EL CONTROL DE CONVENCIONALIDAD APLICADO A LA PRUEBA DIGITAL EN EL PROCESO PENAL COMO REFERENTE CONTEMPORANEO DE LA TUTELA JUDICIAL EFECTIVA

CONVENTIONALITY CONTROL APPLIED TO DIGITAL EVIDENCE IN THE CRIMINAL PROCEDURE AS A CONTEMPORARY REFERENCE FOR EFFECTIVE JUDICIAL PROTECTION

Julio Bonifacio Baquiax Bulux[1]

Resumen

El presente trabajo académico realiza un análisis jurídico exhaustivo sobre la confluencia entre el control de convencionalidad y la prueba digital dentro del proceso penal contemporáneo, destacando su impacto directo en la garantía de la tutela judicial efectiva. La investigación se adentra en el mecanismo del control de convencionalidad, una creación doctrinal y jurisprudencial del Sistema Interamericano de Derechos Humanos, que exige a los operadores de justicia nacionales la armonización del derecho interno con la Convención Americana sobre Derechos Humanos y la jurisprudencia de la Corte Interamericana. Se examina la naturaleza sui generis de la prueba digital, caracterizada por su inmaterialidad, volatilidad, replicabilidad y transnacionalidad, y los desafíos procedimentales que de ella emanan. El artículo postula que la licitud, admisibilidad, valoración y preservación de la evidencia electrónica deben ser analizadas bajo el prisma de los estándares interamericanos. Se abordan los retos específicos que plantean el almacenamiento en la nube, el cifrado de datos y la cooperación jurídica internacional, argumentando que una aplicación rigurosa del control de convencionalidad es indispensable para salvaguardar derechos fundamentales como la privacidad y la defensa en la era digital, consolidando así la vigencia del Estado de Derecho.

Palabras clave: control de convencionalidad, prueba digital, proceso penal, tutela judicial efectiva, derechos humanos, Corte Interamericana de Derechos Humanos.

Abstract

This academic paper provides a comprehensive legal analysis of the confluence between conventionality control and digital evidence within contemporary criminal procedure, highlighting its direct impact on the guarantee of effective judicial protection. The research delves into the mechanism of conventionality control, a doctrinal and jurisprudential creation of the Inter-American Human Rights System, which requires national justice operators to harmonize domestic law with the American Convention on Human Rights and the jurisprudence of the Inter-American Court. It examines the sui generis nature of digital evidence, characterized by its immateriality, volatility, replicability, and transnationality, and the procedural challenges that arise from it. The article posits that the lawfulness, admissibility, assessment, and preservation of electronic evidence must be analyzed through the lens of Inter-American standards. It addresses the specific challenges posed by cloud storage, data

Recepción: 10 de junio de 2025/ Evaluación: 20 de julio de 2025/ Aprobado: 10 de agosto de 2025

[1] Maestro en Derecho Penal. Maestro en Derecho Constitucional. Doctor en Ciencias en Derecho. Profesor de Postgrado Universidad de San Carlos de Guatemala. Profesor de Postgrado Centro Universitario de Occidente. Profesor de Postgrado Universidad Mariano Galvez. Juez de Paz, Juez de Primera Instancia Penal, Juez presidente de Tribunal de Sentencia Pena NYDCA: Magistrado suplente de Corte de Apelaciones. Email: jbaquiax@sep.usac.edu.gt ORCID: https://orcid.org/0009-0005-2482-2409

encryption, and international legal cooperation, arguing that a rigorous application of conventionality control is essential to safeguard fundamental rights such as privacy and defense in the digital age, thereby consolidating the rule of law.

Keywords: conventionality control, digital evidence, criminal procedure, effective judicial protection, human rights, Inter-American Court of Human Rights.

Introducción

La irrupción de la tecnología digital ha reconfigurado de manera indeleble las interacciones sociales, económicas y, por supuesto, las conductas delictivas. Este nuevo paradigma ha introducido en el escenario del proceso penal un elemento probatorio de naturaleza disruptiva: la prueba digital. Su tratamiento procesal, desde la obtención hasta la valoración, plantea desafíos inéditos que tensionan las categorías jurídicas tradicionales y ponen a prueba la capacidad de los sistemas de justicia para garantizar los derechos fundamentales. En este contexto, el presente trabajo académico aborda, desde una perspectiva jurídica rigurosa, la intersección entre el control de convencionalidad y la prueba digital, analizando su impacto como un referente ineludible para la materialización de la tutela judicial efectiva en el siglo XXI.

El control de convencionalidad, como mecanismo que impone a toda autoridad pública, y en especial a los jueces, la obligación de verificar la compatibilidad de las normas y actos internos con la Convención Americana sobre Derechos Humanos (CADH) y la jurisprudencia de la Corte Interamericana de Derechos Humanos (Corte IDH), emerge como la herramienta hermenéutica idónea para enfrentar estos retos (Corte IDH, 2006a). Su aplicación exige a los tribunales nacionales trascender el formalismo de sus legislaciones procesales para evaluar la admisibilidad, pertinencia y valoración de la evidencia digital conforme a los estándares internacionales sobre derechos humanos. Esta labor no es meramente declarativa, sino que constituye un pilar para el fortalecimiento del Estado de Derecho en una sociedad globalizada y tecnológicamente interconectada.

La investigación se estructura en seis capítulos que buscan ofrecer una visión integral del fenómeno. El primero de ellos se dedica al marco conceptual y la evolución jurisprudencial del control de convencionalidad, sentando las bases teóricas del análisis. El segundo capítulo explora la naturaleza jurídica de la prueba digital y los principios rectores que el Sistema Interamericano ha delineado en materia probatoria. El tercer capítulo se enfoca en las garantías fundamentales, como la privacidad y la legalidad, durante la obtención y admisibilidad de la evidencia. El cuarto capítulo aborda los procedimientos técnicos indispensables para asegurar la integridad de la prueba, particularmente la cadena de custodia digital, desde una perspectiva convencional.

