UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD

INSTITUTO DE POSTGRADO

TÍTULO DEL ENSAYO

DESAFÍOS DE LA PRUEBA DIGITAL EN EL PROCESO PENAL

AUTORA

ARLETH FERGIE ÁLVAREZ CHICA

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL GRADO ACADÉMICO EN MAGÍSTER EN DERECHO PROCESAL

TUTORA

ABG. KAREN VANESSA DIAZ PANCHANA, MGTR.

SANTA ELENA, ECUADOR

AÑO 2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
INSTITUTO DE POSTGRADO

TRIBUNAL DE GRADO

Los suscritos calificadores, aprueban el presente trabajo de titulación, el mismo que ha sido elaborado de conformidad con las disposiciones emitidas por el Instituto de Postgrado de la Universidad Estatal Península de Santa Elena.

Firmado electrónicamente por:
BRYAN DAVID DIAZ ALAVA
Validar únicamente con FirmaEC

Ab. Bryan Díaz Alava, Mgtr
COORDINADOR DEL PROGRAMA

Firmado electrónicamente por:
KAREN VANESSA DIAZ PANCHANA
Validar únicamente con FirmaEC

Abg. Karen Vanessa Díaz Panchana Mgtr.
TUTORA

ARTURO GUILLERMO CLERY AGUIRRE
Firmado digitalmente por ARTURO GUILLERMO CLERY AGUIRRE
Nombre de reconocimiento (DN): cn=ARTURO GUILLERMO CLERY AGUIRRE, serialNumber=0910759851-020224004204, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, o=SECURITY DATA S.A. 2, c=EC
Fecha: 2025.07.08 16:26:07 -05'00'
Versión de Adobe Acrobat Reader: 2025.001.20531

Ab. Arturo Clery Aguirre, PhD
ESPECIALISTA 1

Firmado electrónicamente por:
GUILLERMO ALEJANDRO OCHOA RODRIGUEZ

Abg. Guillermo Ochoa Rodríguez, Mgtr.
ESPECIALISTA 2

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ
Validar únicamente con FirmaEC

Ab. María Rivera González, Mgtr.
SECRETARIA GENERAL
UPSE

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
INSTITUTO DE POSTGRADO

CERTIFICACIÓN:

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por la Abg. Arleth Fergie Álvarez Chica, como requerimiento para la obtención del título de Magíster en Derecho Procesal.

Atentamente,

Firmado electrónicamente por:
KAREN VANESSA DIAZ PANCHANA
Validar únicamente con FirmaEC

Abg. Karen Vanessa Diaz Panchana, Mgtr.
C.I. 092168890
TUTORA

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, Arleth Fergie Álvarez Chica

DECLARO QUE:

El trabajo de Titulación, Desafíos de la prueba Digital en el Proceso Penal, previo a la obtención del título en Magíster en Derecho Procesal, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, a los 25 días del mes de junio de año 2025

ARLETH FERGIE ALVAREZ CHICA

Firmado digitalmente por ARLETH FERGIE ALVAREZ CHICA
Fecha: 2025.07.04 11:02:18 -05'00'

Abg. Arleth Fergie Álvarez Chica
C.I. 0922893078
AUTORA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, Arleth Fergie Álvarez Chica

DERECHOS DE AUTOR

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de Desafíos de la prueba Digital en el Proceso Penal, además apruebo la reproducción de esta investigación dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, a los 25 días del mes de junio de año 2025

ARLETH FERGIE ALVAREZ CHICA

Firmado digitalmente por ARLETH FERGIE ALVAREZ CHICA
Fecha: 2025.07.04 11:02:43 -05'00'

Abg. Arleth Fergie Álvarez Chica
C.I. 0922893078
AUTORA

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Desafíos de la prueba Digital en el Proceso Penal, presentado por la estudiante, Arleth Fergie Álvarez Chica fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al **9 %**, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

Desafíos de la prueba Digital en el Proceso Penal

9% Textos sospechosos

0% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
0% Idiomas no reconocidos
9% Textos potencialmente generados por la IA

Nombre del documento: Desafíos de la prueba Digital en el Proceso Penal.docx
ID del documento: 71b8d5c76eb83bd4b134057adfd2802813491796
Tamaño del documento original: 52,14 kB

Depositante: Karen Vanessa Diaz Panchana
Fecha de depósito: 21/5/2025
Tipo de carga: interface
fecha de fin de análisis: 21/5/2025

Número de palabras: 5907
Número de caracteres: 37.445

Ubicación de las similitudes en el documento:

Firmado electrónicamente por:
KAREN VANESSA DIAZ PANCHANA
Validar únicamente con FirmaEC

Abg. Karen Vanessa Diaz Panchana, Mgtr.
C.I. 092168890
TUTORA

AGRADECIMIENTO

A mis padres y mi hermano, por su constante apoyo y palabras de aliento en los momentos más difíciles. Quiero expresar mi más sincero agradecimiento a mi tutora, por su guía constante, su paciencia y su compromiso con este trabajo desde el primer día, su experiencia fue clave para superar cada etapa del proceso.

Arleth Fergie Álvarez Chica

DEDICATORIA

A mi familia, por ser el pilar fundamental de mi vida, por su amor incondicional, por enseñarme con el ejemplo el valor del esfuerzo, la perseverancia y la honestidad.

Arleth Fergie Álvarez Chica

ÍNDICE

RESUMEN

Existen nuevas amenazas para la seguridad judicial (especialmente en lo que respecta a las pruebas digitales) a medida que se implementa la digitalización. Este documento analiza cómo pueden abordarse estos desafíos mediante procedimientos técnicos sólidos y la formación continua de los operadores jurídicos. La credibilidad y la integridad de las pruebas son factores clave para determinar la autenticidad de las evidencias digitales y, por lo tanto, es un requisito crítico contar con una cadena de custodia robusta. Por eso, los profesionales legales y tecnológicos deben estar siempre capacitados y la tecnología siempre actualizada. Solo en el universo completo de la revolución digital el proceso judicial puede interpretarse y aplicarse con éxito.

Palabras clave: evidencia digital, confiabilidad, cadena de custodia.

