

Revista Iberoamericana de Derecho, Cultura y Ambiente



Edición N° 3. Julio de 2023

NUEVAS MODALIDADES PROBATORIAS DEL ÁMBITO PENAL: LA EVIDENCIA DIGITAL Y LA PRUEBA ELECTRÓNICA

Ph.D. Paul Enrique Franco Zamora¹

Resumen

El avance tecnológico está asociado a la administración de justicia, siendo un aliado indiscutible del ingreso de la era judicial digitalizada. Dentro de la jurisdicción ordinaria penal se introdujeron diferentes componentes del Derecho Informático que, con la finalidad de cambiar la costumbre tradicional de dictar resoluciones, dieron curso a la virtualización de las etapas procesales. El presente artículo, realiza un repaso jurídico de los logros más trascendentales que desató la aplicación de la ofimática al procedimiento penal; bajo esta premisa, con la ayuda del método de Derecho Comparado, fueron estudiados los sistemas penales para identificar experiencias positivas del uso de medios tecnológicos en el juzgamiento de hechos punitivos, con énfasis, el análisis está dirigido a las repercusiones de la evidencia digital y la prueba electrónica. La etapa probatoria cumple una labor fundamental durante la averiguación material de los ilícitos penales, razón por la que, empleando el método exegético, quedaron establecidas reglas y criterios procesales para el efectivo recojo de la evidencia digital así como la producción de la prueba electrónica, pues ambos instrumentos del juicio criminal, en un futuro próximo, requieren de parámetros concretos que coadyuven en la elaboración de fallos jurisdiccionales revestidos de elementos cibernéticos.

Abstract

¹ Ph.D. en Derecho por la Universidad Mayor, Real y Pontificia de San Francisco Xavier de Chuquisaca. Magíster en Derecho Procesal Constitucional y Derecho Constitucional por la Universidad Andina Simón Bolívar. Abogado por la Universidad Mayor, Real y Pontificia de San Francisco Xavier de Chuquisaca. Presidente del Tribunal Constitucional Plurinacional de Bolivia.

Technological progress is associated with the administration of justice, being an indisputable ally of the entry of the digitalized judicial era. Within the ordinary criminal jurisdiction, different components of Computer Law were introduced, which, with the purpose of changing the traditional custom of issuing resolutions, gave way to the virtualization of the procedural stages. This article makes a legal review of the most transcendental achievements unleashed by the application of office automation to the criminal procedure; under this premise, with the help of the Comparative Law method, criminal systems were studied to identify positive experiences of the use of technological means in the trial of punitive facts, with emphasis, the analysis is directed to the repercussions of digital proof and electronic evidence. The evidentiary stage plays a fundamental role during the material investigation of criminal offenses, which is why, using the exegetical method, rules and procedural criteria were established for the effective collection of digital proof and the production of electronic evidence, since both instruments of the criminal trial, in the near future, require specific parameters to assist in the development of judicial decisions coated with cybernetic elements.

Palabras clave

Cibernética penal; evidencia digital; juzgamiento virtual de hechos punitivos; ofimática procesal de delitos; y, prueba electrónica.

Introducción

El enjuiciamiento de los tipos penales representa una actividad jurisdiccional en la que intervienen múltiples factores y disciplinas. A partir de la comisión de cualquier ilícito delictivo, se activan una serie de mecanismos de orden policial, fiscal, pericial, judicial y sancionatorio, donde las tendencias digitalizadas han prestado colaboración.

La revolución tecnológica ingresó a la Ciencia Penal con dos objetivos principales. El primero, colaborar en la prevención de delitos, por lo que fueron incluidos sistemas de rastreo de posibles delincuentes, análisis del flujo de información para detectar ilícitos, e implementación de alertas o comunicaciones precisas de la comisión de crímenes. El propósito segundo, está representado por la implementación de la ofimática, tanto en las etapas procesales como cada una de las piezas probatorias, que determinarán la inocencia o culpabilidad de los acusados (Vivar Vera, 2021, p. 265).

