LA INTELIGENCIA ARTIFICIAL COMO HERRAMIENTA PROBATORIA EN EL SISTEMA PENAL:

DESAFÍOS JURÍDICOS Y GARANTÍAS PROCESALES

Publicado por
PUERTO MADERO EDITORIAL
Buenos Aires, Argentina

DERECHO • JUSTICIA • TECNOLOGÍA

La Inteligencia Artificial como Herramienta Probatoria en el Sistema Penal: Desafíos Jurídicos y Garantías Procesales

ISBN: 978-631-6557-82-7

ISBN: 978-631-6557-82-7

PUERTO MADERO EDITORIAL

La Inteligencia Artificial como Herramienta Probatoria en el Sistema Penal: Desafíos Jurídicos y Garantías Procesales

AUTOR:

Julio Cesar Romero Amores
Dayana Elizabeth Quintero Cepeda
Jonathan Eduardo López Poveda
Nathalie Fernanda Gómez Suárez

ISBN: 978-631-6557-82-7

ISBN: 978-631-6557-82-7

PUERTO MADERO EDITORIAL

Primera Edición, junio 2026

La Inteligencia Artificial como Herramienta Probatoria en el Sistema Penal: Desafíos Jurídicos y Garantías Procesales.

ISBN: 978-631-6557-82-7
DOI: https://doi.org/10.55204/PMEA.131

Editado por:
Sello editorial: ©Puerto Madero Editorial Académica
Nº de Alta: 933832

Editorial: © Puerto Madero Editorial Académica
CUIL: 20630333971
Calle 45 N491 entre 4 y 5
Dirección de Publicaciones Científicas
La Plata, Buenos Aires, Argentina
Teléfono: +54 9 221 314 5902
Código Postal: AR1900

Diseño y Producción Editorial: Msc. Santillán Lima, José Luis
Editor: PhD. Verenice Sánchez Castillo

Este libro se sometió a arbitraje bajo el sistema de doble ciego (peer review)

Hecho en Argentina

ISBN: 978-631-6557-82-7

AUTORES

JULIO CESAR ROMERO AMORES
Investigador independiente, Guayaquil, Guayas, Ecuador.
jromero@solutocg.com
https://orcid.org/0009-0000-1969-037X

DAYANA ELIZABETH QUINTERO CEPEDA
Investigador Independiente, Quito, Pichincha, Ecuador.
daitaquinte@live.com
https://orcid.org/0000-0002-4140-1746

JONATHAN EDUARDO LÓPEZ POVEDA
Investigador independiente, Guayaquil, Guayas, Ecuador.
info@lopezygomez.com
https://orcid.org/0009-0009-7058-4279

NATHALIE FERNANDA GÓMEZ SUÁREZ
Investigador independiente, Guayaquil, Guayas, Ecuador.
gerencia@lopezygomez.com
https://orcid.org/0009-0002-2227-7599

ISBN: 978-631-6557-82-7

ÍNDICE

ISBN: 978-631-6557-82-7

ISBN: 978-631-6557-82-7

ISBN: 978-631-6557-82-7

ÍNDICE DE TABLAS

ISBN: 978-631-6557-82-7

ISBN: 978-631-6557-82-7

ÍNDICE DE FIGURAS

ISBN: 978-631-6557-82-7

INTRODUCCIÓN

La inteligencia artificial se ha convertido en una de las transformaciones tecnológicas más relevantes para los sistemas jurídicos contemporáneos. Su capacidad para procesar grandes volúmenes de información, identificar patrones, organizar datos, analizar imágenes, audios, videos, documentos y metadatos, ha generado nuevas posibilidades para la investigación penal y para la gestión de elementos probatorios dentro del proceso. Sin embargo, su incorporación al sistema penal no puede ser entendida únicamente como un avance técnico, sino como un fenómeno jurídico complejo que exige examinar sus límites, riesgos y condiciones de validez frente a las garantías procesales.

El proceso penal se desarrolla dentro de un marco constitucional que limita el ejercicio del poder punitivo del Estado. En el caso ecuatoriano, la Constitución reconoce al Ecuador como un Estado constitucional de derechos y justicia, lo cual exige que toda actuación estatal, incluida la investigación penal y la actividad probatoria, se someta al respeto de los derechos fundamentales, la tutela judicial efectiva, el debido proceso, la defensa, la motivación y la presunción de inocencia (Constitución de la República del Ecuador, 2008, arts. 1, 75 y 76). Esta perspectiva resulta esencial cuando se pretende incorporar herramientas tecnológicas capaces de influir en la obtención, análisis o valoración de información relevante para un proceso penal.

El Código Orgánico Integral Penal establece que su finalidad es “normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso” (Código Orgánico Integral Penal [COIP], 2014, art. 1). Esta disposición permite afirmar que la eficiencia investigativa no puede separarse del respeto a las garantías procesales. En consecuencia, cualquier uso de inteligencia artificial en materia penal debe ser compatible con los principios de legalidad, inocencia, contradicción, igualdad, motivación, imparcialidad, privacidad y objetividad previstos en el propio COIP (2014, art. 5).

La inteligencia artificial puede ser útil para fortalecer la investigación criminal, especialmente cuando permite organizar grandes cantidades de datos, detectar relaciones

ISBN: 978-631-6557-82-7

entre personas, hechos o lugares, analizar contenido digital, apoyar pericias informáticas o identificar posibles manipulaciones audiovisuales. No obstante, esa utilidad no convierte a la inteligencia artificial en una fuente autónoma de verdad. Por el contrario, su empleo dentro del proceso penal debe ser sometido a control jurídico, técnico y judicial, pues sus resultados pueden contener errores, sesgos, limitaciones metodológicas o problemas de explicabilidad.

La doctrina reciente ha advertido que la incorporación de inteligencia artificial en la justicia penal genera una tensión entre eficiencia y garantías. Furingo (2025) señala que la integración de la IA en la justicia penal "genera tensiones entre la eficiencia judicial y el respeto de los derechos y garantías procesales fundamentales" (p. 102). Esta afirmación resulta especialmente relevante para el presente estudio, porque el problema no radica únicamente en determinar si la inteligencia artificial puede ser utilizada dentro del proceso penal, sino en establecer en qué condiciones puede ser admitida, contradicha y valorada sin afectar la legitimidad de la decisión judicial.

En el ámbito probatorio, el COIP reconoce como medios de prueba el documento, el testimonio y la pericia (COIP, 2014, art. 498). Además, admite el contenido digital como medio probatorio conforme a las reglas del propio Código (COIP, 2014, art. 499). Esto permite sostener que los resultados obtenidos o procesados mediante inteligencia artificial no deberían ser tratados como un medio de prueba independiente, sino como elementos que deben ingresar al proceso a través de las categorías probatorias reconocidas por el sistema penal, principalmente mediante prueba documental, contenido digital o prueba pericial.

La cadena de custodia ocupa un lugar central dentro de esta discusión. El COIP dispone que la cadena de custodia se aplica a elementos físicos o contenido digital materia de prueba, con la finalidad de garantizar su autenticidad, identidad, estado original, recolección, manejo, análisis y conservación (COIP, 2014, art. 456). En el caso de herramientas de inteligencia artificial, este requisito adquiere especial importancia, pues no basta con presentar un resultado algorítmico; es necesario demostrar de dónde provienen los datos, cómo fueron obtenidos, qué herramienta fue utilizada, bajo qué parámetros operó,

ISBN: 978-631-6557-82-7

qué margen de error presenta y si el procedimiento puede ser explicado y contradicho por las partes.

La protección de datos personales también constituye un eje esencial del análisis. La Ley Orgánica de Protección de Datos Personales tiene por objeto garantizar el ejercicio del derecho a la protección de datos personales, incluyendo el acceso, decisión y protección sobre dicha información (Ley Orgánica de Protección de Datos Personales [LOPDP], 2021, art. 1). Esta norma resulta especialmente importante cuando la inteligencia artificial procesa datos biométricos, imágenes faciales, registros de ubicación, datos sensibles o información susceptible de identificar directa o indirectamente a una persona. La propia ley define el dato biométrico como aquel dato personal único relacionado con características físicas, fisiológicas o conductuales que permite o confirma la identificación única de una persona, como imágenes faciales o datos dactiloscópicos (LOPDP, 2021, art. 4).

En este sentido, el uso de inteligencia artificial en el sistema penal debe analizarse desde una doble perspectiva. Por un lado, puede contribuir a mejorar la eficacia de la investigación criminal, la gestión de información y el análisis de evidencia digital. Por otro lado, puede generar riesgos graves cuando se utiliza sin transparencia, sin control pericial, sin posibilidad real de contradicción o sin supervisión humana significativa. Estos riesgos son mayores cuando se trata de reconocimiento facial, sistemas predictivos, análisis de perfiles, vigilancia masiva, deepfakes, extracción de metadatos o evaluación automatizada de información vinculada a una persona procesada.

La literatura especializada también ha destacado la existencia de vacíos normativos en Ecuador respecto al uso de sistemas inteligentes dentro del proceso penal. Herrera Mamarandi, Gordón Lucero y Gutierrez Romero (2026) sostienen que la inteligencia artificial puede optimizar procesos investigativos y fortalecer el análisis de evidencia digital, pero también genera desafíos relacionados con transparencia algorítmica, debido proceso, autenticidad de la prueba tecnológica, sesgo algorítmico y protección de derechos fundamentales (p. 824). Esta observación permite justificar la necesidad de una revisión bibliográfica orientada no solo a describir el fenómeno, sino también a proponer criterios jurídicos de control.

ISBN: 978-631-6557-82-7

El presente libro parte de una premisa central: la inteligencia artificial puede operar como herramienta probatoria auxiliar dentro del sistema penal, pero no debe sustituir la función del juez, la actividad pericial ni el derecho de las partes a conocer, cuestionar y refutar la prueba. Una condena penal no puede apoyarse acríticamente en resultados algorítmicos opacos, no verificables o no sometidos a contradicción. La valoración judicial debe permanecer sometida a la sana crítica, a la motivación reforzada y al estándar de duda razonable.

Desde esta perspectiva, esta obra desarrolla una revisión bibliográfica sobre la inteligencia artificial como herramienta probatoria en el sistema penal, con especial atención a sus desafíos jurídicos y garantías procesales. El análisis se estructura en cinco capítulos. El primer capítulo examina los fundamentos de la prueba penal y las garantías del debido proceso. El segundo capítulo aborda la inteligencia artificial y su impacto en la transformación del sistema penal. El tercer capítulo analiza la naturaleza de la inteligencia artificial como herramienta probatoria. El cuarto capítulo estudia la admisibilidad, fiabilidad y desafíos jurídicos de la prueba asistida por IA. Finalmente, el quinto capítulo desarrolla las garantías procesales, la valoración judicial y una propuesta de protocolo para el uso de inteligencia artificial probatoria.

Metodológicamente, el libro se desarrolla como una investigación de revisión bibliográfica, documental y jurídico-doctrinal. Se examinan normas ecuatorianas, doctrina académica, artículos científicos y documentos especializados sobre inteligencia artificial, prueba penal, prueba digital, protección de datos personales, debido proceso y garantías procesales. Esta revisión permite identificar criterios comunes, vacíos normativos y estándares mínimos para que el uso de inteligencia artificial en el proceso penal sea compatible con el Estado constitucional de derechos y justicia.

CAPÍTULO I.

Fundamentos de la prueba penal y garantías del debido proceso

ISBN: 978-631-6557-82-7

CAPÍTULO I.

1 Fundamentos de la prueba penal y garantías del debido proceso

La prueba penal constituye uno de los pilares fundamentales del proceso penal contemporáneo. A través de ella se reconstruyen los hechos jurídicamente relevantes, se verifica la existencia de una infracción y se determina, dentro de los límites constitucionales y legales, la posible responsabilidad de la persona procesada. En este sentido, la prueba no puede ser entendida como una simple acumulación de información, indicios o elementos técnicos, sino como una actividad procesal sometida a reglas de legalidad, contradicción, inmediación, defensa, igualdad de armas, motivación y valoración racional.