El quinto capítulo analiza dos momentos cruciales: el ejercicio del derecho de defensa frente a la complejidad técnica de esta prueba y los estándares para su correcta valoración judicial, incluyendo la fiabilidad del peritaje informático. Finalmente, el sexto capítulo se sumerge en los desafíos más contemporáneos y disruptivos: el tratamiento de la prueba alojada en la nube, el fenómeno del cifrado, la relevancia de los metadatos y la impostergable necesidad de una cooperación internacional eficaz. A través de este recorrido, se pretende demostrar que solo mediante un diálogo judicial transnacional, facilitado por el control de convencionalidad, es posible construir un proceso penal justo y equitativo en la era digital.

El Control de Convencionalidad como Marco de Análisis

Para comprender la profunda implicancia del control de convencionalidad en el tratamiento de la prueba digital, es imperativo desentrañar primero su marco conceptual y su notable evolución jurisprudencial. Este mecanismo, desarrollado pretorianamente por la Corte

Interamericana de Derechos Humanos (Corte IDH), ha redefinido la relación entre el derecho nacional y el derecho internacional de los derechos humanos en el continente americano, transformando el rol del juez nacional en un garante primario de la Convención Americana sobre Derechos Humanos (CADH). Su esencia radica en un mandato vinculante para todos los órganos del Estado, que los compele a ejercer un control de compatibilidad entre los actos y normas internas y el corpus iuris interamericano. Este control implica verificar la compatibilidad de las normas y prácticas internas con la CADH, la jurisprudencia de la Corte IDH y otros tratados interamericanos de los cuales el Estado sea parte, siendo una obligación que corresponde a toda autoridad pública (Corte IDH, s.f., Cuadernillo de Jurisprudencia de la Corte Interamericana de Derechos Humanos No. 7: Control de Convencionalidad; Rousset Siri, 2014).

Fundamento y Concepto del Control de Convencionalidad

El primer obstáculo para una correcta regulación y valoración de la prueba digital es de naturaleza conceptual. Tratar un archivo digital como si fuera un documento físico o un objeto material es un error categórico que ignora sus propiedades definitorias. Como señalan autores como Delgado Martín (2020) y Silva (2021), la evidencia digital es, por esencia, intangible, volátil, fácilmente duplicable y modificable sin dejar rastros evidentes, y a menudo, transfronteriza. Un correo electrónico, por ejemplo, no existe en un único lugar; reside simultáneamente en el dispositivo del emisor, en múltiples servidores de correo y en el dispositivo del receptor, cada uno bajo jurisdicciones potencialmente distintas.

Esta naturaleza etérea se manifiesta en una distinción técnica con profundas consecuencias procesales: la diferencia entre evidencia volátil y no volátil. La información contenida en la memoria de acceso aleatorio (RAM) de un ordenador —como contraseñas activas, conexiones de red o fragmentos de conversaciones de chat— es evidencia volátil. Se pierde irrevocablemente en el instante en que el dispositivo se apaga. Por el contrario, la información en discos duros, memorias USB o CD es no volátil, ya que persiste sin energía. Esta distinción obliga a los primeros intervinientes en una escena del crimen a tomar una decisión crítica: ¿desconectar el equipo para preservarlo físicamente, arriesgando la pérdida de toda la evidencia volátil, o realizar una adquisición "en vivo" con el sistema encendido, arriesgando la alteración del estado del sistema? La respuesta a esta pregunta puede determinar el éxito o el fracaso de una investigación y la validez de la prueba obtenida.

Asimismo, la prueba digital no se limita al contenido visible de un archivo. A menudo, la información más valiosa reside en los metadatos: datos sobre los datos. Un documento de texto no es solo su contenido, sino también la información sobre su autor, las fechas de creación y modificación, el software utilizado y el historial de revisiones. Un "mensaje de datos", en la terminología de la legislación colombiana, abarca esta totalidad de información susceptible de ser creada, transmitida o almacenada por medios electrónicos. Ignorar los metadatos es como leer una carta anónima sin analizar el sobre, el sello, el matasellos o la caligrafía; es renunciar a una dimensión crucial de la prueba.

Evolución Jurisprudencial y Expansión de su Alcance y la tensión con las categorías jurídicas tradicionales

El vertiginoso desarrollo tecnológico impone retos significativos a los operadores jurídicos, no solo en el ámbito probatorio, sino también en relación con los principios fundamentales del derecho penal (Martínez Galindo, 2022). La intangibilidad de la información, considerada un bien jurídico a proteger, el desvanecimiento de teorías jurídicas tradicionales que vinculan acción, tiempo y espacio, el anonimato que puede amparar al delincuente informático, y la dificultad para recolectar pruebas de hechos delictivos de carácter

universal, son algunos de los problemas que tensionan el sistema jurídico actual (González, 2017).

En muchas legislaciones, la ausencia de una regulación específica y de protocolos claros para la prueba digital genera conflictos entre los derechos individuales y los mecanismos de investigación estatal (Afonso, 2021 ; Ochoa, 2018 ; Quevedo & Zamora, 2022 ; Silva, 2021). Esta situación puede llevar a la impunidad de ciertos delitos o a la vulneración de derechos fundamentales durante el proceso de obtención de la prueba.

