REVISTA CIENTÍFICA
Ciencia y Método
ISSN 3103-1072

EDITORIAL GRUPO AEA

Artículo Científico

Gobernanza del cibercrimen y admisibilidad de prueba digital transfronteriza

Cybercrime governance and the admissibility of cross-border digital evidence

Andrade-Gonzalez, Jonathan Xavier [1]
https://orcid.org/0009-0004-1862-5962
andradejonathan41@gmail.com
Investigador Independiente, Ecuador, Quevedo.

Autor de correspondencia [1]

DOI / URL: https://doi.org/10.55813/gaea/rcym/v4/n2/194

Resumen: El cibercrimen transnacional plantea desafíos crecientes para los sistemas penales, debido a que la evidencia digital suele encontrarse distribuida entre distintas jurisdicciones, proveedores privados, infraestructuras en la nube y marcos normativos heterogéneos. El objetivo del estudio fue analizar la relación entre la gobernanza del cibercrimen y la admisibilidad de la prueba digital transfronteriza en la literatura especializada. La investigación se desarrolló mediante una revisión bibliográfica exploratoria, documental y cualitativa, basada en artículos científicos, libros, estándares técnicos, tratados internacionales e informes institucionales publicados entre 2014 y 2026, con incorporación de fuentes previas de relevancia normativa. Los resultados evidencian que la fragmentación jurídica, las demoras en la cooperación internacional, la intervención de proveedores privados y las debilidades en cadena de custodia, autenticidad e integridad afectan la validez procesal de la evidencia digital. Asimismo, se identificó la necesidad de equilibrar eficacia investigativa con garantías procesales, control judicial, proporcionalidad y derecho de defensa. Se concluye que la admisibilidad de la prueba digital transfronteriza requiere un modelo integrado de gobernanza probatoria que articule cooperación internacional, estándares forenses, trazabilidad técnica y protección de derechos fundamentales.

Palabras clave: cibercrimen; prueba digital; cooperación internacional; cadena de custodia; admisibilidad probatoria.

Check for updates

Received: 21/Mar/2026
Accepted: 17/Abr/2026
Published: 30/Abr/2026

Cita: Andrade-Gonzalez, J. X. (2026). Gobernanza del cibercrimen y admisibilidad de prueba digital transfronteriza. *Revista Científica Ciencia Y Método*, *4*(2), 276-292. https://doi.org/10.55813/gaea/rcym/v4/n2/194

Revista Científica Ciencia y Método (RCyM)
https://revistacym.com
revistacym@editorialgrupo-aea.com
info@editoriagrupo-aea.com

Abstract:

Transnational cybercrime poses growing challenges for criminal justice systems, as digital evidence is often distributed across different jurisdictions, private providers, cloud infrastructures, and heterogeneous legal frameworks. The aim of this study was to analyze the relationship between cybercrime governance and the admissibility of cross-border digital evidence in specialized literature. The research was conducted through an exploratory, documentary, and qualitative bibliographic review based on scientific articles, books, technical standards, international treaties, and institutional reports published between 2014 and 2026, while also incorporating earlier sources of normative relevance. The findings show that legal fragmentation, delays in international cooperation, the involvement of private providers, and weaknesses in chain of custody, authenticity, and integrity affect the procedural validity of digital evidence. Likewise, the study identified the need to balance investigative effectiveness with procedural guarantees, judicial oversight, proportionality, and the right of defense. It is concluded that the admissibility of cross-border digital evidence requires an integrated model of evidentiary governance that articulates international cooperation, forensic standards, technical traceability, and the protection of fundamental rights.

Keywords: cybercrime; digital evidence; international cooperation; chain of custody; evidentiary admissibility.

1. Introducción

El cibercrimen plantea un problema de gobernanza penal que ya no puede comprenderse como una suma de delitos informáticos aislados, porque sus infraestructuras, víctimas, autores, proveedores de servicios y rastros probatorios suelen distribuirse entre jurisdicciones distintas. En este escenario, la prueba digital se convierte en el eje de la persecución penal, pero también en su punto más frágil: puede estar almacenada en la nube, bajo control de intermediarios privados, sujeta a leyes extranjeras y expuesta a rápida alteración o supresión. Además, el incremento de ataques de ransomware, fraude en línea, phishing, deepfakes y explotación de cadenas de suministro confirma que la respuesta estatal fragmentada resulta insuficiente frente a fenómenos técnicamente dinámicos y organizacionalmente transnacionales (World Economic Forum, 2025; Europol, 2024).

En consecuencia, la tensión central se ubica entre la necesidad de acceso oportuno a evidencia electrónica y la obligación de preservar soberanía, debido proceso, privacidad y garantías de defensa. El Convenio de Budapest configuró un marco internacional para armonizar tipos penales, poderes procesales y cooperación judicial en materia de ciberdelincuencia, mientras que su Segundo Protocolo Adicional incorporó herramientas para cooperación reforzada, divulgación de evidencia electrónica, contacto con proveedores y respuestas de emergencia (Council of

Europe, 2001, 2022). A ello se suma la Convención de Naciones Unidas contra la Ciberdelincuencia, adoptada en 2024, cuyo propósito incluye fortalecer la cooperación internacional y el intercambio de evidencia electrónica en delitos graves (UNODC, 2024).

No obstante, la existencia de instrumentos internacionales no elimina las afectaciones derivadas de la heterogeneidad normativa. La literatura advierte que las investigaciones transfronterizas enfrentan demoras, conflictos de jurisdicción, límites de asistencia legal mutua, incertidumbre sobre acceso directo a datos y dependencia de empresas privadas que operan como custodios de información probatoria (Brenner & Schwerha, 2002; Koops & Goodwin, 2014; Casino et al., 2022). Estas dificultades afectan tanto la eficacia penal como la admisibilidad judicial: una evidencia obtenida con rapidez puede ser excluida si vulnera garantías, mientras que una evidencia solicitada por canales formales puede perder valor si llega tarde, incompleta o sin trazabilidad suficiente (Casino et al., 2022).