Como puede notarse, el artículo presentado se enfoca en la etapa de recojo y producción de pruebas dentro del enjuiciamiento de delitos, principalmente, a través del empleo de medios informáticos que derivaron en la incorporación de la llamada evidencia digital y también la denominada prueba electrónica, dos herramientas que adquieren una particular relevancia en la modernización de la justicia penal (Insa Mérida et al., 2008, p. 144).

El problema más común que advierten las legislaciones penales sobre la etapa probatoria, en los que se recurre a medios tecnológicos, está fundamentado por los procedimientos específicos utilizados en la obtención, conservación y presentación de pruebas electrónicas, junto a las dificultades surgidas en el coleccionado de la evidencia digital, considerados como dos problemáticas latentes de la jurisdicción ordinaria debido a que, ante la falta de su regulación, cada juzgador tiene prácticas propias para dar curso a este tipo de pruebas, dada la ausencia de reglas precisas respecto a la manera en que son ofrecidas o

solicitadas.

A estas dos falencias, se suman las interrogantes que los juristas han planteado con relación al valor probatorio que puede otorgárseles, más aún, tomando en cuenta que las Tecnologías de la Información y Comunicación (TIC's) poseen principios propios que, por sus particularidades, a veces complejiza la reproducción de una evidencia digitalizada. Otro aspecto, de debate entre académicos del Derecho, contempla la posibilidad de acudir a la inteligencia artificial como prueba científica del procedimiento penal (Estrada, 2021, p. 1385).

De lo que antecede, se colige que la investigación desarrolla dichos elementos para captar las actuales problemáticas en la tramitación de los medios probatorios con componentes informáticos y recoger la experiencia de los países que, a través de una reglamentación propia o la praxis cotidiana, apostaron por incluirlos en las fases del juzgamiento penal. El influjo de la cibernética y la ofimática en estrados judiciales es irreversible quedando, sin lugar a dudas, una deuda intelectual para efectuar estudios, tal es el caso del presente documento, que guíen a los operadores jurídicos en las diligencias de cualquier evidencia con enfoque digital, antes y durante la obtención de pruebas de índole electrónico.

Materiales y métodos

El coleccionado de información literaria exigió el uso del método bibliográfico, donde se desprende el conocimiento de los modelos teóricos que respaldan el ingreso de la cibernética en las etapas procesales. A través de fichas bibliográficas, pudo desglosarse las tendencias actuales de la virtualización en el juzgamiento de hechos punitivos, además de los principales aportes de juristas que justifican el empleo de medios informáticos en las fases del procedimiento criminal.

En el caso del análisis de normas jurídicas y el estudio de legislación comparada, se recurrió al método exegético que permitió la sistematización de experiencias favorables de la evidencia digital y la prueba electrónica, durante el enjuiciamiento de ilícitos de orden penal. Las fichas de interpretación exegética facilitaron la comprensión de cómo el fenómeno ofimático coadyuva en el aparato judicial, sobre todo, fueron detalladas las formas en que la fase probatoria resultó beneficiada con estas herramientas tecnológicas.

Resultados

1. Evidencia digital y prueba electrónica, dos grandes aliados del proceso penal

Para demostrar la comisión de conductas delictivas suele acudirse a los mecanismos probatorios, que acrediten la verdad material de los hechos acaecidos. Entonces, gracias a la globalización de la tecnología, las piezas procesales empezaron a sufrir una modificación sustancial, pasando de la presentación rústica de evidencias a la producción electrónica de pruebas que fortalecen la etapa de modernización judicial.

Así pues, por evidencia digital debe entenderse el registro y flujo de datos almacenados en un sistema cibernético; este conjunto de información, queda depositado en un código binario (o formato digital) a través de conexiones de red, archivos multimedia, discos duros, memorias externas y todo género de soporte ofimático, susceptibles de guardar datos.

Por lo manifestado, toda la información probatoria que se almacena en un tipo de archivo es considerado digital, pues requiere del uso de un software especializado para su ejecución. Cuando los datos informáticos están relacionados al juzgamiento de ilícitos, entonces, se comprende la existencia de la evidencia digital. La información preliminar y los datos posteriores generados durante la comisión de un hecho delictivo o que sirvan durante su averiguación, forman parte de la evidencia digital; entre ellas, puede citarse los mensajes de texto, las ubicaciones en línea, el historial de navegación en la red, extractos bancarios, movimientos económicos, y un sinnúmero de recursos informáticos que fuesen empleados para perpetrar el delito.

