en concordancia con las exigencias del Convenio de Budapest. La propuesta pretende disminuir los tiempos de respuesta, pasando de periodos de meses a solo algunos días, mediante la implementación de formatos de solicitud que respeten los parámetros internacionales de privacidad, pero que al mismo tiempo aseguren la entrega oportuna de la información necesaria para identificar a los verdaderos extorsionadores. Al agilizar estos trámites, se busca que la justicia penal sea verdaderamente eficaz y no quede reducida a un simbolismo frente a los delitos de carácter transnacional.

Análisis crítico de los hallazgos

El examen global de la prueba digital en los casos de extorsión pone en evidencia una brecha preocupante entre el nivel de complejidad tecnológica alcanzado por los delincuentes y la capacidad de respuesta del Estado ecuatoriano. A lo largo de esta investigación, se ha evidenciado que, si bien el marco normativo reconoce la existencia del documento electrónico, la práctica procesal adolece de una falta de estandarización técnica. Al contrastar el modelo ecuatoriano con el sistema europeo (Convenio de Budapest), la principal diferencia

radica en la agilidad para la obtención de datos transfronterizos; mientras Europa goza de una red de cooperación disponible en todo momento, Ecuador sigue dependiendo de exhortos diplomáticos que pueden tardar meses, periodo en el cual por el corto tiempo que tiene el documento digital, suele resultar en su inminente desaparición.

Un punto crítico de discusión es la Cifra Negra de la extorsión. El incremento del 174.9% en las denuncias oficiales es solo la "punta del iceberg". El miedo de las víctimas a que sus datos privados sean expuestos durante el peritaje, sumado a la desconfianza en la protección de su identidad, alimenta un sistema de impunidad. La legislación actual no contempla protocolos para la autenticidad de pruebas generadas por IA, lo que podría llevar a una crisis de validez en donde las pruebas reales sean descartadas por sospechas de manipulación, o viceversa.

Conclusiones

Se concluye de manera clara que el sistema judicial ecuatoriano atraviesa una crisis de confianza técnica en la etapa de preservación de la evidencia digital. La investigación demuestra que la integridad de la prueba se ve afectada desde el primer contacto policial, principalmente por la falta generalizada de laboratorios forenses certificados y por el uso inadecuado de herramientas tecnológicas. La practica frecuente de manipular dispositivos incautados sin emplear bloqueadores de escritura (write blockers) constituye una vulneracion grave al principio de mismidad de la prueba. Esta falencia técnica no solo debilita la teoria del caso de la Fiscalia, sino que también abre una oportunidad para que las defensas técnicas soliciten, y muchas veces consigan, la exclusión de evidencias esenciales por ruptura de la cadena de custodia. En definitiva, mientras no se estandarice el uso de protocolos científicos inalterables, la prueba digital en los delitos de extorsion continuara siendo vista como una evidencia frágil y fácilmente impugnable.

La presente investigación establece que la extorsión digital ha pulverizado las fronteras físicas del Estado, transformándose en un fenómeno de carácter transnacional. No obstante, se ha constatado que la normativa procesal ecuatoriana sigue anclada a una concepción clásica de territorialidad que resulta anacrónica frente a la realidad de la computación en la nube. El hecho de que la evidencia se encuentre con frecuencia almacenada en servidores extranjeros genera conflictos de jurisdicción que la legislación vigente no logra resolver con la rapidez necesaria. En este sentido, se determina que la soberanía digital del Ecuador depende de los tratados internacionales, en especial al Convenio de Budapest. Sin este marco de cooperación, el acceso a datos de suscriptores y meta datos en poder de grandes corporaciones tecnológicas seguirá siendo un tramite burocratico lento que favorece la impunidad del extorsionador trasfronterizo.

Finalmente, a pesar de los esfuerzos de modernización de los codigos sustantivos, persiste una brecha importante de conocimiento técnico entre los operadores de justicia. Se concluye

que una parte significativa de jueces y fiscales no cuenta con las competencias necesarias para valorar de forma autonoma elementos técnicos como los algoritmos de integridad (hash) o la interpretación de meta datos. Esta limitación no solo afecta la correcta apreciación de la prueba, sino que también incrementa la dependencia excesiva de los informes periciales, lo que puede derivar en decisiones judiciales basadas mas en la autoridad técnica que en un análisis critico propio del juzgador. Esta carencia de formación especializada deriva en una "dependencia pericial absoluta", donde el juzgador delega su facultad de valoración en el experto informático, aceptando sus conclusiones sin realizar el analisis respectivo. Esta situación es particularmente grave en las audiencias de juicio, donde la falta de capacidad de contradicción técnica impide que se cuestione la metodología del perito, transformando la pericia en una suerte de prueba que vulnera el principio de inmediación y la sana crítica.

Referencias bibliográficas

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. Registro Oficial Suplemento 180. Quito, Ecuador.