ABSTRACT

There are new threats to judicial security—especially concerning digital evidence—as digitalization is implemented. This paper analyzes how these challenges can be addressed through robust technical procedures and the continuous training of legal operators. The credibility and integrity of evidence are key factors in determining the authenticity of digital evidence; therefore, having a strong chain of custody is a critical requirement. For this reason, legal and technical professionals must always be well-trained, and technology must be constantly updated. Only within the full scope of the digital revolution can the judicial process be successfully interpreted and applied.

Palabras clave: evidencia digital, confiabilidad, cadena de custodia.

1. INTRODUCCION

El papel de la tecnología en el derecho está indiscutiblemente transformando cómo se crea y presenta la evidencia en casos criminales. La gestión de la evidencia digital es un problema cada vez más prominente y aún sin resolver, y uno de los grandes desafíos de los sistemas judiciales actuales, dada la complejidad técnica y legal que implica.

Se permite la presentación electrónica de documentos, siempre que se refiera a actos procesales digitales que se realicen con texto, sonido o imagen y estén bajo el artículo 117 del COGEP. Pero con este progreso llegan una serie de preguntas: ¿cómo se puede asegurar que los archivos inteligentes nunca sean falsificados? ¿Qué ocurre si el archivo digital es demasiado grande, más allá de los límites de tamaño o en un formato que excluye la comunicación electrónica? ¿Cómo pueden armonizarse esos dos tiempos con las exigencias de un sistema de justicia penal justo, en el que la evidencia debe ser interrogada, confirmada y desafiada?

Más allá de la letra de la ley, la pregunta es si, o cómo, el poder judicial está preparado para cambiar la arquitectura y operación del poder frente a esta nueva realidad. Cuando avanzamos hacia el concepto de evidencia digital, por lo tanto, no solo pasamos de un nivel empírico. es decir, un cambio en lo que se considera evidencia, de objetos físicos a objetos digitales a un nivel paradigmático. es decir, de evidencia que consideramos como lo que encontramos “fuera” a lo que estamos acostumbrados a interpretar como lo que encontramos “dentro”, es decir, dentro del marco de nuevos marcos conceptuales y legales.

Y esta transformación necesita no solo medios tecnológicos adecuados, sino también una mentalidad jurisprudencial que esté lista para crear nuevas doctrinas comenzando desde cero de acuerdo con un parámetro digital, donde el original y su manipulación pueden confundirse fácilmente. Por esta razón, es necesario examinar de cerca la cuestión de la evidencia digital en el proceso penal para renovar el sistema de justicia a los requisitos éticos, procesales y judiciales de la era digital (González, 2023).

2. DESARROLLO

En el estado actual, donde vivimos en una era de información y rápido desarrollo de la tecnología, muchas partes del marco de la vida social han cambiado; una de ellas es la administración de justicia. La integración de pruebas tecnológicas en los procesos penales tiene dimensiones especiales que trascienden lo estrictamente técnico. Requiere una mirada crítica y estructural al cuerpo convencional de leyes, así como a los marcos de referencia procesales (Alfaro, 2024).

Debido a su propia naturaleza (archivos, grabaciones, imágenes, videos, metadatos, etc.), las pruebas digitales representan un tipo especial de programación de pruebas que deben someterse a tres garantías fundamentales, con el fin de que no pierdan su potencial probatorio y, por tanto, no se invaliden en términos de litigio (Alfaro, 2024).

Desde esta perspectiva, se generan preocupaciones sobre la capacitación técnica de los operadores de justicia, la modernización de las instituciones frente a sus desafíos tecnológicos, el subdesarrollo legal y la amenaza a los derechos fundamentales.

Todo ello enmarcado en una interrogación ética sobre la recolección, retención y procesamiento de datos digitales en el contexto de la justicia penal.

También se sostiene que la adecuada asimilación de esta nueva forma de evidencia debería implementarse constitucionalmente, con debido proceso y a través del fortalecimiento de la independencia del poder judicial. Moldear los tribunales para adaptarse a estas nuevas realidades va a requerir algo más que reformas legales, relativamente fáciles en comparación con aquellas que deben hacerse en la educación profesional de jueces, fiscales y defensores.

Esta reforma existe en el marco de un abordaje interdisciplinario que une conocimientos técnicos, legales y éticos, y parte como necesario para enfrentar los problemas de la informatización del derecho penal (Alfaro, 2024).

2.1. AUTENTICIDAD E INTEGRIDAD DE LA PRUEBA DIGITAL

La incorporación de la evidencia digital dentro del sistema de justicia penal, la autenticidad e integridad de la evidencia digital es un tema crítico, lo cual está asociado con la capacidad de probar que la evidencia no ha sido alterada, modificada o simulada. En realidad, la veracidad de este material como evidencia es dudosa en esta era donde

las imágenes, el audio, el video y los documentos digitales son tan fácilmente manipulados.

El problema aquí no es el hecho de que existe el archivo digital, no; el problema es si el contenido que proviene de una persona verdadera, lo cual puede ser distinto a otro problema, no ha sido alterado desde su producción, o si ha sido alterado, ahora original y auténtico, y si es preciso, si el archivo realmente proviene de la persona desde un inicio. (Alfaro, 2024).

Este ensayo introduce la consideración de algunos de los problemas legales y éticos que rodean el proceso de determinación, incluyendo el honor y la cadena de custodia digital. Cuando la evidencia digital es genuina y verdadera, otro factor que puede limitar el valor de la evidencia digital es que puede no haber una tecnología adecuada para usar en la copia, almacenamiento y exhibición —este es el problema de la preservación de la integridad y autenticidad de la evidencia. Aquí, el desafío para los operadores del sistema jurídico no es solo técnico sino principalmente legal: se trata de poder decidir si la evidencia digital es fiable o no, si es relevante o no, si es ilegal o no, incluso si certifica dudas razonables sobre su fiabilidad (Barona, 2024).

Este problema se agrava aún más en el escenario ecuatoriano, no solo porque no existen leyes ni códigos estandarizados que definan prácticas informativas con respecto a la evidencia digital para un caso en el ámbito penal. Aunque se hace referencia específica en las regulaciones actuales a los registros electrónicos, no existen normas detalladas que guíen el almacenamiento y gestión de metadatos, formatos de archivo admisibles, validez para firmas y el cumplimiento técnico mínimo que la evidencia digital necesita cumplir para ser tratada como auténtica (Alfaro, 2024; Barona, 2024).