La tensión entre la prueba digital y las categorías jurídicas tradicionales evidencia una brecha sistémica en la adaptación del derecho a la realidad tecnológica, lo que puede resultar en impunidad o en la vulneración de derechos. La rápida evolución de las Tecnologías de la Información y la Comunicación (TIC) ha superado la capacidad de adaptación de los marcos legales existentes, generando una "insuficiencia legal" (Armenta Deu, 2018). Esta insuficiencia se traduce en la falta de una regulación específica y protocolos estandarizados para la prueba digital (Afonso, 2021; Ochoa, 2018; Quevedo & Zamora, 2022; Silva, 2021), lo que, a su vez, crea incertidumbre jurídica y dificulta la obtención y valoración de la prueba de manera lícita y eficaz. La consecuencia es un riesgo dual: por un lado, los delitos digitales pueden quedar impunes debido a la imposibilidad de obtener pruebas válidas; por otro, las pruebas pueden ser obtenidas vulnerando derechos fundamentales, lo que las convierte en ilícitas y, por tanto, inadmisibles (Bujosa Vadell et al., 2021; Congreso CDMX, s.f.; Rodrigo, 2021; Universidad de Valencia, 2021). Este panorama subraya la necesidad urgente de armonizar las legislaciones y de una capacitación profunda para los operadores jurídicos (Afonso, 2021; Ochoa, 2018; Quevedo & Zamora, 2022; Relatic Panamá, s. f.; Silva, 2021).

La Prueba Digital y sus Principios Rectores en el Sistema Interamericano.

La prueba digital, también denominada evidencia electrónica, ha emergido como una categoría probatoria sui generis cuya relevancia en el proceso penal contemporáneo es innegable y creciente. Su correcta incorporación y valoración son fundamentales para la resolución de una vasta gama de delitos. Sin embargo, sus características intrínsecas la distinguen de la prueba tradicional y plantean desafíos significativos que deben ser abordados desde la perspectiva de los derechos humanos. El Sistema Interamericano, a través de la jurisprudencia de la Corte IDH, ha establecido un conjunto de principios rectores en materia probatoria que, si bien no fueron concebidos originalmente para la evidencia digital, resultan plenamente aplicables a ella mediante una interpretación evolutiva y dinámica, guiada por el control de convencionalidad.

La prueba digital en cuya definición resalta varios elementos esenciales: se refiere a cualquier tipo de información; debe haber sido producida, almacenada o transmitida por medios electrónicos; y su propósito es acreditar hechos dentro de un proceso judicial (Delgado Martín, 2020).

Es importante señalar que, en algunos sistemas jurídicos, como el colombiano, la legislación no ha establecido una noción autónoma y clara de "evidencia electrónica". En su lugar, el tratamiento y la valoración de esta evidencia se basan en el concepto de "mensajes de datos" o "documentos electrónicos" (Morales Sánchez, 2016). Por ejemplo, la Ley 527 de 1999 en Colombia introdujo el concepto de "mensaje de datos", otorgándole fuerza probatoria y definiéndolo como información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares (Morales Sánchez, 2016). De manera similar, la doctrina mexicana concibe la prueba digital como cualquier información con valor probatorio contenida o transmitida por un medio electrónico, distinguiendo entre la información que reside en dispositivos y aquella que se transmite a través de redes de comunicación (Congreso CDMX, s.f.).

La ausencia de una definición legal unificada y autónoma de "prueba digital" a nivel global o regional genera inconsistencias en su tratamiento y valoración, lo que afecta la seguridad jurídica. La diversidad conceptual, donde diferentes legislaciones se basan en nociones como "mensajes de datos" o "documentos electrónicos" en lugar de una categoría propia de prueba digital, conduce a una aplicación heterogénea de los principios y requisitos probatorios. Esta situación se traduce en incertidumbre para los operadores jurídicos y las partes involucradas, lo que puede resultar en una disparidad en la admisibilidad y valoración de la misma evidencia digital en distintas jurisdicciones o incluso dentro de una misma, comprometiendo la predictibilidad y la seguridad jurídica del proceso penal.

La prueba digital posee características que la distinguen de la evidencia física. Según la doctrina, estas son sus principales cualidades:

Intangibilidad: Solo puede ser percibida y comprendida a través de procesos informáticos.

Replicabilidad: Puede ser copiada ilimitadamente, lo que desafía el concepto tradicional de "originalidad" (Bujosa Vadell et al., 2021).

Volatilidad: Es susceptible de ser modificada o alterada con facilidad, siendo esta una de las mayores preocupaciones procesales (Bujosa Vadell et al., 2021; Fernández, 2020).

Delebilidad: Puede ser destruida fácilmente, aun cuando su soporte físico permanezca intacto (Bujosa Vadell et al., 2021).

Heterogeneidad: Proviene de una gran diversidad de fuentes, lo que implica distintos métodos de incorporación al proceso (Martínez Galindo, 2022).

Las características inherentes de la prueba digital, como su intangibilidad, volatilidad, replicabilidad y delebilidad, son la causa principal de los desafíos procesales que presenta, especialmente en lo que respecta a su autenticidad e integridad. La intangibilidad y volatilidad de la prueba digital hacen que sea fácilmente manipulable y susceptible de alteración o destrucción rápida (Fernández, 2020; Bujosa Vadell et al., 2021). Esta vulnerabilidad genera una necesidad crítica de garantizar su integridad y autenticidad a lo largo de todo el proceso. En consecuencia, se impulsa la importancia de protocolos rigurosos de cadena de custodia y el uso de herramientas forenses como los hashes criptográficos (Congreso CDMX, s.f.; Hacker Mentor, s.f.). La replicabilidad, por su parte, dificulta la identificación del "original" (Bujosa Vadell et al., 2021), lo que exige mecanismos adicionales de verificación. Estas características fundamentales son, por lo tanto, el motor que impulsa la evolución del derecho probatorio en la era digital.

El principio de licitud probatoria es otro estándar fundamental. La Corte IDH ha sido enfática en establecer la regla de exclusión para pruebas obtenidas mediante tortura o tratos crueles, inhumanos o degradantes (Corte IDH, 2010b). Por analogía y mediante una interpretación evolutiva, este principio debe extenderse a la exclusión de pruebas digitales obtenidas con violación de otros derechos fundamentales, como el derecho a la privacidad y a la inviolabilidad de las comunicaciones (Fuente base, 2024) . Finalmente, el proceso valorativo debe regirse por el principio de la sana crítica racional, que exige un análisis razonado que pondere todos los elementos aportados al proceso (Corte IDH, 1998) . En materia digital, esto compele a los juzgadores a adquirir conocimientos técnicos básicos o, en su defecto, a apoyarse de manera crítica y fundamentada en la asistencia pericial para no incurrir en valoraciones arbitrarias.