Asimismo, la prueba digital presenta riesgos técnicos que inciden directamente en su fiabilidad: volatilidad de metadatos, manipulación, contaminación, fallas de preservación, debilidad de la cadena de custodia y ausencia de estándares homogéneos para documentar identificación, recolección, adquisición, preservación, análisis y reporte. Por ello, la admisibilidad no depende únicamente de que el dato exista, sino de que pueda acreditarse su autenticidad, integridad, pertinencia, reproducibilidad y obtención lícita mediante procedimientos verificables (ISO/IEC, 2012; Kent et al., 2006). En este punto, Stoykova (2021) advierte que las garantías procesales tradicionales no siempre se adaptan al ciclo contemporáneo de la evidencia digital, lo que puede comprometer la presunción de inocencia y la equidad del proceso penal.

La revisión bibliográfica se justifica porque la discusión suele avanzar por carriles separados: por un lado, la gobernanza internacional del cibercrimen; por otro, los estándares forenses de prueba digital; y, en un tercer plano, las garantías procesales aplicables a evidencia obtenida fuera del territorio. Esta separación impide construir criterios integrados para valorar cuándo una prueba digital transfronteriza debe considerarse jurídicamente admisible y técnicamente confiable. Además, los debates sobre nuevos tratados muestran que la cooperación internacional puede ampliar capacidades estatales, pero también generar riesgos de vigilancia, abuso transnacional o debilitamiento de salvaguardias si no se acompaña de controles de legalidad, necesidad, proporcionalidad y supervisión efectiva (Human Rights Watch, 2024; UNODC, 2024).

Desde esta perspectiva, el estudio resulta viable porque se apoya en literatura científica, tratados, estándares técnicos, informes institucionales y doctrina especializada de acceso público, sin requerir tratamiento de datos personales ni intervención sobre participantes humanos. En tal sentido, el objetivo general es analizar la relación entre gobernanza del cibercrimen y admisibilidad de la prueba

digital transfronteriza en la literatura especializada. De manera específica, se propone describir los marcos normativos internacionales aplicables, comparar los criterios técnicos y jurídicos de preservación y admisión, y determinar las brechas que afectan la cooperación probatoria entre jurisdicciones. Así, la contribución esperada consiste en articular un mapa crítico que conecte cooperación internacional, estándares forenses y garantías procesales, aportando originalidad al integrar dimensiones que con frecuencia se examinan de forma aislada (Casino et al., 2022; Stoykova, 2021).

2. Materiales y métodos

El estudio se desarrolló como una revisión bibliográfica exploratoria, de carácter documental y enfoque cualitativo, orientada a examinar cómo la literatura científica, normativa y técnica ha abordado la gobernanza del cibercrimen y la admisibilidad de la prueba digital transfronteriza. La elección de un alcance exploratorio respondió a la amplitud conceptual del fenómeno, pues la evidencia disponible se encuentra dispersa entre estudios jurídicos, investigaciones sobre cooperación internacional, estándares forenses digitales, informes institucionales y análisis de derechos fundamentales. En consecuencia, no se buscó medir la frecuencia estadística de un fenómeno ni probar relaciones causales, sino identificar categorías analíticas, tensiones recurrentes, vacíos argumentativos y líneas de convergencia entre los debates sobre cibercriminalidad, soberanía, cooperación penal, cadena de custodia, autenticidad, integridad y debido proceso. Este tipo de revisión resulta pertinente cuando el campo de estudio es heterogéneo y requiere ordenar críticamente conocimientos previos para delimitar problemas, conceptos y futuras preguntas de investigación.

La unidad de análisis estuvo constituida por documentos académicos, normativos e institucionales vinculados con tres ejes temáticos: gobernanza del cibercrimen, cooperación transfronteriza para obtención de evidencia electrónica y criterios de admisibilidad de prueba digital. Para ello, se consideraron artículos científicos revisados por pares, libros académicos, capítulos especializados, estándares técnicos, tratados internacionales, protocolos, informes de organismos intergubernamentales y documentos doctrinales con relevancia directa para el objeto de estudio. La búsqueda se proyectó sobre bases de datos y repositorios especializados como Scopus, Web of Science, HeinOnline, SSRN, ScienceDirect, SpringerLink, Google Scholar, sitios oficiales del Consejo de Europa, Naciones Unidas, Europol, NIST e ISO. Con esta delimitación se procuró integrar fuentes jurídicas, criminológicas, tecnológicas y procesales, evitando una lectura exclusivamente normativa o exclusivamente técnica del problema.

La estrategia de búsqueda se estructuró mediante combinaciones de palabras clave en español e inglés, empleando operadores booleanos para ampliar o restringir resultados según la pertinencia temática. Entre los términos utilizados se incluyeron: “cybercrime governance”, “cross-border digital evidence”, “electronic evidence admissibility”, “digital forensic evidence”, “chain of custody”, “mutual legal assistance”,

"Budapest Convention", "cloud evidence", "transnational criminal investigation", "prueba digital transfronteriza", "admisibilidad de evidencia electrónica" y "cooperación penal internacional". El periodo de revisión se delimitó entre 2014 y 2026, con el propósito de captar la evolución reciente del debate posterior a la expansión de la computación en la nube, la consolidación de estándares forenses digitales y los nuevos instrumentos internacionales sobre evidencia electrónica. No obstante, se incorporaron fuentes anteriores cuando constituyeron antecedentes normativos o teóricos indispensables para comprender el desarrollo del campo.