Batallas, F. E. (2023). Principio de contradicción en audiencias telemáticas. Yachana, 42–56. https://doi.org/10.62325/10.62325/yachana.v12.n1.2023.852

Briones, J. A., Barcia, S. G., & Soledispa, J. D. (2024). El testimonio anticipado como valor probatorio en los delitos sexuales. Ciencia Latina Revista Científica Multidisciplinar, 8(4), 7677–7698. https://doi.org/10.37811/cl_rcm.v8i4.12938

Cárdenas, K. (2021). La valoración de la prueba en procesos penales: Una perspectiva constitucional. Scielo Analytics. http://scielo.sld.cu/scielo.php?pid=S2218-36202021000200160&script=sci_arttext&tlng=en

Conde, D. I., Carrillo, A. M., & Hidalgo, V. M. (2023). El principio de contradicción en la prueba testimonial y el derecho a la defensa - Ecuador. Santiago, 380–397. https://santiago.uo.edu.cu/index.php/stgo/article/download/17514/5102

Constitución de la República del Ecuador. (2008, octubre 20). Registro Oficial 449. Asamblea Nacional del Ecuador. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Costaín, M. (2024). Derecho procesal penal, fundamentos, estructura, conceptos básicos y su relación con la teoría del delito. Corporación de Estudios y Publicaciones CEP.

Falconí, F. P., & Sotomayor, P. J. (2022). Vulneración de la garantía del debido proceso en el derecho a la defensa del investigado, afectada por la toma del testimonio anticipado en delitos sexuales. Revista Metropolitana de Ciencias Aplicadas, 5(1). https://www.redalyc.org/articulo.oa?id=721778113012

Gómez, J. A., & Zurita, A. C. (2023). La valoración de la prueba testimonial: Interrogatorio, contrainterrogatorio. Revista Metropolitana de Ciencias Aplicadas, 37–46. https://doi.org/10.62452/xr09gj90

Guerra, Á. L. (2022). Aplicación de la prueba indiciaria en el proceso penal ecuatoriano y la duda razonable. Revista Metropolitana de Ciencias Aplicadas, 128–137. https://doi.org/10.62452/vzhkgk23

Martínez, A. K., & Idrovo, L. M. (2022). Vulneración del principio de inmediación y contradicción en audiencias telemáticas del Tribunal de Garantías Penales. Iustitia Socialis, 117–144. https://doi.org/10.35381/racji.v7i1.1767

Palacios, I. C., & Peñafiel, S. A. (2022). Práctica del testimonio anticipado en el delito de tráfico ilícito de migrantes en el Cañar. Dominio de las Ciencias, 8(1). https://dialnet.unirioja.es/servlet/articulo?codigo=8383477

Paredes, K. D., & Solorzano, M. B. (2021). La valoración de la prueba en procesos penales: Una perspectiva constitucional. Revista Universidad y Sociedad, 13(2). http://scielo.sld.cu/scielo.php?pid=S2218-36202021000200160&script=sci_arttext&tlng=en

Polo, V. A., & Vázquez, A. F. (2024). Vacío jurídico en el Código Orgánico Integral Penal respecto a la necesidad del procesado de comparecer a la toma del testimonio anticipado. Religación: Revista de Ciencias Sociales y Humanidades, 9, 36. https://dialnet.unirioja.es/servlet/articulo?codigo=9412083

Pulla, D. J. (2023). Valoración del testimonio anticipado como prueba frente al principio de inmediación en el sistema acusatorio penal. Revista InveCom, 3(2), 1–21. https://doi.org/10.5281/zenodo.8056886

Resolución 117-2014. (2014). Protocolo para el uso de la cámara de Gesell. Consejo de la Judicatura. https://www.funcionjudicial.gob.ec/resources/pdf/resoluciones/2014cj/117-2014.pdf

Robayo, J. A., & Zurita, A. C. (2023). La eficacia de la prueba y el principio de economía procesal en materia civil. Revista Metropolitana de Ciencias Aplicadas, 192–200. https://doi.org/10.62452/87hwc391

Rodríguez, Y. L. (2024). Testimonio anticipado en el ámbito de los delitos sexuales en el Ecuador. Diálogos Avanzados sobre Derecho e Institucionalismo Contemporáneo, 6(9). https://doi.org/10.56124/aula24.v6i9.004

Romero, A. A., & León, A. A. (2023). La contradicción como derecho y principio en la prueba de oficio. Ciencia Latina Revista Científica Multidisciplinar, 7(5), 2453–2477. https://doi.org/10.37811/cl_rcm.v7i5.7894

Romero, C. J., & Cabrera, E. E. (2022). Vulneración del principio de contradicción con la práctica probatoria. Revista Arbitrada Interdisciplinaria Koinonía, 417–433. https://dialnet.unirioja.es/servlet/articulo?codigo=8651458

Ruiz, E. A., Peñafiel, E. A., Soria, Y. L., & Segarra, H. G. (2025). Restricciones procesales para la realización del testimonio anticipado en el proceso penal ecuatoriano. Revista UGC, 3(1), 147–155. https://universidadugc.edu.mx/ojs/index.php/rugc/article/view/83

Salas, F. L. (2021). Fiabilidad de la prueba testimonial: Breve análisis desde la psicología del testimonio y los errores de la memoria. Prolegómenos, 24(48), 53–67. https://doi.org/10.18359/prole.5701

Sánchez, F. (2025). Manual de estrategias en litigación penal y bases de argumentación jurídica. Corporación de Estudios y Publicaciones CEP.

Torres, D. F., Quintana, J. X., & Villa, C. A. (2022). Las audiencias telemáticas en materia penal y la correcta producción de los medios de prueba. Dilemas contemporáneos: Educación, política y valores. https://doi.org/10.46377/dilemas.v9i.3018

Velepucha, M. (2023). Violación y abuso sexual en el Código Orgánico Integral Penal. LEX ET LITTERAE.

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A.
Nota:
El artículo no es producto de una publicación anterior.