De esta apreciación puede colegirse que, el manejo de un dispositivo móvil o un ordenador (de escritorio o portátil) deja un rastro susceptible de acreditar determinados hechos dentro del juicio. Sin embargo, existen procedimientos que la evidencia digital debe cumplir a los fines de garantizar su análisis confiable; por tanto, al igual que la Medicina Forense, la ofimática permitió el paso del Análisis Forense Digital, cuyo propósito implica el examen de la evidencia digitalizada para comprender su alcance y otorgar mayor convicción a los operadores jurídicos (Parra de Gallo, 2022, p. 442).

En cambio, el momento en que la evidencia digital sigue una cadena de pasos para verificar su autenticidad y es presentada en un determinado proceso jurisdiccional, adquiere la calidad de prueba electrónica. En otras palabras, la evidencia digital es la fuente probatoria que demuestra la posible comisión de un delito, y una vez que los profesionales expertos certifican su autenticidad se convertirá en prueba electrónica, a reproducirse en un proceso penal (Borges Blázquez, 2018, p. 543).

Con base a lo manifestado, la evidencia digital y la prueba electrónica no deben entenderse como sinónimos, sino consisten en elementos complementarios. Lastimosamente, los sujetos procesales o sus abogados confunden que la impresión de mensajes o publicaciones de redes sociales constituye evidencia y prueba a adjuntarse dentro de un escrito judicial; sin embargo, con la diferenciación expuesta puede concluirse que la evidencia digital está relacionada a los datos guardados en un archivo informático y que, tras su revisión minuciosa por los expertos del área y comprobada su validez, puede anexarse en calidad de prueba electrónica.

De esta manera, las partes del procedimiento penal pueden alegar la existencia de posibles registros informáticos de la comisión del delito, pero no necesariamente adquirirá la calidad de prueba electrónica pues, para que ésta resulte invocada dentro del juicio criminal, se exige el cumplimiento de una serie de pasos, que serán desarrollados en el siguiente apartado. En suma, los dispositivos cibernéticos almacenan información que, en el campo judicial, puede considerarse evidencia digital; empero, si los expertos forenses demuestran que estos archivos son confiables para el juzgamiento penal, recién adquirirá la calidad de prueba electrónica.

Las legislaciones de los países deben distinguir esta terminología, para evitar mayores confusiones entre los juzgadores y los propios litigantes. Por esta razón, el análisis forense de los datos informáticos hace posible el recojo de rastros contundentes que contribuyan en el esclarecimiento de los tipos penales, demostrando el carácter relevante de la evidencia digital y la prueba electrónica como aliados estratégicos del juzgamiento de hechos punitivos.

2. Reglas específicas durante la obtención y conservación de la evidencia digital

La evidencia obtenida por medios ofimáticos está sujeta a cinco reglas básicas que, independientemente de la norma adjetiva penal, suelen aplicarse con la finalidad de evitar su excesiva manipulación (Ochoa Arévalo, 2018, p. 40). Desafortunadamente, las personas modifican archivos, alteran datos o eliminan información comprometedor, justificativo para que las actividades probatorias estén presididas por un listado de principios que pasan a detallarse.

La primera regla exige que la evidencia digital pueda presentarse en un determinado tribunal de justicia. Por ejemplo, no toda la información almacenada en la red es susceptible de difundirse ya que, con la confidencialidad de las bases de datos, existen restricciones para producirlas abiertamente en un juicio penal; en rigor, ante cualquier archivo digital, los profesionales encargados del análisis forense digital deben procurar que los datos informáticos sean difundidos, sin ninguna prohibición dentro de las etapas probatorias.

La información sensible que compromete los intereses de menores de edad o el flujo económico de las cuentas de ahorro con carácter confidencial, representan los casos más comunes a considerarse por los expertos en Derecho Informático, al momento de realizar las pericias. No toda evidencia digital es libre de socialización en el proceso judicial, cada país establece limitaciones en cuanto a la propagación de datos públicos, caso contrario se pondría en riesgo la seguridad jurídica del resto de la población.