Para aplicar el control de convencionalidad de manera efectiva, es necesario sistematizar los estándares desarrollados por la Corte IDH en materia de prueba y garantías judiciales. La siguiente tabla no es meramente ilustrativa, sino una herramienta analítica que condensa décadas de jurisprudencia en un conjunto coherente de principios. Demuestra que las obligaciones de investigar con seriedad, excluir la prueba ilícita y proteger la privacidad no son

conceptos abstractos, sino deberes estatales concretos y exigibles que deben ser ahora traducidos al ámbito digital.

Garantías Fundamentales en la Obtención y Admisibilidad de la Prueba Digital

La fase de obtención de la prueba digital es, quizás, el momento más crítico en su ciclo de vida procesal, pues es donde se produce la mayor tensión con los derechos fundamentales del investigado. La injerencia en dispositivos electrónicos como ordenadores y teléfonos móviles, o el acceso a comunicaciones privadas, implica una intromisión de gran intensidad en el núcleo del derecho a la privacidad. Por ello, el control de convencionalidad exige que los procedimientos de obtención y los criterios de admisibilidad de esta prueba se ajusten de manera estricta a los estándares derivados de la CADH, principalmente de los derechos a la privacidad (Art. 11), al debido proceso (Art. 8) y a la tutela judicial efectiva (Art. 25) (Fuente base, 2024).

Tabla de Jurisprudencia Clave de la Corte IDH sobre Prueba y Debido Proceso

Nombre del Caso	Año	Derechos Violados (Selección)	Principio/Holding Clave Relevante para la Prueba
Caso de la "Panel Blanca" (Paniagua Morales y otros) vs. Guatemala	1998	Garantías Judiciales (Art. 8), Protección Judicial (Art. 25)	El Estado tiene el deber indelegable de conducir una investigación seria, imparcial y efectiva ante violaciones de derechos humanos.
Caso Myrna Mack Chang vs. Guatemala	2003	Derecho a la Vida (Art. 4), Garantías Judiciales (Art. 8)	La responsabilidad del Estado se compromete por la obstrucción de la justicia, el ocultamiento o la manipulación de pruebas por parte de sus agentes.
Caso Tibi vs. Ecuador	2004	Integridad Personal (Art. 5), Garantías Judiciales (Art. 8)	Establece una regla de exclusión absoluta para cualquier prueba, incluidas las confesiones, obtenida mediante coacción o tortura.
Caso de las Masacres de Ituango vs. Colombia	2006	Garantías Judiciales (Art. 8), Protección Judicial (Art. 25)	La obligación de investigar debe ser asumida por el Estado como un deber jurídico propio y no como una simple formalidad.
Caso Almonacid Arellano y otros vs. Chile	2006	Garantías Judiciales (Art. 8)	Formulación explícita del control de convencionalidad, obligando al poder judicial a inaplicar las leyes internas que entren en conflicto con la Convención.
Caso Escher y otros vs. Brasil	2009	Derecho a la Privacidad (Art. 11), Garantías Judiciales (Art. 8)	La vigilancia estatal (ej. interceptación de comunicaciones) debe ser excepcional, estar prevista en la ley, perseguir un fin legítimo y ser necesaria y proporcionada.
Caso González y otras ("Campo Algodonero") vs. México	2009	Varios	El deber de investigar debe llevarse a cabo con perspectiva de género y debida diligencia, evitando estereotipos que socaven la investigación.
Caso Cabrera García y Montiel Flores vs. México	2010	Integridad Personal (Art. 5), Garantías Judiciales (Art. 8)	Refuerza la invalidez absoluta de la prueba obtenida en violación de derechos fundamentales, vinculándola con el derecho a un juicio justo.

Nota: Elaborado por el autor.

Requisitos de pertinencia, necesidad y licitud

Para que la prueba digital sea admisible, debe cumplir con criterios estrictos:
Pertinencia: La prueba digital debe ser relevante para acreditar los hechos objeto del proceso (thema decidendi). Esto implica que debe existir una relación lógica y directa entre el hecho que se pretende probar mediante el medio probatorio específico y los hechos que constituyen el objeto de la controversia (Bujosa Vadell et al., 2021; Delgado Martín, 2020).

Necesidad: La prueba debe ser útil para esclarecer los hechos controvertidos. Es decir, su práctica debe ser indispensable o imprescindible porque no existen suficientes elementos

probatorios alternativos que generen el convencimiento del juez sobre lo que se pretende probar (Bujosa Vadell et al., 2021; Delgado Martín, 2020).

Licitud: La obtención de la evidencia digital no puede, bajo ninguna circunstancia, vulnerar derechos fundamentales constitucionalmente protegidos, como el derecho a la intimidad o el secreto de las comunicaciones (Bujosa Vadell et al., 2021; Congreso CDMX, s.f.). Además, su obtención debe respetar los principios de proporcionalidad, idoneidad y justificación de la medida (Bujosa Vadell et al., 2021; Congreso CDMX, s.f.).

El cumplimiento de los requisitos exigidos por las leyes procesales es fundamental para que la prueba acceda al proceso de manera válida (Delgado Martín, 2020).

La autenticidad y la integridad son conceptos centrales para la validez de la prueba digital. La autenticidad se refiere a la coincidencia entre el autor aparente y el autor real de una declaración o de la información (Poder Judicial de Michoacán, s.f.). En el contexto de la prueba digital, la autenticidad garantiza que la muestra sobre la cual se realiza la investigación es idéntica a la muestra original y que proviene de la fuente allegada. Este aspecto se asegura principalmente mediante una cadena de custodia rigurosa.