En un Estado constitucional de derechos y justicia, la actividad probatoria no se justifica únicamente por su capacidad para descubrir hechos, sino por la forma en que dichos hechos son obtenidos, incorporados, discutidos y valorados dentro del proceso. La búsqueda de la verdad penal no puede realizarse a cualquier costo. Por ello, la prueba debe producirse conforme a garantías que impidan arbitrariedades, abusos investigativos, afectaciones a la dignidad humana o decisiones condenatorias basadas en información ilícita, incompleta, no contradicha o técnicamente deficiente.

La doctrina procesal contemporánea ha destacado que el problema de la prueba no se reduce a la existencia de medios probatorios, sino a la justificación racional de las decisiones judiciales sobre los hechos. Taruffo (2011) sostiene que los problemas relativos a la prueba y a la justificación de las decisiones sobre los hechos tienen una importancia teórica y práctica central para el derecho. Esta idea permite comprender que la prueba penal no es un simple mecanismo instrumental, sino una garantía de racionalidad frente al poder punitivo del Estado.

Ferrer Beltrán (2007) también ha insistido en que el análisis de la prueba debe orientarse a determinar bajo qué condiciones puede considerarse racionalmente probada una hipótesis fáctica. Esta perspectiva resulta especialmente relevante para el proceso penal,

ISBN: 978-631-6557-82-7

donde no basta con formular una acusación verosímil, sino que se exige una construcción probatoria suficiente, legal, contradictoria y motivada, capaz de superar el estándar de duda razonable.

El presente capítulo desarrolla los fundamentos de la prueba penal y las garantías del debido proceso como base indispensable para analizar, en los capítulos posteriores, el uso de la inteligencia artificial como herramienta probatoria en el sistema penal. Antes de examinar la admisibilidad de resultados algorítmicos, la prueba digital, los sistemas biométricos, la detección de deepfakes o los riesgos de la opacidad tecnológica, es necesario establecer los principios jurídicos que regulan toda actividad probatoria penal.

Desde esta perspectiva, la inteligencia artificial no puede ser incorporada al proceso penal como una herramienta neutral, automática o infalible. Cualquier tecnología que participe en la obtención, procesamiento, clasificación o análisis de información probatoria debe someterse a los mismos estándares que rigen la prueba penal tradicional, e incluso a controles reforzados cuando su funcionamiento resulte opaco, técnicamente complejo o difícilmente comprensible para las partes procesales.

Figura 1 Fundamentos de la prueba penal y garantías del debido proceso

ISBN: 978-631-6557-82-7

1.1 La prueba penal como fundamento de la decisión judicial

La decisión judicial penal debe construirse sobre la base de hechos probados y no sobre intuiciones, conjeturas, prejuicios, presunciones infundadas o resultados técnicos no verificados. La prueba es el mecanismo jurídico que permite transformar una afirmación fáctica en un elemento susceptible de valoración judicial. En materia penal, esta función adquiere una relevancia superior, porque la decisión puede afectar derechos fundamentales como la libertad personal, la honra, la intimidad, el patrimonio, la seguridad jurídica y el proyecto de vida de la persona procesada.

El Código Orgánico Integral Penal establece que la prueba tiene como finalidad llevar a la o al juzgador al convencimiento sobre los hechos y circunstancias materia de la infracción, así como sobre la responsabilidad de la persona procesada (COIP, 2014, art. 453). Esta disposición permite identificar tres elementos esenciales: primero, la prueba debe referirse a hechos; segundo, esos hechos deben guardar relación con la infracción penal; y tercero, la actividad probatoria debe permitir establecer o descartar la responsabilidad penal de la persona procesada.

Por tanto, la prueba no cumple una función meramente formal. Su importancia radica en que condiciona la legitimidad de la sentencia. Una resolución condenatoria que no se apoya en prueba legalmente practicada, suficientemente debatida y racionalmente valorada carece de fundamento jurídico. En cambio, una decisión absolutoria puede derivarse de la insuficiencia probatoria, de la existencia de duda razonable o de la exclusión de elementos obtenidos con vulneración de derechos.

La prueba penal cumple, además, una función de límite frente al poder punitivo. El Estado no puede sancionar sobre la base de sospechas, perfiles de riesgo, intuiciones policiales, inferencias estadísticas o conclusiones tecnológicas no verificadas. En el proceso penal, la persona procesada no debe demostrar su inocencia; corresponde a la acusación construir una hipótesis fáctica suficientemente acreditada mediante prueba lícita, pertinente, útil, conducente y contradicha.

ISBN: 978-631-6557-82-7

Gascón Abellán (2010) explica que el conocimiento judicial de los hechos posee una naturaleza institucionalizada, porque no se produce de manera libre o espontánea, sino dentro de reglas procesales que condicionan la forma en que se obtiene y valora la información. Esta idea es fundamental para el proceso penal: el juez no accede a los hechos de manera directa, sino a través de medios de prueba sometidos a reglas jurídicas. Por ello, la verdad procesal no depende únicamente de la información disponible, sino de la forma legítima en que dicha información ingresa al juicio.

En el sistema penal ecuatoriano, la prueba debe ser entendida dentro de un proceso oral, adversarial y contradictorio. Esto significa que los elementos de convicción obtenidos durante la investigación no adquieren automáticamente la calidad de prueba plena. De acuerdo con el COIP, las investigaciones y pericias practicadas durante la investigación alcanzan valor probatorio una vez que son presentadas, incorporadas y valoradas en la audiencia oral de juicio (COIP, 2014, art. 454). Esta regla impide que el juicio penal se convierta en una simple ratificación de actuaciones investigativas previas.

La prueba penal, en consecuencia, es una garantía para todas las partes. Para la Fiscalía, permite sustentar una acusación. Para la víctima, permite acceder al esclarecimiento de los hechos y a la reparación integral. Para la persona procesada, constituye un límite frente al poder punitivo, porque impide que sea condenada sin prueba suficiente, legal y contradicha. Para el juez, representa la base racional de su decisión.

Esta comprensión resulta especialmente relevante frente al uso de inteligencia artificial. Un resultado algorítmico, un informe generado con apoyo tecnológico o un análisis automatizado de datos no pueden sustituir la actividad probatoria. Su eventual utilidad dependerá de que dicho resultado sea incorporado al proceso mediante un medio de prueba reconocido, pueda ser explicado por un perito, sea sometido a contradicción y sea valorado conforme a criterios jurídicos y técnicos verificables.

ISBN: 978-631-6557-82-7

Tabla 1 Funciones de la prueba penal en el proceso

Función de la prueba	Contenido jurídico	Relevancia frente a la IA probatoria
Función cognoscitiva	Permite reconstruir hechos relevantes para el proceso	La IA puede apoyar el análisis, pero no sustituye la comprobación jurídica del hecho
Función garantista	Limita el poder punitivo del Estado	Impide que resultados algorítmicos se usen sin control legal y contradictorio
Función contradictoria	Permite que las partes discutan la información probatoria	Exige acceso a metodología, datos, parámetros y margen de error
Función justificativa	Sustenta la motivación de la sentencia	Obliga al juez a explicar por qué otorga valor al resultado técnico
Función decisoria	Sirve de base para condenar o absolver	La IA no puede convertirse en fundamento exclusivo de responsabilidad penal

La tabla evidencia que la prueba penal cumple varias funciones simultáneas. No solo sirve para conocer hechos, sino también para limitar el poder estatal, garantizar contradicción y justificar racionalmente la sentencia. Esta estructura funcional será determinante al analizar, en los capítulos siguientes, los límites del uso de inteligencia artificial como herramienta probatoria.

1.2 Finalidad de la prueba y búsqueda de la verdad procesal

La finalidad de la prueba penal se relaciona con la búsqueda de una verdad procesal construida conforme a reglas jurídicas. Esta verdad no puede confundirse con una verdad absoluta, matemática o puramente tecnológica. En el proceso penal, la verdad se alcanza

ISBN: 978-631-6557-82-7

mediante una actividad regulada por normas constitucionales y procesales, en la que las partes presentan sus teorías, aportan elementos de prueba, contradicen las afirmaciones contrarias y permiten al juez formar una convicción racional.

El COIP establece que la prueba busca llevar al juzgador al convencimiento sobre los hechos, las circunstancias de la infracción y la responsabilidad penal de la persona procesada (COIP, 2014, art. 453). Sin embargo, ese convencimiento no puede formarse de cualquier manera. Debe derivarse de pruebas producidas en el proceso, respetando los principios de oportunidad, inmediación, contradicción, libertad probatoria, pertinencia, exclusión e igualdad de oportunidades para la prueba (COIP, 2014, art. 454).

La verdad procesal, por tanto, no depende únicamente de la cantidad de información disponible, sino de la calidad jurídica de su incorporación al proceso. En materia penal, no toda información útil para conocer un hecho puede ser utilizada como prueba. Existen límites relacionados con la dignidad humana, la intimidad, la legalidad de la obtención, la cadena de custodia, la pertinencia, la contradicción y el derecho a la defensa. La información obtenida con vulneración de derechos, aunque pueda parecer esclarecedora desde el punto de vista fáctico, carece de legitimidad procesal.

Taruffo (2011) sostiene que el proceso judicial debe aspirar a una determinación racional de los hechos, evitando tanto el escepticismo absoluto como la idea ingenua de que la verdad se alcanza de forma automática. En el proceso penal, esta afirmación permite ubicar la prueba como un instrumento racional, pero limitado. La decisión sobre los hechos no es una certeza metafísica; es una conclusión justificada a partir de medios de prueba legalmente incorporados y valorados bajo criterios racionales.

González Lagier (2005) destaca la importancia de la inferencia probatoria en la construcción judicial de los hechos. Esta idea resulta útil para comprender que la prueba no habla por sí sola. El juez debe razonar a partir de indicios, testimonios, documentos, pericias y otros elementos, conectándolos mediante inferencias justificadas. Por ello, la valoración de la prueba exige argumentación, no simple acumulación de datos.

ISBN: 978-631-6557-82-7

Esta idea es esencial para el análisis posterior de la inteligencia artificial. Los sistemas inteligentes pueden procesar grandes volúmenes de datos, detectar patrones o generar predicciones; sin embargo, esa capacidad técnica no equivale a verdad procesal. La verdad penal no se produce por acumulación de datos ni por autoridad tecnológica, sino por la incorporación legítima de información al juicio y por su valoración racional en condiciones de contradicción.

En este sentido, el proceso penal debe evitar dos extremos. El primero consiste en rechazar toda innovación tecnológica por temor a sus riesgos. El segundo consiste en aceptar acríticamente cualquier resultado producido por herramientas digitales bajo la falsa creencia de que la tecnología es objetiva. Ambos extremos son problemáticos. La tecnología puede contribuir a la investigación penal, pero solo será jurídicamente válida cuando respete los estándares de legalidad, transparencia, control pericial y contradicción.

Por ello, la finalidad de la prueba no debe ser confundida con la eficiencia investigativa. Un sistema penal puede ser más rápido o tecnificado, pero si sacrifica garantías, pierde legitimidad. En materia penal, la eficiencia solo es aceptable si se encuentra subordinada al debido proceso.

Tabla 2 Verdad procesal y límites de la prueba penal

Aspecto	Alcance jurídico	Riesgo frente a herramientas de IA
Verdad procesal	Reconstrucción de hechos mediante reglas jurídicas	Confundir resultado algorítmico con verdad objetiva
Legalidad	Obtención conforme a Constitución y ley	Usar datos obtenidos ilícitamente
Contradicción	Posibilidad de discutir la prueba	Impedir a la defensa conocer el método tecnológico
Racionalidad	Valoración mediante inferencias justificadas	Atribuir valor automático a porcentajes o predicciones

ISBN: 978-631-6557-82-7

Motivación	Explicación judicial de la decisión sobre los hechos	Aceptar conclusiones técnicas sin análisis propio

La tabla permite observar que la verdad procesal es una construcción jurídica y racional. Su legitimidad no depende solo de la información disponible, sino del respeto a las reglas que permiten convertir esa información en prueba válida.