Una segunda regla está fundamentada por la autenticidad de la evidencia digital. La alteración de archivos es sumamente frecuente y, desde la rama pericial-forense, resulta indispensable que la evidencia analizada tenga relación directa con el ilícito penal a investigar. Muchas veces, con fines investigativos, es colectada toda información generada aunque no tenga vínculo alguno con el hecho delictivo, o trata de tergiversarse la evidencia para que se adecúe a lo que las partes o el juez busca. De esta manera, pruebas electrónicas contraproducentes pueden presentarse en el proceso judicial cuando, de manera preliminar, no se comprueba la veracidad de la evidencia.

Para contentar a las partes que intervienen en el proceso o demostrar el peso de los insumos virtuales en el juzgamiento de delitos, se modifican los archivos o intenta darse un sentido diferente que aparente un relacionamiento con los sucesos investigados, no obstante, esta regla limita el recojo de datos manifiestamente irrelevante al proceso penal. Es obligación de las autoridades fiscales y judiciales tomar en cuenta que los requerimientos emitidos de acceso a las bases de datos guarden estrecha correspondencia con los hechos delictivos porque, de lo contrario, resultarán lesionados los derechos fundamentales de la población.

Con la intención de acceder a las comunicaciones privadas o conocer los movimientos económicos de la ciudadanía, puede autorizarse (vía fiscal o judicial) la entrega de información privada con escasa vinculación, lo que demuestra la pertinencia de exigir que la evidencia digital sea manejada con absoluta reserva, sin conculcar otros derechos consagrados constitucionalmente.

Los indicios representan la tercera regla, por lo que las evidencias digitales necesitan resguardarse de manera íntegra. La suficiencia de la evidencia digital

constituye la suma de varios indicios, entonces, no basta con identificar uno de ellos, sino habrá de colectarse varios elementos para alcanzar la verdad histórica de los hechos. Cuando la evidencia se halla incompleta o no ofrece un panorama amplio a los fines de demostrar la inocencia o la culpabilidad de la persona procesada penalmente, es preferible continuar con las indagaciones hasta obtener mayores argumentos que otorguen convicción al juzgador.

Con esta apreciación, un solo indicio informático colectado puede tacharse de insuficiente y generará debate entre los actores del proceso penal; por el contrario, de conseguirse múltiples indicios con directa conexitud con el tipo penal, se aumentan las probabilidades de alcanzar la evidencia digital dado que, con la acumulación de elementos probatorios, mayores son las expectativas de contar con pruebas electrónicas.

La cuarta regla fundamental consiste en la confiabilidad de la evidencia digital, y supone el cumplimiento de una metodología especializada de análisis y presentación de resultados que garanticen el esclarecimiento concreto de los hechos penales. El grado de confiabilidad de una evidencia digital determina el punto de debate judicial pues, así como prevalecen posturas que confían en que los indicios comprueban la culpabilidad, también existen opiniones discrepantes respecto al valor de la prueba electrónica, aspecto primordial que será desglosado más adelante.

El entendimiento sencillo y comprensión fácil refleja la última regla de la evidencia digital, porque el empleo excesivo del lenguaje técnico-informático repercute en la escasa comprensión por los operadores de justicia quienes, al pertenecer a distintos niveles generacionales, no cuentan con los mismos conocimientos para interpretar los indicios recogidos por los expertos. Mientras se utilicen conceptos concretos y obviando tecnicismos, la evidencia digital podrá catalogarse como un aliado estratégico de la averiguación de los ilícitos.

En suma, las reglas propuestas dan curso a la obtención de indicios para fortalecer la evidencia digital. De esta manera, cuando se trata de coadyuvar en la investigación de hechos criminales, el cumplimiento de cada etapa procesal reviste de suma importancia al momento de viabilizar el dictado de una resolución judicial amparada en medios probatorios.