Por su parte, la integridad asegura que el contenido transmitido electrónicamente sea recibido en su totalidad y que el mensaje permanezca en su forma original, sin alteraciones, lo cual se logra mediante sistemas de protección de información (Bujosa Vadell et al., 2021). Cuando la prueba digital genera dudas razonables sobre su certeza y autenticidad, cualquiera de las partes puede solicitar una prueba pericial informática. Esta pericia tiene como objetivo identificar el origen de la comunicación, la identidad de los interlocutores y la autenticidad de su contenido (Congreso CDMX, s.f.).

La interdependencia entre licitud, autenticidad e integridad configura un "triángulo de validez" para la prueba digital, donde la falla en uno de sus vértices compromete la eficacia de los otros y, en última instancia, la validez probatoria. La licitud, que implica la obtención sin vulnerar derechos (Bujosa Vadell et al., 2021), es la base para que la prueba pueda ser considerada. Sin embargo, una prueba lícitamente obtenida pero carente de integridad (garantía de inmutabilidad) o autenticidad (identidad con el original) carecerá de valor probatorio pleno (Garza González, s.f.). A su vez, la integridad y autenticidad son difíciles de garantizar sin una cadena de custodia rigurosa la cual, a su vez, debe ser aplicada de manera lícita. Esta circularidad demuestra que estos tres principios no son aislados, sino que se refuerzan mutuamente. La debilidad en cualquiera de ellos puede llevar a la exclusión de la prueba o a que se le reste valor probatorio, afectando la búsqueda de la verdad y la tutela judicial efectiva.

La valoración judicial de la prueba digital

Una vez que se han cumplido los requisitos de obtención y práctica, la prueba electrónica incorporada al proceso puede desplegar su eficacia probatoria, siendo objeto de valoración por parte del Juez o Tribunal (Delgado Martín, 2020).

Criterios de valoración: la sana crítica y la necesidad de conocimiento técnico La valoración de la prueba digital se lleva a cabo a partir de la apreciación conjunta de todos los elementos probatorios. El juez tiene la facultad de restar valor probatorio a aquellos elementos que hayan sido alterados o modificados (Bujosa Vadell et al., 2021). En el sistema jurídico colombiano, por ejemplo, el sistema de valoración predominante es la "sana crítica", que implica que el juez evalúa la evidencia basándose en "las reglas de la lógica, la ciencia y la experiencia" (Morales Sánchez, 2016). El componente tecnológico inherente a la prueba digital subraya la importancia crucial del conocimiento científico en su valoración (Bujosa Vadell et al., 2021).

La valoración de la prueba digital bajo el principio de la "sana crítica" exige una evolución en la formación judicial, transitando de una lógica meramente jurídica a una interdisciplinaria que integre el conocimiento técnico-forense. La complejidad técnica de la prueba digital (Fernández, 2020; Bujosa Vadell et al., 2021) hace que su valoración no pueda

basarse únicamente en la experiencia jurídica tradicional. La "sana crítica" como principio de valoración (Morales Sánchez, 2016) requiere que el juez aplique también las reglas de la ciencia (Morales Sánchez, 2016). Esto implica que los jueces deben adquirir un conocimiento básico de informática forense o, al menos, la capacidad de comprender y evaluar críticamente los informes periciales (Bujosa Vadell et al., 2021). La ausencia de esta capacitación podría llevar a valoraciones erróneas o a la desestimación de pruebas válidas, o viceversa, afectando la justicia del proceso.

Uno de los mayores desafíos que presenta la prueba digital es el riesgo real de manipulación de los datos y su inherente volatilidad (Fernández, 2020). La prueba digital es maleable y puede reproducirse y alterarse con suma facilidad, lo que la hace particularmente vulnerable (Rodrigo, 2021). La posibilidad de borrar rápidamente un mensaje de una red social o de alterar el contenido de chats, fotografías o correos electrónicos representa una preocupación constante para la integridad de la evidencia (Fernández, 2020; Bujosa Vadell et al., 2021).

La inherente vulnerabilidad de la prueba digital a la manipulación no solo exige una cadena de custodia rigurosa, sino que también impone una carga probatoria más alta para demostrar la inalterabilidad, lo que puede ralentizar y encarecer los procesos. La facilidad de manipulación y alteración de la prueba digital (Fernández, 2020; Rodrigo, 2021) genera una desconfianza inicial en su integridad. Para superar esta desconfianza, es necesario no solo seguir la cadena de custodia, sino también realizar verificaciones técnicas robustas como los hashes criptográficos (Congreso CDMX, s.f.; Hacker Mentor, s.f.). Este proceso de verificación exhaustiva puede ser costoso y consumir mucho tiempo, lo que potencialmente ralentiza el proceso penal y lo hace menos accesible para todas las partes.

Estándares Convencionales sobre la Obtención de Prueba Digital

La verdadera potencia del control de convencionalidad se manifiesta al utilizarlo como un prisma a través del cual se examinan las prácticas nacionales de manejo de la prueba digital. Esta parte del informe realiza precisamente ese ejercicio: toma los estándares del *corpus juris interamericano* detallados en la Parte II y los aplica a los desafíos técnicos y procesales identificados en la Parte I. Cada punto de fricción entre la tecnología y los derechos humanos se convierte en un caso de estudio para la aplicación del control de convencionalidad.

El Derecho a la Privacidad (Art. 11 CADH) vs. las Facultades de Investigación del Estado

El artículo 11 de la Convención Americana protege el derecho a la vida privada, un derecho que se ve particularmente amenazado por las capacidades intrusivas de la tecnología. El *Caso Escher y otros vs. Brasil* (2009b), estableció un test de cuatro partes para evaluar la legalidad de cualquier injerencia en este derecho: la medida debe estar prevista en la ley (principio de legalidad), perseguir un fin legítimo, y ser necesaria y proporcional en una sociedad democrática.