1.3 Presunción de inocencia, carga probatoria y estándar de prueba

La presunción de inocencia constituye una garantía estructural del proceso penal. No se trata de una simple fórmula declarativa, sino de una regla de trato, una regla probatoria y una regla de juicio. Como regla de trato, exige que la persona procesada sea considerada inocente mientras no exista sentencia condenatoria ejecutoriada. Como regla probatoria, impone a la acusación la carga de demostrar la responsabilidad penal. Como regla de juicio, obliga a absolver cuando persista duda razonable.

El COIP recoge expresamente este principio al establecer que toda persona mantiene su estatus jurídico de inocencia y debe ser tratada como tal mientras no se ejecutoríe una sentencia que determine lo contrario (COIP, 2014, art. 5, núm. 4). Asimismo, reconoce el principio de duda a favor del reo, según el cual el juzgador, para dictar sentencia condenatoria, debe tener convencimiento de la culpabilidad penal de la persona procesada más allá de toda duda razonable (COIP, 2014, art. 5, núm. 3).

Estos principios definen el estándar de prueba penal. A diferencia de otros ámbitos jurídicos, en el proceso penal no basta con una mera probabilidad, sospecha o indicio débil. La condena exige un grado elevado de certeza racional, construido a partir de prueba legalmente obtenida, presentada en juicio, sometida a contradicción y valorada de manera motivada. Cuando la prueba no alcanza ese estándar, la respuesta constitucionalmente adecuada es la ratificación de inocencia.

Ferrer Beltrán (2007) explica que el problema de la prueba no consiste únicamente en saber qué elementos fueron presentados, sino en determinar cuándo una hipótesis fáctica puede considerarse racionalmente probada. Esta reflexión resulta especialmente importante para el proceso penal, donde la hipótesis acusatoria debe superar un estándar exigente. La

ISBN: 978-631-6557-82-7

existencia de indicios, coincidencias o resultados automatizados puede orientar una investigación, pero no necesariamente justificar una condena.

La carga probatoria recae principalmente sobre quien acusa. La persona procesada no está obligada a demostrar su inocencia, pues esta se presume constitucional y legalmente. De ahí que cualquier sistema probatorio que desplace de forma directa o indirecta la carga de la prueba hacia la defensa resulte incompatible con el debido proceso. Esto podría ocurrir, por ejemplo, si se presenta un resultado algorítmico como verdad técnica indiscutible y se exige a la defensa demostrar que el sistema falló, sin haber tenido acceso suficiente a la metodología, los datos o los parámetros utilizados.

La presunción de inocencia también impone límites al uso de tecnologías predictivas. Un sistema de inteligencia artificial que clasifica a una persona como riesgosa, sospechosa o probable autora de una infracción no puede ser utilizado como fundamento autónomo de responsabilidad penal. La responsabilidad penal debe basarse en hechos probados, no en perfiles, probabilidades estadísticas o asociaciones generadas por patrones históricos.

La jurisprudencia interamericana ha insistido en la centralidad de las garantías judiciales dentro del proceso penal. En el caso Barreto Leiva vs. Venezuela, la Corte Interamericana de Derechos Humanos analizó garantías vinculadas a la comunicación previa de la acusación, el tiempo y medios adecuados para la defensa, la asistencia de defensor y la posibilidad de interrogar testigos y peritos (Corte IDH, 2009). Estos estándares son relevantes para la IA probatoria porque la defensa solo puede ser real si conoce y puede cuestionar los elementos utilizados en su contra.

Furingo (2025) advierte que la integración de la inteligencia artificial en la justicia penal genera tensiones entre la eficiencia judicial y el respeto a las garantías procesales, especialmente cuando existen sesgos u opacidad algorítmica que pueden afectar la tutela judicial efectiva, el derecho de defensa o la presunción de inocencia. Esta advertencia permite comprender que la presunción de inocencia no solo se vulnera mediante una

ISBN: 978-631-6557-82-7

condena sin prueba, sino también mediante prácticas tecnológicas que atribuyen peligrosidad o culpabilidad a partir de patrones no transparentes.

En consecuencia, la presunción de inocencia debe operar como límite frente a cualquier forma de automatización probatoria. La inteligencia artificial puede auxiliar la investigación, pero no puede invertir la carga de la prueba, sustituir la valoración judicial ni reducir el estándar probatorio exigido para una condena penal.

Tabla 3 Presunción de inocencia y prueba asistida por IA

Dimensión de la presunción de inocencia	Contenido	Riesgo frente a IA
Regla de trato	La persona debe ser tratada como inocente durante el proceso	Etiquetamiento como sospechosa por perfil algorítmico
Regla probatoria	La acusación debe probar la responsabilidad penal	Trasladar a la defensa la carga de refutar un sistema opaco
Regla de juicio	La duda razonable obliga a absolver	Condenar con base en probabilidades o coincidencias no corroboradas
Garantía de defensa	La persona debe poder controvertir la prueba	Imposibilidad de acceder a metodología, datos o margen de error
Límite al poder punitivo	El Estado debe justificar racionalmente la acusación	Uso acrítico de predicciones o análisis automatizados

ISBN: 978-631-6557-82-7

Esta tabla evidencia que la presunción de inocencia debe proyectarse sobre todo el ciclo probatorio. Si la IA interviene en la investigación, admisión o valoración de la prueba, su uso debe ser controlado para evitar que una inferencia tecnológica debilite el estándar penal de prueba.

1.4 Principios rectores de la actividad probatoria penal

La actividad probatoria penal se encuentra regida por principios que garantizan la legitimidad del proceso. Estos principios no son formalidades accesorias, sino condiciones necesarias para que la prueba pueda ser admitida, practicada y valorada válidamente.

El COIP establece que el anuncio y la práctica de la prueba se rigen por los principios de oportunidad, inmediación, contradicción, libertad probatoria, pertinencia, exclusión e igualdad de oportunidades para la prueba (COIP, 2014, art. 454). Cada uno de estos principios cumple una función específica dentro del sistema probatorio y adquiere particular importancia frente al uso de herramientas tecnológicas.

El principio de oportunidad exige que la prueba sea anunciada en la etapa procesal correspondiente y practicada, como regla general, en la audiencia de juicio. Esta regla impide sorpresas procesales y garantiza que las partes conozcan previamente los elementos que serán debatidos. En materia de prueba tecnológica o asistida por inteligencia artificial, la oportunidad probatoria adquiere especial relevancia, porque la defensa necesita tiempo suficiente para analizar informes técnicos, solicitar aclaraciones, preparar contrainterrogatorios o requerir pericias independientes.

El principio de inmediación exige la presencia del juzgador y de las partes en la práctica de la prueba. Su importancia radica en que el juez debe percibir directamente la producción probatoria y no limitarse a revisar documentos o informes elaborados fuera del debate oral. En el caso de pericias tecnológicas, la inmediación permite que el perito explique su metodología, responda preguntas y aclare las limitaciones del análisis realizado.

El principio de contradicción reconoce el derecho de las partes a conocer oportunamente y controvertir las pruebas. Esta garantía es esencial en todo proceso penal,

ISBN: 978-631-6557-82-7

pero se vuelve aún más importante cuando la prueba se basa en procedimientos técnicos complejos. Si una parte no puede comprender, examinar o cuestionar el método utilizado para generar un resultado, la contradicción se convierte en una formalidad vacía.

El principio de libertad probatoria permite demostrar los hechos y circunstancias pertinentes por cualquier medio que no sea contrario a la Constitución, los instrumentos internacionales de derechos humanos ni la ley (COIP, 2014, art. 454). Esta regla abre la puerta a la incorporación de nuevos medios tecnológicos, incluida la evidencia digital o los resultados producidos con apoyo de inteligencia artificial. Sin embargo, la libertad probatoria no significa ausencia de límites. Todo medio probatorio debe respetar derechos fundamentales y cumplir criterios de pertinencia, legalidad y fiabilidad.

El principio de pertinencia exige que las pruebas se refieran directa o indirectamente a los hechos o circunstancias relativos a la infracción, sus consecuencias o la responsabilidad penal de la persona procesada (COIP, 2014, art. 454). Esto impide que se incorporen datos irrelevantes, excesivos o invasivos. En el contexto de inteligencia artificial, la pertinencia resulta clave para evitar el uso indiscriminado de grandes bases de datos, perfiles o información personal que no guarde relación real con el objeto del proceso.

El principio de exclusión determina que toda prueba o elemento de convicción obtenido con violación de derechos establecidos en la Constitución, los instrumentos internacionales de derechos humanos o la ley carece de eficacia probatoria y debe excluirse de la actuación procesal (COIP, 2014, art. 454). Este principio constituye una garantía frente a abusos investigativos y frente a la tentación de justificar medios ilícitos por sus resultados aparentemente útiles.

Finalmente, la igualdad de oportunidades para la prueba exige garantizar igualdad material y formal entre los intervinientes. En procesos donde se utilicen herramientas de inteligencia artificial, esta igualdad puede verse afectada si solo una de las partes tiene acceso al sistema, a los datos, al software, a los parámetros o a los conocimientos técnicos necesarios para discutir el resultado.

ISBN: 978-631-6557-82-7

Tabla 4 Principios probatorios y exigencias frente a IA

Principio probatorio	Exigencia general	Exigencia específica frente a IA
Oportunidad	Anuncio y práctica en el momento procesal correspondiente	Entrega anticipada de informes técnicos y metodología
Inmediación	Presencia judicial en la práctica probatoria	Comparecencia del perito que explique la herramienta
Contradicción	Posibilidad de refutar la prueba	Acceso a datos, parámetros, margen de error y limitaciones
Libertad probatoria	Uso de medios no prohibidos por la ley	Admisión de evidencia digital siempre que respete derechos
Pertinencia	Relación con los hechos del proceso	Evitar análisis masivo de datos irrelevantes
Exclusión	Ineficacia de prueba obtenida con vulneración de derechos	Excluir resultados producidos con datos ilícitos
Igualdad de oportunidades	Equilibrio entre las partes	Permitir pericia independiente o revisión técnica de la defensa

La tabla permite observar que los principios tradicionales de la prueba penal continúan siendo aplicables frente a la inteligencia artificial. La tecnología no crea un

ISBN: 978-631-6557-82-7

espacio probatorio autónomo ni exento de garantías; por el contrario, exige aplicar estos principios con mayor rigor.

1.5 Legalidad, pertinencia, utilidad y conducencia de la prueba

La admisibilidad de la prueba penal exige que los elementos ofrecidos cumplan condiciones mínimas de legalidad, pertinencia, utilidad y conducencia. Estos criterios permiten filtrar la información que ingresa al proceso y evitar que el debate judicial se contamine con elementos ilícitos, irrelevantes, innecesarios o incapaces de demostrar los hechos controvertidos.

La legalidad implica que la prueba debe haber sido obtenida, conservada, presentada y practicada conforme a la Constitución y la ley. En materia penal, este requisito tiene una dimensión especialmente estricta, porque el Estado cuenta con amplias facultades investigativas que pueden afectar derechos fundamentales. Registros, allanamientos, incautaciones, interceptaciones, análisis de dispositivos, extracción de datos o tratamientos de información personal deben realizarse con base normativa suficiente y bajo control judicial cuando corresponda.

La pertinencia exige una relación lógica entre la prueba y los hechos materia del proceso. Una prueba es pertinente cuando contribuye a esclarecer la existencia de la infracción, sus circunstancias, sus consecuencias o la posible responsabilidad de la persona procesada. Esta exigencia impide que el proceso penal se convierta en una exploración indiscriminada de la vida privada de las personas.

La utilidad supone que la prueba aporte algo relevante al debate. Un elemento puede ser pertinente en sentido amplio, pero inútil si resulta repetitivo, innecesario o incapaz de ofrecer información significativa. En el ámbito tecnológico, este criterio permite cuestionar la incorporación de informes extensos, bases de datos masivas o resultados automatizados que no agregan valor real a la determinación de los hechos.