3. Criterios de admisibilidad de la prueba electrónica

Con el ingreso de la era tecnológica es común que el proceso penal considere la pertinencia de introducir pruebas con componentes electrónicos. El mundo jurídico plantea una serie de interrogantes sobre la posibilidad de admitir medios probatorios apoyados en el uso de la ofimática, una de las preguntas más frecuentes recae en los criterios de admisibilidad de la prueba electrónica.

Según Ionarrado en el anterior apartado, la evidencia digital contiene reglas específicas para que los indicios informáticos, en una faceta procedimental, adquieran la categoría de prueba electrónica que será incorporada durante el juzgamiento penal. No obstante, desde el Derecho Probatorio se plantea que las reglas de admisibilidad de todo elemento conducente a la averiguación del hecho queden instituidas en los códigos procedimentales, motivo por el que las legislaciones adjetivo-penales intentan regular la recepción y producción de pruebas de manera general, y sin distinguir si pertenecen o no al área cibernética.

Este inconveniente, fue acomplejándose con la globalización y el uso masivo del internet, provocando que las reglas de admisibilidad de la prueba (en sede penal) sean incongruentes con el contexto jurídico; es más, por desconocimiento de cómo producir la prueba electrónica, desde la praxis judicial, se plantearon directrices generales, habitualmente nominadas como criterios de admisión (Vadell et al., 2021, p. 1370).

A partir de la doctrina, pueden dilucidarse al menos cuatro criterios universalmente aceptados para admitir la prueba electrónica. Aunque las normas procesales pueden variar entre los países, lo cierto es que surgen voces compartidas respecto a la producción de medios probatorios electrónicos.

La primera directriz, compartida por gran parte de las legislaciones penales, está justificada por la obtención lícita de la prueba. La información relevante para el proceso penal no debe vulnerar los derechos fundamentales de la población; en todo caso, cuando los expertos desarrollan actividades de rastillaje virtual, deben considerar que cualquier invasión en la esfera de los derechos constitucionales puede dar lugar a la ilicitud de la prueba electrónica. Por ejemplo, el ingreso a correos electrónicos como herramienta de comunicación de posibles actos delictivos requiere de la autorización del titular, no pudiendo arbitrariamente unirse a esta base de datos sin el consentimiento expreso de quien tenga las credenciales de acceso.

Las órdenes emanadas por las autoridades fiscales o judiciales posibilitan la investigación penal; naturalmente, en mérito a esta previsión jurídica, el derecho constitucional a la inviolabilidad de las comunicaciones no resulta vulnerado cuando existe previa autorización expresa porque, de lo contrario, la prueba electrónica no produciría ningún efecto legal.

El segundo criterio de admisibilidad corresponde a la cadena de custodia que cumple la prueba electrónica. Cuando la evidencia digital se transforma en medio probatorio electrónico persisten pasos rigurosos que limitan cualquier intento de manipulación ofimática; de esta manera, la ética de los profesionales en el área informática es crucial para que, en las etapas de análisis de los indicios, no subsistan dudas respecto a que la prueba electrónica haya sufrido una alteración.

El proceso de acceso, obtención, transferencia y almacenamiento de los datos debe contemplar una metodología segura y evitar cualquier filtrado de información. Muchas veces, de forma anticipada, se cuenta con informes anticipados del contenido de la evidencia o son difundidos los hallazgos concretos de la pericia, entonces, las pruebas electrónicas tendrán que sujetarse a una determinada cadena de custodia, a ser verificada por las autoridades judiciales. De no contarse con un procedimiento riguroso de reserva de datos analizados, esto derivará en tachas sobre la prueba electrónica, toda vez que no se trataría de un mecanismo probatorio indubitado (es decir, que no admite duda).

Un tercer aspecto trascendental constituye la facilitación de los medios de exhibición. Por el principio de publicidad de los procesos penales, la prueba electrónica tendrá que reproducirse en la etapa probatoria del juicio y, tal cual quedó expresado con anterioridad, los sujetos procesales junto a los juzgadores deben comprender plenamente su contenido. Por citar, durante la invocación de una prueba electrónica donde se compruebe la suplantación de la personalidad o el robo de credenciales de acceso, resulta contraproducente alegar que un

determinado país no posee tecnología suficiente para establecer quien se encuentra utilizando la cuenta, o aquellas situaciones donde es sumamente complicado entender los resultados de la pericia por el uso excesivo del lenguaje cibernético.

