FACULTAD DE DERECHO

DESAFÍOS PROCESALES EN LA PERSECUCIÓN Y PREVENCIÓN DE DELITOS ECONÓMICOS

Autora: Clara Blanco Barrón
5º E-3 A
Tutora: Sara Díez Riaza
Derecho Procesal

Madrid
Junio 2025

Resumen

La digitalización acelerada del proceso penal plantea desafíos inéditos para la persecución y prevención de delitos económicos en España, especialmente ante la proliferación de criptoactivos, contratos inteligentes y sistemas de inteligencia artificial. Este trabajo analiza críticamente las carencias del marco procesal vigente en materia de prueba digital, responsabilidad penal en entornos automatizados y formación tecnológica de los operadores jurídicos. A partir de una revisión doctrinal, jurisprudencial y normativa, se propone una reforma integral articulada en tres ejes: la creación de una regulación autónoma y garantista de la prueba digital en la LECrim, el desarrollo de un modelo de compliance 4.0 con auditorías algorítmicas y mecanismos de supervisión automatizada, y la implantación de un plan nacional de formación y certificación tecnológica obligatoria para jueces, fiscales, abogados y peritos. La propuesta integra estándares internacionales como la ISO/IEC 27037:2012 y el Reglamento MiCA, y persigue cerrar la brecha tecnológica, reforzar la igualdad de armas y preservar las garantías procesales en la era digital.

Palabras clave: prueba digital, blockchain, smart contracts, inteligencia artificial, compliance 4.0, cadena de custodia, responsabilidad penal, formación tecnológica, ISO/IEC 27037:2012, Reglamento MiCA.

Abstract

The accelerated digitalization of criminal proceedings in Spain presents unprecedented challenges for the investigation and prosecution of economic crimes, particularly in the context of cryptoassets, smart contracts, and artificial intelligence systems. This thesis critically examines the shortcomings of the current procedural framework regarding digital evidence, criminal liability in automated environments, and the technological training of legal professionals. Through a doctrinal, jurisprudential, and regulatory review, it proposes a comprehensive reform based on three pillars: the creation of an autonomous and rights-based regulation of digital evidence in the Criminal Procedure Act (LECrim); the development of a compliance 4.0 model with continuous algorithmic audits and automated supervisory mechanisms; and the implementation of a national plan for mandatory technological certification and training for judges, prosecutors, lawyers,

and forensic experts. The proposal integrates international standards such as ISO/IEC 27037:2012 and the MiCA Regulation, aiming to bridge the technological gap, strengthen equality of arms, and safeguard procedural guarantees in the digital age.

Keywords: digital evidence, blockchain, smart contracts, artificial intelligence, compliance 4.0, chain of custody, criminal liability, legal-tech training, ISO/IEC 27037:2012, MiCA Regulation.

ÍNDICE

Listado de abreviaturas

AI / IA: Inteligencia Artificial

BOE: Boletín Oficial del Estado

CE: Constitución Española

CEJ: Centro de Estudios Jurídicos

CGPJ: Consejo General del Poder Judicial

CP: Código Penal

DAOs: Decentralized Autonomous Organizations (Organizaciones Autónomas Descentralizadas)

DeFi: Decentralized Finance (Finanzas Descentralizadas)

ENAC: Entidad Nacional de Acreditación

FJ: Fundamento Jurídico

GAFI: Grupo de Acción Financiera Internacional

ISO/IEC: International Organization for Standardization / International Electrotechnical Commission

LECrim: Ley de Enjuiciamiento Criminal

LO: Ley Orgánica

MiCA: Markets in Crypto-Assets (Reglamento UE 2023/1114)

STS: Sentencia del Tribunal Supremo

TEDH: Tribunal Europeo de Derechos Humanos

UE: Unión Europea

Abreviaturas latinas (en cursiva):

Cfr.: compárese

ibid.: en el mismo lugar

id.: el mismo autor

op. cit.: obra citada

p.: página

pp.: páginas

vid.: véase

1. INTRODUCCIÓN

1.1. Planteamiento y relevancia del estudio

La irrupción de tecnologías disruptivas como *blockchain*, la inteligencia artificial (IA) y los contratos inteligentes ha reconfigurado radicalmente la naturaleza de los delitos económicos en España, desbordando los mecanismos tradicionales del Derecho procesal penal. La sofisticación de la criminalidad tecnológica, que opera en entornos descentralizados y transfronterizos, evidencia una brecha crítica entre la vanguardia delictiva y la capacidad de respuesta de un sistema judicial anclado, en gran medida, en paradigmas probatorios y de imputación decimonónicos. Este desfase no solo compromete la eficacia persecutoria del Estado, sino que también genera graves riesgos para las garantías procesales fundamentales, erosionando la seguridad jurídica y la tutela judicial efectiva en la era digital.

La relevancia de este estudio se intensifica en el contexto actual, marcado por la progresiva digitalización de la Administración de Justicia —impulsada por el Plan Justicia 2030— y por la consolidación de un marco normativo europeo que, como el Reglamento MiCA, reconoce la entidad económica y jurídica de los criptoactivos. Sin embargo, esta modernización se revela incompleta si no va acompañada de una adaptación profunda del proceso penal, capaz de gestionar la complejidad de la prueba digital, la atribución de responsabilidad en sistemas algorítmicos y la necesaria capacitación de los operadores jurídicos. Este trabajo aborda, por tanto, una cuestión de máxima actualidad y trascendencia: cómo construir un proceso penal que, sin renunciar a sus garantías históricas, sea capaz de responder con eficacia a los desafíos de la cibercriminalidad del siglo XXI.

1.2. Justificación procesal

La pertinencia procesal de esta investigación se fundamenta en tres carencias estructurales del sistema español:

- **Insuficiencia normativa de la prueba digital:** La Ley de Enjuiciamiento Criminal (LECrim) carece de una regulación autónoma para la prueba digital. Esta omisión obliga a los tribunales a un forzado encaje de evidencias tecnológicas (registros *blockchain*, metadatos, comunicaciones cifradas) en las categorías

tradicionales de la prueba documental o pericial. Como han advertido tanto la doctrina (Magro Servet, Barona Vilar) como la jurisprudencia (STS 326/2019), esta asimilación es técnicamente inadecuada y procesalmente riesgosa, pues ignora las características de volatilidad, intangibilidad y duplicabilidad de la evidencia digital, generando incertidumbre sobre su admisibilidad, cadena de custodia y valoración.

- **Crisis de los modelos de imputación penal:** La emergencia de organizaciones autónomas descentralizadas (DAOs) y sistemas de IA con capacidad de decisión autónoma desafía los pilares clásicos de la responsabilidad penal. Las figuras de autoría, participación y dolo, diseñadas para la acción humana directa, resultan insuficientes para atribuir responsabilidad en delitos cometidos por o a través de algoritmos opacos. La aplicación analógica de la responsabilidad penal de las personas jurídicas (arts. 31 bis y ss. CP) se revela inadecuada para estructuras no jerárquicas, exigiendo el desarrollo de nuevos modelos de imputación que consideren el "dolo tecnológico" y la distribución de responsabilidades entre programadores, usuarios y supervisores.
- **Brecha competencial de los operadores jurídicos:** La eficacia de cualquier reforma procesal queda supeditada a la capacidad técnica de quienes deben aplicarla. La falta de formación especializada y obligatoria para jueces, fiscales y abogados en materias como ciberseguridad, *blockchain* forense o auditoría algorítmica perpetúa una desigualdad de armas en el proceso. Esta brecha competencial, apenas abordada por iniciativas como el Marco de Competencias Digitales del Centro de Estudios Jurídicos (CEJ), se traduce en una vulneración del derecho a la contradicción y a una defensa eficaz cuando la prueba de cargo es de naturaleza tecnológica compleja.

1.3. Preguntas de investigación

Este trabajo busca dar respuesta a las siguientes cuestiones centrales:

1. ¿De qué manera puede reformarse la Ley de Enjuiciamiento Criminal para integrar una regulación autónoma de la prueba digital que garantice su autenticidad, integridad y contradicción, en línea con estándares internacionales como la ISO/IEC 27037:2012?

2. ¿Son los modelos dogmáticos tradicionales de autoría y participación penal adecuados para atribuir responsabilidad en delitos cometidos mediante inteligencia artificial y organizaciones autónomas descentralizadas (DAOs)? ¿Qué nuevos criterios de imputación son necesarios para evitar la impunidad tecnológica?
3. ¿Cómo puede diseñarse un modelo de formación especializada para operadores jurídicos que sea obligatorio, dinámico y eficaz para cerrar la brecha competencial y asegurar la igualdad de armas en procesos penales con un componente tecnológico elevado?

1.4. Objetivos

Para responder a estas preguntas, esta investigación se marca los siguientes objetivos:

- **Analizar críticamente** el estado actual de la legislación, la jurisprudencia y la doctrina española en relación con la prueba digital y la responsabilidad penal en entornos tecnológicos, identificando sus principales déficits y contradicciones.
- **Evaluar** la insuficiencia de las categorías dogmáticas penales tradicionales para dar respuesta a los nuevos patrones de criminalidad económica ejecutados a través de IA, *smart contracts* y DAOs.
- **Diseñar y formular** una propuesta de reforma integral, articulada y coherente, que aborde los problemas detectados desde una triple perspectiva:
    - Proponiendo una regulación *de lege ferenda* para la prueba digital en la LECrim.
    - Desarrollando un modelo de *compliance* 4.0 con mecanismos de supervisión y responsabilidad adaptados a entornos descentralizados.
    - Estructurando un plan nacional de formación y certificación tecnológica obligatoria para todos los operadores jurídicos.

1.5. Metodología

La consecución de estos objetivos se ha abordado mediante una metodología jurídica multidimensional que combina:

- **Análisis doctrinal y bibliográfico:** Revisión crítica y sistemática de las aportaciones de autores de referencia en la materia (Barona Vilar, Magro Servet, Calaza López, Planchadell-Gargallo, entre otros), así como de las publicaciones más recientes en revistas especializadas nacionales e internacionales.
- **Estudio normativo y jurisprudencial:** Examen detallado de la legislación española y europea aplicable (LECrim, CP, Reglamento MiCA, Directiva sobre pruebas electrónicas) y de la jurisprudencia más relevante del Tribunal Supremo y TEDH (con especial atención a la STS 326/2019).
- **Análisis de estándares técnicos y casos prácticos:** Integración de normas técnicas internacionales (ISO/IEC 27037:2012) y análisis de casos paradigmáticos (hackeo de The DAO, fraudes con IA) para ilustrar los desafíos prácticos y fundamentar las soluciones propuestas.

1.6. Estructura del trabajo

El trabajo se estructura en tres grandes bloques. El **primer bloque (Capítulos 1-3)** establece el marco conceptual y realiza un diagnóstico crítico de la situación actual, abordando la naturaleza de la prueba digital, las dificultades para su tratamiento procesal y los retos que la IA y los *smart contracts* plantean a la imputación penal. El **segundo bloque (Capítulo 4)**, núcleo central de la investigación, desarrolla las propuestas de reforma, detallando el modelo de regulación autónoma de la prueba digital, el sistema de *compliance* 4.0 y el plan de formación especializada. Finalmente, el **tercer bloque (Conclusiones)** sintetiza los hallazgos de la investigación, responde a las preguntas de investigación planteadas y subraya la contribución original del trabajo al debate sobre la modernización garantista de la justicia penal.