La conducencia se refiere a la idoneidad del medio probatorio para demostrar aquello que se pretende acreditar. No todo medio sirve para probar cualquier hecho. Por ejemplo,

ISBN: 978-631-6557-82-7

un análisis algorítmico de patrones puede servir como orientación investigativa, pero no necesariamente como prueba suficiente de responsabilidad penal. De igual forma, un reconocimiento facial puede sugerir una coincidencia, pero requiere validación técnica y corroboración con otros elementos.

Gascón Abellán (2010) advierte que el conocimiento judicial de los hechos se produce dentro de reglas institucionales que condicionan el modo de probar. Esta afirmación permite comprender que la admisibilidad de la prueba no es una barrera arbitraria, sino una condición de racionalidad y legitimidad. La prueba debe ingresar al proceso mediante reglas que garanticen su control y eviten decisiones basadas en información no confiable.

Estos criterios son esenciales para el análisis de la prueba asistida por inteligencia artificial. La IA puede producir resultados aparentemente sofisticados, pero ello no garantiza su admisibilidad. Un resultado algorítmico puede ser inadmisible si se obtuvo mediante datos ilícitos, si carece de relación con los hechos, si no aporta información útil o si el sistema utilizado no es idóneo para demostrar aquello que se pretende probar.

En consecuencia, la legalidad, pertinencia, utilidad y conducencia funcionan como barreras de racionalidad probatoria. Su finalidad no es impedir la innovación, sino asegurar que la tecnología ingrese al proceso penal únicamente cuando sea jurídicamente legítima, procesalmente necesaria y técnicamente adecuada.

Tabla 5 Criterios de admisibilidad aplicados a prueba tecnológica

Criterio	Pregunta de control	Aplicación en IA probatoria
Legalidad	¿La información fue obtenida conforme a la ley?	Verificar autorización, origen lícito de datos y respeto a derechos

ISBN: 978-631-6557-82-7

Pertinencia	¿La prueba se relaciona con los hechos investigados?	Evitar análisis de datos ajenos al objeto procesal
Utilidad	¿La prueba aporta información relevante?	Descartar informes automatizados redundantes o innecesarios
Conducencia	¿El medio es idóneo para probar lo alegado?	Diferenciar coincidencia técnica de prueba suficiente
Controlabilidad	¿Puede ser revisada y discutida por las partes?	Exigir metodología, pericia, trazabilidad y margen de error

La tabla muestra que la admisibilidad de la prueba tecnológica exige algo más que utilidad investigativa. El elemento debe ser jurídicamente legítimo y técnicamente controlable, especialmente cuando puede influir en la responsabilidad penal de una persona.

1.6 Contradicción, inmediación, oralidad y derecho a la defensa

La contradicción, la inmediación, la oralidad y el derecho a la defensa constituyen garantías esenciales de la prueba penal. Estas garantías aseguran que la prueba no sea simplemente presentada ante el juez, sino debatida públicamente por las partes en condiciones de igualdad.

La Constitución reconoce que en todo proceso en el que se determinen derechos y obligaciones debe garantizarse el debido proceso, incluido el derecho a la defensa. Entre sus garantías se encuentra que nadie puede ser privado del derecho a la defensa en ninguna etapa o grado del procedimiento, así como el derecho a ser escuchado en el momento oportuno y en igualdad de condiciones (Constitución de la República del Ecuador, 2008, art. 76).

ISBN: 978-631-6557-82-7

El COIP desarrolla estos principios en materia penal. La contradicción exige que los sujetos procesales puedan presentar argumentos, replicar los argumentos de la contraparte, presentar pruebas y contradecir las que se presenten en su contra (COIP, 2014, art. 5, núm. 13). Esta garantía no se satisface únicamente permitiendo una oposición formal. Para que exista contradicción real, las partes deben contar con información suficiente para comprender el contenido, origen, metodología y alcance de la prueba.

La inmediación exige la presencia del juzgador en la práctica de la prueba. En el juicio penal, este principio permite que el juez observe directamente la producción probatoria, escuche a testigos y peritos, valore sus explicaciones y aprecie las respuestas dadas durante el interrogatorio y contrainterrogatorio. En el caso de la prueba pericial, la inmediación permite que el informe no sea valorado como documento aislado, sino como resultado de una explicación técnica sometida al debate oral.

La oralidad, por su parte, estructura el proceso penal alrededor de audiencias. Según el COIP, el proceso se desarrolla mediante el sistema oral, las decisiones se toman en audiencia y se utilizan medios técnicos para dejar constancia de las actuaciones procesales (COIP, 2014, art. 5, núm. 11). Esta característica fortalece la transparencia y permite que las partes ejerzan sus derechos de manera directa ante el juzgador.

El derecho a la defensa también comprende el acceso a asistencia técnica. El COIP establece que la defensa de toda persona estará a cargo de una abogada o abogado de su elección, sin perjuicio del derecho a la defensa material o a la asignación de un defensor público (COIP, 2014, art. 452). Esta garantía es particularmente importante en procesos donde existan pruebas tecnológicas complejas, porque la defensa jurídica puede requerir apoyo técnico especializado para controvertir adecuadamente los resultados.

La Corte Interamericana de Derechos Humanos, en el caso Ruano Torres y otros vs. El Salvador, desarrolló estándares relevantes sobre defensa técnica y garantías en el proceso penal, destacando la importancia de que el Estado asegure condiciones reales para la defensa de la persona acusada (Corte IDH, 2015). Esta perspectiva es aplicable al uso de inteligencia

ISBN: 978-631-6557-82-7

artificial, porque una defensa meramente formal resulta insuficiente cuando la acusación se apoya en herramientas técnicas complejas.

Cuando se utiliza inteligencia artificial en la actividad probatoria, la contradicción y la defensa enfrentan nuevos desafíos. No basta con entregar a la defensa una conclusión generada por un sistema automatizado. Es necesario permitir el conocimiento suficiente del procedimiento utilizado, los datos procesados, los criterios de análisis, la tasa de error, las limitaciones del sistema y la intervención humana realizada. De lo contrario, la defensa quedaría reducida a cuestionar un resultado que no puede comprender ni verificar.

Por ello, en materia de IA probatoria, el derecho a la defensa debe interpretarse de manera reforzada. La defensa no solo debe conocer el resultado, sino también las condiciones técnicas que permitieron producirlo. Sin este acceso, la contradicción se debilita y el proceso penal corre el riesgo de aceptar como prueba aquello que en realidad no ha sido debidamente controlado.

1.7 Sana crítica, valoración racional y exclusión de la prueba ilícita

La valoración de la prueba constituye el momento en que el juez determina el peso, credibilidad y suficiencia de los elementos probatorios incorporados al proceso. En materia penal, esta valoración debe ser racional, motivada y compatible con el estándar de prueba exigido para una condena. El juez no puede valorar arbitrariamente la prueba ni atribuirle eficacia por simple intuición, autoridad institucional, complejidad técnica o apariencia científica.

El COIP establece que la valoración de la prueba debe considerar su legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales (COIP, 2014, art. 457). Esta disposición es especialmente relevante para el tema de este libro, porque permite vincular la prueba tecnológica y la prueba asistida por inteligencia artificial con criterios de fiabilidad, trazabilidad y aceptación científica.

ISBN: 978-631-6557-82-7

La legalidad exige verificar que el elemento probatorio no haya sido obtenido con vulneración de derechos. La autenticidad supone establecer que el elemento presentado corresponde efectivamente a aquello que se afirma. La cadena de custodia permite acreditar la identidad, estado original, recolección, manejo, análisis y conservación del elemento físico o contenido digital. La aceptación científica y técnica exige que los informes periciales se fundamenten en principios reconocidos, verificables y actualizados.

Ferrer Beltrán (2007) plantea que la valoración racional de la prueba exige condiciones que permitan controlar si una hipótesis fáctica puede considerarse probada. Esto implica que la decisión judicial sobre los hechos debe ser argumentable, revisable y no una simple expresión de convicción subjetiva. En el proceso penal, la sana crítica no autoriza arbitrariedad; exige razonamiento probatorio explícito.

González Lagier (2005) resalta la importancia de la inferencia probatoria, es decir, el paso racional desde los elementos de prueba hacia las conclusiones sobre los hechos. Esta idea permite advertir que un dato, un indicio o un resultado técnico no determinan por sí solos la verdad de una hipótesis penal. El juez debe justificar por qué esos elementos permiten aceptar o rechazar una determinada reconstrucción de los hechos.

La exclusión de la prueba ilícita cumple una función garantista. El COIP dispone que toda prueba o elemento de convicción obtenido con violación de derechos constitucionales, instrumentos internacionales de derechos humanos o la ley carece de eficacia probatoria y debe excluirse del proceso (COIP, 2014, art. 454). Esta regla impide que el Estado obtenga ventajas procesales mediante actuaciones contrarias a derechos fundamentales.

En el contexto de la inteligencia artificial, la exclusión probatoria puede adquirir nuevas dimensiones. Por ejemplo, podría discutirse la exclusión de resultados obtenidos mediante tratamiento ilícito de datos personales, uso de sistemas no autorizados, análisis de información recolectada sin orden judicial, manipulación de evidencia digital o falta de cadena de custodia. También podría cuestionarse la valoración de informes algorítmicos que no sean explicables, reproducibles o técnicamente verificables.

ISBN: 978-631-6557-82-7

La Corte Constitucional del Ecuador, en la sentencia No. 1158-17-EP/21, sistematizó el alcance de la garantía de motivación y destacó la necesidad de fundamentación normativa suficiente y fundamentación fáctica suficiente (Corte Constitucional del Ecuador, 2021). Este criterio resulta particularmente importante para la prueba asistida por IA, porque una sentencia que valore resultados algorítmicos debe explicar no solo la norma aplicable, sino también las razones fácticas y técnicas por las cuales se otorga valor al resultado.

La valoración racional exige que el juez no confunda complejidad técnica con confiabilidad. Un informe elaborado con apoyo de inteligencia artificial puede parecer preciso por su lenguaje técnico, gráficos, porcentajes o modelos estadísticos, pero ello no garantiza que sea jurídicamente suficiente. La prueba tecnológica debe ser examinada con el mismo rigor que cualquier otra prueba, e incluso con mayor cautela cuando su funcionamiento no sea plenamente transparente.

Por tanto, la sana crítica y la valoración racional obligan al juez a explicar por qué otorga valor a una prueba, cómo la relaciona con los demás elementos del proceso y de qué manera supera las dudas planteadas por la defensa. En casos de prueba asistida por IA, la motivación judicial debe incluir un análisis sobre la fiabilidad técnica del sistema, la metodología utilizada, la cadena de custodia, el margen de error, la posibilidad de contradicción y la existencia de corroboración externa.

Tabla 6 Valoración racional de la prueba y control de resultados tecnológicos

Elemento de valoración	Pregunta judicial	Aplicación frente a IA
Legalidad	¿La prueba fue obtenida conforme a derecho?	Verificar origen lícito de datos y autorización correspondiente

ISBN: 978-631-6557-82-7

Autenticidad	¿El elemento corresponde a lo que se afirma?	Confirmar identidad del archivo, imagen, audio, video o metadato
Cadena de custodia	¿Se preservó el estado original?	Revisar trazabilidad, copias forenses y registro de custodios
Fiabilidad técnica	¿El método utilizado es confiable?	Exigir validación, margen de error y aceptación técnica
Contradicción	¿La defensa pudo cuestionar la prueba?	Garantizar acceso a metodología, perito y datos necesarios
Corroboración	¿El resultado se confirma con otros elementos?	Evitar condenas basadas exclusivamente en un algoritmo
Motivación	¿El juez explicó la valoración?	Exigir fundamentación fáctica y normativa suficiente

La tabla permite identificar los elementos mínimos que el juez debe considerar cuando valora prueba tecnológica o asistida por inteligencia artificial. El resultado algorítmico no debe ser valorado como verdad automática, sino como un elemento sujeto a control racional y jurídico.