Por último, se consideran criterios admisibles de la prueba electrónica ciertos requisitos técnicos que avalan su certeza y validez, entre ellos, puede mencionarse la identificación del remitente, la garantía de integridad, el almacenamiento en condiciones de seguridad, información previa al propietario del ordenador u otros relacionados a la firma digital que, en su conjunto, confirman el cumplimiento de un protocolo.

Las legislaciones de los países que incursionaron en el rastreo de evidencia digital y la producción de prueba electrónica, empezaron a modificar sus normas adjetivas para implementar los referidos criterios de admisibilidad. Ejemplo concreto, representan los códigos procesales de España y Colombia que, siguiendo este modelo teórico propuesto, apostaron por introducir requisitos de necesidad, pertinencia, utilidad y legalidad; inclusive, las altas Cortes, Salas o Tribunales de Justicia dictaron resoluciones en la materia, sentando jurisprudencia de consulta para admitir o rechazar la prueba electrónica.

4. Valor probatorio

El tratamiento judicial de la prueba electrónica difiere entre juzgadores, por lo que la valoración de este medio probatorio está limitado por la apreciación particular del operador jurídico. Más allá de fundamentos legales previstos en la normativa procesal, la práctica demuestra que cada autoridad jurisdiccional, según su sana crítica y convicción, define el valor a otorgarse a las pruebas electrónicas (Yepes Gómez et al., 2022, p. 261).

Por ejemplo, en el caso de Estados Unidos, siguiendo los paradigmas emergentes del Derecho Informático, los legisladores incluyeron un régimen probatorio basado en las Reglas Federales de la Evidencia (Federal Rules of Evidence); de hecho, el valor de la prueba electrónica depende de las partes del proceso, vale decir, el sujeto procesal que desee presentar un medio probatorio electrónico tiene la obligación de demostrar, al operador de justicia, que fueron acatadas todas las reglas de la evidencia digital y la aplicabilidad de los criterios de admisibilidad, ambos elementos desarrollados en los apartados anteriores.

Para la judicatura estadounidense, el valor asignado a la prueba electrónica implica que, quienes participan de procesos penales serán los encargados de verificar el cumplimiento de una ruta específica de la cadena de custodia; así pues, si los participantes del procedimiento penal se aseguran que la prueba electrónica es relevante, auténtica y confiable, acrecentará su valor probatorio y el juez no tendrá mayores dudas respecto a su autenticidad.

En el orden jurídico colombiano o chileno, las juzgadoras y los juzgadores asumen la sana crítica y libre convicción para valorar cualquier prueba con componentes electrónicos. Sin embargo, por disposición de la normativa procesal y decretos legislativos inherentes al servicio judicial de Colombia o Chile, el valor probatorio de medios electrónicos tiene el mismo tratamiento que los documentos físicos, por tanto, también es común recurrir al sistema de tarifa legal o prueba tasada, lo que equivale a la aplicación rigurosa realizada por el juez, conforme al valor expresado en la ley; en otras palabras, los juristas no necesitan razonar

sobre la implicancia de la prueba electrónica pues la norma fija el valor de las pruebas, siendo el juzgador responsable de dar curso a lo dispuesto en ella.

Argentina presenta singulares particularidades ya que, si bien la ley penal rige para todo el país, cada provincia está facultada de reglamentar aspectos concernientes a las pruebas judiciales y su validez en los procedimientos. Ante la ausencia de manuales, guías, protocolos o reglamentos de recojo de la evidencia digital o directrices de admisibilidad de la prueba electrónica, la justicia argentina opta por concederles valor probatorio, con base a la sana crítica y libre convicción de cada operador jurídico.

La administración judicial de Bolivia, durante el enjuiciamiento de hechos delictivos, sigue la tendencia de los países latinoamericanos estudiados. Los tribunales o jueces penales son los encargados de asignar el valor correspondiente a los elementos probatorios acorde a las reglas de la sana crítica, fundamentando los motivos por lo que asume dicha postura, en base a la apreciación conjunta y armónica de toda la prueba esencial producida, conforme reza el artículo 173 del adjetivo penal boliviano.