2. MARCO CONCEPTUAL Y NORMATIVO DE LA PRUEBA DIGITAL EN EL PROCESO PENAL

2.1. Concepto y naturaleza jurídica de la prueba digital

La prueba digital, también denominada prueba electrónica o *digital evidence*, constituye un elemento central en la investigación y persecución de delitos económicos en la era tecnológica. Su conceptualización exige superar enfoques reduccionistas que la equiparan a meros soportes informáticos, para adoptar una perspectiva holística que integre su naturaleza dinámica y su función probatoria en el proceso penal. Delgado Martín la define como "toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio"[1], concepto que engloba tanto datos almacenados (correos electrónicos, registros *blockchain*, archivos en la nube) como flujos de información en tiempo real (transacciones en plataformas DeFi, comunicaciones cifradas).

Desde una perspectiva jurídica, la naturaleza de la prueba digital ha sido objeto de intenso debate doctrinal, evidenciando la tensión entre innovación tecnológica y marcos normativos tradicionales. La Sentencia del Tribunal Supremo (Sala de lo Penal), núm. 326/2019, de 20 de junio, marcó un hito al reconocer que los registros *blockchain* pueden constituir hechos indicadores en procesos penales, aunque condicionó su eficacia probatoria a la validación pericial para acreditar su integridad[2].

Este criterio jurisprudencial encuentra respaldo técnico en la ISO/IEC 27037:2012[3], que fundamenta la necesidad de protocolos específicos para la evidencia digital precisamente por sus características diferenciales: propensión a la alteración (volatilidad), dependencia de soportes tecnológicos (intangibilidad) y capacidad de duplicación exacta (replicabilidad)[4].

---

[1] Delgado Martín, J., "La prueba digital. Concepto, clases y aportación al proceso", *Diario La Ley*, n.º 6, Sección Ciberderecho, 11 de abril de 2017, p. 12.
[2] Tribunal Supremo, Sala de lo Penal, Sentencia 326/2019, de 20 de junio, FJ 4.º y 5.º [vLex, Ref. 797938401].
[3] ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition and preservation of digital evidence, International Organization for Standardization, Ginebra, 2012.
[4] Barona Vilar, S., *Algoritmización del Derecho y de la Justicia*, Tirant lo Blanch, Valencia, 2021, pp. 595-602.

La evolución normativa europea ha intentado abordar estas deficiencias conceptuales. El artículo 3.8 del Reglamento (UE) 2023/1543, sobre órdenes europeas de producción y conservación de pruebas electrónicas, define las "pruebas electrónicas" como "los datos de los abonados, datos de tráfico o datos de contenido almacenados por un prestador de servicios, o en nombre de un prestador de servicios, en formato electrónico". Sin embargo, esta definición, centrada en aspectos operativos transfronterizos, no resuelve los problemas sustantivos de admisibilidad y valoración que persisten en el ordenamiento interno español[5].

Precisamente esta carencia normativa es la que denuncia la doctrina especializada. Calaza López, ofrece un análisis crítico del marco probatorio español, demostrando que la LECrim —especialmente los arts. 326 a 330, diseñados para pruebas documentales físicas— fuerza un "encaje anacrónico" de evidencias tecnológicas (*blockchain*, metadatos, IA forense) en categorías analógicas, generando inseguridad jurídica y asimetrías procesales[6].

Esta crítica doctrinal converge con la posición jurisprudencial más autorizada. Magro Servet, magistrado del Tribunal Supremo, subraya que la prueba digital no debe tratarse como una simple modalidad de la documental, pues "su naturaleza, fuentes y riesgos son radicalmente distintos". El autor es categórico al afirmar que la "prueba digital se nos presenta en este escenario como «algo más» que la prueba documental", exigiendo un estatuto procesal autónomo que reconozca su especificidad técnica y garantista[7].

[5] Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y conservación de pruebas electrónicas en procesos penales, (DOUE L 191, 28 de julio de 2023).
[6] Calaza López, S., *La prueba como pieza clave para la construcción de la realidad procesal*, Dykinson, Madrid, 2025.
[7] Magro Servet, V., "¿Cómo aportar la prueba digital en el proceso penal?", *Diario La Ley*, n.º 9563, 2021, pp. 15-18.

Esta carencia normativa genera consecuencias prácticas inmediatas que el magistrado sistematiza con precisión:

1. Inseguridad procedimental sobre cómo, cuándo y en qué condiciones debe aportarse la prueba digital.
2. Déficits en la cadena de custodia para garantizar la autenticidad, integridad y trazabilidad de los elementos digitales, especialmente ante la volatilidad y facilidad de manipulación de estos soportes.
3. Riesgo de indefensión estructural por la ausencia de plazos claros para la impugnación y la falta de protocolos específicos para la preconstitución y reproducción de la prueba digital en juicio[8].

Para paliar estas deficiencias, Magro Servet enfatiza la necesidad de una pericial informática especializada que valide la autenticidad y autoría de la prueba digital cuando esta sea impugnada, estableciendo un modelo de contradicción técnica que preserve el derecho de defensa. Su propuesta culmina en el reconocimiento expreso de la autonomía de la prueba digital como nuevo medio probatorio, equiparable a la testifical, pericial o documental, pero con reglas propias sobre proposición, práctica, impugnación y valoración adaptadas a la realidad tecnológica[9].

Esta exigencia de autonomía procesal encuentra respaldo en la jurisprudencia europea. El Tribunal Europeo de Derechos Humanos (TEDH), en el caso Big Brother Watch and Others v. United Kingdom (Gran Sala, 25 de mayo de 2021), estableció que la obtención y tratamiento de datos digitales debe respetar el artículo 8 del Convenio Europeo, exigiendo proporcionalidad, garantías legales claras y control independiente. Significativamente, el TEDH subrayó la necesidad de "salvaguardas de extremo a extremo" y criticó la falta de autorización independiente en los regímenes de vigilancia masiva, destacando que la mera posibilidad de que las comunicaciones sean seleccionadas sin autorización previa genera un riesgo de abuso incompatible con el Estado de Derecho[10].

[8] *Id.*
[9] Magro Servet, V., *op. cit*., p. 7.
[10] Tribunal Europeo de Derechos Humanos, Gran Sala, sentencia Big Brother Watch and Others v. United Kingdom, de 25 de mayo de 2021, demandas núms. 58170/13, 62322/14 y 24960/15, §§ 346-356.

La convergencia entre doctrina nacional y jurisprudencia europea evidencia que el problema trasciende las fronteras nacionales. La doctrina de Magro Servet es inequívoca: la prueba digital constituye un *tertium genus* que no puede seguir dependiendo de la lógica y los requisitos de la prueba documental tradicional. Su autonomía es imprescindible para garantizar la seguridad jurídica, la igualdad de armas y la tutela judicial efectiva en los procesos penales del siglo XXI[11].

En definitiva, como sintetiza Barona Vilar, la legislación procesal española permanece anclada en paradigmas decimonónicos que no reconocen la prueba digital como categoría autónoma, obligando a los tribunales a subsumirla forzadamente en figuras tradicionales (documental o pericial). Esta situación genera no solo incertidumbre interpretativa, sino dificultades prácticas en la valoración judicial que comprometen tanto la eficacia investigadora como las garantías procesales fundamentales, haciendo urgente una reforma legislativa integral que dote de coherencia y eficacia al tratamiento procesal de la evidencia digital.

2.2. Características diferenciales de la prueba digital: duplicabilidad, intangibilidad, volatilidad y deleble

La prueba digital presenta una serie de rasgos que la distinguen radicalmente de los medios probatorios tradicionales, imponiendo retos inéditos al proceso penal. Entre estas características destacan la duplicabilidad, intangibilidad, volatilidad y su carácter deleble, aspectos que inciden directamente en la obtención, conservación, valoración y eficacia de la evidencia digital en sede judicial.

En primer lugar, la duplicabilidad es una de las notas más relevantes de la evidencia digital. A diferencia de los documentos físicos, que pueden deteriorarse o perder autenticidad con cada reproducción, la información digital puede copiarse un número ilimitado de veces sin merma de calidad ni alteración del contenido. Esta facilidad técnica, si bien favorece la conservación y el análisis forense, incrementa el riesgo de proliferación de copias no controladas, lo que puede dificultar la identificación del original y comprometer la cadena de custodia.

[11] Magro Servet, V., *op. cit.*, p. 15.

Como subraya Barona Vilar, la integridad de la prueba digital solo puede garantizarse mediante la implementación de protocolos rigurosos, como la generación de huellas digitales (*hash*) y la certificación pericial de cada copia forense[12]. La norma internacional ISO/IEC 27037:2012 exige que toda copia destinada a ser utilizada en juicio cuente con documentación técnica que acredite su correspondencia exacta con el original y la ausencia de manipulación durante el proceso de duplicación[13].

La intangibilidad constituye otro rasgo esencial: la prueba digital no se presenta en un soporte físico perceptible, sino que existe como una secuencia de bits almacenada en dispositivos electrónicos o transmitida por redes telemáticas. Esta naturaleza inmaterial introduce una mediación tecnológica entre el hecho y su percepción judicial, obligando a recurrir a herramientas informáticas para la visualización, extracción y análisis de la evidencia. De ahí que, como advierte la doctrina, la intangibilidad incremente la dependencia del proceso penal respecto de la prueba pericial informática y exija un control reforzado sobre la fiabilidad de los instrumentos utilizados para acceder y presentar la evidencia en juicio. En palabras de Calaza López, la fiabilidad y la integridad de la prueba digital dependen tanto de la competencia técnica de los operadores como de la existencia de protocolos claros y auditables para cada fase del tratamiento de la evidencia[14].

La volatilidad de la prueba digital implica que determinados datos pueden desaparecer, alterarse o sobrescribirse con extrema facilidad, ya sea por el funcionamiento ordinario de los sistemas, por acciones deliberadas de los usuarios o por el simple transcurso del tiempo. Este carácter efímero obliga a una actuación especialmente diligente y rápida por parte de los investigadores y de la autoridad judicial, pues la demora en la adopción de medidas cautelares puede provocar la pérdida irreversible de información relevante para la causa.

El legislador europeo, consciente de este riesgo, ha impuesto en el art. 78 del Reglamento MiCA y en los arts. 5-7 de la Directiva (UE) 2023/1544 obligaciones de conservación de registros para los proveedores de servicios digitales; sin embargo, como advierte la

[12] Barona Vilar, S., *Algoritmización del Derecho y de la Justicia*, *op cit*., pp. 597-601.
[13] ISO/IEC 27037:2012, *Guidelines for identification, collection, acquisition and preservation of digital evidence.*, sección 6.1.
[14] Calaza López, S., *op cit.*, pp. 112-114.

doctrina especializada, estas medidas resultan insuficientes ante la realidad de sistemas descentralizados (ej: DAOs) y redes cifradas (ej: monederos no custodios), donde la ausencia de un intermediario centralizado imposibilita el cumplimiento efectivo de las obligaciones de registro[15].

Por último, la delebilidad o carácter deleble de la prueba digital hace referencia a la facilidad con la que los datos pueden ser modificados, eliminados o destruidos, tanto de manera intencionada como accidental. Esta fragilidad exige la adopción de protocolos de preservación y custodia especialmente estrictos, así como la utilización de tecnologías que permitan registrar de manera fehaciente cualquier acceso, modificación o intento de alteración de la evidencia digital. La jurisprudencia más reciente ha anulado pruebas obtenidas en procedimientos en los que no se acreditó de forma suficiente la inalterabilidad de los datos desde su recogida hasta su presentación en juicio, poniendo de manifiesto la relevancia de la cadena de custodia digital como garantía esencial de la prueba[16].