1.8 Conclusión del capítulo

La prueba penal es el fundamento racional y jurídico de la decisión judicial. Su función no consiste únicamente en aportar información al proceso, sino en permitir que los hechos sean establecidos conforme a reglas constitucionales y legales. En un Estado constitucional de derechos y justicia, la actividad probatoria debe respetar la presunción de

ISBN: 978-631-6557-82-7

inocencia, el derecho a la defensa, la contradicción, la igualdad de armas, la inmediación, la oralidad, la motivación y la exclusión de la prueba ilícita.

El análisis desarrollado permite afirmar que la prueba penal se encuentra sometida a un sistema de límites orientado a evitar decisiones arbitrarias. La legalidad, la pertinencia, la utilidad, la conducencia, la autenticidad, la cadena de custodia y la aceptación científica o técnica son criterios indispensables para determinar si un elemento probatorio puede ingresar y ser valorado dentro del proceso.

La doctrina probatoria contemporánea refuerza esta comprensión. Taruffo, Ferrer Beltrán, Gascón Abellán y González Lagier coinciden, desde distintas perspectivas, en que la prueba judicial exige racionalidad, justificación, control y motivación. La decisión sobre los hechos no puede ser una expresión de intuición judicial ni una aceptación acrítica de información técnica. Debe ser el resultado de una inferencia probatoria justificada y sometida a garantías procesales.

Estos fundamentos son esenciales para el estudio de la inteligencia artificial como herramienta probatoria. La IA no puede ser considerada una fuente autónoma de verdad ni un sustituto de la valoración judicial. Sus resultados solo podrán tener relevancia procesal cuando sean obtenidos legalmente, incorporados mediante medios probatorios reconocidos, explicados técnicamente, sometidos a contradicción y valorados de manera racional por el juez.

El proceso penal no debe rechazar la tecnología, pero tampoco debe subordinarse a ella. La inteligencia artificial puede contribuir a la investigación penal y al análisis probatorio, siempre que permanezca sometida al derecho, al control humano y a las garantías procesales. La legitimidad del sistema penal no depende únicamente de su capacidad para sancionar, sino de su capacidad para hacerlo respetando los derechos fundamentales.

CAPÍTULO II.

Inteligencia artificial y transformación del sistema penal

ISBN: 978-631-6557-82-7

CAPÍTULO II.

2 Inteligencia artificial y transformación del sistema penal

El capítulo anterior estableció que la prueba penal constituye el fundamento racional de la decisión judicial y que su validez depende del respeto a principios como legalidad, contradicción, defensa, presunción de inocencia, motivación y valoración racional. A partir de esa base, corresponde analizar ahora la inteligencia artificial como fenómeno tecnológico que está transformando el funcionamiento de los sistemas penales contemporáneos.

La inteligencia artificial ha dejado de ser una herramienta exclusiva de laboratorios, centros de investigación o empresas tecnológicas para convertirse en un instrumento utilizado por administraciones públicas, instituciones de seguridad, fiscalías, órganos judiciales, sistemas financieros, plataformas digitales y entidades privadas. En el ámbito penal, su incorporación plantea un escenario especialmente complejo porque se vincula con la investigación criminal, la gestión de evidencia digital, el análisis de patrones delictivos, la identificación biométrica, el procesamiento masivo de datos y, en algunos casos, con herramientas de apoyo a la toma de decisiones.

Sin embargo, la transformación del sistema penal mediante inteligencia artificial no puede analizarse únicamente desde la eficiencia. Si bien la IA puede contribuir a reducir tiempos, organizar grandes volúmenes de información y apoyar investigaciones complejas, también puede generar riesgos relevantes para derechos fundamentales. Entre estos riesgos se encuentran la opacidad algorítmica, los sesgos en los datos, la falta de explicabilidad, la vigilancia masiva, la afectación a la privacidad, la desigualdad de armas procesales y la posible debilitación de la presunción de inocencia.

Furingo (2025) advierte que la integración de la inteligencia artificial en la justicia penal genera tensiones entre la eficiencia judicial y el respeto de los derechos y garantías procesales fundamentales. Esta tensión constituye el punto de partida del presente capítulo: la inteligencia artificial puede aportar herramientas útiles al sistema penal, pero su incorporación debe someterse a controles jurídicos, técnicos y éticos compatibles con el Estado constitucional de derechos.

ISBN: 978-631-6557-82-7

Por esta razón, el capítulo desarrolla una aproximación conceptual y jurídica a la inteligencia artificial, explica sus principales modalidades, identifica sus aplicaciones en el sistema penal y examina sus beneficios y riesgos desde una perspectiva garantista. Además, incorpora estándares internacionales sobre IA confiable, derechos humanos, gobernanza, transparencia, supervisión humana y gestión de riesgos, con el objetivo de situar el debate penal ecuatoriano dentro de una discusión global más amplia.

2.1 Aproximación conceptual a la inteligencia artificial

La inteligencia artificial puede entenderse, en términos generales, como un conjunto de sistemas tecnológicos capaces de realizar tareas que normalmente exigirían algún grado de inteligencia humana, como reconocer patrones, clasificar información, aprender de datos, formular predicciones, generar respuestas, identificar objetos, interpretar lenguaje o apoyar procesos de toma de decisiones.

Russell y Norvig (2021) explican la inteligencia artificial a partir de la construcción de agentes capaces de percibir su entorno y actuar racionalmente frente a determinados objetivos. Esta aproximación permite comprender la IA no como una entidad con conciencia, sino como un sistema diseñado para procesar información y producir resultados bajo determinadas reglas, modelos o parámetros. Desde una perspectiva jurídica, esta distinción es fundamental: la IA no razona jurídicamente, no interpreta derechos fundamentales y no asume responsabilidad moral o institucional por sus resultados.

En materia penal, la inteligencia artificial debe ser comprendida como una herramienta de apoyo, no como un sujeto decisor ni como una autoridad probatoria. Puede generar recomendaciones, clasificaciones, coincidencias, alertas o predicciones, pero tales resultados requieren interpretación humana, validación técnica y control jurídico. En consecuencia, su relevancia dentro del sistema penal depende de que sus resultados puedan ser explicados, auditados y discutidos por los sujetos procesales.

Desde el punto de vista funcional, la IA opera mediante datos de entrada, modelos de procesamiento y resultados de salida. Estos resultados pueden consistir en una coincidencia facial, una clasificación de riesgo, una alerta sobre manipulación audiovisual,

ISBN: 978-631-6557-82-7

una transcripción automatizada, un análisis de patrones financieros o una relación entre datos aparentemente dispersos. Sin embargo, ninguna de estas salidas equivale por sí sola a una verdad penal. Son productos técnicos que deben ser examinados dentro del marco del debido proceso.

La UNESCO (2022) advierte que los sistemas de IA plantean cuestiones éticas vinculadas con derechos humanos, privacidad, no discriminación, democracia, Estado de derecho y toma de decisiones. Esta preocupación se intensifica en el proceso penal, porque las consecuencias de una decisión pueden afectar directamente la libertad personal, la honra, la intimidad, la presunción de inocencia y el derecho a la defensa.

En el caso ecuatoriano, el análisis debe ubicarse dentro del modelo constitucional vigente. Toda innovación tecnológica utilizada por instituciones policiales, fiscales o judiciales debe respetar el bloque de garantías constitucionales y legales que protegen a la persona frente al poder punitivo del Estado. La inteligencia artificial puede modernizar la justicia penal, pero no puede desplazar los límites constitucionales que legitiman el proceso.

Por ello, el concepto jurídico de IA en materia penal debe construirse desde una premisa básica: la IA puede asistir al sistema penal, pero no sustituirlo. Puede apoyar la investigación, pero no reemplazar la prueba. Puede auxiliar al perito, pero no suprimir la explicación técnica. Puede servir al juez como insumo informativo, pero no reemplazar la motivación judicial.

2.2 Algoritmos, aprendizaje automático y aprendizaje profundo

Para comprender la incidencia de la inteligencia artificial en el sistema penal es necesario explicar tres conceptos básicos: algoritmo, aprendizaje automático y aprendizaje profundo.

Un algoritmo es una secuencia ordenada de instrucciones destinada a resolver un problema o ejecutar una tarea. En términos simples, puede entenderse como un procedimiento lógico que recibe datos de entrada, los procesa y genera un resultado. En el contexto penal, un algoritmo podría utilizarse para ordenar expedientes, analizar bases de

ISBN: 978-631-6557-82-7

datos, identificar coincidencias biométricas, clasificar imágenes, detectar patrones de comunicación o relacionar información proveniente de distintas fuentes.

El aprendizaje automático, también conocido como machine learning, es una modalidad de inteligencia artificial en la que el sistema aprende a partir de datos. A diferencia de un programa tradicional, que ejecuta instrucciones previamente definidas, el aprendizaje automático permite identificar patrones y mejorar su desempeño con base en ejemplos previos. En materia penal, esto puede aplicarse al análisis de imágenes, reconocimiento facial, predicción de zonas con mayor incidencia delictiva, detección de fraudes o clasificación de información digital.

El aprendizaje profundo, o deep learning, es una forma más compleja de aprendizaje automático basada en redes neuronales artificiales. Este tipo de sistema puede procesar datos de mayor complejidad, como imágenes, audios, videos o lenguaje natural. Su utilidad es evidente en actividades como reconocimiento de voz, detección de rostros, análisis de video, traducción automática, identificación de objetos, generación de contenido o detección de patrones no evidentes para el análisis humano ordinario.

Sin embargo, mientras más complejo es el sistema, más difícil puede ser explicar cómo llegó a un resultado. Este problema es conocido como opacidad algorítmica o caja negra. Furingo (2025) explica que la caja negra aparece cuando se desconoce el contenido, la funcionalidad, la estructura o la programación del algoritmo, de modo que no es posible saber con claridad cómo la IA alcanzó el resultado final. En el proceso penal, esta situación es especialmente delicada porque la defensa debe poder conocer y cuestionar los elementos utilizados en su contra.

Pasquale (2015) utiliza la expresión sociedad de la caja negra para referirse al creciente uso de sistemas opacos que influyen en decisiones sociales, económicas e institucionales. Esta reflexión es trasladable al ámbito penal: cuando un sistema tecnológico influye en una investigación, en una pericia o en una decisión judicial, su opacidad no es solo un problema técnico, sino un problema de legitimidad democrática y procesal.

Si un sistema de IA identifica a una persona como sospechosa, clasifica una conducta como riesgosa o afirma que una imagen corresponde a determinado individuo, la defensa

ISBN: 978-631-6557-82-7

debe poder conocer cómo se obtuvo esa conclusión. De lo contrario, el resultado algorítmico se convierte en una afirmación técnica difícil de controvertir, afectando el derecho a la defensa y la contradicción probatoria.

Tabla 7 Diferencias básicas entre algoritmo, aprendizaje automático y aprendizaje profundo

Concepto	Característica principal	Ejemplo en materia penal	Riesgo jurídico principal
Algoritmo	Ejecuta instrucciones o reglas definidas	Organización de expedientes o búsqueda de coincidencias simples	Automatización sin revisión humana
Aprendizaje automático	Aprende patrones a partir de datos	Identificación de patrones delictivos o clasificación de evidencia digital	Reproducción de sesgos presentes en los datos
Aprendizaje profundo	Procesa información compleja mediante redes neuronales	Reconocimiento facial, análisis de video o detección de deepfakes	Opacidad técnica y dificultad de explicación

La tabla permite observar que no toda herramienta tecnológica tiene el mismo nivel de complejidad ni el mismo riesgo jurídico. Mientras un algoritmo simple puede ser relativamente comprensible, los sistemas de aprendizaje profundo pueden generar resultados técnicamente sofisticados, pero difíciles de explicar. Por ello, el nivel de control judicial, pericial y defensivo debe aumentar conforme aumenta la complejidad del sistema utilizado.

2.3 Inteligencia artificial predictiva, generativa y analítica

La inteligencia artificial puede clasificarse de distintas maneras. Para el análisis jurídico penal resulta útil distinguir entre IA predictiva, IA generativa e IA analítica, porque cada una plantea utilidades y riesgos distintos.