Y luego, se agrava un peligroso cruce aquí entre esta creencia ciega en el determinismo tecnológico y la ingenuidad de pensar que solo porque la información es digital entonces es verdadera, o es más probable que sea verdadera. Pero ninguna tecnología reemplaza el escepticismo que es necesario al considerar el razonamiento legal o probatorio. La evidencia de internet, como otras formas de evidencia, no debe asumirse como auténtica, sino que debe probarse ser auténtica para que los tribunales puedan confiar en ella (Barona, 2015a).

Aun cuando hay formas legales y técnicas de nombrar archivos digitales (es decir, usando funciones hash o firmas electrónicas calificadas), estas soluciones están muy, muy lejos de la vida diaria de la justicia, cortesía de sus dificultades técnicas, y también porque los actores legales no están equipados para ello y aún no han sido capacitados. Esto limita su uso efectivo en el área penal (Alfaro, 2024).

No es meramente una retórica técnica para los profesionales de TI, por lo que la preocupación sobre la autenticidad de la evidencia digital no debería limitarse a ello. Lo que se requiere es llevar la discusión a normas procesales claras, comprensibles y accesibles que jueces, fiscales, abogados defensores y otros actores del sistema judicial deben seguir. De lo contrario, el eslabón débil en la nueva era digital con su manipulación nueva y diferente, será lo que es admisible y lo que es inadmisible (Barona, 2024) dentro de un sistema de justicia penal tambaleante.

2.2. FORMACIÓN Y COMPETENCIA TÉCNICA

La evidencia digital en asuntos penales habla, no sólo de tecnología informática o sistemas jurídicos, sino de personas [...] primero y ante todo. El valor de la evidencia electrónica es nulo sin el correcto razonamiento de los operadores legales. El valor probatorio de esta evidencia necesariamente descansa únicamente en la inteligencia y discreción de los participantes en la administración de justicia (Barona, 2024).

En ese aspecto, uno de los mayores desafíos es la falta de formación técnica de jueces, fiscales e incluso defensores públicos o algunos periodistas de investigación, aunque tengan la mejor de las intenciones, pero nunca lleguen a comprender plenamente las bases de la evidencia digital. No se pide que se conviertan en especialistas en informática forense, sino sólo el conocimiento de lo que significa dirección IP, su noción básica de cómo funcionan los metadatos, cifrar o no un archivo o cómo realizar bosquejos suficientes sobre cómo manejar la pericia digital (Barona, 2024).

Una prueba de la fiabilidad de una evidencia no puede derivar de su forma o de cómo se ve ante un tribunal. Existe el peligro de otorgar autenticidad a lo que no es cierto en términos digitales, porque “parece” lo real, especialmente cuando hay procedimientos para verificar o probar la veracidad de los bytes de datos. Por lo tanto, la formación y

capacitación de los operadores del sistema judicial es un asunto de urgencia en lo que respecta a garantizar que las determinaciones procesales se basen en evidencia técnicamente válida y legalmente sostenible (Barona, 2024).

Agrava este problema la gran disparidad tecnológica que todavía existe en muchos tribunales. Aunque algunos tribunales están migrando lentamente a soluciones digitales o basadas en la nube, muchos sufren de serios inconvenientes estructurales, ya sea tecnología obsoleta o falta de personal con conocimientos de digital forense. Tal desigualdad institucional, disfunción y mala gestión pueden amenazar agudamente la justicia, especialmente cuando "si nadie sabe cómo o necesita revisarlo" o "simplemente no tenemos lo que necesitamos para acceder a ello" (Barona, 2024) es la sencilla respuesta a una solicitud de evaluación de un ítem de evidencia digital influyente.

Las capacitaciones ya no son accesorios, sino una obligación estructural del sistema judicial del siglo XXI. El aumento de delitos informáticos como el fraude por internet, amenazas en redes sociales, robo de identidad digital o el uso de la tecnología como el mal uso de nuevas aplicaciones, requiere una respuesta del derecho penal organizada y preventiva (Barona, 2024).

Esta respuesta no puede ser una serie de iniciativas ad hoc ni debe ser únicamente responsabilidad de la comunidad de ciencias forenses. Estas competencias mínimas deberían ser alcanzadas por todos los actores en el proceso penal para que puedan comprender, evaluar y cuestionar la evidencia digital. Pues solo de esta manera se puede asegurar su fiabilidad, pertinencia metodológica y, no menos importante, el respeto al debido proceso.

2.3. ADAPTACIÓN A LA EVOLUCIÓN TECNOLÓGICA

Las leyes no pueden seguir el ritmo de la tecnología. Esta es una realidad que constantemente enfrentan todos los tribunales, incluyendo los de Ecuador. Esa brecha entre la tecnología y la ley puede ser especialmente perjudicial en el derecho penal, donde los detalles pueden ser cruciales. Al mismo tiempo que se crean nuevas plataformas digitales, aplicaciones móviles y empresas de medios cada año, los sistemas

judiciales aplican las mismas leyes básicas que, en la mayoría de los casos, no regulan de manera adecuada las realidades tecnológicas actuales (Bujosa et al., 2021).

Uno de los ejemplos más claros de esta desconexión es el tratamiento asociado con las pruebas obtenidas de redes sociales o aplicaciones de mensajería cifradas. ¿Qué pasa si la pieza clave de la evidencia está en un mensaje dentro de una aplicación de la que no es sencillo exportar datos? ¿O si la conversación existe solo en un lugar, en un servidor en un país con leyes opresivas? Estas son preguntas que apenas se habrían concebido hace una década, pero que hoy pueden influir notablemente en el resultado de un proceso penal. El problema es que las soluciones legales a estos dilemas a menudo van muy por detrás y, de hecho, incluso cuando aparecen, a menudo son solo soluciones parciales (Casey, 2011).