En definitiva, estas características diferenciales de la prueba digital exigen una adaptación del proceso penal, tanto en el plano normativo como en la praxis forense, para salvaguardar los principios de legalidad, contradicción y defensa en el nuevo contexto tecnológico. Como desarrolla Barona Vilar, la transformación digital de la justicia y la irrupción de la inteligencia artificial están propiciando una "interconexión colaborativa entre los humanos y las máquinas" y una "colaboración asistencial de la máquina" en la función jurisdiccional, lo que obliga a repensar las categorías probatorias clásicas y a dotar a la prueba digital de un estatuto propio que garantice tanto su eficacia como el respeto a los derechos fundamentales y las garantías procesales[17].

[15] Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (MiCA) (DOUE L 150, de 9 de junio de 2023); Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 20 de septiembre de 2023, relativa a las pruebas electrónicas en procesos penales (DOUE L 237, de 26 de septiembre de 2023).
[16] Tribunal Supremo, Sala de lo Penal, Sentencia 326/2019, de 20 de junio, FJ 4.º y 5.º [vLex, Ref. 797938401].
[17] Barona Vilar, S., *Algoritmización del Derecho y de la Justicia*, *op cit*., pp. 555 y 559.

3. RETOS PROCESALES DE LA PRUEBA DIGITAL EN EL PROCESO PENAL

3.1. La prueba blockchain: validez probatoria y estándares de admisibilidad

La transformación digital de la justicia penal ha propiciado la irrupción de nuevas fuentes de prueba, entre las que destaca la tecnología *blockchain*. Como señala Barona Vilar, la "algoritmización de las fuentes" implica la utilización de herramientas que no solo almacenan datos, sino que los seleccionan y configuran en documentos específicos, susceptibles de ser incorporados al proceso como prueba documental[18]. Esta técnica permite crear automáticamente documentos que pueden ser empleados en cualquier tipo de proceso, empleando desde la generación automática de registros hasta búsquedas codificadas en grandes volúmenes de información, extrayendo lo esencial para un determinado ámbito objetivo o subjetivo.

En este contexto, la *blockchain* se presenta como una fuente algorítmica que, gracias a su estructura descentralizada y su sistema de registros inmutables, aporta un plus de fiabilidad técnica a la evidencia digital. Sin embargo, como advierte Barona Vilar, la mera automatización y la confianza en la neutralidad tecnológica no pueden sustituir los estándares de garantías procesales exigidos en el proceso penal[19]. La autora insiste en que la validez probatoria de los registros *blockchain* debe ser objeto de un control judicial reforzado, que asegure tanto la autenticidad e integridad de la evidencia como el respeto al derecho de defensa y a la contradicción[20].

La doctrina especializada en técnicas de clasificación automática de documentos subraya que estas herramientas permiten no solo la organización eficiente de grandes volúmenes de información, sino también la identificación de documentos relevantes para su incorporación al proceso penal[21].

[18] Barona Vilar, S., "Justicia con algoritmos e Inteligencia Artificial, ¿acuerpando garantías y derechos procesales o liquidándolos?", *Derechos y Libertades*, núm. 51, junio 2024, p. 108.
[19] *Ibid.*, pp. 108-109.
[20] *Ibid.*, p. 109.
[21] C. Figuerola, J. L. Alonso Berrocal, A. F. Zazo Rodríguez y E. Rodríguez, "Algunas técnicas de Clasificación Automática de Documentos", *Cuadernos de Documentación Multimedia*, vol. 15, 2004, pp. 3-12.

En particular, la técnica del *predictive coding* —codificación predictiva— ha demostrado ser especialmente útil en litigios complejos, ya que posibilita la revisión y selección ágil y precisa de la documentación relevante, superando en eficacia a los métodos tradicionales de búsqueda manual[22].

No obstante, la adopción de estas tecnologías plantea desafíos en términos de admisibilidad probatoria. Como advierte Solar Cayón, la codificación predictiva, al igual que otras técnicas algorítmicas, debe ser sometida a un escrutinio judicial que garantice la transparencia del proceso de selección y la posibilidad de contradicción por las partes[23]. La *blockchain*, en tanto que fuente algorítmica, no puede ser considerada infalible per se, sino que su valor probatorio dependerá de la posibilidad de auditar los algoritmos y de verificar la integridad de los registros aportados.

La tecnología *blockchain* se inscribe plenamente en lo que Barona Vilar denomina el fenómeno de "algoritmización de las fuentes" probatorias, donde convergen "una serie de instrumentos que inciden en la función que desempeñan los jueces, a saber, en la *Judge Craft*, esto es, tanto en la *Judicial Decision* como en su proceso de elaboración a través de la constatación probatoria"[24]. Este enfoque es especialmente relevante para la *blockchain*, cuya estructura distribuida y criptográficamente securizada genera registros que, por su propia naturaleza técnica, pueden configurar documentos específicos con valor probatorio autónomo.

La autora subraya que estas herramientas tecnológicas pueden aplicarse "a cualquier tipo de proceso y emplea técnicas diversas que pueden desde realizar un documento maquinicamente, hasta establecer una búsqueda codificada en numerosos documentos que permitan extraer lo esencial referido a un determinado ámbito objetivo o subjetivo"[25].

[22] *Ibid.*, pp. 7-9.
[23] J. I. Solar Cayón, “La codificación predictiva: inteligencia artificial en la averiguación procesal de los hechos relevantes”, *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, vol. XI, 2018, pp. 100-101.
[24] Barona Vilar, S., "Justicia con algoritmos e Inteligencia Artificial, ¿acuerpando garantías y derechos procesales o liquidándolos?" *op cit.*, p. 107.
[25] *Ibid.*, p. 108.

En el caso de la *blockchain*, esta capacidad se manifiesta en la generación automática de registros inmutables que documentan transacciones, contratos inteligentes y transferencias de activos digitales con una precisión temporal y criptográfica que supera los métodos probatorios tradicionales.

No obstante, Barona Vilar advierte sobre los riesgos inherentes a la incorporación acrítica de estas tecnologías en el proceso penal. La autora plantea que "Esos resultados algorítmicos facilitan las decisiones en la Justicia, simplifican trámites, pero comportan cada vez mayor automatización, surgiendo dudas acerca de qué grado de algoritmización debería entenderse como el adecuado, quién puede diseñar estos modelos algorítmicos y con qué condiciones"[26].

Esta reflexión resulta capital para la prueba *blockchain*, donde el riesgo de "delegación acrítica" en sistemas tecnológicos puede vulnerar principios procesales fundamentales. Como señala la autora, emerge "la duda acerca de cómo garantizar el debido proceso, especialmente el derecho de defensa y la contradicción, evitando el recurso fácil a considerar la fría neutralidad (falsa) de los algoritmos y por ende su infalibilidad"[27].

Barona Vilar propone criterios específicos para la admisión de pruebas tecnológicas que resultan directamente aplicables a la *blockchain*. En primer lugar, establece "la posibilidad de excluir como prueba los resultados que se aportan al proceso por la aplicación de estos sistemas, cuando es la única base probatoria de la sentencia condenatoria"[28]. Este estándar es especialmente relevante en casos donde registros *blockchain* constituyen el único sustento probatorio de la acusación.

Asimismo, la autora advierte sobre la necesidad de "reforzar el principio de presunción de inocencia, dado que en ciertos casos el sistema algorítmico termina provocando una propulsión hacia la presunción de culpabilidad"[29]. En el contexto *blockchain*, esto implica que la mera existencia de un registro distribuido no puede invertir la carga probatoria ni generar presunciones automáticas de veracidad que comprometan la posición del investigado.

---

[26] *Id.*
[27] *Ibid.*, p. 109.
[28] *Id.*
[29] *Id.*

Finalmente, Barona Vilar subraya que "Las herramientas algorítmicas allanan la valoración judicial de la prueba, superponiéndose al *in dubio pro reo*, en cuanto el sistema algorítmico pueda convencer directamente al juzgador sobre la culpabilidad, más allá de toda posible duda razonable"[30]. Por ello, exige "incorporar en la norma procesal las salvedades para evitarlo y muy especialmente garantizar desde los principios que permiten abrigar la tutela efectiva, la exigencia de la debida motivación de la decisión, espejo de la valoración"[31].

Desde una perspectiva crítica, el capítulo permite advertir que el verdadero desafío no reside únicamente en determinar si la *blockchain* es válida como prueba, sino en evitar que su estructura técnica y su sofisticación operativa generen una *asimetría epistémica* entre los actores del proceso. El acusado, sus abogados e incluso el propio juez pueden encontrarse en situación de inferioridad técnica frente a las entidades que producen, controlan o presentan estos registros. Este desequilibrio amenaza con distorsionar la igualdad de armas procesal y con generar situaciones de *indefensión tecnológica*.

Por tanto, el verdadero eje del debate no está en la admisibilidad de la prueba tecnológica como tal, sino en la reconstrucción procesal de sus garantías. En un proceso penal cada vez más digitalizado, la tecnología debe subordinarse al Derecho, no a la inversa. Y si bien el proceso no puede mantenerse impermeable a la realidad tecnológica, tampoco puede abdicar de sus fundamentos garantistas en nombre de la eficiencia o de la inmutabilidad matemática.

En definitiva, resulta esencial para entender que la tecnología blockchain y la inteligencia artificial, pese a sus potencialidades, no pueden desplazar el control judicial ni los principios fundamentales del proceso penal. La introducción de estos sistemas debe hacerse bajo una perspectiva crítica, garantista y siempre subordinada a la protección de derechos y garantías, evitando caer en la ilusión de una neutralidad tecnológica que, en la práctica, puede generar nuevos riesgos de indefensión y desigualdad[32].

[30] *Id.*
[31] *Id.*
[32] Barona Vilar S., "Dataización de la justicia (Algoritmos, Inteligencia Artificial y Justicia, ¿el comienzo de una gran amistad?)", *Revista Boliviana. de Derecho*, nº 36, 2023, p. 40.

3.2. Análisis de la STS 326/2019 y jurisprudencia posterior

La Sentencia del Tribunal Supremo (Sala de lo Penal), núm. 326/2019, de 20 de junio, constituye un precedente fundamental para la incorporación de las criptomonedas, específicamente los Bitcoins, al marco jurídico-penal español. Este fallo, emitido en el contexto de un delito de estafa continuada, aborda cuestiones esenciales como la calificación jurídica de los Bitcoins, su tratamiento probatorio y las garantías procesales en casos que involucran activos digitales. Su análisis revela la tensión entre la innovación tecnológica y la rigidez normativa, así como los desafíos que plantea la prueba digital en un sistema legal tradicionalmente anclado en categorías decimonónicas.

El caso resuelto por la STS 326/2019 gira en torno a una estafa en la que los perjudicados invirtieron Bitcoins en una plataforma que prometía gestionarlos para obtener ganancias. El acusado, administrador único de la empresa, incumplió su obligación de reinvertir los fondos, alegando fallos técnicos e insolvencia.

La Sala Penal del Tribunal Supremo confirmó la condena por estafa, pero el aspecto más relevante radica en su pronunciamiento sobre la naturaleza jurídica de los Bitcoins. La sentencia establece que los Bitcoins no son dinero electrónico, sino "activos patrimoniales inmateriales", carentes de un valor único y universal, cuyo precio fluctúa según la oferta y demanda en plataformas especializadas. Esta calificación descarta su equiparación con el dinero fiduciario y los excluye de la protección específica reservada a los medios de pago regulados (art. 1.2 de la Ley 21/2011, de dinero electrónico)[33].