ISBN: 978-631-6557-82-7

La inteligencia artificial predictiva se orienta a anticipar eventos, comportamientos o riesgos a partir de datos históricos. En materia penal, puede utilizarse para identificar zonas de mayor incidencia delictiva, estimar riesgos de reincidencia, detectar patrones de fraude, priorizar investigaciones o elaborar mapas de criminalidad. Su utilidad radica en la capacidad de procesar grandes bases de datos y detectar correlaciones que podrían pasar inadvertidas para los operadores humanos.

No obstante, este tipo de IA plantea riesgos relevantes. Si el sistema se alimenta con datos históricos afectados por prácticas discriminatorias, desigualdades estructurales o sesgos institucionales, puede reproducir o amplificar esos sesgos. Barocas y Selbst (2016) advierten que los sistemas basados en grandes datos pueden heredar prejuicios de decisiones previas o reflejar sesgos existentes en la sociedad. En materia penal, esto puede traducirse en vigilancia selectiva, perfilamiento indebido o criminalización anticipada.

La inteligencia artificial generativa, por su parte, es capaz de producir contenido nuevo, como textos, imágenes, audios, videos, simulaciones o respuestas automatizadas. Su impacto penal es doble. Por un lado, puede apoyar tareas legítimas, como ordenar información, generar hipótesis preliminares o estructurar documentos de trabajo. Por otro lado, puede ser utilizada para crear contenido falso, suplantar voces, manipular imágenes o producir deepfakes, lo cual plantea desafíos directos para la autenticidad de la prueba digital.

La inteligencia artificial analítica se utiliza para examinar, clasificar y organizar información. En la investigación penal puede servir para analizar grandes volúmenes de documentos, revisar comunicaciones, detectar vínculos entre personas, ordenar datos financieros, identificar metadatos o encontrar coincidencias en bases de datos. Esta modalidad puede fortalecer la eficiencia investigativa, pero también requiere límites relacionados con legalidad, proporcionalidad, finalidad específica y protección de datos personales.

Citron (2008) advierte que los sistemas automatizados pueden afectar el debido proceso cuando sustituyen decisiones individualizadas por operaciones tecnológicas poco transparentes. Esta advertencia es relevante para el proceso penal porque la automatización

ISBN: 978-631-6557-82-7

puede reducir la capacidad real de defensa si la persona afectada no comprende cómo fue evaluada, clasificada o vinculada a un hecho investigado.

Tabla 8 Tipos de IA y su impacto en el sistema penal

Tipo de IA	Función principal	Posible utilidad penal	Riesgo procesal
IA predictiva	Anticipar riesgos o comportamientos	Mapas delictivos, análisis de reincidencia, priorización investigativa	Criminalización anticipada o perfilamiento indebido
IA generativa	Crear contenido nuevo	Apoyo documental, simulaciones, organización de información	Creación de deepfakes, audios o documentos falsos
IA analítica	Procesar y clasificar información	Análisis de evidencia digital, documentos, metadatos y comunicaciones	Tratamiento masivo de datos y afectación a la privacidad

Esta clasificación permite advertir que la IA no tiene un único uso ni un único nivel de riesgo. En el sistema penal, su impacto depende del tipo de herramienta, de la finalidad institucional, de los datos utilizados, del grado de intervención humana y de la posibilidad de control por las partes. Por ello, el análisis jurídico no debe limitarse a preguntar si la IA puede utilizarse, sino para qué se usa, con qué límites, bajo qué control y con qué consecuencias procesales.

2.4 Aplicaciones de la IA en la administración de justicia penal

La inteligencia artificial puede intervenir en diferentes momentos del sistema penal. Sus aplicaciones no se reducen al juicio, sino que pueden aparecer desde la prevención del delito hasta la ejecución de decisiones judiciales. En términos generales, puede utilizarse en cuatro grandes ámbitos: prevención, investigación, gestión procesal y apoyo al análisis probatorio.

ISBN: 978-631-6557-82-7

En la fase de prevención, la IA puede emplearse para analizar patrones de criminalidad, elaborar mapas de riesgo, identificar zonas de mayor incidencia delictiva o detectar comportamientos anómalos en entornos digitales. Estas herramientas pueden ayudar a diseñar políticas públicas de seguridad; sin embargo, también pueden generar prácticas de vigilancia excesiva o perfilamiento social si no existen límites normativos claros.

En la investigación criminal, la IA puede apoyar el análisis de evidencia digital, el reconocimiento facial, la identificación biométrica, la revisión de cámaras de seguridad, el procesamiento de metadatos, la detección de conexiones entre hechos y personas, y la clasificación de información en investigaciones complejas. Herrera Mamarandi, Gordón Lucero y Gutierrez Romero (2026) señalan que los sistemas basados en algoritmos, aprendizaje automático, reconocimiento facial, análisis predictivo y procesamiento masivo de datos han permitido optimizar procesos investigativos, facilitar la identificación de patrones delictivos y fortalecer técnicas de análisis forense.

En la gestión procesal, la IA puede contribuir a organizar expedientes, clasificar documentos, buscar jurisprudencia, generar alertas de plazos o identificar precedentes relevantes. Este uso administrativo puede mejorar la eficiencia judicial sin afectar directamente la valoración probatoria, siempre que no se convierta en sustituto de la función jurisdiccional.

En el análisis probatorio, la IA puede apoyar la revisión de grandes volúmenes de documentos, audios, videos, imágenes o registros digitales. También puede ayudar a detectar manipulación de archivos, inconsistencias, coincidencias biométricas o patrones de comunicación. No obstante, cuando la IA incide en información que puede influir en la responsabilidad penal, el nivel de control debe ser más estricto.

El Reglamento Europeo de Inteligencia Artificial, Reglamento (UE) 2024/1689, resulta relevante como referencia comparada porque adopta un enfoque basado en riesgos y presta especial atención a usos de IA vinculados con identificación biométrica, aplicación de la ley y sistemas de alto riesgo. Aunque no es norma aplicable directamente en Ecuador,

ISBN: 978-631-6557-82-7

ofrece criterios útiles para comprender que ciertos usos de IA en materia penal requieren mayores salvaguardias.

Tabla 9 Aplicaciones de la IA según la etapa del sistema penal

Etapa	Aplicación posible	Beneficio esperado	Control necesario
Prevención	Mapas de riesgo y análisis predictivo	Orientación de políticas de seguridad	Evitar perfilamiento y vigilancia discriminatoria
Investigación	Reconocimiento facial, análisis de evidencia digital, metadatos	Rapidez y organización de información compleja	Legalidad, cadena de custodia y autorización judicial cuando corresponda
Gestión procesal	Clasificación de expedientes, búsqueda documental	Celeridad y eficiencia administrativa	Supervisión humana y trazabilidad
Análisis probatorio	Detección de patrones, deepfakes o coincidencias técnicas	Apoyo al trabajo pericial	Explicabilidad, pericia, contradicción y valoración judicial

La tabla muestra que la IA no siempre tiene el mismo impacto jurídico. Su uso administrativo puede presentar riesgos menores que su empleo probatorio o predictivo. Cuando la herramienta se aproxima a la identificación de personas, la valoración de evidencia o la determinación de riesgos penales, se requiere un control reforzado, porque sus resultados pueden influir directamente en derechos fundamentales.

2.5 Uso de IA en investigación criminal, fiscalía y actividad judicial

La investigación criminal contemporánea se enfrenta a fenómenos delictivos cada vez más complejos. Delitos informáticos, crimen organizado, corrupción, lavado de activos, violencia digital, fraude electrónico, explotación de datos personales, manipulación audiovisual y delincuencia económica generan grandes cantidades de información que

ISBN: 978-631-6557-82-7

difícilmente pueden ser analizadas con métodos tradicionales. En este contexto, la IA aparece como una herramienta capaz de apoyar la labor investigativa.

En el ámbito policial, la IA puede utilizarse para analizar cámaras de videovigilancia, identificar rostros, comparar huellas, detectar placas vehiculares, examinar redes sociales, procesar datos de geolocalización o relacionar incidentes aparentemente aislados. También puede apoyar tareas de ciberinteligencia, identificación de patrones de fraude o análisis de comunicaciones.

En el ámbito fiscal, la IA puede ayudar a organizar expedientes complejos, clasificar información, identificar líneas de investigación, revisar grandes volúmenes de documentos, analizar datos financieros o detectar vínculos entre personas naturales, jurídicas, cuentas bancarias, dispositivos y ubicaciones. No obstante, la Fiscalía no puede delegar en un sistema automatizado la construcción de la teoría del caso ni la decisión sobre la imputación penal. La IA puede orientar, pero no sustituir el criterio jurídico del fiscal.

En la actividad judicial, la IA puede emplearse para gestión documental, búsqueda de precedentes, sistematización de jurisprudencia, alertas procesales o análisis de carga de trabajo. Sin embargo, su uso debe mantenerse claramente separado de la decisión judicial. La sentencia penal exige motivación, valoración racional de la prueba y responsabilidad institucional del juez. Ningún sistema automatizado puede reemplazar la deliberación judicial ni la explicación pública de las razones de la decisión.

Desde la perspectiva ecuatoriana, el debate es especialmente relevante porque existen retos relacionados con la ausencia de regulación específica sobre el empleo de herramientas de IA durante investigaciones criminales y la generación de evidencia en juicios penales. Herrera Mamarandi et al. (2026) advierten que en Ecuador la aplicación de IA en investigación penal todavía se encuentra en una etapa inicial y carece de un cuerpo normativo expreso que delimite aplicaciones, mecanismos de supervisión y restricciones legales.

La Ley Orgánica de Protección de Datos Personales aporta criterios relevantes para este debate, porque reconoce la importancia de la legalidad, proporcionalidad y necesidad en ciertos tratamientos de datos vinculados con seguridad, defensa del Estado, prevención,

ISBN: 978-631-6557-82-7

investigación, detección o enjuiciamiento de infracciones penales. Aunque esta ley no regula de forma integral la IA penal, sí ofrece una base para analizar los límites del tratamiento de datos personales, biométricos, sensibles o automatizados en contextos de investigación.

Por ello, el uso de IA en investigación criminal, Fiscalía y actividad judicial debe obedecer a criterios mínimos: finalidad legítima, base legal, proporcionalidad, necesidad, supervisión humana, trazabilidad, documentación del sistema utilizado, protección de datos personales y posibilidad de contradicción cuando sus resultados ingresen al proceso penal.

2.6 Beneficios de la IA en la gestión y análisis probatorio

La incorporación de inteligencia artificial al sistema penal puede ofrecer beneficios importantes cuando se utiliza con fines legítimos y bajo control jurídico. Entre estos beneficios se encuentran la eficiencia investigativa, la reducción de tiempos, la identificación de patrones complejos, la organización de información masiva, el apoyo a la prueba pericial y la detección de manipulación digital.

Uno de los principales beneficios es la capacidad de procesar grandes volúmenes de información. En investigaciones complejas, puede existir una cantidad significativa de documentos, mensajes, registros financieros, imágenes, videos, audios, ubicaciones, dispositivos y metadatos. La IA puede ayudar a ordenar esta información, identificar coincidencias y presentar patrones relevantes para la investigación.

Otro beneficio es el apoyo al análisis de evidencia digital. La criminalidad contemporánea deja rastros en entornos tecnológicos: dispositivos móviles, redes sociales, plataformas digitales, correos electrónicos, cámaras de seguridad, bases de datos, transacciones electrónicas y registros de navegación. La IA puede facilitar la detección de relaciones entre estos elementos, siempre que el acceso a la información haya sido legal y que se respete la cadena de custodia.

También puede contribuir a la detección de contenido manipulado. La existencia de deepfakes, audios sintéticos e imágenes alteradas exige herramientas técnicas capaces de analizar autenticidad, origen, metadatos y posibles inconsistencias. Sin embargo, el

ISBN: 978-631-6557-82-7

resultado producido por una herramienta de IA debe ser validado por peritos y no valorado como verdad automática.