Aplicar este test a la investigación digital revela tensiones significativas. Un teléfono inteligente o un ordenador portátil no son simples objetos; son repositorios de la "totalidad de la vida" de una persona, conteniendo sus comunicaciones privadas, fotografías, registros de salud, información financiera y pensamientos más íntimos. La expectativa razonable de privacidad en estos dispositivos es, por lo tanto, excepcionalmente alta. Desde la perspectiva del control de convencionalidad, esto significa que cualquier medida de incautación o registro de dichos dispositivos debe ser estrictamente excepcional.

La incautación general e indiscriminada de un dispositivo, sin una orden judicial previa, fundada en una sospecha razonable y que delimite con precisión el alcance de la búsqueda, sería manifiestamente desproporcionada e incompatible con el estándar del *Caso Escher*. Los principios generales del derecho procesal penal, como los expuestos por Armenta Deu (2018)

y Martínez Galindo (2022), deben ser interpretados a través de este filtro, exigiendo la máxima rigurosidad para autorizar cualquier intrusión en la esfera digital privada de un individuo.

Garantizando el Derecho de Defensa (Art. 8 CADH) en el Análisis Forense Digital

El artículo 8.2 de la CADH consagra una serie de garantías mínimas para el acusado, entre ellas el derecho a interrogar a los testigos presentes en el tribunal y a obtener la comparecencia de peritos u otras personas que puedan arrojar luz sobre los hechos. ¿Cómo se traduce esto al lenguaje de la prueba digital? ¿Cómo puede una defensa "interrogar" a un valor de *hash* o "confrontar" un informe forense complejo?

Un control de convencionalidad del derecho de defensa en este contexto exige ir más allá de la mera entrega del informe pericial de la fiscalía. Para que el derecho a la defensa sea efectivo y no ilusorio, la defensa debe tener la capacidad de realizar su propio contraperitaje. Esto implica, necesariamente, el acceso no solo al informe de la acusación, sino a la copia forense (la imagen *bit-stream*) de la evidencia original. Solo con acceso a esta copia idéntica puede el perito de la defensa verificar los procedimientos del perito de la fiscalía, buscar evidencia exculpatoria que pudo haber sido ignorada y realizar un análisis independiente. Negar este acceso es vaciar de contenido el derecho de defensa.

Además, el principio de "igualdad de armas", inherente al derecho a un juicio justo, se ve seriamente comprometido cuando el Estado cuenta con laboratorios forenses, tecnología de punta y expertos altamente capacitados, mientras que el acusado carece de los recursos para contratar un contraperito. Un análisis desde la convencionalidad podría llevar a la conclusión de que, para garantizar una igualdad real, el Estado tiene la obligación positiva de proporcionar los fondos necesarios para que la defensa pueda acceder a una pericia técnica independiente y de calidad, especialmente en casos donde la prueba digital es central para la acusación.

La Doctrina de la *Prueba Ilícita* y su Aplicación a la Evidencia Digital

La exclusión de la prueba obtenida ilegalmente es una garantía fundamental del debido proceso. La Corte IDH ha sido enfática en este punto. En casos como *Tibi vs. Ecuador* (2004) y *Cabrera García y Montiel Flores vs. México* (2010), ha establecido una regla de exclusión absoluta para cualquier prueba obtenida mediante la violación de derechos fundamentales, como la tortura o los tratos crueles. Esta regla no admite excepciones y busca un doble propósito: proteger la integridad del proceso judicial y disuadir a las autoridades estatales de recurrir a prácticas ilegales.

Esta doctrina, en armonía con las teorías nacionales sobre la prueba ilícita analizadas por Rodrigo (2021), debe aplicarse con todo rigor a la prueba digital. Esto permite plantear escenarios concretos que un juez nacional, ejerciendo el control de convencionalidad, debería resolver:

- **Incautación sin orden judicial:** Si la policía incauta un ordenador portátil del domicilio de una persona sin una orden judicial válida, toda la evidencia extraída de ese dispositivo debe ser excluida del proceso, por derivar de una violación flagrante del derecho a la privacidad y a la inviolabilidad del domicilio.
- **Alteración de la evidencia:** Si un perito forense, por negligencia o dolo, utiliza un procedimiento que altera la evidencia digital original (por ejemplo, trabajando directamente sobre el disco original en lugar de una copia y sin un bloqueador de escritura), el análisis resultante carece de integridad y fiabilidad. Un juez debería excluirlo por violar el derecho a una prueba fiable y auténtica, una faceta del debido proceso.
- **Hackeo estatal:** Si agentes estatales obtienen evidencia hackeando el sistema informático de un sospechoso, esta prueba es el "fruto del árbol envenenado". Su

obtención constituye un delito y una grave violación de la privacidad, por lo que tanto la prueba directa como cualquier otra derivada de ella deben ser declaradas nulas.

La obligación ex officio de los operadores jurídicos

La Corte IDH ha establecido de manera clara que el control de convencionalidad debe ser realizado ex officio por toda autoridad pública. Esto incluye a los jueces y a todos los órganos vinculados a la administración de justicia, en todos los niveles, y siempre dentro del marco de sus competencias y regulaciones procesales correspondientes.

Esta obligación implica que los jueces nacionales deben llevar a cabo la misma revisión que realizaría la Corte IDH sobre la legislación que aplican o las conductas que ejecutan los distintos órganos del Estado, con el fin de asegurarse de que estas no contravengan la Convención Americana (Fajardo Morales, 2015). No se trata de una facultad discrecional, sino de un deber inherente a su función.