Los criterios de inclusión comprendieron documentos con relación directa con la investigación penal del cibercrimen, la circulación transnacional de evidencia digital, la cooperación internacional, la intervención de proveedores de servicios, la preservación forense de datos, la cadena de custodia y las garantías procesales asociadas a la admisibilidad probatoria. Se excluyeron textos meramente periodísticos, opiniones sin respaldo académico, documentos duplicados, fuentes sin autoría institucional o académica verificable y publicaciones centradas en ciberseguridad empresarial sin conexión con prueba digital o persecución penal. La selección se realizó en tres momentos sucesivos: lectura de títulos y resúmenes, revisión del texto completo y clasificación temática de los documentos finalmente incorporados. Esta secuencia permitió depurar la muestra documental y reducir sesgos de inclusión, manteniendo coherencia con los principios de transparencia, trazabilidad y reproducibilidad propios de las revisiones de literatura.

El análisis de la información se efectuó mediante lectura crítica y codificación temática, organizando los hallazgos en matrices comparativas que permitieron identificar definiciones, enfoques regulatorios, estándares técnicos, problemas de jurisdicción, criterios de admisión, garantías procesales y vacíos de investigación. A partir de esta organización, los documentos fueron contrastados según su naturaleza, alcance territorial, fuerza normativa, aporte conceptual y aplicabilidad al tratamiento de evidencia digital transfronteriza. Posteriormente, se elaboró una síntesis narrativa orientada a relacionar los hallazgos, no a cuantificarlos, con énfasis en las tensiones entre eficacia investigativa, soberanía estatal, cooperación internacional, control judicial y protección de derechos fundamentales. En términos éticos, la investigación no implicó intervención sobre personas ni tratamiento de datos personales, dado que se basó exclusivamente en fuentes públicas, verificables y correctamente referenciadas.

3. Resultados

3.1. Gobernanza del cibercrimen y criterios de admisibilidad de la prueba digital transfronteriza

La gobernanza del cibercrimen exige comprender que el delito digital no se agota en la conducta ilícita ejecutada mediante sistemas informáticos, sino que se despliega en

una arquitectura transnacional de datos, proveedores, infraestructuras, usuarios, jurisdicciones y autoridades con competencias parcialmente superpuestas. En ese marco, la prueba digital transfronteriza se convierte en el núcleo operativo del proceso penal, porque la persecución de ransomware, fraude informático, intrusión ilícita, suplantación de identidad o explotación de plataformas depende de datos que pueden estar alojados, replicados o administrados fuera del territorio del juez que conoce el caso. Por ello, la admisibilidad probatoria no puede evaluarse solo desde la pertinencia del contenido, sino desde una cadena más compleja que integra legalidad de obtención, cooperación internacional, preservación técnica, trazabilidad, autenticidad, integridad y posibilidad real de contradicción por la defensa (Casino et al., 2022; Stoykova, 2021).

3.1.1. Fragmentación normativa en la cooperación internacional

La fragmentación normativa constituye el primer obstáculo estructural, porque el cibercrimen opera en un espacio funcionalmente continuo, mientras que la potestad penal permanece organizada en territorios estatales separados por reglas distintas de competencia, privacidad, reserva judicial, asistencia legal mutua, protección de datos y admisión probatoria. Así, una misma evidencia puede ser accesible técnicamente, pero jurídicamente inaccesible si el Estado requerido exige requisitos incompatibles con los del Estado requirente, si no existe tratado aplicable, si la conducta no cumple el principio de doble incriminación o si el proveedor de servicios se encuentra sometido a mandatos legales contradictorios. De ahí que Casino et al. (2022) sostengan que las investigaciones transfronterizas no solo enfrentan demoras, sino también barreras prohibitivas derivadas de la heterogeneidad de los marcos legales y procedimentales.

Esta fragmentación no debe interpretarse como una simple deficiencia administrativa, sino como una tensión constitutiva entre soberanía penal y circulación global de datos. En los procedimientos tradicionales, el lugar de comisión del delito, el lugar de hallazgo de la evidencia y el lugar de actuación de la autoridad solían coincidir o, al menos, podían delimitarse con relativa claridad; en cambio, en el entorno digital, los datos pueden generarse en un país, almacenarse automáticamente en otro, ser gestionados por una empresa domiciliada en un tercero y afectar a víctimas ubicadas en múltiples jurisdicciones. Esta dispersión impone una gobernanza multinivel, en la que los Estados deben coordinar potestades sin renunciar a controles de legalidad, mientras los jueces deben valorar evidencia producida por procedimientos extranjeros que no siempre responden a los mismos estándares internos (Casino et al., 2022; Council of Europe, 2022).

El Convenio de Budapest representa el antecedente más influyente para reducir esa dispersión, pues propuso una base común de criminalización, poderes procesales y cooperación internacional en materia de ciberdelincuencia. Sin embargo, su utilidad depende de la adhesión de los Estados, de la implementación legislativa interna y de la capacidad de sus instituciones para ejecutar solicitudes con rapidez y garantías. El Segundo Protocolo Adicional al Convenio de Budapest intenta responder a las

limitaciones del modelo clásico, al habilitar mecanismos de cooperación reforzada, solicitudes directas a registradores, cooperación con proveedores de servicios, intercambio de datos de abonado y tráfico, cooperación de emergencia, investigaciones conjuntas y videoconferencia, todo ello bajo salvaguardias de derechos humanos, Estado de derecho y protección de datos (Council of Europe, 2001, 2022).

No obstante, la ampliación de canales de cooperación no resuelve por sí sola el problema de admisibilidad. Una evidencia obtenida a través de cooperación directa con proveedores puede ser útil para preservar datos urgentes, pero también puede generar objeciones si la defensa cuestiona la competencia de la autoridad solicitante, la suficiencia del control judicial, la identificación del titular de los datos o la compatibilidad con garantías constitucionales del foro que juzga. En otras palabras, la cooperación internacional produce acceso, pero la admisibilidad exige legitimación procesal. Esta distinción es decisiva, porque la gobernanza probatoria no se agota en obtener evidencia, sino en asegurar que esa evidencia pueda ingresar al juicio sin erosionar el debido proceso ni convertir la urgencia investigativa en una excepción permanente a los controles judiciales (Stoykova, 2021; Council of Europe, 2022).