Uno de los ejes centrales del fallo es la validez de la prueba digital asociada a las transacciones con Bitcoins. La Sala subraya que, aunque la tecnología *blockchain* garantiza la inmutabilidad de los registros, esto no exime de acreditar la integridad y autenticidad de la evidencia mediante protocolos forenses. Esta exigencia de rigor técnico se extiende a la cadena de custodia digital. La trazabilidad de los Bitcoins debe ser documentada mediante estándares técnicos internacionalmente reconocidos, como los

[33] Tribunal Supremo, Sala de lo Penal, Sentencia 326/2019, de 20 de junio, FJ 4.º y 5.º [vLex, Ref. 797938401]. Véase también: Sedeño López, J. F., "Naturaleza jurídica de las criptomonedas", *Revista de Contabilidad y Tributación*, n.º 455, 2019, pp. 145-150.

sellos de tiempo (RFC 3161) y la correcta gestión de la evidencia según la norma ISO/IEC 27037:2012[34].

En el ámbito de la responsabilidad civil, la STS 326/2019 niega la restitución *in natura* de los Bitcoins, ordenando en su lugar la indemnización del valor económico perdido[35]. La Sala argumenta que, al no ser moneda de curso legal, su restitución material resultaría impracticable debido a la volatilidad de su cotización.

La jurisprudencia española ha establecido criterios clave para interpretar los delitos económicos vinculados a criptomonedas, tanto cuando estas son instrumento (medio de transferencia de fondos ilícitos) como objeto material (activo blanqueado).

En blanqueo de capitales, el anonimato técnico de las criptomonedas dificulta el rastreo del origen ilícito de los fondos. Sin embargo, la Audiencia Provincial de Asturias (Sección 4.ª), Sentencia 37/2015, de 6 de febrero, resolvió que las entidades financieras deben aplicar medidas de diligencia debida reforzada para verificar la procedencia de los fondos utilizados en operaciones con criptomonedas, incluso si la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo no las incluye expresamente como sujetos obligados[36]. Esta doctrina sienta un precedente para exigir controles antifraude en transacciones con activos digitales, evitando que el sistema financiero se convierta en cómplice pasivo de operaciones opacas[37].

En el ámbito fiscal, la equiparación de las criptomonedas a activos financieros tradicionales es clara. La Resolución de la Dirección General de Tributos V1069-19 (2019) estableció que las ganancias por venta de bitcoins deben declararse como rentas del ahorro, aplicándose los mismos tipos impositivos que a las plusvalías de acciones (19%-28%). Este criterio, ratificado en consultas posteriores de 2024, consolida un régimen fiscal estricto que persigue la evasión mediante activos digitales[38].

---

[34] ISO/IEC 27037:2012, *Guidelines for identification, collection, acquisition and preservation of digital evidence.*
[35] STS 326/2019, FJ 6.º; Sedeño López, J. F., *op. cit.*, pp. 150-152.
[36] Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (BOE núm. 103, de 29 de abril de 2010).
[37] Audiencia Provincial de Asturias (Sección 4.ª), Sentencia 37/2015, de 6 de febrero, FJ 3.º. ECLI:ES:APAS:2015:37; Véase: https://www.databitlaw.tech/analisis-de-la-sentencia-ap-de-asturias-sobre-el-blanqueo-de-capitales-y-bitcoin/
[38] Resolución Vinculante de la DGT, V1069-19, de 20 de mayo de 2019. Disponible en: https://www.iberley.es/resoluciones/resolucion-vinculante-dgt-v1069-19-20-05-2019-1523984

A la luz de lo expuesto, cabe señalar que, si bien la STS 326/2019 representa un paso relevante en el tratamiento judicial de los criptoactivos, revela también una limitación estructural del modelo procesal vigente a la hora de enfrentar fenómenos jurídicamente novedosos como las transacciones distribuidas, los entornos algorítmicos y los activos digitales no centralizados. La aproximación adoptada por el Alto Tribunal —consistente en subsumir los hechos en categorías procesales tradicionales— ofrece una solución pragmática a corto plazo, pero plantea importantes dudas en términos de coherencia sistemática y de suficiencia garantista.

En efecto, el esfuerzo interpretativo desplegado en esta sentencia parte de un presupuesto que merece una reflexión crítica: la idea de que las nuevas realidades tecnológicas pueden ser adecuadamente reconducidas, sin necesidad de reforma normativa, al esquema probatorio clásico basado en la prueba documental, la prueba pericial y los principios generales de valoración judicial. Sin embargo, esta operación de traslación conceptual —por muy sofisticada que sea— puede acabar generando una tensión artificial entre la forma procesal y la naturaleza sustantiva del objeto probatorio.

Desde esta perspectiva, estimo que la jurisprudencia debería avanzar, con la debida prudencia y sin renunciar a los principios del proceso penal, hacia el reconocimiento explícito de la singularidad de la prueba digital y algorítmica, mediante la construcción doctrinal de categorías propias, acordes con la ontología técnica de los criptoactivos y los entornos de decisión automatizada. Esta evolución permitiría, entre otros objetivos, dotar de mayor seguridad jurídica a operadores y justiciables, clarificar las exigencias en materia de autenticación y contradicción, y garantizar un estándar mínimo de tutela judicial efectiva en casos donde intervienen sistemas tecnológicos complejos.

Así, resultaría oportuno que el legislador —y, en su defecto, la jurisprudencia— impulse el desarrollo de una teoría procesal de la prueba tecnológica que contemple:

(i) un estatuto jurídico-procesal específico para los criptoactivos utilizados como objeto o medio de delito;

(ii) un régimen autónomo de admisibilidad, conservación, valoración y contradicción de pruebas generadas por sistemas algorítmicos;

Y (iii) un marco garantista para el tratamiento procesal de evidencias digitales distribuidas, incluyendo mecanismos reforzados de custodia, certificación y peritaje.

En definitiva, no se trata de abandonar los fundamentos clásicos del Derecho procesal penal, sino de reformular su aplicación para preservar su eficacia y legitimidad frente a una criminalidad que evoluciona al ritmo de la innovación tecnológica. El desafío consiste, por tanto, en conjugar continuidad institucional con capacidad adaptativa, de modo que el proceso penal siga siendo —también en el entorno digital— un instrumento al servicio de los derechos fundamentales y del principio de legalidad penal.

3.3. Imputación de responsabilidad penal en delitos cometidos mediante inteligencia artificial y smart contracts

La digitalización y la progresiva "algoritmización" de la sociedad han generado una mutación disruptiva en los patrones de criminalidad y en los fundamentos de la imputación penal. Barona Vilar advierte que la justicia se enfrenta a una "hibridación" inédita entre humanos y máquinas, donde los algoritmos no solo asisten, sino que en ocasiones sustituyen a los operadores jurídicos, planteando el riesgo de convertir la justicia en "frío dato estadístico-matemático" y erosionar el modelo humano de garantías y derechos[39].

Solar Cayón subraya que la IA jurídica no es solo una herramienta, sino un agente que reconfigura el mercado de servicios jurídicos y la propia concepción de la responsabilidad, introduciendo incertidumbres sobre la autoría y la culpabilidad en el ciberespacio[40]. La doctrina española coincide en que, en el estado actual de la técnica y del Derecho, la IA carece de personalidad jurídica y de capacidad de culpabilidad. Sin embargo, la autonomía y opacidad de los sistemas algorítmicos ("caja negra") generan zonas de sombra en la atribución de responsabilidad, especialmente en delitos cometidos sin intervención humana directa o con mínima supervisión[41].

[39] Barona Vilar, S., "Justicia con algoritmos e Inteligencia Artificial, ¿acuerpando garantías y derechos procesales o liquidándolos?" *op cit.*, pp. 83-85.
[40] Solar Cayón, J. I., *La inteligencia artificial jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*, Aranzadi, Navarra, 2019, pp. 45-67.
[41] Bueno de Mata, F., "Macrodatos, inteligencia artificial y proceso: luces y sombras", *Revista General de Derecho Procesal*, n.º 51, 2020, pp. 1-31.

Para determinar si existe dolo —es decir, intención de delinquir— en estos casos, es fundamental analizar el grado de intervención humana en el funcionamiento de la IA. Barona Vilar, recogiendo la doctrina internacional[42], distingue tres escenarios de intervención humana en sistemas automatizados:

- *Man in the loop*: Control humano directo sobre la IA. El dolo es imputable al usuario o programador si se prueba conocimiento y voluntad de delinquir.
- *Man on the loop*: Supervisión humana con posibilidad de intervención. Aquí la responsabilidad puede fundarse en dolo eventual o imprudencia grave, si el sujeto acepta el riesgo de un resultado ilícito por omisión de controles.
- *Man out of the loop*: Autonomía total de la IA. La imputación solo es viable si se acredita dolo en la programación (diseño fraudulento) o una omisión grave de controles (culpa in vigilando). Barona Vilar acuña el término "dolo tecnológico" para describir estos supuestos, en los que la intencionalidad se traslada al momento de la configuración o entrenamiento del algoritmo[43].

Un ejemplo paradigmático de los límites del Derecho penal tradicional ante estos nuevos desafíos es el caso conocido como "hackeo de The DAO" en 2016. The DAO era un fondo de inversión digital gestionado por un programa informático. Un usuario aprovechó un error en el diseño del programa para transferirse a sí mismo una gran cantidad de dinero digital, sin necesidad de manipular el sistema de forma ilegal ni de vulnerar contraseñas, sino simplemente siguiendo los pasos previstos por el propio programa. El daño se produjo por el mero funcionamiento automático del software, lo que dificultó identificar y responsabilizar penalmente a una persona concreta, ya que la acción delictiva se produjo sin una manipulación externa evidente[44].

Este tipo de supuestos obliga a repensar la función de la pena y la prevención general en el ciberespacio. Si la atribución de responsabilidad se diluye entre programadores, usuarios y plataformas, el riesgo de impunidad aumenta y la eficacia preventiva del Derecho penal se ve seriamente comprometida.

---

[42] H. Surden, "Artificial Intelligence and Law: An Overview", *Georgia State University Law Review*, Vol. 35, Issue 1, 2019, p. 1308; M. Gabriel, *El sentido del pensamiento*, Pasado & Presente, 2020, p. 235.
[43] Barona Vilar, S., "Justicia con algoritmos e Inteligencia Artificial, ¿acuerpando garantías y derechos procesales o liquidándolos?", *op cit.*, pp. 110-111.
[44] Yampolskiy, R., "Incident Number 50: The DAO Hack", en McGregor, S. (ed.), *Artificial Intelligence Incident Database*, Responsible AI Collaborative, 2016

Como subraya Barona Vilar, este tipo de casos demuestra que la automatización de la voluntad mediante código no exime de responsabilidad si existe un diseño inicial orientado a resultados ilícitos[45]. Por ello, la práctica procesal exige cada vez más auditorías técnicas y periciales independientes para reconstruir la cadena de decisiones de la IA y valorar la intencionalidad en el diseño o uso del sistema.

La imputación de responsabilidad penal en el marco de delitos cometidos mediante inteligencia artificial y *smart contracts* plantea, a juicio del autor, no solo una cuestión técnico-jurídica, sino un verdadero reto estructural para los principios básicos del Derecho penal, en particular los de personalidad de la pena, culpabilidad y legalidad. El desplazamiento del centro de gravedad de la acción delictiva —desde sujetos físicos hacia sistemas automatizados con capacidad de ejecución autónoma— obliga a reconsiderar las categorías dogmáticas clásicas bajo una lógica funcional, sistémica y adaptativa.