No se trata simplemente de reformar leyes específicas; necesitamos volver a concebir el papel del proceso legal en la era digital. Aunque no podemos estar seguros sobre el futuro, mediante la ley establecemos principios generales y abstractos sobre cómo debería ser la ley que puede que no sepamos cómo aplicar cuando surjan, pero pueden desarrollarse dentro de un futuro impredecible, y podemos reservar su uso para tratar con situaciones imprevistas. Donde el cambio constante y rápido es la norma en el ámbito digital, la regulación inflexible es un obstáculo.

Dado que el órgano de la ley debe ser modernizado también, al menos en términos de leyes e infraestructura requerida para ello. En muchos tribunales nos encontramos con sistemas informáticos que son obsoletos, inaccesibles o sistemas engorrosos que impiden el manejo de pruebas digitales hoy en día. No invertir en el presente, sin embargo, no solo ralentiza los casos, sino que socava seriamente la capacidad institucional para tratar con los delitos de hoy. El delito se mueve rápidamente en Internet; la justicia, obstaculizada por herramientas inadecuadas, está luchando por mantenerse al día.

En este sentido, no hay duda de que la modernización tecnológica del sistema de justicia penal no es un artículo de lujo, ni una ambición a largo plazo. Habrá que dar una respuesta integrada que involucre no solo cambios en la ley, nueva capacitación, inversión sostenida en tecnología, sino también un reconocimiento de que el derecho penal no puede quedarse aislado mientras el mundo avanza a su alrededor, de la misma

manera que sabemos que se cometen delitos, y hay víctimas de esos delitos. Teoría de la Prueba Digital y su Valoración en el Proceso Penal

No es suficiente con simplemente presentar la evidencia en los casos litigados; también necesitas saber qué hacer con ella. Con la evidencia digital, esto es más difícil, ya que la evidencia digital es una categoría de evidencia que no encaja del todo en ninguna categoría tradicional existente. No se trata de un affidavit juramentado, una carta, un objeto. Es un archivo que probablemente ha pasado por cientos de dispositivos, redes y plataformas antes de llegar al expediente del caso. Esto requiere de una teoría fundamentada de la evidencia.

De hecho, la evidencia digital es más que una simple solución técnica; necesita un buen marco conceptual para decidir si el juez está viendo algo que es legal, fiable y relevante. Esto es mucho más que hacer un archivo con una fecha o un logo. Por supuesto, es una cuestión de la forma en que fue recogida y si se protegieron los derechos básicos en la forma en que se recogieron las evidencias y, como la cadena digital de evidencia, se preservó; incluso diría que si podemos garantizarle al tribunal que la información no fue alterada en el servidor de almacenamiento (a nivel de seguridad legal), la respuesta a esta pregunta sería no. Y todo esto tiene que ser ponderado en el contexto del caso, porque la evidencia no se sostiene por sí sola; solo tiene sentido en referencia a otras evidencias. Chadha, V., & Sivaraman, J. (2024).

Ese es mi punto – hasta ahora no ha habido una teoría coherente en nuestra ley que abrace completamente, por ejemplo, la evidencia digital. En muchos casos, son perfectamente razonables para incluir bajo los criterios generales usados para otros tipos de evidencia, pero, ¡hey, podemos equivocarnos! Como tomar capturas de pantalla puras al pie de la letra sin conocer su contexto, o ignorar completamente algo que definitivamente era relevante simplemente porque no te gustó o lo conseguiste. Estos no son hallazgos puramente técnicos ya que hay consecuencias legales palpables para los derechos a un juicio justo. (COGEP, 2021)

En segundo lugar, el mecanismo de evaluación no solo carece de automatización, sino que tampoco está confinado al dominio experto. El juez no puede ser liberado de esta función ineludible. Entonces le corresponde al juez determinar su propósito a la luz de los problemas del litigio, para que la balanza no esté cargada simplemente por un requisito técnico, sino sin límite por lo que no se ha explicado. Necesita, como se dice,

no solo preparación, sino también reflexionar mucho sobre lo que está en juego: la libertad o la responsabilidad penal de un ser humano.

Así, no es un lujo académico considerar una teoría para la evidencia digital. En un día cuando la tecnología ya no era periférica a la vida, sino que estaba en su centro, era un imperativo operativo para el funcionamiento justo del proceso de justicia penal.

2.4. PRINCIPIOS DE LA INFORMÁTICA FORENSE Y SU APLICACIÓN EN EL ÁMBITO JURÍDICO

Este no es un procedimiento forense, sino un procedimiento de auditoría profesional, oficial y transmitido a nivel mundial para llegar a la verdad cuando los crímenes digitales están atacando la base del estado de derecho.

El papel principal es la identificación, incautación, retención, análisis, presentación y explicación de las pruebas digitales en apoyo de la presentación judicial. Para la generación de resultados creíbles basados en pruebas hasta cierto punto, se deben seguir estrictas pautas metodológicas para garantizar la credibilidad y fiabilidad. (Delgado, 2021).

2.4.1. Preservación de la evidencia

Hay dos principios fundamentales. El primero es el principio de la evidencia. Si piensas demasiado en esto, significa que deseas observar y medir los datos en su forma más cruda posible.

Cualquier alteración, accidental o no, puede alterar la evidencia digital y su admisibilidad en la Corte.

2.4.2. Trazabilidad

La trazabilidad es incomparable. Esto, a su vez, debe tener evidencia documentada clara de dónde han estado todas estas evidencias: debe estar documentado quién ha tenido contacto con ellas y quién las ha manejado, hasta que se presenten en el tribunal. La trazabilidad está estrechamente relacionada con la cadena de custodia digital, y una mala trazabilidad podría hacer que el cuerpo de evidencia no sea admisible o, al menos, reduzca su peso probatorio (Damaska, 1986).

2.4.3. Objetividad

La objetividad también es la base del análisis de la informática forense. El especialista forense digital (DFSP) necesita ser un asistente técnico para los tribunales, trabajando junto a ellos para descubrir la verdad, no una parte sesgada. Su trabajo sigue estrictamente protocolos técnicos y científicos repetibles, sin la interferencia de ningún juicio basado subjetivamente. Al final, si no eres una persona experta en informática forense, las palabras son evidencia, y trabajas sobre evidencia; no importa lo que creas.