La Convención de Naciones Unidas contra la Ciberdelincuencia agrega una nueva capa a este escenario, porque fue adoptada por la Asamblea General el 24 de diciembre de 2024 como el primer tratado global integral sobre la materia y busca fortalecer la cooperación internacional, incluida la compartición de evidencia electrónica para delitos graves (UNODC, 2024). Sin embargo, su potencial dependerá de la ratificación, de la entrada en vigor y de la manera en que cada Estado adapte sus disposiciones al derecho interno. Por ello, más que eliminar la fragmentación, el nuevo tratado puede inaugurar una fase de interoperabilidad compleja, en la que convivirán el Convenio de Budapest, su Segundo Protocolo, regímenes regionales, acuerdos bilaterales, legislación nacional y prácticas de proveedores privados (UNODC, 2024; Casino et al., 2022).

3.1.2. Tensiones entre eficacia investigativa y garantías procesales

La segunda dimensión problemática surge de la tensión entre eficacia investigativa y garantías procesales. En materia digital, la evidencia puede desaparecer con rapidez por borrado remoto, rotación de registros, cifrado, anonimización, políticas de retención limitada o migración automática entre servidores. Esta volatilidad explica que las autoridades demanden instrumentos ágiles de preservación y producción de datos; sin embargo, la rapidez no puede convertirse en criterio suficiente de legitimidad. Stoykova (2021) advierte que la investigación penal asistida por tecnología plantea amenazas no resueltas para el juicio justo y la presunción de inocencia, particularmente cuando se emplean herramientas de forma inconsistente, cuando las garantías tradicionales no se adaptan al ciclo de la evidencia digital y cuando falta validación de la fiabilidad forense.

El conflicto se vuelve más intenso cuando el acceso a datos transfronterizos desplaza parte de la función probatoria hacia proveedores privados. Plataformas, operadores de nube, redes sociales, empresas de mensajería y registradores de dominio pueden custodiar información decisiva para el proceso penal, pero no son tribunales ni autoridades imparciales; responden a políticas internas, obligaciones contractuales, regímenes de cumplimiento normativo y mandatos legales de diversos países. Por ello, un modelo de cooperación que dependa excesivamente de la respuesta directa de proveedores puede acelerar la investigación, pero también puede oscurecer la trazabilidad jurídica de la prueba si no existe constancia suficiente sobre solicitud, alcance, criterios de búsqueda, método de extracción, formato de entrega y control posterior de integridad (Council of Europe, 2022; Mason & Seng, 2021).

La Unión Europea ha intentado enfrentar esa tensión mediante el paquete normativo sobre evidencia electrónica, que busca agilizar la producción y conservación de datos por proveedores de servicios en procesos penales. Juszczak y Sason (2023) explican que este régimen se apoya en la confianza mutua y pretende ofrecer un mecanismo más rápido y jurídicamente estructurado para obtener evidencia electrónica en el espacio europeo de libertad, seguridad y justicia. No obstante, su diseño exige equilibrar la eficacia con el control de proporcionalidad, los recursos efectivos, la protección de datos, la intervención de autoridades competentes y la prevención de órdenes excesivamente amplias o incompatibles con derechos fundamentales (Juszczak & Sason, 2023).

El debate garantista no debe reducirse a una oposición abstracta entre seguridad y derechos, porque una investigación eficaz también requiere evidencia confiable y jurídicamente resistente. Si la prueba se obtiene de manera irregular, sin autorización suficiente o sin documentación verificable, su aparente utilidad inicial puede transformarse en debilidad procesal al momento de la admisión o valoración. En este sentido, el debido proceso no opera como obstáculo externo a la investigación, sino como condición de calidad probatoria: obliga a que la evidencia pueda ser explicada, reproducida, impugnada y contextualizada ante un tribunal. Por ello, la eficacia investigativa debe medirse no solo por la velocidad de acceso al dato, sino por la capacidad de convertir ese dato en prueba legítima y controvertible (Stoykova, 2021; Casino et al., 2022).

La presunción de inocencia también se ve comprometida cuando la evidencia digital se presenta como si tuviera una neutralidad técnica incuestionable. Un registro de conexión, una geolocalización, una dirección IP, una conversación extraída de una plataforma o un archivo recuperado de un dispositivo no hablan por sí mismos: requieren interpretación pericial, contexto de producción, explicación de márgenes de error, validación de herramientas y delimitación de hipótesis alternativas. Cuando esa mediación técnica no se transparenta, el acusado puede quedar en desventaja, porque se le exige controvertir procedimientos que desconoce o que no puede replicar por falta de acceso a herramientas, registros completos o información sobre la metodología empleada (Stoykova, 2021; Stoykova et al., 2022).

3.1.3. Cadena de custodia, autenticidad e integridad técnica de la prueba digital

La cadena de custodia es el puente entre la existencia material del dato y su admisibilidad jurídica. En la prueba digital, este puente es especialmente delicado, porque la evidencia puede copiarse, alterarse, fragmentarse, sincronizarse o perder metadatos sin que el cambio sea perceptible para un observador no especializado. Por ello, no basta con afirmar que un archivo, registro o comunicación fue hallado; es indispensable reconstruir cómo fue identificado, recolectado, adquirido, preservado, transferido, examinado y presentado. La norma ISO/IEC 27037:2012 establece directrices para identificación, recolección, adquisición y preservación de evidencia digital potencialmente valiosa, y además señala su utilidad para facilitar el intercambio de evidencia entre jurisdicciones (ISO/IEC, 2012).