El modelo actual, sustentado en la acción u omisión humana directa, se muestra insuficiente ante estructuras donde la causalidad material está difuminada, el control humano es limitado y el nexo entre voluntad y resultado se encuentra mediado por capas de diseño algorítmico y ejecución automática. La respuesta penal basada en la imputación personal exclusiva —bien por dolo directo, bien por imprudencia o culpa in vigilando— corre el riesgo de generar lagunas de impunidad en supuestos de criminalidad distribuida, especialmente en ecosistemas tecnológicos donde los intervinientes son múltiples, anónimos y geográficamente dispersos.

Desde esta perspectiva, resulta necesario avanzar hacia una reconstrucción procesal de la imputación penal en clave funcional, que permita atribuir responsabilidad en función del grado de dominio técnico, poder de configuración del sistema, y control efectivo sobre el riesgo creado. Esta aproximación exige abandonar el paradigma estrictamente individualista de autoría para explorar modelos de responsabilidad por estructuras, que reconozcan la participación de múltiples agentes humanos y corporativos en la génesis de comportamientos delictivos mediados por tecnología.

[45] Barona Vilar, S., *Algoritmización del Derecho y de la Justicia, op. cit*., p. 203.

La figura de la "coautoría funcional algorítmica" propuesta en este trabajo aspira a ofrecer un marco conceptual intermedio que preserve los principios del Derecho penal de acto, pero permita imputar responsabilidad en contextos donde el resultado se produce mediante una interacción compleja entre código, usuarios y plataformas. En este sentido, se propone que la responsabilidad se distribuya no únicamente por la titularidad formal de la acción, sino en atención al rol técnico desempeñado, la capacidad de previsión sobre el comportamiento del sistema, y el grado de intervención (activa o por omisión) en el diseño o activación del mismo.

Este modelo podría ser especialmente útil en delitos cometidos mediante *smart contracts* programados con finalidades fraudulentas, algoritmos entrenados con sesgos intencionados o sistemas desplegados sin las debidas garantías de supervisión. La clave estará en establecer criterios normativos claros de imputación, combinando el análisis técnico-forense de la arquitectura algorítmica con los principios procesales de contradicción, culpabilidad y defensa efectiva.

En conclusión, mientras no se reconozca la necesidad de adaptar la teoría del delito a las realidades digitales automatizadas, el Derecho penal corre el riesgo de ser superado por la velocidad de la innovación tecnológica. Resulta imprescindible abordar este proceso desde una perspectiva interdisciplinar, que combine conocimientos jurídicos, técnicos y ético-políticos, sin renunciar a los pilares garantistas del orden penal. De lo contrario, se corre el riesgo de que la automatización y la descentralización se conviertan en espacios opacos de impunidad, debilitando tanto la eficacia preventiva del sistema como su legitimidad constitucional.

3.4. Impacto de la Inteligencia Artificial en la práctica jurídica y el proceso penal: Hacia un equilibrio entre eficacia tecnológica y garantías procesales

La irrupción de la inteligencia artificial en la práctica jurídica y procesal española ha supuesto un cambio de paradigma que afecta tanto a la organización de la justicia como a las garantías procesales y la igualdad de armas entre las partes. Solar Cayón ofrece un análisis exhaustivo del impacto de la IA en el mercado de servicios jurídicos y, por extensión, en la práctica procesal penal. Destaca que los sistemas de IA jurídica han dejado de ser una promesa futurista para convertirse en herramientas cotidianas en la gestión de grandes volúmenes de información, la elaboración automática de documentos, la detección de patrones de fraude y el asesoramiento predictivo sobre el resultado de litigios[46].

Sin embargo, advierte que esta automatización, si bien incrementa la eficiencia y la capacidad de análisis de macrodatos en investigaciones penales, también entraña el riesgo de una "delegación cognitiva" por parte de los operadores jurídicos, quienes podrían aceptar sin el debido control crítico los resultados generados por algoritmos. Esto, a su vez, vaciaría de contenido el principio de inmediación judicial y la valoración personal de la prueba, pilares esenciales del proceso penal. Por ello, Solar Cayón insiste en que la introducción de la IA debe ir acompañada de una revisión profunda de los esquemas de control, transparencia y responsabilidad, así como de una formación técnica adecuada de los operadores jurídicos para evitar la indefensión técnica y la asimetría de recursos entre las partes[47].

En paralelo, Beiro Magán sistematiza los principales desafíos institucionales que supone la digitalización y automatización de la justicia penal. Señala que la gestión masiva de datos judiciales y el uso de software con aprendizaje automático están transformando la organización y los flujos de trabajo en la Administración de Justicia[48]. No obstante, advierte que la falta de interoperabilidad entre sistemas, la obsolescencia de la LECrim y la insuficiente formación tecnológica del personal judicial comprometen tanto la eficacia como la seguridad jurídica del proceso penal.

---

[46] Solar Cayón, J. I., *op cit.*, pp. 45-67.
[47] *Ibid.*
[48] Beiro Magán, J. M., "Retos tecnológicos de la Administración de Justicia española para la tercera década del siglo XXI", *Pensamiento Crítico*, n.º 13, 2019, pp. 1-15.

Para Beiro Magán, la implantación de IA en la justicia española requiere una profunda reforma organizativa y normativa, que contemple la estandarización de protocolos, la certificación de herramientas y la formación obligatoria en competencias digitales para todos los actores del sistema judicial[49].

Desde una perspectiva de garantías, De Asís Pulido desarrolla la noción de "debido proceso tecnológico" como exigencia constitucional en la era digital. Sostiene que la digitalización y la implementación de sistemas algorítmicos en la justicia penal requieren adaptar los derechos procesales clásicos, en especial el derecho de defensa y la contradicción, a los nuevos riesgos. Advierte sobre la opacidad de los sistemas de IA —las llamadas "cajas negras procesales"— y la dificultad de auditar sus criterios de decisión, lo que puede desembocar en situaciones de indefensión material si no se garantiza el acceso de la defensa a los metadatos, algoritmos y bases de datos empleadas. De Asís Pulido concluye que preservar el equilibrio procesal en este contexto exige reconocer un derecho al debido proceso tecnológico, que incluya transparencia explicativa, posibilidad de peritaje contradictorio y auditoría independiente de los sistemas utilizados[50].

El análisis de Bueno de Mata sobre el uso de big data y sistemas predictivos en la investigación penal subraya los riesgos de sesgo algorítmico y discriminación. Si bien la IA permite la creación de perfiles de riesgo y la identificación de patrones delictivos con una eficacia inédita, estos modelos pueden reproducir y amplificar discriminaciones estructurales presentes en los datos históricos. La justicia predictiva basada en correlaciones estadísticas puede, por tanto, llevar a decisiones automatizadas que afecten desproporcionadamente a grupos vulnerables. Bueno de Mata enfatiza la necesidad de auditorías de impacto ético y mecanismos de control que permitan identificar y corregir sesgos algorítmicos en el proceso penal[51].

[49] *Ibid.*
[50] De Asís Pulido, M., "Derecho al debido proceso e inteligencia artificial", *Revista Derechos Humanos y Educación,* 1(7), 2021, pp. 139-159.
[51] Bueno de Mata, F., *op cit.,* pp. 1-31.

La problemática de la prueba digital y la inmediación judicial es abordada por Gascón Inchausti, quien advierte sobre la "externalización del proceso penal" y la "sumisión pericial estructural" derivadas de la creciente complejidad técnica de la prueba digital y la IA. La dependencia de informes periciales y herramientas tecnológicas puede vaciar de contenido el principio de inmediación judicial y convertir al juez en un mero validador de conclusiones técnicas ajenas. Gascón Inchausti aboga por la creación de protocolos de transparencia algorítmica, la formación de jueces técnicos especializados y la obligatoriedad de dictámenes periciales contradictorios financiados por el Estado para garantizar la igualdad de armas y la contradicción efectiva en el proceso penal económico[52].

En cuanto al sesgo algorítmico y la discriminación procesal, Borges Blázquez ofrece una taxonomía detallada de los sesgos que pueden afectar a la justicia penal: sesgos de entrada (provenientes de datos históricos), de confirmación (refuerzo de hipótesis previas), de retroalimentación (incorporación de falsos positivos) y de implementación (interpretación humana sesgada). Advierte que la aplicación acrítica de sistemas de IA puede perpetuar desigualdades y comprometer el principio de igualdad ante la ley, por lo que aboga por mecanismos de *debiasing* activo, auditorías continuas y la participación de comités éticos en la supervisión de los sistemas utilizados[53].

Por último, Martín Diz plantea la necesidad de un "constitucionalismo algorítmico" que adapte los principios tradicionales del proceso penal a la realidad de la inteligencia artificial. Propone tres pilares para este nuevo modelo: la transparencia radical (publicidad de los criterios de ponderación y márgenes de error), la proporcionalidad dinámica (graduación de la intervención tecnológica según el riesgo para los derechos fundamentales) y el control ciudadano (participación de colectivos afectados en el diseño de las herramientas). Martín Diz subraya que solo una articulación normativa y procesal que garantice la auditabilidad, la contradicción y la revisión humana de las decisiones

[52] Gascón Inchausti, F., "Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial", en J. Conde Fuentes & G. Serrano Hoyo (Eds.), *La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro*, Atelier, Barcelona, 2019, pp. 191-206.

[53] Borges Blázquez, R., "El sesgo de la máquina en la toma de decisiones en el proceso penal", *Revista Ius et Scientia*, 6(2), 2020, pp. 54-71.

automatizadas puede evitar que la eficacia tecnológica erosione las garantías constitucionales del proceso penal[54].

El estudio demuestra que la generalización de herramientas algorítmicas en la fase de investigación, prueba y decisión judicial exige una respuesta jurídicamente estructurada, no solo para preservar la seguridad jurídica y la igualdad procesal, sino para evitar que el juicio penal devenga en un ejercicio de validación formal de resultados previamente generados por sistemas opacos. La asimetría técnica entre partes, la pérdida de control del juez sobre los fundamentos reales de las decisiones y la dificultad de contradicción efectiva frente a productos algorítmicos son amenazas reales que afectan, en última instancia, a la legitimidad misma del proceso penal como espacio de garantía frente al poder punitivo del Estado.

En definitiva, el proceso de incorporación de la inteligencia artificial al ámbito penal no puede concebirse como un simple fenómeno de modernización técnica, sino como un reto constitucional y garantista de primer orden, que obliga a reinterpretar desde sus cimientos la arquitectura del proceso penal. La eficiencia algorítmica y la capacidad de predicción no pueden legitimar por sí mismas decisiones que afecten a los derechos fundamentales de las personas investigadas.

En este marco, resulta imprescindible recordar, como advierte Díez Riaza, que: "Nunca debemos desviarnos del fin principal de toda esta modernización y transformación digital ya que no puede ser considerado como un fin en sí mismo, sino que ha de ser instrumental para lograr el fin superior del derecho a la tutela judicial efectiva que se logra con un juez imparcial, entre otros parámetros, y si la tecnología no sirve a ese fin, esta no puede ser válida"[55]. Solo desde esta perspectiva teleológica —donde la innovación se subordina a la protección de garantías sustantivas— será posible diseñar un proceso penal tecnológicamente avanzado y, al mismo tiempo, profundamente respetuoso con los valores constitucionales del Estado de Derecho.