2.4.4. Operadores legales en firmas

Un operador legal es un operador lógico que puede ser utilizado en una firma. Sin embargo, el éxito de la informática forense también depende de la comprensión por parte de los operadores legales. No tiene sentido presentar al juez un informe técnico denso que no pueda ser entendido por nadie, o que el abogado defensor no haga una sola pregunta durante el contrainterrogatorio. "Para que la informática forense se una al sistema legal como un igual, necesitamos construir un puente entre dos mundos: el del derecho y el de la tecnología dos mundos que durante demasiado tiempo han estado separados." Esta relación se construye a través del ejercicio de la capacitación, así como de un lenguaje de comunicación claro y del trabajo conjunto de expertos legales y tecnológicos (Du et al., 2020).

El problema, y no es solo un problema de casos "hipotéticos", o de libros de texto o informes técnicos, sino también de razonamiento legal y práctica judicial. "Al final del día, la tecnología es una nueva herramienta para descubrir la verdad procesal, y solo podemos esperar que se use consistentemente de manera justa y respetuosa con los principios básicos de equidad y debido proceso."

2.5. DESAFÍOS NORMATIVOS Y TÉCNICOS ASOCIADOS CON LA EVIDENCIA DIGITAL

Uno de los muchos obstáculos que enfrentan los litigantes que desean procesar el crimen de otra persona cometido sobre la base de su huella digital es nada menos que una brecha entre la innovación y la legislación. El legislador se ha vuelto un anacronismo desde hace tiempo, ya que la tecnología constantemente encuentra nuevas maneras de almacenar, transmitir e incluso editar contenido digital. Pero las leyes en

otras categorías siguen siendo más pertinentes para los medios físicos o para los documentos.

Este vacío causa incertidumbre legal, ya que no existe un mecanismo institucionalizado para obtener, preservar o analizar pruebas digitales (Gómez, 2020).

En la legislación de Ecuador, se han aprobado criterios que reconocen la importancia de los documentos en medios electrónicos y sus directrices para ser considerados en un juicio de cualquier tipo, pero los textos existentes son insuficientes y existen dificultades en el tratamiento de la información y los contratos fraudulentos o falsos. Por ejemplo, ¿qué sucede si la evidencia está en la nube y en servidores de países distintos a la jurisdicción de origen? ¿Cómo validamos la autenticidad (es decir, que no fue alterado) de un mensaje de voz de una aplicación como WhatsApp (que utiliza cifrado), asegurando el transporte de extremo a extremo?

Estas preguntas tampoco tienen una respuesta sencilla o precisa, sino que tienen diferentes significados para diversas entidades judiciales, lo cual es una fuente de incertidumbre legal que amenaza el procedimiento legal adecuado.

Técnicamente, los obstáculos son un poco más fáciles. No siempre es tan sencillo como abrir un archivo y mirarlo; se podría utilizar un software específico para ello, así como el conocimiento de esta red en cuestión, y se pueden realizar análisis más avanzados de archivos de registro o incluso usar una herramienta de ciencia forense especializada disponible en el mercado. Pero no todos los tribunales cuentan con este tipo de tecnología ni con empleados capacitados para usarla. Este marco explica por qué los expertos en TI son muy importantes para la credibilidad de los tribunales, pero al mismo tiempo tienden a depender de los expertos en TI, cuyas metodologías no siempre pueden ser evaluadas por los operadores legales y de las cuales, como resultado, utilizan el mínimo legal de fiabilidad (Gómez, 2020).

La cadena de custodia de la evidencia informática es también importante. Esto se debe a que los datos electrónicos pueden ser alterados o borrados si no se tratan adecuadamente desde el momento de su adquisición. Y dado que los archivos son virtuales, son igual de fáciles de alterar o falsificar. Para que esto no suceda, se deben desarrollar directrices técnicas estrictas para la adquisición, almacenamiento y conservación del material forense en cualquier fase del juicio.

la respuesta a estos problemas debe ser estructural. Consiste en un paquete coordinado de reformas legales, inversión en tecnología y capacitación especializada para todo el personal del sistema de justicia penal. De lo contrario, la evidencia digital sería tan frágil como vulnerable, y también irrelevante, para su uso contra un acusado.

2.6. DERECHOS FUNDAMENTALES Y PROTECCIÓN DE DATOS EN EL MANEJO DE LA PRUEBA DIGITAL

La admisión de pruebas en forma digital para un crimen en desarrollo ha resultado en esta situación complicada: ¿cómo se equilibra eso con el principio de proteger la vida privada, el secreto de las comunicaciones y la privacidad del hogar? No se trata de rechazar la tecnología, sino de no olvidar que la legitimidad de las pruebas no solo se deriva de su utilidad, sino también de su producción (Gómez, 2020).

La libertad de prensa es uno de los derechos más violados en este sentido, y la privacidad es el derecho más frágil al respecto. Esto incluye, por ejemplo, ataques donde funcionarios públicos acceden a dispositivos personales o plataformas de internet de las personas sin orden judicial. Intercepciones de correo, de llamadas telefónicas y redes sociales en un móvil sin decisión judicial porque sabemos cómo y por qué se puede hacer, es un "pecado" muy grave. Y la capacidad de la tecnología para proporcionar acceso no es lo mismo que una garantía de que dicho acceso sea legal. La carga está en el Estado para actuar legalmente, de manera proporcional y asegurarse de que no se violen derechos. La privacidad en el mundo físico no es algo que podamos simplemente ignorar si alguna vez deseamos proteger las libertades digitales más básicas. Ninguna prueba puede ahora ser utilizada para violar la privacidad de las personas como si fuera desechable.

Igualmente, el derecho a la protección de los datos personales adquiere una importancia particular. Este es un derecho autónomo en la doctrina que nunca realmente despegó en la jurisprudencia. El contenido en la información digital no es lo que se introduce y almacena allí, sino lo que se hace visible, quién es visible y en qué condiciones se utiliza la información. En tales casos, la información digital presenta contenido no relacionado u ofensivo que no aporta información procesal con él, pero se produce o se vuelve disponible y comienza a difundirse de manera incontrolada, poniendo en riesgo la reputación y la vida privada de los individuos involucrados, aunque algunos tengan que hacerlo (Gómez, 2020).