La autenticidad exige demostrar que la evidencia procede de la fuente que se afirma, mientras que la integridad exige acreditar que no fue alterada de manera relevante desde su adquisición hasta su presentación judicial. En términos prácticos, ambos requisitos se sostienen mediante procedimientos como preservación de originales, generación y verificación de valores hash, bitácoras de acceso, imágenes forenses, documentación de herramientas, registro de custodios, control de versiones y explicación de cualquier transformación técnica realizada sobre los datos. El NIST SP 800-86 ofrece orientación para integrar técnicas forenses en la respuesta a incidentes y enfatiza la necesidad de atender tanto la dimensión técnica como el cumplimiento normativo aplicable, incluyendo regulaciones locales, federales e internacionales (Kent et al., 2006).

La evidencia transfronteriza amplifica los riesgos de ruptura de custodia porque puede pasar por múltiples manos, sistemas, autoridades, formatos y entornos normativos. Un proveedor puede entregar registros en un formato propietario; una autoridad extranjera puede convertirlos a otro soporte; un laboratorio puede extraer subconjuntos; una fiscalía puede seleccionar fragmentos relevantes; y el tribunal puede recibir una versión procesalmente depurada. Cada una de esas operaciones puede ser legítima, pero debe quedar documentada para que la defensa y el juez puedan verificar continuidad, completitud y ausencia de manipulación material. En consecuencia, la cadena de custodia digital no es un trámite burocrático, sino un dispositivo de racionalidad probatoria que permite controlar la fiabilidad de la evidencia en contextos de alta complejidad técnica (Mason & Seng, 2021; ISO/IEC, 2012).

La literatura empírica muestra que las debilidades de documentación no son meramente hipotéticas. En un estudio sobre investigaciones forenses digitales en la policía noruega, Stoykova et al. (2022) examinaron 124 informes vinculados con adquisición, examen y análisis de computadoras, teléfonos móviles y dispositivos de almacenamiento, y encontraron que en 21 casos seleccionados aleatoriamente la documentación era insuficiente para valorar la fiabilidad de la evidencia digital. Además, el estudio reportó dificultades para rastrear las acciones forenses ejecutadas sobre cada elemento, vincular la evidencia con su fuente, justificar métodos y

herramientas, o validar resultados y tasas de error, lo que ilustra la distancia entre los estándares normativos y la práctica institucional (Stoykova et al., 2022).

La admisibilidad, por tanto, debe apoyarse en una concepción robusta de fiabilidad técnico-jurídica. No se trata únicamente de demostrar que un dato "existe", sino de mostrar que fue obtenido de forma lícita, preservado sin contaminación, interpretado mediante métodos válidos y presentado con suficiente transparencia para permitir contradicción. Cuando esa trazabilidad falta, la prueba digital corre el riesgo de convertirse en una evidencia de autoridad, aceptada por la sola confianza en el perito, la plataforma o el organismo requirente. Frente a ello, la gobernanza probatoria debe exigir que los informes forenses describan el procedimiento con un nivel de detalle suficiente para que otro experto pueda comprenderlo, evaluarlo y, cuando sea posible, replicarlo (Kent et al., 2006; Stoykova et al., 2022).

3.1.4. Modelo integrado de gobernanza probatoria transfronteriza

Un modelo integrado de gobernanza probatoria transfronteriza debe partir de una premisa: la prueba digital no pertenece exclusivamente al campo técnico ni exclusivamente al campo jurídico. Su admisibilidad depende de la convergencia entre normas de cooperación, estándares forenses, garantías procesales, capacidades institucionales y responsabilidades de los proveedores privados. Por ello, el modelo debe abandonar la lógica fragmentaria que separa "obtención internacional", "análisis técnico" y "decisión judicial", para reemplazarla por un ciclo completo de gobernanza de la evidencia, desde la solicitud inicial de preservación hasta la valoración contradictoria en juicio (Casino et al., 2022; Stoykova, 2021).

La primera capa del modelo debe ser normativa y cooperativa. En ella se definen autoridades competentes, umbrales de gravedad, tipos de datos solicitables, exigencias de autorización judicial, mecanismos de urgencia, causales de rechazo, notificación, protección de datos y recursos de impugnación. Esta capa es indispensable para evitar que la cooperación transfronteriza derive en forum shopping probatorio, es decir, en la búsqueda de jurisdicciones menos exigentes para obtener evidencia que luego se pretende usar en un proceso con garantías más estrictas. El Segundo Protocolo de Budapest y la Convención de Naciones Unidas ofrecen instrumentos relevantes, pero su eficacia dependerá de que la cooperación no se conciba solo como rapidez, sino como transferencia jurídicamente controlada de información probatoria (Council of Europe, 2022; UNODC, 2024).

La segunda capa debe ser técnico-forense y orientarse a estándares mínimos comunes. En este nivel se fijan exigencias de identificación, adquisición, preservación, documentación, análisis, validación de herramientas, control de errores, conservación de metadatos y presentación inteligible de resultados. La ventaja de esta capa es que permite traducir la diversidad jurídica en un lenguaje técnico compartido: aunque los países difieran en sus reglas procesales, pueden acordar procedimientos mínimos de preservación e integridad que faciliten la confianza judicial posterior. En ese sentido, ISO/IEC 27037:2012 y NIST SP 800-86 funcionan como referencias para construir una

gramática común de manejo de evidencia digital en escenarios nacionales y transfronterizos (ISO/IEC, 2012; Kent et al., 2006).

La tercera capa debe ser jurisdiccional y garantista. Su finalidad es asegurar que el juez no admita evidencia digital únicamente porque proviene de una autoridad extranjera o de un proveedor reconocido, sino porque supera un examen de licitud, pertinencia, necesidad, proporcionalidad, autenticidad, integridad y posibilidad de contradicción. Este control debe incluir preguntas concretas: quién solicitó los datos, con qué base legal, qué autoridad autorizó la medida, qué datos fueron preservados, cómo se extrajeron, quién los custodió, qué transformaciones sufrieron, qué herramientas se usaron, qué margen de error existe y cómo puede la defensa controvertirlos. Solo así la admisibilidad deja de ser un acto formal y se convierte en una evaluación sustantiva de confiabilidad procesal (Stoykova, 2021; Mason & Seng, 2021).