---

[54] Martín Diz, F., "Inteligencia artificial y proceso: garantías frente a eficiencia en el entorno de los derechos procesales fundamentales", en F. Jiménez Conde & R. Bellido Penadés (Eds.), *Justicia: ¿Garantías vs. eficacia?,* Tirant lo Blanch, Valencia, 2019, pp. 815-827.

[55] Díez Riaza, S., "Un nuevo mecanismo de la inmersión digital de la justicia: la carpeta justicia y su dependencia de la portabilidad y la interoperabilidad de los datos", en Calaza López, S. (Dir.), Yáñez Vivero, F. (Dir.), Donado Vara, A. (Coord.), Jiménez Muñoz, F.J. (Coord.), *Digitalización del servicio público de justicia e inteligencia artificial judicial*, pp. 91, Dykinson, Madrid, 2024.

4. PROPUESTAS DE REFORMA Y MODELOS DE GOBERNANZA PARA LA PRUEBA DIGITAL Y LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL

4.1. Reforma legislativa: hacia una regulación autónoma de la prueba digital

La ausencia de una regulación autónoma y sistemática de la prueba digital en la LECrim constituye, a juicio de buena parte de la doctrina y la práctica forense, una de las carencias más relevantes del proceso penal español contemporáneo. A pesar de la creciente centralidad que esta clase de evidencias ha adquirido en la investigación y enjuiciamiento de delitos, la legislación procesal continúa apoyándose, en gran medida, en categorías tradicionales que dificultan un tratamiento adecuado de este fenómeno emergente[56].

Como es bien sabido, la prueba digital presenta unas características técnicas —intangibilidad, duplicabilidad, facilidad de alteración o volatilidad— que hacen aconsejable la articulación de un marco jurídico específico, que contemple no solo su obtención y conservación, sino también su incorporación y valoración conforme a principios de legalidad, contradicción y proporcionalidad. La jurisprudencia reciente, junto con diversas aportaciones doctrinales, ha comenzado a delinear criterios interpretativos útiles; sin embargo, la dispersión normativa y la falta de previsiones claras generan, en la práctica, zonas de incertidumbre que pueden traducirse en consecuencias relevantes para la igualdad de armas y la tutela judicial efectiva[57].

Por todo ello, la reforma legislativa debe abordar, al menos, los siguientes ejes:

- Siguiendo la doctrina de Planchadell-Gargallo, **resulta imprescindible dotar a la Ley de Enjuiciamiento Criminal de una regulación específica sobre prueba digital**, que supere la actual dispersión normativa y adapte los protocolos de obtención, conservación y valoración de la evidencia tecnológica a la realidad forense[58].
- El **reconocimiento expreso de la prueba digital como medio autónomo**, diferenciando entre fuente de prueba (el soporte o sistema que contiene la información digital) y medio de prueba (el instrumento procesal para su

[56] Magro Servet, V., *op cit.,* pp. 15-18.
[57] Delgado Martín, J., *op cit.,* pp. 12-20.
[58] Planchadell-Gargallo, Andrea, "Breves apuntes sobre digitalización del proceso penal español a la luz del Real Decreto-ley 6/2023", *Rev. Bras. de Direito Processual Penal*, v. 10, n. 2, 2024, pp. 4, 12, 14, 16.

incorporación y valoración), y estableciendo criterios claros para su admisión, contradicción y valoración judicial[59].

- La **regulación detallada de la cadena de custodia digital**, incorporando estándares internacionales como la ISO/IEC 27037:2012, y fijando obligaciones precisas para la documentación, preservación y trazabilidad de la evidencia digital desde su obtención hasta su presentación en juicio[60].
- La **introducción de presunciones de integridad y mecanismos de impugnación específicos**: siguiendo la experiencia comparada y la doctrina, la ley debe establecer presunciones *iuris tantum* de autenticidad para registros *blockchain* públicos y sistemas certificados, permitiendo a la parte contraria impugnar la prueba mediante peritaje contradictorio, y garantizando siempre el derecho de defensa y la igualdad de armas.
- El **derecho de acceso a los metadatos, logs y algoritmos empleados en la obtención y análisis de la prueba digital**, así como la posibilidad de solicitar peritajes independientes financiados públicamente en supuestos de especial complejidad técnica.

En mi opinión, esta reforma no debe abordarse desde una lógica meramente técnica, sino también desde una perspectiva garantista y pedagógica. Garantista, porque debe asegurar que los derechos fundamentales —en particular, la intimidad, la defensa y la presunción de inocencia— se respeten también en el entorno digital, sin excepciones ni lagunas. Pedagógica, porque la incorporación de nuevos tipos de prueba exige también un esfuerzo formativo y de adaptación institucional, que permita a jueces, fiscales, letrados y peritos afrontar con solvencia los desafíos que plantea esta realidad tecnológica en permanente evolución.

Conviene recordar que el proceso penal no es un fin en sí mismo, sino un instrumento al servicio de la justicia. Por ello, no deberíamos resignarnos a forzar el encaje de la prueba digital en estructuras normativas pensadas para un contexto analógico. Como ya ocurrió en su día con la incorporación de la prueba científica, o con la regulación de las intervenciones de las comunicaciones, el ordenamiento debe ir adaptándose, con

[59] Delgado Martín, J., *op cit.* pp. 12-20.
[60] ISO/IEC 27037:2012, *Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence*.

prudencia, pero sin demora, a los cambios que impone la realidad social y tecnológica. Solo así podrá mantener su legitimidad y eficacia.

En definitiva, dotar a la prueba digital de un estatus jurídico autónomo y coherente no supone un privilegio para la tecnología, sino una expresión de respeto a los principios rectores del proceso penal. En un contexto en el que lo digital ha dejado de ser excepcional para convertirse en estructural, postergar esta reforma equivale a asumir una disfunción prolongada del sistema. Como juristas, nuestra responsabilidad es anticipar los retos que plantea el uso de estas evidencias y contribuir, desde el análisis técnico y la reflexión crítica, a construir un proceso penal que sea al mismo tiempo eficaz, garantista y ajustado a nuestro tiempo.

4.2. Propuesta de modelo de compliance 4.0: equilibrio entre automatización y garantías procesales

La evolución de los entornos económicos y tecnológicos ha tensionado de forma significativa los marcos tradicionales de responsabilidad penal corporativa y control preventivo. Frente a una criminalidad económico-digital cada vez más descentralizada, automatizada y transfronteriza, resulta razonable plantear si los actuales programas de *compliance* —basados en estructuras normativas estáticas y revisiones ex post— pueden seguir desempeñando una función verdaderamente eficaz de prevención y detección. En este sentido, la propuesta de un modelo de *compliance* 4.0 no solo es oportuna, sino necesaria[61].

Ahora bien, lo que aquí se propone no es una mera actualización técnica de los sistemas de cumplimiento, sino una redefinición estructural de los mecanismos de control, asentada sobre tecnologías de supervisión continua y registros inmutables, pero también articulada en torno a un principio irrenunciable: el respeto a las garantías procesales en un Estado de Derecho. La tensión entre eficiencia preventiva y tutela judicial no debe resolverse a favor de una ni otra dimensión de forma mecánica. El reto consiste en armonizarlas, integrando la innovación tecnológica en el orden jurídico sin erosionar sus fundamentos garantistas.

[61] Rich & Asociados, "La nueva era del compliance penal en la Industria 4.0", *Blog Jurídico*, 2024. Disponible en https://www.rich-asociados.com/la-nueva-era-del-compliance-penal-en-la-industria-4-0/

Desde una perspectiva analítica, el *compliance* 4.0 se articula como un sistema distribuido de control, en el que la lógica normativa se embebe en la arquitectura tecnológica de la organización. Esto implica un salto cualitativo: pasamos de un *compliance* interpretativo, basado en el juicio humano y sujeto a evaluación contextual, a un *compliance* computacional, en el que las reglas se ejecutan automáticamente mediante *smart contracts* y *oráculos* externos. Esta automatización de la norma genera indudables beneficios —especialmente en entornos de alta complejidad transaccional—, pero también plantea interrogantes procesales de fondo.

Entre ellos, cabría destacar al menos tres. En primer lugar, ¿cómo preservar el principio de presunción de inocencia cuando un sistema automatizado activa medidas cautelares sin intervención judicial previa? En segundo lugar, ¿es posible garantizar un auténtico derecho de defensa frente a decisiones derivadas de algoritmos opacos o entrenados con datos sesgados? Y, en tercer lugar, ¿qué margen tiene el juez penal para revisar decisiones generadas automáticamente por protocolos codificados cuya lógica escapa a los lenguajes jurídicos tradicionales?

A mi juicio, estas preguntas no deben responderse con una oposición frontal a la automatización, sino con una exigencia de diseño institucional inteligente, donde las capacidades técnicas se integren dentro de un ecosistema jurídico controlado y auditado. El uso de tecnologías como la *blockchain notarial*, la encriptación con *zero-knowledge proofs* o las APIs judiciales seguras puede ofrecer respuestas prácticas que, lejos de debilitar las garantías procesales, las refuercen. Pero ello exige también un marco normativo claro, una cultura organizativa responsable y un compromiso institucional con la transparencia.

Desde esta perspectiva, el *compliance* 4.0 no debe entenderse como un fin en sí mismo, sino como una herramienta al servicio de un modelo de gobernanza ética y jurídica. Su éxito dependerá menos de la sofisticación técnica de sus componentes que de su capacidad para insertarse en un entramado procesal coherente con los valores constitucionales. Esto implica no solo un rediseño normativo, sino también una transformación formativa de los operadores jurídicos, que deberán adquirir competencias para interactuar críticamente con tecnologías emergentes sin caer ni en la fascinación acrítica ni en el rechazo tecnófobo.

Como reflexión personal, considero que la verdadera innovación jurídica no consiste en incorporar tecnologías de vanguardia, sino en conservar los principios fundamentales del proceso penal dentro de un mundo cambiante. La incorporación de algoritmos al cumplimiento normativo plantea cuestiones inéditas, pero también ofrece una oportunidad única para repensar el Derecho procesal desde una lógica de anticipación, equilibrio y control. En este sentido, el *compliance* 4.0 debe ser concebido no solo como un instrumento de prevención penal, sino como una plataforma institucional que garantice que la transformación digital se realice con legitimidad, transparencia y control jurisdiccional efectivo.

4.3. Formación especializada para operadores jurídicos: puente entre tecnología y garantías procesales

La implementación acelerada de tecnologías disruptivas en la Administración de Justicia ha generado una paradoja preocupante: mientras las herramientas digitales prometen mayor eficiencia procesal, la falta de formación especializada de los operadores jurídicos puede convertirse en el principal obstáculo para la efectividad del sistema y, más grave aún, en una amenaza directa a las garantías procesales fundamentales.

El Marco de Competencias Digitales para la formación del personal de Justicia elaborado por el Centro de Estudios Jurídicos en 2023 reconoce explícitamente que "Tal y como establece la Estrategia europea de formación judicial, los profesionales de la justicia deben ser conscientes del impacto que las herramientas y las tecnologías digitales tienen en los casos tramitados y estar preparados para utilizarlas correctamente en su práctica diaria. Además, deben garantizar la protección adecuada de los derechos de las personas y sus datos personales en el espacio digital, en concreto para que las partes puedan acceder a los expedientes y asistir a las audiencias judiciales. En este contexto, es necesario promover las capacidades digitales en Justicia para que jueces, fiscales, el personal judicial y los demás profesionales de la justicia puedan utilizar y aplicar las tecnologías y herramientas digitales de manera eficaz en garantía de los derechos y libertades."[62].