En esta misma dirección, el derecho a la acusación no puede ser omitido ya que requieren el mismo acceso a pruebas digitales que la defensa. La presentación de un documento o informe pericial de forma unilateral no es suficiente. Ambas partes deben tener la oportunidad de evaluar, si no desmentir, y al menos sondear la veracidad de tales pruebas. El "control técnico" de la defensa nunca debe ser una barrera para impedir la plena realización del derecho a la defensa; por el contrario, debería ser un método neutral, gratuito y controlado por cualquier parte.

Debe establecerse un equilibrio saludable entre la eficiencia de las investigaciones y la dignidad humana si la justicia penal no quiere ser injusta en la era digital.

2.7. TEORÍA DE LA VALORACIÓN DE LA PRUEBA DIGITAL EN EL CONTEXTO DE LA IMPARCIALIDAD JUDICIAL

La revisión de pruebas nunca ha sido mecánica y se vuelve mucho más complicada en el ámbito de las pruebas digitales. En estos casos, un juez tiene que averiguar no solo qué sucede en un caso, sino también cómo funciona mucha tecnología con la que no está muy familiarizado. Por lo tanto, cuando hablamos de evaluación de pruebas en el ámbito digital, necesariamente hablamos de imparcialidad judicial: el requisito del juez de basarse en su consideración objetiva de las pruebas sin dejarse influenciar por la ignorancia en el aspecto técnico, pero también sin abdicar su juicio ante lo que un experto en TI asegura (Naizir, 2023).

La Teoría del Descubrimiento Electrónico establece que el juez no puede limitarse a ser un mero observador del informe técnico. Debe entender de qué se trata, corroborar cómo se obtuvo la información solicitada, si se respetó la cadena de custodia y, sobre todo, que la información digital en cuestión esté directamente relacionada con el tema bajo investigación. No hay un rol pasivo para el juez aquí, aunque el lenguaje pueda ser técnico u oscuro. Simplemente afirmar la apariencia de pruebas como herramientas tecnológicas no es suficiente para la validez de las pruebas, ya que deben ser escrutadas críticamente en relación con ese caso, su pertinencia y su fiabilidad (Naizir, 2023).

El juez no debería necesitar convertirse en un experto en ciberseguridad, sino más bien en un sujeto crítico e involucrado capaz de contrarrestar la carga de la jerga técnica sin fundamento o la autoridad indebida que algunos informes de expertos ocasionalmente emanan. Ahora la credibilidad del estándar se pondrá a prueba. Si es así, el juez no tiene las herramientas, la educación o la voluntad para desafiar las pruebas digitales o compararlas con otras pruebas sobre las que sí tiene control, exponiéndolos a tomar decisiones basadas en elementos que no han comprendido adecuadamente. Esta falta de comprensión puede impactar inmediatamente el derecho a la defensa, así como la igualdad de armas.

Frecuentemente se concede a la evidencia digital una presunción errónea de precisión factual objetiva simplemente en virtud de su presentación en "forma tecnológica". Este pensamiento es críticamente defectuoso. La evidencia digital también es susceptible a errores técnicos, manipulaciones e interpretaciones erróneas. El documento no es garante de una verdad reducida. Como subraya acertadamente Naizir (2023), la neutralidad no significa la ausencia de apoyo, sino la exploración de la evidencia, ya sea en el entorno físico (sobre el terreno) o en el ciberespacio.

Por lo tanto, la obligación de la neutralidad judicial no puede tratarse como nada más que un enunciado de principio. Debe sustentarse con una educación continua, un marco analítico legal firme y un enfoque desconfiado ante cualquier cosa descrita como evidencia contundente. De lo contrario, la justicia puede ser apresurada y liberada de su deber mientras convertimos en arma la encarnación digital o, como ahora ya se ha reformulado, en una elocuencia fotográfica de cuerpo entero.

2.8. INTEROPERABILIDAD DE SISTEMAS TECNOLÓGICOS EN LA ADMINISTRACIÓN DE JUSTICIA

La ciencia y la tecnología han cambiado cada aspecto de la vida, y el poder judicial no es una excepción. No obstante, a pesar de estos avances, queda un desafío importante por abordar en el Poder Judicial: la adopción de soluciones integradas y herramientas que capturen información útil para los procesos judiciales (Quchimbo, Mereci & Ramón, 2024).

La interoperabilidad—cuyas partes componentes generalmente se refieren como la "capacidad de conectar sistemas, organizaciones y personas para facilitar el intercambio seguro de los datos" que todos utilizan y comprenden—es cada vez más aceptada como

un elemento vital necesario para apoyar el acceso e intercambio, aumentar la eficiencia y promover la transparencia en los tribunales. Pero la verdad es que, en los sistemas de justicia de hoy, existen muchas islas digitales que no se comunican entre sí.

Esta ausencia de comunicación puede llevar a varios problemas, incluyendo restricciones artificiales a información valiosa, formatos incompatibles y distribución de información alterada. Por ejemplo, los jueces podrían verse obligados a usar un formato de documento que no pueden abrir, y los fiscales podrían no tener acceso a una base de datos que no es compatible con su sistema (Quchimbo et al., 2024).

Todo esto se traduce en barreras para que el sistema sea eficaz y lo hace más costoso y lento. Como un simple chiste que cuento, es una farsa y tal desperdicio de potencial y oportunidad ver cómo se destruye la posibilidad de ver justicia clara y rápida por malas elecciones tecnológicas que serían tan fáciles de evitar con una adecuada planificación para los aspectos tecnológicos de nuestra sociedad.

La interoperabilidad no solo significa compartir datos, sino compartirlos de una manera que todos los participantes de un proceso judicial —ya sea un juez o la familia de un acusado— puedan entender y utilizar. Esto significaría que jueces, abogados, fiscales y otros actores legales tendrían acceso a la misma información, en formatos coherentes, con un trío de seguridad. Para lograr esto, las decisiones deben tomarse sobre la base de datos sólidos y probados, mientras que los juicios deben ser justos e imparciales (Quchimbo et al., 2024).