Para la legislación española, tal cual impone la Ley N° 59 de 19 de diciembre de 2003, las pruebas de origen electrónico gozan de similar validez que el resto de los documentos físicos; en rigor, durante la asignación del valor hacia a la prueba electrónica ofrecida por las partes procesales, el personal de los estrados judiciales utilizas mismas reglas e idénticos criterios invocados en los elementos probatorios comunes.

Discusión

Las TIC's no deberían acarrear nuevos conflictos en la jurisdicción penal, no obstante, la evidencia digital y la prueba electrónica merecen un tratamiento judicial especializado. La paridad de los medios probatorios cibernéticos con las tradicionales pruebas físicas constituye el punto de discusión que mayor repercusión ha generado entre los juristas (Galvis Lugo et al., 2019, p. 190).

A lo largo de la investigación, pudo dilucidarse la diferencia fundamental entre evidencia digital y prueba electrónica, empero, conseguir que estos mecanismos probatorios no sean objeto de discusión en el juicio penal, requiere de iniciativas legislativas o reglamentarias que promuevan una igual equivalencia con las rústicas pruebas de corte documental. Por los motivos señalados, el desafío próximo de las autoridades judiciales comprende la estandarización íntegra de los instrumentos probatorios de rasgos informáticos con las herramientas de prueba impresa, situación que exige del compromiso sostenido de las entidades públicas, pero igualmente demanda la participación de sectores involucrados en la investigación de hechos delictivos.

El segundo componente de reflexión está determinado por la inteligencia artificial aplicada al proceso penal, en especial, el uso de algoritmos para la valoración de pruebas electrónicas. Las percepciones de juristas varían en torno a delegar esta actividad valorativa a la inteligencia artificial o, más al contrario, hay quienes defienden que el juicio penal no debe encomendarse a otros softwares especializados (Gamba Cifuentes, 2021, p. 23).

Aunque permanece una división de criterios, sobre la posibilidad de acceder a la inteligencia artificial para descifrar la evidencia digital y seleccionar aquellos

medios probatorios electrónicos que guarden relación con la investigación de ilícitos penales, subsisten corrientes armonizadores de ambos criterios.

Por una parte, los defensores del empleo de la informática avanzada (con fines de rastrear todo indicio digitalizado) plantean que, al tratarse de datos codificados con perspectiva cibernética, lo correcto significa que los sistemas sofisticados de inteligencia artificial sean utilizados para valorar la pertinencia de los instrumentos probatorios electrónicos propuestos por las partes; esto, significa que la evidencia digital y la prueba electrónica sean sometidos a una valoración de programas informáticos que determinen si dichos medios probatorios son aceptados o desestimados.

El otro sector de expertos jurídicos, manifiesta su disconformidad con la cibernética para otorgarle valor a una prueba electrónica. Su reticencia se debe, principalmente, a los efectos perjudiciales surgidos cuando la valoración de un insumo virtual queda encomendada a un programa artificial, cuyas conclusiones no siempre tomarán en consideración las reglas de recojo de la evidencia digital, ni tampoco podrá garantizarse el cumplimiento de los criterios de admisibilidad de medios probatorios electrónicos.

Con el propósito de equilibrar los dos extremos de la balanza, emana una tercera que intenta acomodarlos bajo un lineamiento concreto; es decir, los juzgadores pueden solicitar la intervención de la inteligencia artificial para obtener un nuevo conocimiento en la materia y, sin abandonar la sana crítica y la libre convicción que les compete plenamente, habrán de valorar la prueba electrónica con el apoyo (de carácter subsidiario) de la ofimática. Entonces, el personal judicial puede basarse en el sistema de tarifa legal, además de acudir al modelo de sana crítica y libre convicción al momento de fijar valor a la prueba electrónica pero, en situaciones sumamente especiales, asimismo le es permitido conocer los informes provenientes de la inteligencia artificial, a los fines de dictar una resolución penal desde la esfera del Derecho Cibernético.