[62] Centro de Estudios Jurídicos, *Marco de Competencias Digitales para la formación del personal de Justicia*, Madrid, 2023, pp. 8-9.

En primer lugar, el Marco parte de una concepción integral de la competencia digital, estructurando la formación en cinco grandes áreas: derechos y deberes digitales, entorno de Justicia digital, accesibilidad y atención a la ciudadanía, transformación digital y gestión del cambio, y seguridad y sostenibilidad en entornos digitales[63]. Esta aproximación multidimensional permite superar el tradicional reduccionismo instrumental —centrado en el mero manejo de herramientas informáticas— para situar la formación tecnológica como un elemento transversal y estratégico, alineado con la protección de los derechos fundamentales y la igualdad de acceso a la Justicia en el entorno digital[1].

Un aspecto especialmente relevante es la función del Marco como guía para el diseño de planes docentes, así como su utilidad como herramienta de autodiagnóstico para los propios operadores jurídicos. El documento promueve la identificación de los conocimientos, capacidades y actitudes necesarias para el desempeño profesional en un contexto sometido a transformación digital acelerada, estableciendo descriptores claros para cada nivel competencial. Esta metodología facilita tanto la evaluación objetiva de las carencias formativas como la planificación de itinerarios de capacitación adaptados a los distintos perfiles profesionales del sector justicia[64].

El Marco destaca, además, por su orientación participativa y dinámica. La apertura de una consulta pública para la validación y retroalimentación del texto, dirigida tanto a profesionales como a la ciudadanía, refuerza la legitimidad y pertinencia de la propuesta, asegurando que las competencias definidas respondan a las demandas reales del sistema judicial y de la sociedad. Esta dimensión participativa constituye un avance significativo respecto a modelos previos, tradicionalmente diseñados de forma unilateral y poco permeables a la experiencia práctica de los operadores[65].

[63] *Id.,* p. 13.
[64] *Id.*, p. 10.
[65] *Id.,* p. 12.

Desde la perspectiva de las garantías procesales, el Marco se alinea expresamente con la Estrategia Europea de Formación Judicial 2021-2024[66], subrayando la necesidad de que jueces, fiscales y personal judicial no solo dominen las tecnologías, sino que sean capaces de identificar y gestionar los riesgos asociados a la protección de datos personales, la transparencia algorítmica y la accesibilidad universal. Este enfoque ético y garantista es imprescindible para evitar que la digitalización se traduzca en nuevas formas de exclusión o indefensión, especialmente para los colectivos más vulnerables[67].

No obstante, un análisis crítico revela que, pese a la precisión en la definición de áreas competenciales y objetivos formativos, la propuesta adolece de ciertas carencias estructurales que pueden limitar su impacto real en la práctica procesal. La efectividad del Marco dependerá en gran medida de la voluntad política y de la dotación de recursos suficientes para convertir los estándares definidos en formación obligatoria, evaluable y periódica para todos los operadores jurídicos. Actualmente, el Marco se configura como una referencia orientadora, pero no existe un mandato normativo que obligue a jueces, fiscales, abogados y peritos a acreditar periódicamente su capacitación en competencias digitales críticas. Esta ausencia de obligatoriedad puede perpetuar la brecha tecnológica y la desigualdad de armas en el proceso penal, especialmente en el ámbito de la prueba digital y la gestión de evidencias complejas.

Además, el Marco reconoce la necesidad de actualización continua, pero no concreta un protocolo institucional ni un sistema de revisión periódica que permita adaptar los contenidos formativos a la rápida evolución tecnológica y a la aparición de nuevos riesgos jurídicos y procesales.

La transformación digital del delito económico y la irrupción de tecnologías como *blockchain*, inteligencia artificial y *smart contracts* exigen una revisión dinámica y flexible de las competencias requeridas, algo que el Marco, en su versión actual, deja en un plano meramente programático[68].

---

[66] Comisión Europea, "Garantizar la justicia en la UE: estrategia europea sobre la formación judicial para 2021-2024", Comunicación COM(2020) 713 final de 2.12.2020, disponible en EUR-Lex (https://eur-lex.europa.eu/ES/legal-content/summary/european-judicial-training-strategy-2021-2024.html.
[67] *Id.,* p. 9.
[68] *Id.,* p. 12.

Sobre la base de este diagnóstico, la propuesta de este trabajo de investigación se formula se articula precisamente como respuesta a estos déficits detectados en el Marco del CEJ, planteando un modelo de formación especializada que supere sus limitaciones y garantice la efectividad de las garantías procesales en el entorno digital. En concreto, se propone:

- La incorporación de la formación digital como requisito legal y deontológico obligatorio para todos los operadores jurídicos, con certificación periódica y evaluación práctica de competencias críticas (gestión de pruebas *blockchain*, auditoría de IA, preservación de cadena de custodia digital, etc.).
- El establecimiento de un fondo estatal específico y blindado presupuestariamente para la formación tecnológica del sector justicia, gestionado por un organismo independiente y con participación de universidades, colegios profesionales y peritos acreditados.
- La creación de un observatorio permanente de actualización tecnológica y jurídica, encargado de revisar y adaptar el Marco de Competencias Digitales cada dos años, integrando las novedades normativas, jurisprudenciales y técnicas, así como los riesgos emergentes detectados en la práctica forense.
- El desarrollo de protocolos de colaboración con centros de excelencia y entidades certificadoras (ENAC, INCIBE), para asegurar una formación práctica, multidisciplinar y homologada a nivel europeo, más allá de la mera capacitación teórica.

En definitiva, el presente análisis ha demostrado que la formación especializada en competencias digitales para operadores jurídicos constituye un imperativo constitucional de primer orden, que trasciende la mera actualización técnica para convertirse en una garantía estructural del Estado de Derecho en la era digital.

La paradoja identificada al inicio de este trabajo —entre la promesa de eficiencia tecnológica y el riesgo de erosión de las garantías procesales— encuentra su resolución únicamente a través de un modelo formativo que haga de los operadores jurídicos verdaderos arquitectos garantistas de la transformación digital, y no meros espectadores de esta.

El Marco de Competencias Digitales del Centro de Estudios Jurídicos, pese a sus indudables méritos estructurales y metodológicos, adolece de una carencia fundamental: la ausencia de mecanismos normativos que conviertan la excelencia digital en una exigencia deontológica obligatoria y evaluable. Esta limitación no es meramente procedimental, sino que compromete la propia esencia del derecho fundamental a la tutela judicial efectiva en el entorno digital, al perpetuar una desigualdad de armas que puede resultar determinante en la resolución de controversias complejas que involucren pruebas tecnológicas avanzadas.

La propuesta aquí formulada supera esta limitación estructural mediante la articulación de un sistema integral que combina obligatoriedad normativa, sostenibilidad presupuestaria, actualización continua y excelencia académica. La incorporación de la formación digital como requisito legal y deontológico obligatorio, respaldada por un fondo estatal blindado y un observatorio permanente de actualización, no representa una carga adicional para el sistema, sino una inversión estratégica en la calidad institucional de la Justicia española. La colaboración con centros de excelencia y entidades certificadoras asegura, además, que esta formación se sitúe en los estándares más elevados de rigor académico y aplicabilidad práctica.

Desde una perspectiva más amplia, esta propuesta contribuye a resolver una de las tensiones más complejas del constitucionalismo contemporáneo: la preservación de los valores democráticos y garantistas en un contexto de aceleración tecnológica sin precedentes. Al convertir a los operadores jurídicos en agentes activos de la digitalización garantista, se construye un modelo de innovación judicial que no sacrifica la protección de derechos fundamentales en el altar de la eficiencia, sino que hace de ambos objetivos elementos sinérgicos y mutuamente reforzantes.

La relevancia de esta aportación se inserta en la estrategia de modernización impulsada por el Plan Justicia 2030[69]. En un contexto en el que la digitalización de la Justicia se ha consolidado como prioridad institucional, la propuesta española de formación garantista puede convertirse en un modelo de referencia, demostrando que la excelencia tecnológica

[69] Ministerio de Justicia, Plan Justicia 2030, disponible en https://www.justicia2030.es

y la protección de las garantías procesales no solo son compatibles, sino mutuamente necesarias.

La formación especializada propuesta no es, por tanto, simplemente una respuesta técnica a un problema coyuntural, sino una apuesta estratégica por un modelo de Justicia que preserve, en el entorno digital, todos los valores que caracterizan al Estado de Derecho democrático. En esta perspectiva, los operadores jurídicos no son meros usuarios de tecnologías diseñadas por terceros, sino co-creadores responsables de un ecosistema judicial que pone la innovación al servicio de la justicia, y no la justicia al servicio de la innovación.

El éxito de esta propuesta determinará, en última instancia, si la transformación digital de la Justicia española se consolida como un proceso de modernización garantista o degenera en una mera automatización que erosione las conquistas históricas del debido proceso. La elección entre ambos caminos no es inevitable: es una decisión política e institucional que debe adoptarse con plena conciencia de sus implicaciones para las generaciones futuras y con el compromiso inquebrantable de hacer de la tecnología una aliada, y no una amenaza, para la realización efectiva de los derechos fundamentales en el siglo XXI.

5. CONCLUSIONES

La investigación desarrollada en este Trabajo de Fin de Grado ha puesto de manifiesto que el proceso penal español y europeo se enfrenta a un reto estructural sin precedentes ante la digitalización acelerada de la criminalidad económica. La irrupción de tecnologías como *blockchain*, los *smart contracts* y la inteligencia artificial ha desbordado los marcos normativos y procesales tradicionales, generando una brecha crítica entre la sofisticación de los ilícitos y la capacidad de respuesta de los operadores jurídicos y del propio sistema de garantías.

En primer lugar, se ha evidenciado la **insuficiencia del marco normativo actual** para dar respuesta a la complejidad y volatilidad de la prueba digital. La LECrim, anclada en categorías decimonónicas, fuerza el encaje de evidencias tecnológicas en figuras como la prueba documental o la pericial, lo que produce inseguridad jurídica, desigualdad de armas y riesgos de indefensión. La jurisprudencia reciente, especialmente la STS 326/2019, ha reconocido el valor probatorio de los registros *blockchain*, pero ha condicionado su eficacia a validaciones periciales ad hoc, trasladando al perito informático funciones que deberían corresponder al órgano judicial. Esta situación es especialmente problemática en contextos tecnológicamente complejos, como los registros en *blockchains* públicas o los algoritmos de inteligencia artificial, donde la ausencia de regulación específica sobre la cadena de custodia y la autenticidad de la prueba digital genera un "limbo jurídico" que debilita tanto la eficacia persecutoria como las garantías defensivas.

En segundo lugar, el trabajo ha evidenciado que la **atribución de responsabilidad penal en entornos automatizados y descentralizados plantea desafíos sin precedentes para la dogmática penal**, particularmente tras la entrada en vigor del Reglamento MiCA (2023/1114 UE) y los recientes desarrollos jurisprudenciales. La ejecución de fraudes mediante *smart contracts* autoejecutables o la operativa de DAOs diluye las categorías clásicas de autoría y participación, exigiendo una relectura crítica del dolo tecnológico y de los criterios de imputación objetiva. La aplicación analógica de figuras como los arts. 31 bis a 31 quater CP —diseñados para responsabilidad corporativa tradicional— resulta insuficiente ante sistemas donde la toma de decisiones se distribuye algorítmicamente entre múltiples actores humanos y no humanos.