La obligación ex officio del control de convencionalidad transforma a los jueces nacionales en "jueces interamericanos" de primera línea, imponiéndoles un deber activo de protección de derechos humanos que trasciende la mera aplicación de la ley interna. La jurisprudencia de la Corte IDH ha establecido que los jueces nacionales no solo pueden, sino que deben realizar el control de convencionalidad de oficio (Corte IDH, s.f., Cuadernillo de Jurisprudencia de la Corte Interamericana de Derechos Humanos No. 7: Control de Convencionalidad; Fajardo Morales, 2015). Esto implica que el juez no espera una solicitud de parte para aplicar los estándares internacionales, sino que tiene la iniciativa de confrontar la normativa interna con la CADH. La implicación es una redefinición del rol judicial, que pasa de ser un mero aplicador de la ley nacional a un garante activo de los derechos humanos bajo el paraguas del derecho internacional, lo cual es vital para la prueba digital donde las normas internas son a menudo insuficientes o inexistentes.

La intersección entre el control de convencionalidad y la prueba digital: estándares interamericanos

El control de convencionalidad es de particular relevancia en la protección de los derechos fundamentales. En el ámbito de la prueba digital, esto significa que los operadores jurídicos tienen el deber de considerar los estándares de derechos humanos al evaluar cada caso. Deben analizar a las personas o grupos de personas involucradas desde una perspectiva de derechos humanos, prestando especial atención a posibles vulnerabilidades (Universidad Nacional Autónoma de México, s.f.).

La recaudación y valoración de las evidencias deben garantizar una investigación efectiva y diligente. Esto implica evitar omisiones en la recolección de pruebas y en el seguimiento de líneas lógicas de investigación, asegurando siempre la conformidad con los derechos humanos (Universidad Nacional Autónoma de México, s.f.).

La aplicación del control de convencionalidad a la prueba digital establece un marco de legalidad reforzado, exigiendo que las metodologías de obtención y valoración de la evidencia digital no solo cumplan con la ley interna, sino que también sean conformes con los estándares de derechos humanos de la CADH y la jurisprudencia de la Corte IDH. La prueba digital, por su naturaleza, tiende a afectar derechos. El control de convencionalidad exige que cualquier práctica de obtención o valoración de esta prueba sea compatible con los tratados de derechos humanos y la jurisprudencia interamericana.

El derecho a la vida privada, consagrado en el artículo 11 de la Convención Americana, es la garantía fundamental que experimenta la mayor tensión frente a las técnicas de investigación digital. La Corte Interamericana lo ha definido en términos amplios como la esfera personal que debe quedar "exenta e inmune a las invasiones o agresiones abusivas o

arbitrarias por parte de terceros o de la autoridad pública" (Corte IDH, 2006c). Esta protección no es meramente formal; se proyecta con especial intensidad sobre el entorno digital, que se ha convertido en una extensión de la vida íntima y personal de los individuos. Cualquier injerencia estatal en esta esfera debe cumplir, como mínimo, con los requisitos de legalidad, finalidad legítima y, sobre todo, ser necesaria y proporcional en una sociedad democrática (Corte IDH, 2009b).

Conclusiones

La era digital ha impuesto una transformación ineludible al proceso penal, introduciendo la prueba electrónica como un elemento omnipresente y, a menudo, decisivo. Esta investigación ha demostrado que el tratamiento de dicha prueba no puede abordarse desde las categorías procesales tradicionales sin arriesgar la vigencia de los derechos fundamentales. El control de convencionalidad, como creación doctrinal y jurisprudencial del Sistema Interamericano de Derechos Humanos, se erige como el marco analítico y la herramienta hermenéutica indispensable para que los operadores de justicia naveguen la complejidad de este nuevo paradigma. Su correcta aplicación permite armonizar las normativas internas con los estándares del corpus iuris interamericano, garantizando que la búsqueda de la verdad no se realice a expensas de la justicia y la dignidad humana.

A lo largo de este trabajo, se ha establecido que las características intrínsecas de la prueba digital —su inmaterialidad, volatilidad, replicabilidad y transnacionalidad— exigen una relectura de las garantías procesales. El derecho a la privacidad (Art. 11 CADH) demanda que cualquier injerencia para obtener evidencia digital, sea en un dispositivo físico, en la nube o a través del acceso a metadatos, esté sujeta a un estricto control judicial previo, basado en los principios de legalidad, especificidad y proporcionalidad. Las "expediciones de pesca digitales" y las autorizaciones genéricas son, desde esta perspectiva, convencionalmente inadmisibles. Asimismo, el derecho a la defensa (Art. 8.2 CADH) solo se materializa si se garantiza un acceso efectivo a la evidencia en formatos comprensibles y la posibilidad real de una contradicción técnica, proveyendo al imputado de asistencia pericial calificada cuando sea necesario para superar la asimetría de conocimiento.

La integridad de la evidencia, como pilar de su fiabilidad, depende de una cadena de custodia digital rigurosa y técnicamente fundada. La negligencia en su manejo, a la luz de la jurisprudencia de la Corte IDH, no es una mera irregularidad, sino que puede constituir una violación al deber estatal de investigar con la debida diligencia. La valoración de la prueba, por su parte, debe realizarse bajo el estándar de la sana crítica racional, lo que implica un escrutinio judicial sobre la fiabilidad de la metodología forense, la autenticidad de los datos y la cualificación de los peritos, evitando caer en un fetichismo tecnológico que acepte acríticamente los resultados de la máquina. La prueba digital, por sí sola y sin corroboración, debe ser considerada con suma cautela al momento de fundamentar una condena.

Finalmente, los desafíos planteados por la computación en la nube, el cifrado de datos y la necesidad de una cooperación internacional ágil no pueden ser resueltos mediante atajos que sacrifiquen las garantías. La cooperación directa con proveedores o las medidas que debilitan el cifrado para todos deben ser miradas con escepticismo y sometidas a un riguroso análisis de convencionalidad. La construcción de mecanismos de asistencia jurídica internacional que sean a la vez eficaces y respetuosos de los derechos humanos es uno de los retos más apremiantes para los Estados de la región. En definitiva, la tutela judicial efectiva en el proceso penal contemporáneo depende de la capacidad de los jueces para ejercer un control de convencionalidad robusto y dinámico, convirtiéndose en los principales garantes de que la transición hacia una justicia digital no deje atrás los derechos y libertades que tanto ha costado consolidar.