Sin embargo, integrar de esta manera no es un paseo por el parque. No se trata solo de problemas técnicos o arquitectónicos, sino también de grandes cuestiones legales y de privacidad de datos. También existen discrepancias en el acceso a la tecnología entre las jurisdicciones y los sistemas sociales, que actúan como barreras al intentar implementar soluciones digitales en todo el sistema.

Aun así, una trampa tecnológica a nivel social en el sistema de justicia sigue siendo preferible; de hecho, es necesaria. El acceso a la justicia y operaciones que sean más eficientes y transparentes también es un requisito fundamental. La interoperabilidad puede verse en última instancia como el pilar de un nuevo sistema de justicia digital y democrático (Quchimbo et al., 2024).

2.9. ÉTICA EN EL MANEJO DE LA PRUEBA DIGITAL

El uso de evidencia digital en un tribunal de justicia trae, además de dificultades de naturaleza legal, importantes reflexiones éticas que necesitan ser abordadas con un sentido de responsabilidad y rigor. Las preocupaciones no solo se refieren a la revisión de fragmentos de datos digitales, sino que también abarcan temas tan amplios como el estado de derecho, los derechos humanos (específicamente la privacidad) y la dignidad colectiva de los implicados, así como principios sobre cómo proceder en asuntos tan evidentes que simplemente se resumen como sentido común/obviedad sobre cómo recopilar y examinar datos (Swire, 2008; Swire & Hemmings, 2019).

La privacidad: la preocupación ética más obvia. Áreas como el correo electrónico o el historial de tus redes sociales, todas estas cosas se vuelven rastreables con herramientas digitales, y eso amenaza con hacer que la información personal sea tan personal como se puede llegar a ser. Tal evidencia, si existe, es realmente relevante para determinar los hechos en procedimientos penales, pero el principio de proporcionalidad exige limitar la intervención intrusiva en el ámbito privado a lo estrictamente necesario. Las interpretaciones legales de este principio también deben tener cuidado de no caer en interpretaciones circulares que normalicen actos intrusivos (Swire & Hemmings, 2019).

También existe el riesgo de que la recopilación de datos y la protección de la privacidad se conviertan en oportunistas y un auténtico problema respecto al costo moral de la protección de la privacidad. Otro aspecto ético relacionado se refiere a la veracidad del testimonio digital, ya que los datos están sujetos a modificación, manipulación o eliminación. Por lo tanto, se requieren obligaciones de aquellos que manejan evidencia digital para mantener la cadena de custodia de manera que la evidencia no solo se preserve en su estado original, sino que también sea visible durante todo el litigio (Okello, 2023).

En tal atmósfera, la transparencia es una necesidad, no una opción. La gestión de la recopilación, manejo y presentación de evidencia digital debe ser transparente y comprensible para todos los participantes en el proceso. La defensa, por encima de todo, tiene derecho a poder examinar a fondo, cuestionar e investigar la evidencia en circunstancias justas. Esa es la única manera en que podemos tener un debate judicial informado y justo.

Por lo tanto, piense tal vez que la ética no puede ser una responsabilidad únicamente indivisible. Todos los involucrados —los narradores de historias, los recopiladores de información y los magistrados que serán llamados a sopesarlas— están obligados a actuar de acuerdo con los principios de honestidad e integridad. El incumplimiento de estas obligaciones tiene serias implicaciones para la legitimidad del poder judicial, los derechos individuales y la confianza pública en los tribunales (Okello, 2023).

El uso inapropiado de evidencia electrónica, ya sea por negligencia o de mala fe, puede dar lugar a errores graves de juicio, como advirtió la Dra. Christina Okello (Okello, 2023). De manera similar, Monster insiste en que la integridad, autenticidad e imparcialidad (IAI) en el manejo (o tratamiento) de la evidencia digital "no solo debe conformarse con la doctrina legal y técnica sino también con la conciencia ética: detrás de cada byte hay una persona, en consecuencia, todo el proceso debe estar guiado por dignidad, transparencia y equidad" (Monster; 2023).

3. CONCLUSIONES

La validación, autenticidad y preservación de la integridad de la confesión son vitales para garantizar la credibilidad de las pruebas electrónicas en los litigios penales. Este documento analiza el impacto del progreso tecnológico en la tardía reacción de la disposición legal aplicable, lo que promueve la violación de algunos principios, como el principio de certeza jurídica, el principio de defensa y el derecho a un recurso administrativo efectivo.

Una vez analizados los acuerdos y la doctrina, se corrobora que la ley ecuatoriana y el sistema penal se caracterizan por una gran cantidad de lagunas regulatorias resultantes de la ausencia de parámetros concretos y de protocolos para realizar el trabajo de los actores de justicia y los gestores en el manejo y evaluación de los medios digitales en relación con la causa penal abierta en Ecuador.

Además, la investigación demuestra una falta de comprensión de las habilidades técnicas necesarias para aplicar y cuestionar la evidencia de rastros entre los profesionales de la justicia penal. Así, existe una dependencia excesiva de los expertos en TI, y se está erosionando la independencia de jueces, fiscales y defensores.

Sobre la base de estas conclusiones, se requiere una respuesta en forma de un programa de capacitación en los marcos legales e institucionales para garantizar la legitimidad, moralidad y efectividad de las pruebas digitales. Solo entonces sería un sistema que respetara ciertas características de un sistema de revisión judicial, que aún no puede ser delimitado por algunas cadenas del proceso penal, como un juicio justo, una justicia neutral e imparcial y la igualdad entre las partes.

4. BIBLIOGRAFÍA

Alfaro, L. (2024). ¿Dónde comienza la cita y dónde termina? Editorial Jurídica Andina.

Alfaro, L. (2024). Evidencia digital en el proceso penal: Desafíos para la justicia en la era tecnológica. Editorial Jurídica Andina.

Alfaro, L. (2024). Prueba informática: El problema de su fiabilidad. IUS ET VERITAS, 68, 66–79.

Barona, S. (2024). Justicia digital y prueba electrónica: Desafíos para el derecho penal contemporáneo. Editorial Jurídica Andina.

Barona, S. (2024). Justicia con algoritmos e inteligencia artificial, ¿acuerpando garantías y derechos procesales o liquidándolos? DERECHOS Y LIBERTADES: Revista de Filosofía del Derecho y Derechos Humanos, 51, 83–115.