En tercer lugar, **la utilización de inteligencia artificial en la investigación penal**, aunque aporta eficiencia en la detección y análisis de patrones delictivos, introduce riesgos significativos de sesgo, opacidad y vulneración del derecho de defensa. La investigación ha puesto de relieve que la falta de transparencia de los sistemas algorítmicos y la ausencia de formación técnica de los operadores jurídicos pueden desembocar en situaciones de indefensión material. La jurisprudencia y la doctrina coinciden en que el uso de IA en el proceso penal solo es legítimo si se garantiza el acceso de la defensa a los metadatos, los criterios de ponderación y los márgenes de error, así como la posibilidad de impugnar los informes algorítmicos mediante peritajes independientes.

A partir de este diagnóstico, el trabajo articula una propuesta de **reforma procesal integral** que responde a los retos de la transformación digital y la criminalidad tecnológica, estructurándose en tres ejes complementarios:

(1) la elaboración de una **regulación autónoma y sistemática de la prueba digital en la Ley de Enjuiciamiento Criminal**, que reconozca su especificidad técnica, garantice la autenticidad, integridad y fiabilidad de la evidencia digital conforme a estándares internacionales (como la ISO/IEC 27037:2012) y refuerce los derechos de contradicción y defensa mediante protocolos claros de cadena de custodia y peritaje especializado[70];

(2) el diseño de un **modelo de *compliance* 4.0**, capaz de integrar auditorías algorítmicas continuas, mecanismos de supervisión automatizada y atribución dinámica de responsabilidades en entornos descentralizados —incluyendo la utilización de *smart contracts* de supervisión y sistemas de bloqueo automático validados por revisión judicial ex post—, todo ello alineado con las exigencias del Reglamento MiCA (UE 2023/1114) y las mejores prácticas internacionales[71];

(3) la implantación de un **plan nacional de formación y certificación tecnológica obligatoria para jueces, fiscales, abogados y peritos**, que supere la voluntariedad actual, cierre la brecha digital en la Administración de Justicia y garantice la igualdad de

[70] Véase Planchadell-Gargallo, Andrea, "Breves apuntes sobre digitalización del proceso penal español a la luz del Real Decreto-ley 6/2023", *Rev. Bras. de Direito Processual Penal*, v. 10, n. 2, 2024, pp. 4, 12, 14, 16; Pol. Con. (Edición núm. 102) Vol. 10, No 1, Enero 2025, pp. 1742-1775; ISO/IEC 27037:2012.
[71] Reglamento (UE) 2023/1114 (MiCA), art. 18; STS 45/2024; Verizon Data Breach Investigations Report 2025.

armas en el proceso penal actual, en línea con el Marco de Competencias Digitales del CEJ y los objetivos del Plan Justicia 2030[72].

Reflexión final y proyección futura

La presente investigación pone de manifiesto que el proceso penal se enfrenta a una transformación de calado estructural. No se trata de un simple tránsito hacia nuevas herramientas o metodologías, sino de un **momento de inflexión histórico** en el que la justicia penal debe repensarse a sí misma para preservar su legitimidad en la era digital. La irrupción de tecnologías disruptivas —desde los sistemas de inteligencia artificial hasta la descentralización blockchain— no plantea únicamente desafíos técnicos, sino también interrogantes de fondo sobre el equilibrio entre eficiencia procesal y tutela de derechos.

A lo largo del trabajo se ha abordado con detenimiento la creciente "algoritmización" de la justicia, entendida como el empleo sistemático de tecnologías en funciones tradicionalmente humanas: análisis de pruebas, toma de decisiones, gestión del riesgo. Esta transformación, inevitable en muchos aspectos, sitúa al jurista ante una disyuntiva que no es meramente retórica: **¿reforzará la tecnología las garantías procesales, o acelerará su erosión?** La respuesta, en mi opinión, no radica en rechazar la innovación ni en asumirla sin crítica, sino en **construir marcos normativos adaptativos**, capaces de incorporar lo tecnológico sin renunciar al núcleo de valores que da sentido al proceso penal.

En este contexto, el *compliance* 4.0 y la propuesta de una prueba digital autónoma no deben interpretarse como simples innovaciones técnicas. Son, en rigor, **nuevos paradigmas de gobernanza algorítmica**, que reclaman una lectura procesal desde las claves del control, la transparencia y la proporcionalidad. La arquitectura institucional que articule estas herramientas será decisiva para determinar si el Derecho penal del futuro sigue siendo garantista o se convierte, inadvertidamente, en un instrumento de automatismo incontrolado.

[72] Centro de Estudios Jurídicos, *op cit.*; Ministerio de Justicia, Plan Justicia 2030.

Uno de los elementos que esta investigación considera ineludible es la **formación tecnológica obligatoria de los operadores jurídicos**. No se trata solo de actualizar competencias, sino de reconocer que **la comprensión crítica de las tecnologías jurídicas es hoy una condición de posibilidad del ejercicio efectivo de la función jurisdiccional**. Un juez que no entienda cómo funciona un algoritmo de clasificación de riesgo, un fiscal que no pueda verificar un hash blockchain o un abogado que desconozca los protocolos de custodia digital, no podrán garantizar ni exigir justicia en un entorno en que los hechos ya no se producen solo en el mundo físico, sino también en la lógica binaria de los sistemas distribuidos. Esta carencia puede convertirse, de forma inadvertida, en un nuevo factor de **desigualdad procesal**, dejando al margen a quienes no dispongan de medios o conocimientos especializados.

Con todo, este trabajo no quiere transmitir una visión alarmista, sino una **oportunidad de evolución consciente**. Lejos de representar una amenaza, la digitalización del proceso penal puede —si se orienta con criterio y rigor— convertirse en una vía para **fortalecer el Estado de Derecho**, dotando a la justicia de instrumentos más precisos, trazables, auditables y, en última instancia, más confiables. La justicia del futuro será algorítmica en parte, pero no debe ser deshumanizada. **Tecnología y derechos no son esferas incompatibles**, siempre que se asuman los principios del Derecho como límites infranqueables.

En definitiva, la **criminalidad 4.0** ya no es una hipótesis, sino una realidad palpable: los delitos se cometen con velocidad y sofisticación crecientes, en territorios que desafían las categorías jurídico-espaciales tradicionales. Si el sistema procesal no evoluciona con la misma agilidad —no desde la urgencia, pero sí desde la reflexión estratégica— corre el riesgo no solo de volverse ineficaz, sino también de quedar **deslegitimado socialmente**. El desafío está planteado: modernizar sin claudicar; innovar sin desnaturalizar. La responsabilidad recae en nuestra generación jurídica. La inercia ya no es una opción.

6. BIBLIOGRAFÍA

I. Legislación

- Ley de Enjuiciamiento Criminal (LECrim).

- Código Penal (CP).

- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (BOE 29 de abril de 2010).

- Ley 21/2011, de 26 de julio, de dinero electrónico (BOE 27 de julio de 2011).

- Reglamento (UE) 2023/1114, del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (MiCA) (DOUE 9 de junio de 2023).

- Reglamento (UE) 2023/1543, del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre órdenes europeas de producción y conservación de pruebas electrónicas (DOUE 20 de julio de 2023).

- Directiva (UE) 2023/1544, del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre conservación de registros por proveedores de servicios digitales (DOUE 20 de julio de 2023).

- Constitución Española (CE).

II. Jurisprudencia

- Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 326/2019, de 20 de junio.

- Audiencia Provincial de Asturias (Sección 4.ª), Sentencia 37/2015, de 6 de febrero.

- Tribunal Europeo de Derechos Humanos (Gran Sala), caso Big Brother Watch and Others v. United Kingdom, sentencia de 25 de mayo de 2021.

III. Obras doctrinales

- Barona Vilar, S., *Algoritmización del Derecho y de la Justicia*, Tirant lo Blanch, Valencia, 2021.

- Barona Vilar, S., "Dataización de la justicia (Algoritmos, Inteligencia Artificial y Justicia, ¿el comienzo de una gran amistad?)", *Revista Boliviana. de Derecho*, nº 36, 2023.

- Barona Vilar, S., "Justicia con algoritmos e Inteligencia Artificial, ¿acuerpando garantías y derechos procesales o liquidándolos?", *Derechos y Libertades*, núm. 51, 2024.

- Beiro Magán, J. M., "Retos tecnológicos de la Administración de Justicia española para la tercera década del siglo XXI", *Pensamiento Crítico*, n.º 13, 2019.

- Borges Blázquez, R., "El sesgo de la máquina en la toma de decisiones en el proceso penal", *Revista Ius et Scientia*, 6(2), 2020.

- Bueno de Mata, F., "Macrodatos, inteligencia artificial y proceso: luces y sombras", *Revista General de Derecho Procesal*, n.º 51, 2020.

- Calaza López, S., *La prueba como pieza clave para la construcción de la realidad procesal*, Dykinson, Madrid, 2025.

- De Asís Pulido, M., "Derecho al debido proceso e inteligencia artificial", *Revista Derechos Humanos y Educación,* 1(7), 2021.

- Delgado Martín, J., "La prueba digital. Concepto, clases y aportación al proceso", *Diario La Ley*, n.º 6, Sección Ciberderecho, 2017.

- Díez Riaza, S., "Un nuevo mecanismo de la inmersión digital de la justicia: la carpeta justicia y su dependencia de la portabilidad y la interoperabilidad de los datos", en Calaza López, S. (Dir.), Yáñez Vivero, F. (Dir.), Donado Vara, A. (Coord.), Jiménez Muñoz, F.J. (Coord.), *Digitalización del servicio público de justicia e inteligencia artificial judicial*, Dykinson, Madrid, 2024.

- Gascón Inchausti, F., "Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial", en J. Conde Fuentes & G. Serrano Hoyo (Eds.), *La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro*, Atelier, Barcelona, 2019.

- Magro Servet, V., "¿Cómo aportar la prueba digital en el proceso penal?", *Diario La Ley*, n.º 9563, 2021.

- Martín Diz, F., "Inteligencia artificial y proceso: garantías frente a eficiencia en el entorno de los derechos procesales fundamentales", en F. Jiménez Conde & R. Bellido Penadés (Eds.), *Justicia: ¿Garantías vs. eficacia?,* Tirant lo Blanch, Valencia, 2019.

- Planchadell-Gargallo, Andrea, "Breves apuntes sobre digitalización del proceso penal español a la luz del Real Decreto-ley 6/2023", *Rev. Bras. de Direito Processual Penal*, v. 10, n. 2, 2024.

- . I. Solar Cayón, "La codificación predictiva: inteligencia artificial en la averiguación procesal de los hechos relevantes", *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, vol. XI, 2018.

- Solar Cayón, J. I., *La inteligencia artificial jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*, Aranzadi, Navarra, 2019.

IV. Recursos de internet

- Centro de Estudios Jurídicos, Marco de Competencias Digitales para la formación del personal de Justicia, 2023 (disponible en https://www.cej-mjusticia.es; última consulta 8/06/2025).

- Comisión Europea, "Garantizar la justicia en la UE: estrategia europea sobre la formación judicial para 2021-2024", Comunicación COM(2020) 713 final de 2.12.2020, disponible en EUR-Lex (https://eur-lex.europa.eu/ES/legal-content/summary/european-judicial-training-strategy-2021-2024.html; última consulta 8/06/2025).

- Dirección General de Tributos, Resolución V1069-19 (2019) (disponible en https://www.agenciatributaria.es; última consulta 8/06/2025).

- Verizon Data Breach Investigations Report 2025 (disponible en https://www.verizon.com/business/resources/reports/dbir/; última consulta 8/06/2025).