La IA puede además fortalecer la gestión institucional. En sistemas judiciales con alta carga procesal, puede colaborar en tareas administrativas, clasificación de causas, búsqueda de normativa, identificación de precedentes y organización de documentos. Estos usos pueden mejorar la eficiencia sin afectar directamente derechos fundamentales, siempre que se mantenga supervisión humana.

El NIST AI Risk Management Framework 1.0 propone una aproximación útil para pensar estos beneficios desde la gestión de riesgos. Sus características de IA confiable incluyen validez y confiabilidad, seguridad, resiliencia, responsabilidad, transparencia, explicabilidad, interpretabilidad, privacidad y equidad. Trasladado al sistema penal, esto significa que la utilidad de una herramienta inteligente debe evaluarse junto con su confiabilidad, trazabilidad, explicabilidad y capacidad de control.

Tabla 10 Beneficios de la IA y condiciones para su uso legítimo

Beneficio	Descripción	Condición jurídica necesaria
Eficiencia investigativa	Reduce tiempos de análisis de información compleja	No sacrificar garantías procesales
Análisis de evidencia digital	Organiza documentos, audios, videos y metadatos	Legalidad en la obtención y cadena de custodia
Identificación de patrones	Detecta relaciones entre hechos, personas o lugares	Evitar inferencias automáticas de responsabilidad
Apoyo pericial	Ayuda a examinar autenticidad o manipulación digital	Validación por perito y explicación metodológica
Gestión judicial	Ordena expedientes y facilita búsqueda documental	Supervisión humana y uso no decisorio

ISBN: 978-631-6557-82-7

La tabla permite advertir que los beneficios de la IA no deben analizarse de forma aislada. Cada ventaja tecnológica exige una condición jurídica correlativa. La eficiencia solo es legítima si no debilita derechos; la rapidez solo es aceptable si no sustituye el control judicial; y el análisis automatizado solo puede tener relevancia probatoria si es explicable, verificable y contradicho por las partes.

2.7 Estándares internacionales sobre IA, derechos humanos y justicia penal

El debate sobre inteligencia artificial en el sistema penal no puede limitarse al ámbito nacional. La rapidez con la que evolucionan los sistemas inteligentes ha impulsado la aparición de estándares internacionales orientados a promover una IA confiable, transparente, segura, responsable y compatible con los derechos humanos.

La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO constituye una referencia importante porque vincula el ciclo de vida de los sistemas de IA con valores como dignidad humana, derechos humanos, no discriminación, privacidad, supervisión humana, seguridad, responsabilidad y gobernanza ética. En materia penal, estos principios permiten sostener que ninguna herramienta inteligente debe utilizarse sin evaluación previa de sus impactos sobre derechos fundamentales.

Los Principios de IA de la OCDE, adoptados inicialmente en 2019 y actualizados en 2024, promueven una IA innovadora y confiable que respete los derechos humanos y los valores democráticos. Su relevancia para el sistema penal radica en que la confianza tecnológica no se limita al rendimiento técnico, sino que exige transparencia, robustez, seguridad, rendición de cuentas y gobernanza adecuada.

El NIST AI Risk Management Framework 1.0 propone una metodología de gestión de riesgos basada en funciones como gobernar, mapear, medir y gestionar. Esta aproximación resulta útil para el sistema penal porque permite evaluar los riesgos de una herramienta antes, durante y después de su uso. En la práctica, una Fiscalía, unidad policial, laboratorio forense o tribunal que emplee IA debería poder identificar riesgos, medir errores, gestionar sesgos y documentar decisiones.

ISBN: 978-631-6557-82-7

El Reglamento Europeo de Inteligencia Artificial, Reglamento (UE) 2024/1689, ofrece un referente normativo relevante porque clasifica sistemas de IA según niveles de riesgo y presta especial atención a usos de alto impacto, incluidos algunos vinculados con aplicación de la ley, identificación biométrica y evaluación de personas. Aunque no se trata de una norma ecuatoriana, su enfoque basado en riesgos permite extraer una lección aplicable: mientras mayor sea la afectación potencial sobre derechos fundamentales, más estrictos deben ser los controles.

El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho también constituye un referente importante, porque busca asegurar que las actividades del ciclo de vida de los sistemas de IA sean compatibles con derechos humanos, democracia y Estado de derecho. Este enfoque es especialmente relevante para la justicia penal, donde el uso de IA no puede separarse de la legitimidad democrática del poder punitivo.

Tabla 11 Estándares internacionales útiles para el uso de IA en justicia penal

Instrumento	Enfoque principal	Aporte al sistema penal
UNESCO, Recomendación sobre ética de IA	Derechos humanos, dignidad, no discriminación y supervisión humana	Exige evaluar impactos éticos y proteger garantías fundamentales
OCDE, Principios de IA	IA confiable, centrada en derechos humanos y valores democráticos	Refuerza transparencia, robustez y rendición de cuentas
NIST AI RMF	Gestión de riesgos, confiabilidad, explicabilidad y gobernanza	Permite evaluar riesgos técnicos y organizacionales de sistemas de IA
Reglamento Europeo de IA	Enfoque basado en riesgos y regulación de sistemas de alto impacto	Sirve como referencia para controles reforzados en aplicación de la ley

ISBN: 978-631-6557-82-7

Consejo de Europa, Convenio Marco sobre IA	Compatibilidad con derechos humanos, democracia y Estado de derecho	Vincula IA con legitimidad institucional y control democrático

La tabla muestra que los estándares internacionales no sustituyen la legislación ecuatoriana, pero ofrecen criterios útiles para orientar el uso responsable de IA en materia penal. En ausencia de una regulación penal específica sobre IA probatoria, estos instrumentos pueden servir como referentes interpretativos para construir protocolos, políticas institucionales y criterios de admisibilidad.

2.8 Riesgos jurídicos de los sistemas algorítmicos: opacidad, sesgos y supervisión humana

La inteligencia artificial aplicada al sistema penal presenta riesgos que deben ser analizados con especial cautela. Los más relevantes son la opacidad algorítmica, los sesgos, la afectación a la privacidad, el perfilamiento indebido, la vigilancia masiva y la reducción de supervisión humana.

La opacidad algorítmica surge cuando no es posible conocer de manera suficiente cómo el sistema procesó los datos y produjo un resultado. Este problema afecta directamente el derecho de defensa y la contradicción probatoria. Si la defensa no puede comprender el funcionamiento de la herramienta, difícilmente podrá cuestionar su fiabilidad, sus datos de entrada, su metodología, su margen de error o sus limitaciones.

Los sesgos algorítmicos constituyen otro riesgo central. Un sistema de IA aprende de datos previos. Si esos datos contienen desigualdades, errores, prejuicios o prácticas institucionales discriminatorias, el sistema puede reproducirlas. En materia penal, esto puede traducirse en mayor vigilancia sobre determinados grupos, falsas identificaciones, perfilamientos indebidos o decisiones que afecten de manera diferenciada a personas en situación de vulnerabilidad.

Buolamwini y Gebru (2018) demostraron disparidades relevantes en sistemas comerciales de clasificación facial, especialmente al analizar la intersección entre género y tono de piel. Este tipo de hallazgos es relevante para el derecho penal porque el

ISBN: 978-631-6557-82-7

reconocimiento facial puede ser utilizado en investigaciones criminales, identificación de sospechosos o análisis de videovigilancia. Si el sistema presenta diferencias de precisión entre grupos, su uso sin control puede generar falsos positivos y afectaciones discriminatorias.

La afectación a la privacidad también es relevante. La IA suele operar mediante grandes volúmenes de datos, incluidos datos personales, datos biométricos, ubicaciones, comunicaciones y patrones de comportamiento. En el contexto penal, la recolección automatizada de datos biométricos, información de geolocalización o patrones de conducta digital demanda marcos éticos y legales rigurosos.

El perfilamiento indebido constituye un riesgo específico. La IA predictiva puede clasificar a personas, grupos o territorios como más riesgosos a partir de datos históricos. Sin embargo, en materia penal la responsabilidad debe ser individualizada y basada en hechos probados. Una persona no puede ser tratada como culpable o peligrosa por pertenecer a un grupo estadístico o por coincidir con un patrón generado por datos previos.

La supervisión humana es, por tanto, un requisito esencial. La IA puede asistir, pero no decidir; puede orientar, pero no sustituir; puede procesar información, pero no eliminar la responsabilidad del operador jurídico. El fiscal, el perito y el juez deben conservar capacidad real de análisis, revisión, corrección y rechazo de los resultados producidos por sistemas inteligentes.

Tabla 12 Riesgos jurídicos de la IA en el sistema penal

Riesgo	Manifestación práctica	Garantía afectada	Respuesta jurídica necesaria
Opacidad algorítmica	No se conoce cómo el sistema llegó al resultado	Derecho de defensa y contradicción	Explicabilidad, auditoría y acceso técnico suficiente
Sesgo algorítmico	El sistema reproduce desigualdades de los datos	Igualdad y presunción de inocencia	Evaluación de sesgos y validación independiente

ISBN: 978-631-6557-82-7

Perfilamiento indebido	Clasificación de personas por riesgo o conducta esperada	Presunción de inocencia y privacidad	Prohibición de decisiones basadas solo en perfiles
Vigilancia masiva	Tratamiento indiscriminado de datos personales	Intimidad y protección de datos	Legalidad, necesidad y proporcionalidad
Automatización decisoria	Delegación de decisiones penales en sistemas inteligentes	Motivación judicial y debido proceso	Supervisión humana significativa

La tabla sintetiza los principales riesgos jurídicos de la IA en materia penal. Su importancia radica en mostrar que cada riesgo compromete una garantía concreta y exige una respuesta jurídica específica. No basta con afirmar que la IA es útil o moderna; es necesario diseñar mecanismos de control que impidan que la tecnología debilite el núcleo del proceso penal democrático.

2.9 Conclusión del capítulo

La inteligencia artificial representa una transformación significativa para el sistema penal. Su capacidad para procesar datos, identificar patrones, analizar evidencia digital y apoyar investigaciones complejas puede contribuir a una justicia más eficiente y técnicamente fortalecida. Sin embargo, su incorporación no puede ser acrítica ni automática.

El análisis desarrollado permite afirmar que la IA debe ser comprendida como una herramienta auxiliar, no como una autoridad decisoria ni como una fuente autónoma de verdad. Su uso en el sistema penal debe estar sometido a legalidad, proporcionalidad, transparencia, explicabilidad, auditoría, supervisión humana y respeto pleno de las garantías procesales.

La transformación tecnológica del sistema penal solo será legítima si respeta los principios que justifican el proceso penal en un Estado constitucional de derechos y justicia. La eficiencia no puede reemplazar al debido proceso; la predicción no puede sustituir la prueba; y el algoritmo no puede ocupar el lugar del juez, del fiscal, del defensor ni del perito.

ISBN: 978-631-6557-82-7

Los estándares internacionales revisados permiten reforzar esta conclusión. UNESCO, OCDE, NIST, la Unión Europea y el Consejo de Europa coinciden en que la IA debe desarrollarse y utilizarse bajo criterios de derechos humanos, transparencia, responsabilidad, supervisión humana y gestión de riesgos. Estos criterios son especialmente relevantes para el sistema penal ecuatoriano, donde todavía no existe una regulación penal específica sobre IA probatoria.

En consecuencia, la inteligencia artificial puede fortalecer la investigación penal y la gestión probatoria únicamente cuando se encuentra subordinada al derecho. Si se utiliza sin control, puede convertirse en una amenaza para la presunción de inocencia, la defensa, la privacidad, la igualdad y la motivación judicial. Esta tensión será fundamental para el desarrollo del siguiente capítulo, en el que se analizará específicamente la inteligencia artificial como herramienta probatoria en el proceso penal.

CAPÍTULO III.

La inteligencia artificial como herramienta probatoria en el proceso penal

ISBN: 978-631-6557-82-7

CAPÍTULO III.