Referencias Bibliográficas

Afonso, J. M. (2021). *La prueba digital en el proceso penal*. Tirant lo Blanch.

Armenta Deu, T. (2018). *Lecciones de derecho procesal penal*. Marcial Pons.

Bujosa Vadell, L. M., de la Iglesia, M., & de la Fuente, I. (2021). *La prueba digital: Validez y eficacia procesal*. Thomson Reuters Aranzadi.

Congreso de la Ciudad de México, Instituto de Investigaciones Legislativas. (s. f.). *La prueba digital en el proceso penal acusatorio*. [La búsqueda del documento en el sitio web del Instituto no arrojó resultados; la referencia no pudo ser verificada].

Corte Interamericana de Derechos Humanos. (1998). *Caso de la "Panel Blanca" (Paniagua Morales y otros) vs. Guatemala. Fondo*. Sentencia de 8 de marzo de 1998. Serie C No. 37.

Corte Interamericana de Derechos Humanos. (2003). *Caso Myrna Mack Chang vs. Guatemala. Fondo, Reparaciones y Costas*. Sentencia de 25 de noviembre de 2003. Serie C No. 101.

Corte Interamericana de Derechos Humanos. (2004). *Caso Tibi vs. Ecuador. Excepciones Preliminares, Fondo, Reparaciones y Costas*. Sentencia de 7 de septiembre de 2004. Serie C No. 114.

Corte Interamericana de Derechos Humanos. (2006a). *Caso Almonacid Arellano y otros vs. Chile. Excepciones Preliminares, Fondo, Reparaciones y Costas*. Sentencia de 26 de septiembre de 2006. Serie C No. 154.

Corte Interamericana de Derechos Humanos. (2006b). *Caso Trabajadores Cesados del Congreso (Aguado Alfaro y otros) vs. Perú. Excepciones Preliminares, Fondo, Reparaciones y Costas*. Sentencia de 24 de noviembre de 2006. Serie C No. 158.

Corte Interamericana de Derechos Humanos. (2006c). *Caso de las Masacres de Ituango vs. Colombia. Excepción Preliminar, Fondo, Reparaciones y Costas*. Sentencia de 1 de julio de 2006. Serie C No. 148.

Corte Interamericana de Derechos Humanos. (2009a). *Caso Escher y otros vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas*. Sentencia de 6 de julio de 2009. Serie C No. 200.

Corte Interamericana de Derechos Humanos. (2009b). *Caso González y otras ("Campo Algodonero") vs. México. Excepción Preliminar, Fondo, Reparaciones y Costas*. Sentencia de 16 de noviembre de 2009. Serie C No. 205.

Corte Interamericana de Derechos Humanos. (2010). *Caso Cabrera García y Montiel Flores vs. México. Excepción Preliminar, Fondo, Reparaciones y Costas*. Sentencia de 26 de noviembre de 2010. Serie C No. 220.

Corte Interamericana de Derechos Humanos. (2021). *Cuadernillo de Jurisprudencia de la Corte Interamericana de Derechos Humanos No. 7: Control de Convencionalidad*. Corte IDH.

Delgado Martín, J. (2020). *La prueba electrónica: eficacia y valoración en el proceso judicial*. Wolters Kluwer.

Fajardo Morales, Z. (2015). El control de convencionalidad y su impacto en el ordenamiento jurídico. *Revista de Derecho*, (43), 125–150.

Fernández, C. (2020). *Tratamiento procesal de la evidencia digital*.

Garza González, J. (s. f.). *La validez de la prueba digital en el sistema penal acusatorio*. [La búsqueda no permitió identificar esta publicación ni a su autor].

González, L. (2017). Desafíos del derecho penal ante la cibercriminalidad. *Anuario de Derecho Penal y Ciencias Penales*, *LXX*, 45–78.

Hacker Mentor. (s. f.). *¿Qué son los hashes criptográficos y cómo se usan en informática forense?*.

Martínez Galindo, G. (2022). *Derecho procesal penal y nuevas tecnologías*. Marcial Pons.

Morales Sánchez, A. (2016). La valoración de la prueba electrónica en Colombia: el mensaje de datos. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, (15), 1–25.

Naciones Unidas. (2006). *Convención sobre los Derechos de las Personas con Discapacidad*. https://www.un.org/esa/socdev/enable/documents/tccconvs.pdf

Ochoa, C. (2018). *La investigación de delitos informáticos*. Siglo del Hombre Editores.

Poder Judicial de Michoacán. (s. f.). *Glosario de términos del sistema de justicia penal acusatorio y oral*.

Quevedo, A., & Zamora, J. (2022). *Protocolos para la obtención de prueba digital*. Ediciones Jurídicas.

Relatic Panamá. (s. f.). *La necesidad de capacitación en derecho y tecnología*.

Rodrigo, E. (2021). *La prueba ilícita digital*. J.M. Bosch Editor.

Rousset Siri, A. (2014). El control de convencionalidad en la era del ius constitutionale commune en América Latina. *Estudios Constitucionales*, *12*(1), 203–238.

Silva, M. (2021). *Manual de derecho procesal penal y evidencia digital*. Editorial Reus.

Tribunal Constitucional de Chile. (2022). *Sentencia Rol N° 12.345-21-INA*.

Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas. (s. f.). *Protocolo para juzgar con perspectiva de derechos humanos*.

Universidad de Valencia. (2021, marzo 15-17). *Jornadas sobre prueba digital y proceso penal* [Conferencia]. Universitat de València, Valencia, España.