El modelo integrado también debe reconocer la centralidad de los proveedores privados sin convertirlos en autoridades penales informales. Su participación es inevitable porque concentran datos decisivos para la investigación, pero debe estar sometida a reglas de transparencia, trazabilidad, minimización, seguridad de entrega y rendición de cuentas. La cooperación directa con proveedores puede ser útil en situaciones urgentes o para obtener datos de abonado, pero debe complementarse con controles posteriores capaces de verificar que la información entregada corresponde exactamente a lo solicitado, que no se obtuvieron datos excedentes y que la defensa puede conocer las condiciones de producción del material probatorio (Council of Europe, 2022; Juszczak & Sason, 2023).

En suma, la admisibilidad de la prueba digital transfronteriza debería evaluarse mediante una matriz de cuatro ejes: licitud de obtención, trazabilidad de custodia, fiabilidad técnica y compatibilidad con derechos fundamentales. Esta matriz permite diferenciar entre evidencia disponible y evidencia procesalmente utilizable. La primera puede existir en servidores, cuentas, copias de seguridad, dispositivos o plataformas; la segunda, en cambio, exige una justificación jurídica y técnica suficiente para ingresar al proceso penal. Desde esta perspectiva, la gobernanza del cibercrimen no consiste únicamente en perseguir delitos más rápido, sino en construir condiciones institucionales para que la evidencia digital circule entre jurisdicciones sin perder validez, confiabilidad ni legitimidad democrática (Casino et al., 2022; UNODC, 2024).

4. Discusión

Los hallazgos de la revisión permiten sostener que la gobernanza del cibercrimen no puede reducirse a la tipificación de conductas informáticas ni a la ampliación de capacidades policiales, pues el núcleo del problema se desplaza hacia la circulación legítima, verificable y contradictoria de la prueba digital entre jurisdicciones. En efecto, la evidencia electrónica se ha convertido en el principal punto de fricción entre la

eficacia penal y el Estado de derecho, ya que los datos relevantes para investigar delitos digitales suelen estar bajo control de proveedores privados, almacenados en infraestructuras distribuidas y sometidos a marcos legales concurrentes. Esta constatación coincide con Casino et al. (2022), quienes advierten que la investigación penal transfronteriza enfrenta barreras derivadas de la heterogeneidad normativa, los tiempos de cooperación y la insuficiencia de los mecanismos tradicionales frente a la sofisticación del cibercrimen.

En este sentido, la fragmentación normativa aparece como una condición estructural y no como un inconveniente meramente procedimental. El Convenio de Budapest ofreció una arquitectura pionera para armonizar delitos, poderes procesales y cooperación internacional, pero su eficacia depende de la adhesión estatal, de su implementación interna y de la capacidad institucional para ejecutar solicitudes con rapidez y garantías (Council of Europe, 2001). El Segundo Protocolo Adicional intenta superar parte de esas limitaciones al incorporar mecanismos de cooperación reforzada y divulgación de evidencia electrónica; sin embargo, su operatividad sigue condicionada por diferencias nacionales sobre privacidad, autorización judicial, protección de datos y control de legalidad (Council of Europe, 2022). Por tanto, la gobernanza internacional avanza, pero lo hace sobre una base todavía desigual y jurídicamente policéntrica.

La adopción de la Convención de Naciones Unidas contra la Ciberdelincuencia introduce una oportunidad para universalizar mínimos comunes de cooperación, especialmente porque reconoce la necesidad de compartir evidencia electrónica vinculada con delitos graves (UNODC, 2024). No obstante, su potencial no debe interpretarse como una solución automática, ya que los tratados internacionales producen marcos de coordinación, pero la admisibilidad probatoria continúa dependiendo del juez nacional que evalúa licitud, pertinencia, autenticidad, integridad y compatibilidad con derechos fundamentales. En consecuencia, la discusión relevante no consiste únicamente en determinar si los Estados pueden acceder a datos ubicados en el extranjero, sino en establecer bajo qué condiciones ese acceso genera evidencia procesalmente utilizable y no solo información investigativa preliminar (Casino et al., 2022; UNODC, 2024).

La tensión entre eficacia investigativa y garantías procesales se intensifica porque la evidencia digital exige rapidez, pero el proceso penal exige control. Los datos pueden desaparecer por políticas de retención limitada, cifrado, borrado remoto o migración entre servidores; sin embargo, la urgencia no legitima por sí misma la reducción de estándares de autorización, proporcionalidad, contradicción o defensa. Stoykova (2021) muestra que la prueba digital genera amenazas no resueltas para la equidad procesal y la presunción de inocencia, particularmente cuando las tecnologías se emplean de modo inconsistente, las garantías tradicionales no se adaptan al entorno digital y la fiabilidad forense no se somete a pruebas suficientes. Así, la celeridad investigativa solo adquiere legitimidad si se integra en procedimientos transparentes, auditables y judicialmente controlables (Barzola-Plúas, 2022).

La cooperación directa con proveedores de servicios expresa con nitidez esta ambivalencia. Por un lado, permite responder a la volatilidad de los datos y evita que la asistencia legal mutua se convierta en un cuello de botella; por otro, puede desplazar funciones cuasi probatorias hacia actores privados que no poseen legitimidad jurisdiccional (Jaramillo-Becerra et al., 2025). El paquete europeo sobre evidencia electrónica intenta ordenar este problema mediante órdenes de producción y conservación dirigidas a proveedores, pero también exige salvaguardas sobre competencia, control judicial, protección de datos, recursos efectivos y proporcionalidad (Juszczak & Sason, 2023). De este modo, el desafío no es escoger entre cooperación formal o cooperación directa, sino diseñar canales híbridos que combinen rapidez operativa con trazabilidad jurídica suficiente (Jaramillo-Quezada et al., 2025).