Conclusiones

La evidencia digital, almacenada en diferentes dispositivos (móviles o de escritorio), está sujeta a reglas específicas que rigen su obtención y conservación, por lo que la sumatoria de indicios virtuales rastreados adecuadamente dará lugar al surgimiento de la prueba electrónica, a invocarse en las fases del proceso penal. Para la reproducción de pruebas electrónicas en el juzgamiento de hechos delictivos, deben respetarse los criterios de admisibilidad pues, en razón a estas directrices jurisdiccionales provenientes de la doctrina, dichos mecanismos de averiguación histórica de los hechos no serán tachados, sino coadyuvarán a demostrar la inocencia o culpabilidad de los individuos procesados penalmente.

Las limitaciones hacia el uso de la tecnología y la cibernética en el enjuiciamiento de delitos, tienen relacionamiento con el valor asignado que el juez pueda otorgarle a la prueba electrónica ya que, a pesar de que las legislaciones presentan numerosas alternativas de fijar una valoración objetiva a estos insumos probatorios ofimáticos, todavía existen posturas renuentes a darles un tratamiento jurídico similar a cualquier prueba física o documental. Este panorama, se agrava con las voces de profesionales informáticos que, con el objetivo de brindar mayor certeza sobre los hallazgos obtenidos durante el coleccionado de datos, promueven el ingreso de la inteligencia artificial a la etapa

probatoria penal.

En síntesis, producto del avance tecnológico y la masificación de las TIC's en el ámbito judicial, los operadores jurídicos fueron beneficiados con la implementación de la evidencia digital y la incorporación de la prueba electrónica, dentro del procedimiento penal u otras ramas donde es requerida la comprobación de ciertos sucesos.

Citas y referencias bibliográficas

Borges Blázquez, R. (2018). La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea. *Iuris Tantum Revista Boliviana de Derecho*, 25, 536-549.

Estrada, M. J. P. (2021). La inteligencia artificial como prueba científica en el proceso penal español. *Revista Brasileira de Direito Processual Penal*, 7(2). <https://www.redalyc.org/journal/6739/673972089017/html/>

Galvis Lugo, Á. F., & Bustamante Rúa, M. (2019). La no equivalencia funcional entre la prueba electrónica y la prueba documental: Una lectura desde la regulación procesal colombiana. *Ius et Praxis*, 25(2), 189-222. <https://doi.org/10.4067/S0718-00122019000200189>

Gamba Cifuentes, G. (2021). *La Inteligencia Artificial (IA) y su implementación en la prueba como mecanismo de tutela para los derechos fundamentales*. <http://repository.unilibre.edu.co/handle/10901/20482>

Insa Mérida, F., Lázaro Herrero, C., & García González, N. (2008). Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad.: Un proyecto europeo. *Enlace*, 5(2), 139-152.

Ochoa Arévalo, P. A. (2018). El Tratamiento de la Evidencia Digital, una Guía para su Adquisición y/o Recopilación. *Revista Economía y Política*, 28, 35-49. <https://doi.org/10.25097/rep.n28.2018.03>

Parra de Gallo, H. B. (2022). Propuesta de una guía de actuación forense para entornos de internet de las cosas (IoT). *Computación y Sistemas*, 26(1), 441-460. <https://doi.org/10.13053/cys-26-1-3898>

Vadell, L. M. B., Rúa, M. M. B., & Garzón, L. O. T. (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). <https://www.redalyc.org/journal/6739/673972089016/html/>

Vivar Vera, J. (2021). La sentencia penal, el juez y el algoritmo: ¿Las nuevas tecnologías serán nuestros próximos jueces? *Revista chilena de derecho y tecnología*, 10(1), 231-269. <https://doi.org/10.5354/0719-2584.2021.58785>

Yepes Gómez, M. M., Pérez Benitorevollo, J. A., & Peinado, M. (2022). Aplicación de la Prueba Electrónica en el Marco Normativo Colombiano. *Novum Jus*, 16(1), 253-277. <https://doi.org/10.14718/novumjus.2022.16.1.11>