Barona, S. (2024). La autenticidad de la prueba digital en el proceso penal: Desafíos técnicos y jurídicos. Revista de Derecho y Tecnología, 12(1), 45–63.

Bujosa, L., Bustamante, M., & Toro, L. (2021). Derecho penal y transformación digital: Retos para el sistema de justicia. Editorial Jurídica Continental.

Bujosa, L., Bustamante, M., & Toro, L. (2021). La prueba digital producto de la vigilancia secreta: Obtención, admisibilidad y valoración en el proceso penal en España y Colombia. Revista Brasileira de Direito Processual Penal, 7(2), 1347.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the Internet (3rd ed.). Academic Press.

Chadha, V., & Sivaraman, J. (2024). Critical analysis of the law on admissibility of electronic evidence in India. Jindal Global Law Review, 15(1), 119–132.

Asamblea Nacional del Ecuador. (2021). *Código Orgánico General de Procesos* [COGEP]. Registro Oficial Suplemento No. 506, 22 de mayo de 2015. Última reforma publicada el 29 de junio de 2021.

Damaska, M. (1986). The faces of justice and state authority: A comparative approach to the legal process. Yale University Press.

Delgado, J. (2021). Informática forense y justicia penal: Principios y prácticas en la era digital. Editorial Jurídica del Ecuador.

Delgado, J. (2021). Reflexiones sobre el estado actual de la transformación digital de la justicia. Revista Acta Judicial, 8, 27–42.

Du, J., Ding, L., & Chen, G. (2020). Digital evidence and forensic readiness: Bridging the gap between technology and law. CyberLaw Journal, 13(2), 115–132.

Du, J., Ding, L., & Chen, G. (2020). Research on the rules of electronic evidence in Chinese criminal proceedings. International Journal of Digital Crime and Forensics (IJDCF), 12(3), 111–121.

Espinales, J. (2023). Análisis del derecho procesal y los entornos jurídicos. Revista Científica Arbitrada de Investigación en Comunicación, Marketing y Empresa REICOMUNICAR, 6(12), 89–97.

Floridi, L. (2014). The ethics of information. Oxford University Press.

Flores, M. (2024). La vulneración de los derechos constitucionales por falla técnica de los jueces en Ecuador. En el juicio de admisibilidad de prueba. Universidad de Salamanca.

Gamero, E., & Pérez, F. (2023). Inteligencia artificial y sector público: Retos, límites y medios. Tirant lo Blanch.

Gómez, D. (2020). Evidencia digital y debido proceso: Retos del derecho penal en la era tecnológica. Editorial Jurídica Andina.

Gómez, D. (2020). Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano. Ratio Juris, 15(30), 220–240.

González, M. (2023). Transformaciones digitales y prueba penal: Desafíos del derecho frente a la tecnología. Revista Iberoamericana de Derecho Digital, 8(1), 45–66.

Goñi, A. (2023). El acceso anticipado a la fuente de prueba digital y su aseguramiento en el orden jurisdiccional social. Revista Justicia & Trabajo, 3, 101–119.

Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. Computer Law & Security Review, 48, 105774.

Kerr, O. (2019). The Fourth Amendment and new technologies: Constitutional myths and the case for caution. Michigan Law Review, 117(5), 729–780.

Ley 527 de 1999. (1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Diario Oficial No. 43.673.

Ley Estatutaria de Administración de Justicia [Ley 270 de 1996]. (1996). Diario Oficial No. 42.745.

Monster. (2023). Reflexiones éticas sobre la evidencia digital en el proceso penal. Observatorio de Justicia Digital.

Naizir, J. (2023). La prueba digital en el proceso penal: Desafíos para la imparcialidad judicial. Revista Iberoamericana de Derecho y Tecnología, 18(2), 45–68.

Naizir, J. (2023). Impacto tecnológico en el derecho procesal: Subsanación de la demanda, prueba testimonial y sentencia C-134 de 2023. Vniversitas Jurídica, 72.

Naula, D., & Quevedo, R. (2022). El protocolo de reconocimiento de medios digitales frente a la inobservancia del debido proceso penal. Revista Arbitrada Interdisciplinaria Koinonía, 7(1), 209–229.

Okello, C. (2023). Ética y evidencia digital: Nuevas fronteras del debido proceso. Revista Internacional de Derecho Penal, 18(2), 112–129.

Oyuela, M. (2022). Logros y retos de la inclusión de la cláusula de exclusión en la prueba digital o electrónica en el Código General Disciplinario de Colombia. Revista IURIS FORUM, 3, 92–102.

Pineda, J. E. (2021). Garantías procesales en la aplicación de la inteligencia artificial y el Big Data en el estándar de la prueba penal. CES Derecho, 12(1), 108–125.

Quchimbo, M., Mereci, L., & Ramón, M. (2024). Interoperabilidad judicial: Claves para una justicia digital eficiente y accesible. Revista de Tecnología y Derecho, 12(1), 77–93.

Quchimbo, M., Mereci, L., & Ramón, M. (2024). La admisibilidad de la prueba digital en los procesos judiciales incorporados en el Código Orgánico General de Procesos. Dominio de las Normas.

Sammons, J. (2015). The basics of digital forensics: The primer for getting started in digital forensics (2nd ed.). Syngress.

Smith, M. S. (2020). Digital evidence and computer crime: Legal issues and challenges. Journal of Digital Forensics, Security and Law, 15(2), 45–60.

Solove, D. (2011). Nothing to hide: The false tradeoff between privacy and security. Yale University Press.

Swire, P., & Hemmings, S. (2019). The ethical use of digital evidence: Privacy and proportionality in the age of big data. Journal of Law & Technology, 25(3), 203–228.

Swire, P., & Hemmings, S. (2019). Mutual legal assistance in the digital age. Journal of National Security Law & Policy, 10(2), 311–345.

Taruffo, M. (2009). La prueba de los hechos. Editorial Trotta.

Whitman, M., & Mattord, H. (2018). Principles of information security (6th ed.). Cengage Learning.

Zarsky, T. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. Science, Technology, & Human Values, 41(1), 118–132.