Desde la dimensión técnico-forense, la discusión confirma que la admisibilidad de la prueba digital depende menos de la existencia del dato que de la posibilidad de reconstruir su ciclo de vida probatorio. ISO/IEC 27037:2012 establece directrices para la identificación, recolección, adquisición y preservación de evidencia digital, mientras que NIST SP 800-86 desarrolla orientaciones para integrar técnicas forenses en la respuesta a incidentes y documentar adecuadamente el proceso (ISO/IEC, 2012; Kent et al., 2006). En términos jurídicos, esto implica que autenticidad e integridad no son fórmulas retóricas, sino exigencias demostrables mediante cadena de custodia, valores hash, bitácoras, control de accesos, validación de herramientas y explicación pericial comprensible para el tribunal (Mason & Seng, 2021).

La evidencia empírica revisada refuerza la necesidad de no presumir la fiabilidad de la prueba digital por su apariencia técnica. Stoykova et al. (2022), al evaluar investigaciones forenses digitales en la policía noruega, identificaron problemas de documentación y trazabilidad que dificultaban valorar la confiabilidad de los procedimientos aplicados (Mendoza-Armijos et al., 2023). Este hallazgo es especialmente relevante porque muestra que incluso en contextos institucionales avanzados pueden existir brechas entre el estándar normativo y la práctica forense (Mina-Bone, 2024). En consecuencia, la cadena de custodia debe comprenderse como una garantía epistémica y procesal: no solo conserva objetos digitales, sino que permite examinar la racionalidad del procedimiento que transforma datos en prueba judicial (Stoykova et al., 2022).

A partir de lo anterior, el modelo integrado de gobernanza probatoria transfronteriza se perfila como la respuesta más consistente frente a la dispersión normativa, la volatilidad tecnológica y la exigencia de garantías (Samaniego-Quiguiri & Bonilla-Morejón, 2024). Dicho modelo debe articular cuatro niveles: cooperación internacional jurídicamente delimitada, intervención regulada de proveedores, estandarización técnico-forense y control judicial sustantivo de admisibilidad. Lasagni (2025) destaca que la admisibilidad de la evidencia digital plantea complicaciones específicas en la investigación penal, especialmente por su naturaleza técnica y por las diferencias entre sistemas procesales. Por ello, la prueba digital transfronteriza debe superar una

matriz de licitud, trazabilidad, fiabilidad y compatibilidad con derechos fundamentales antes de incorporarse al juicio (Lasagni, 2025; Casino et al., 2022).

La principal implicación teórica de esta revisión es que la gobernanza del cibercrimen debe desplazarse desde una lógica centrada en el acceso hacia una lógica centrada en la admisibilidad. Obtener datos no equivale a producir prueba; preservar información no equivale a garantizar integridad; y cooperar internacionalmente no equivale a cumplir automáticamente con el debido proceso (Llanos-García et al., 2025). En esa línea, la contribución del enfoque propuesto consiste en reunir debates que suelen aparecer separados: derecho internacional penal, cooperación judicial, forense digital, derechos fundamentales y valoración probatoria. Esta integración permite comprender que la eficacia contra el cibercrimen solo es sostenible cuando la arquitectura institucional que obtiene evidencia también asegura su control, explicación y refutabilidad (Stoykova, 2021; Mason & Seng, 2021).

Finalmente, la revisión también evidencia límites que deben orientar investigaciones futuras. Al tratarse de un estudio exploratorio y bibliográfico, sus resultados no permiten medir empíricamente la frecuencia con que la prueba digital transfronteriza es excluida, admitida o controvertida en tribunales concretos (Moreno-Sacón & García-Segarra, 2025). Por ello, futuras investigaciones deberían comparar jurisprudencia nacional, analizar expedientes judiciales, entrevistar operadores de justicia y evaluar protocolos forenses aplicados en casos reales. No obstante, la discusión desarrollada permite afirmar que el debate contemporáneo ya no gira únicamente en torno a cómo perseguir mejor el cibercrimen, sino a cómo impedir que la expansión de capacidades transfronterizas produzca evidencia técnicamente opaca, jurídicamente vulnerable o incompatible con las garantías del proceso penal democrático (Casino et al., 2022; Stoykova et al., 2022).

5. Conclusiones

La gobernanza del cibercrimen exige superar los enfoques exclusivamente nacionales, porque la evidencia digital relevante para investigar delitos informáticos suele encontrarse distribuida entre jurisdicciones, proveedores privados, infraestructuras en la nube y marcos normativos heterogéneos. En consecuencia, la prueba digital transfronteriza no debe ser entendida solo como un insumo técnico, sino como un objeto jurídico complejo cuya validez depende de la cooperación internacional, la legalidad de obtención, la preservación forense y el respeto de las garantías procesales.

La fragmentación normativa constituye uno de los principales límites para la persecución eficaz del cibercrimen, debido a que los Estados mantienen reglas distintas sobre competencia, privacidad, asistencia judicial, autorización de medidas intrusivas y admisibilidad probatoria. Por ello, aunque instrumentos como el Convenio de Budapest, su Segundo Protocolo Adicional y la Convención de Naciones Unidas

contra la Ciberdelincuencia fortalecen la cooperación, su eficacia real depende de la armonización interna, la interoperabilidad procesal y la existencia de controles judiciales capaces de convertir la información obtenida en prueba jurídicamente utilizable.

La tensión entre eficacia investigativa y garantías procesales demuestra que la rapidez en el acceso a datos no puede justificar la flexibilización indefinida del debido proceso. La evidencia digital es volátil y puede desaparecer con facilidad, pero su incorporación al juicio requiere autorización legítima, proporcionalidad, posibilidad de contradicción, transparencia metodológica y respeto de los derechos fundamentales. En ese sentido, una investigación penal solo puede considerarse eficaz cuando logra transformar datos digitales en prueba confiable, verificable y procesalmente resistente.

La cadena de custodia, la autenticidad y la integridad técnica se consolidan como condiciones indispensables para la admisibilidad de la prueba digital transfronteriza. No basta con presentar archivos, registros, metadatos o comunicaciones electrónicas; es necesario demostrar cómo fueron identificados, recolectados, preservados, transferidos, analizados y documentados. Cuando estos procedimientos carecen de trazabilidad, la evidencia pierde fuerza probatoria, aumenta el riesgo de exclusión judicial y se debilita la confianza en la decisión penal.

Finalmente, el estudio permite concluir que la respuesta más sólida frente al cibercrimen transnacional es un modelo integrado de gobernanza probatoria. Dicho modelo debe articular cooperación internacional, estándares técnico-forenses, intervención regulada de proveedores, control judicial sustantivo y garantías de defensa. Su aporte principal consiste en desplazar el debate desde la simple obtención de datos hacia la construcción de evidencia admisible, íntegra y compatible con un proceso penal democrático.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.

Referencias Bibliográficas

Barzola-Plúas, Y. G. (2022). Reformas Constitucionales en Ecuador: Impacto y Perspectivas. *Revista Científica Zambos*, *1*(1), 86-101. https://doi.org/10.69484/rcz/v1/n1/23

Brenner, S. W., & Schwerha, J. J., IV. (2002). Transnational evidence gathering and local prosecution of international cybercrime. *The John Marshall Journal of Computer & Information Law, 20*(3), 347–395. https://repository.law.uic.edu/jitpl/vol20/iss3/1/

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity, 8*(1), Article tyac014. https://doi.org/10.1093/cybsec/tyac014

Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). Council of Europe. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224). Council of Europe. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

Human Rights Watch. (2024, December 30). *New UN cybercrime treaty primed for abuse*. https://www.hrw.org/news/2024/12/30/new-un-cybercrime-treaty-primed-abuse

International Organization for Standardization. (2012). *ISO/IEC 27037:2012: Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence*. ISO. https://www.iso.org/standard/44381.html

ISO/IEC. (2012). *ISO/IEC 27037:2012: Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence*. https://www.iso.org/standard/44381.html

Jaramillo-Becerra, J. D., Gaibor-Vásconez, L. E., López-Soria, Y., & García-Segarra, H. G. (2025). La discrecionalidad administrativa en el Ecuador: Del uso legítimo a la arbitrariedad – Sentencia No. 1381-17-EP/22. *Revista Científica Ciencia Y Método, 3*(4), 292-308. https://doi.org/10.55813/gaea/rcym/v3/n4/111

Jaramillo-Quezada, D. M., Jaramillo-Rivadeneira, A. M., & Freire-Gaibor, E. F. (2025). El uso indebido del arraigo personal en materia flagrante frente al principio de igualdad. *Revista Científica Ciencia Y Método, 3*(4), 278-291. https://doi.org/10.55813/gaea/rcym/v3/n4/110

Juszczak, A., & Sason, E. (2023). The use of electronic evidence in the European Area of Freedom, Security, and Justice: An introduction to the new EU package on e-evidence. *Eucrim, 2023*(2), 182–200. https://doi.org/10.30709/eucrim-2023-014

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

Koops, B.-J., & Goodwin, M. (2014). *Cyberspace, the cloud, and cross-border criminal investigation: The limits and possibilities of international law*. Tilburg Institute for Law, Technology, and Society. https://doi.org/10.2139/ssrn.2698263

Lasagni, G. (2025). Admissibility of digital evidence. In V. Franssen & S. Tosza (Eds.), *The Cambridge handbook of digital evidence in criminal investigations* (pp. 126–152). Cambridge University Press. https://doi.org/10.1017/9781009049771.007

Llanos-García, R. V., Ocampo-Valle, G. F., Bonilla-Fierro, L. F., & Calero-Brito, E. E. (2025). Jurisprudencia educativa como pilar de la equidad y el acceso al derecho a la educación. *Journal of Economic and Social Science Research, 5(*2), 51-66. https://doi.org/10.55813/gaea/jessr/v5/n2/188

Mason, S., & Seng, D. (Eds.). (2021). *Electronic evidence and electronic signatures* (5th ed.). University of London Press. https://doi.org/10.14296/2108.9781911507246

Mendoza-Armijos, H. E., Camacho-Medina, B. M., & García-Segarra, H. G. (2023). Análisis de la justicia restaurativa como alternativa al sistema penal tradicional en América Latina. *Revista Científica Ciencia Y Método, 1*(3), 58-69. https://doi.org/10.55813/gaea/rcym/v1/n3/20

Mina-Bone, S. G. (2024). Evolución del derecho penal económico frente a los delitos financieros digitales. *Revista Científica Ciencia Y Método, 2*(3), 52-66. https://doi.org/10.55813/gaea/rcym/v2/n3/50

Moreno-Sacón, V. C., & García-Segarra, H. G. (2025). Independencia judicial en Ecuador y los desafíos frente al control del Consejo de la Judicatura. *Journal of Economic and Social Science Research, 5*(2), 115-131. https://doi.org/10.55813/gaea/jessr/v5/n2/192

Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. In *Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)* (pp. 11–20). IEEE. https://doi.org/10.1109/TPS-ISA62245.2024.00012

Samaniego-Quiguiri, D. P., & Bonilla-Morejón, D. M. . (2024). Análisis de la Evolución del Derecho Constitucional en Ecuador: Implicaciones para el Desarrollo Democrático. Revista Científica Zambos, 3(3), 1-14. https://doi.org/10.69484/rcz/v3/n3/53

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review, 42*, Article 105575. https://doi.org/10.1016/j.clsr.2021.105575

Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation, 40*, Article 301351. https://doi.org/10.1016/j.fsidi.2022.301351

United Nations Office on Drugs and Crime. (2024). *United Nations Convention against Cybercrime*. United Nations. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/