3 La inteligencia artificial como herramienta probatoria en el proceso penal

La incorporación de la inteligencia artificial al proceso penal exige precisar su naturaleza jurídica dentro de la actividad probatoria. No basta con afirmar que la IA puede ser útil para investigar delitos, analizar evidencia digital o identificar patrones; es necesario determinar cómo sus resultados pueden ingresar válidamente al proceso, bajo qué categoría probatoria deben ser tratados y qué controles técnicos y jurídicos deben exigirse para evitar afectaciones al debido proceso.

En el sistema penal ecuatoriano, la prueba se encuentra regulada por reglas específicas. El Código Orgánico Integral Penal reconoce como medios de prueba el documento, el testimonio y la pericia (COIP, 2014, art. 498). Esta clasificación resulta fundamental, porque permite sostener que la inteligencia artificial no constituye, por sí misma, un medio de prueba autónomo. En realidad, sus resultados deben ser incorporados al proceso a través de los medios probatorios reconocidos por la ley, especialmente mediante prueba documental, contenido digital o prueba pericial.

La inteligencia artificial puede cumplir distintas funciones probatorias: puede apoyar la obtención de información, procesar grandes volúmenes de datos, clasificar indicios, detectar coincidencias, analizar imágenes o videos, identificar patrones, recuperar archivos, verificar autenticidad digital o auxiliar al perito en investigaciones complejas. Sin embargo, estas funciones no la convierten en una fuente incuestionable de verdad. Sus resultados requieren validación técnica, control judicial, posibilidad de contradicción y valoración racional.

En este contexto, la siguiente figura sintetiza las principales dimensiones de la inteligencia artificial como herramienta probatoria, considerando sus aplicaciones, potencialidades, riesgos y condiciones mínimas de uso legítimo dentro del proceso penal.

ISBN: 978-631-6557-82-7

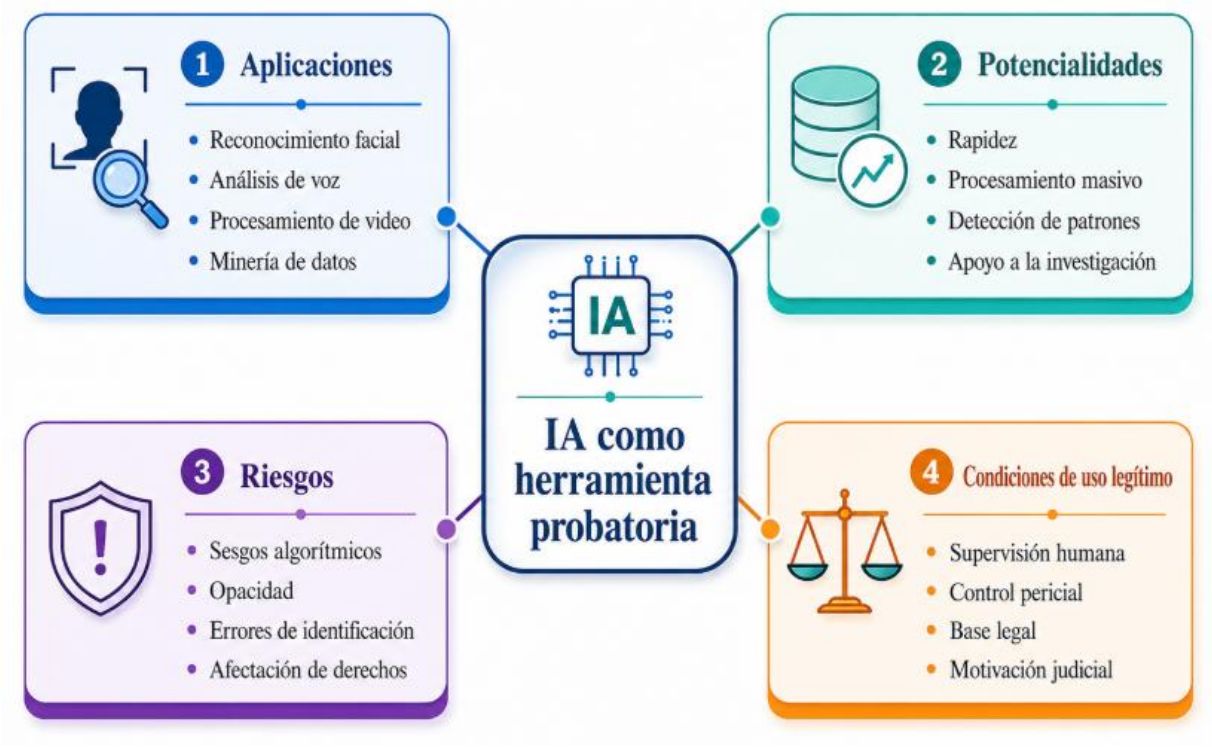

Figura 2 La inteligencia artificial como herramienta probatoria

Este capítulo analiza la inteligencia artificial como herramienta probatoria en el proceso penal. Para ello, se estudia su naturaleza jurídica, su diferencia con la prueba autónoma, su relación con la fuente de prueba y el medio de prueba, sus principales aplicaciones en evidencia digital, biometría, reconocimiento facial, geolocalización, videovigilancia, deepfakes, ciberdelincuencia y delitos económicos, así como la necesidad de validación técnica, pericial y jurídica.

Para comprender adecuadamente el papel de la inteligencia artificial como herramienta probatoria, es necesario visualizar el recorrido que sigue la información tecnológica desde su origen digital hasta su eventual control judicial. Este proceso permite advertir que la IA no actúa de manera aislada ni autónoma, sino dentro de una cadena de fases que exige legalidad, preservación, verificación humana, incorporación procesal y valoración judicial.

ISBN: 978-631-6557-82-7

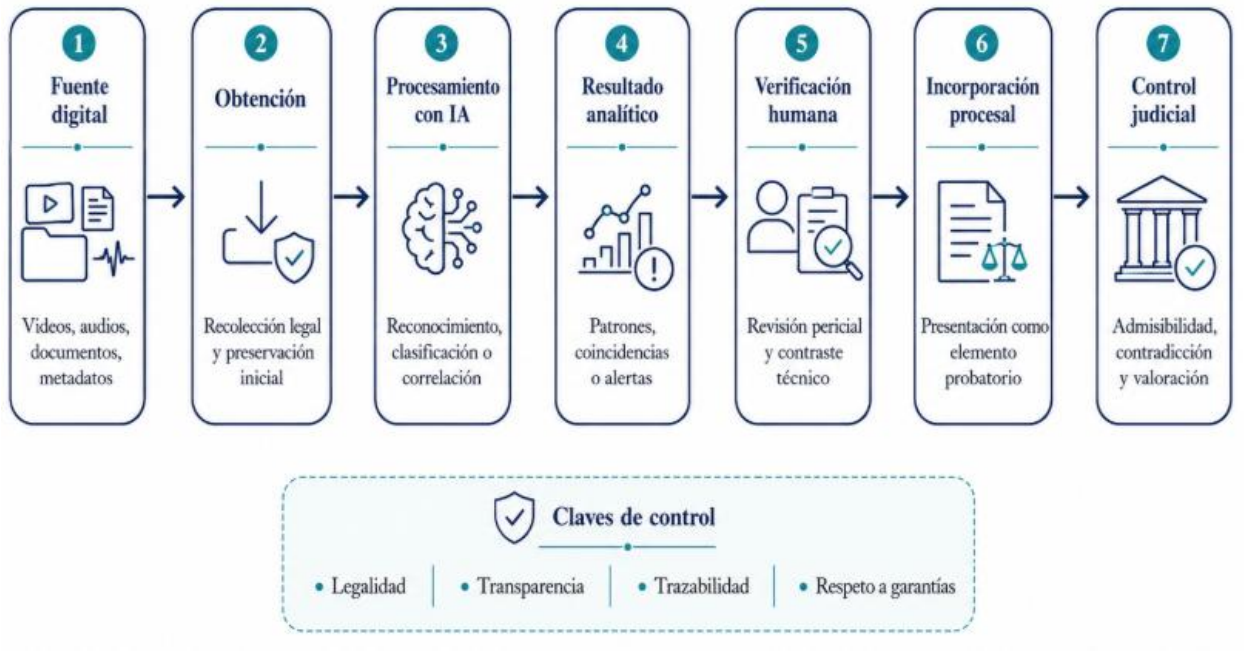

Figura 3 Ciclo de incorporación de la IA en el sistema penal

Como se observa en la figura, la incorporación de la inteligencia artificial al sistema penal no inicia con el resultado algorítmico, sino con la existencia de una fuente digital que debe ser obtenida y preservada de manera legal. Posteriormente, el procesamiento mediante IA puede generar patrones, coincidencias o alertas, pero estos resultados requieren verificación humana, revisión pericial e incorporación procesal válida. Solo después de estas fases pueden ser sometidos a contradicción, admisibilidad y valoración judicial.

3.1 Naturaleza jurídica de la inteligencia artificial en materia probatoria

La naturaleza jurídica de la inteligencia artificial en materia probatoria debe ser entendida desde una premisa inicial: la IA no es sujeto procesal, no declara, no razona jurídicamente y no valora prueba en sentido jurisdiccional. Es una herramienta tecnológica que procesa información y genera resultados a partir de datos, modelos, algoritmos y parámetros previamente definidos o entrenados. Por tanto, su función dentro del proceso penal debe ser auxiliar, instrumental y sometida a control humano.

La inteligencia artificial puede intervenir en la actividad probatoria de varias formas. Puede ayudar a identificar información relevante, organizar evidencia digital, detectar coincidencias, analizar archivos audiovisuales, establecer relaciones entre datos o apoyar

ISBN: 978-631-6557-82-7

informes periciales. Sin embargo, el valor procesal de sus resultados no proviene de la herramienta en sí misma, sino de su incorporación válida al proceso y de la posibilidad de verificar su fiabilidad.

En términos probatorios, la IA debe ser analizada como una herramienta de procesamiento o análisis, no como una prueba independiente. Esto significa que el resultado generado por un sistema inteligente debe conectarse con un medio probatorio legalmente reconocido. Si el resultado se expresa en un informe técnico, normalmente ingresará mediante prueba pericial. Si consiste en un archivo, registro, imagen, audio, video, metadato o informe documental, puede relacionarse con prueba documental o contenido digital. Si se requiere explicación técnica, la intervención del perito será indispensable.

El COIP permite esta lectura porque reconoce como medios de prueba el documento, el testimonio y la pericia (COIP, 2014, art. 498). Además, admite como medio de prueba el contenido digital conforme a las reglas del propio Código (COIP, 2014, art. 499). En consecuencia, el resultado algorítmico debe ser jurídicamente reconducido a una de estas categorías, evitando crear una categoría probatoria informal no regulada.

La inteligencia artificial tampoco debe confundirse con la fuente de prueba. La fuente de prueba es el origen del conocimiento sobre un hecho: una cámara de seguridad, un teléfono celular, una base de datos, una conversación, una imagen, una huella, un documento o un servidor informático. La IA, en muchos casos, no es la fuente original del hecho, sino el instrumento que procesa esa fuente para generar una conclusión técnica. Esta diferencia es esencial, porque permite separar el dato original del resultado producido por el sistema.

Por ejemplo, si un sistema de IA analiza un video de seguridad y concluye que una persona coincide con un rostro registrado en una base de datos, la fuente de prueba será el video, la base de datos y los registros técnicos utilizados. La IA será la herramienta de análisis. El resultado será un indicio técnico que deberá ser validado por un perito, sometido a contradicción y valorado junto con otros elementos.

Desde esta perspectiva, la IA no debe ser presentada al juez como una autoridad técnica autosuficiente. Su resultado debe ser explicado en términos comprensibles: qué

ISBN: 978-631-6557-82-7

datos se usaron, cuál fue el procedimiento aplicado, qué sistema se empleó, qué margen de error existe, qué limitaciones presenta, si hubo intervención humana y si el método utilizado posee aceptación técnica suficiente.

3.2 La IA como herramienta auxiliar y no como prueba autónoma absoluta

La inteligencia artificial debe ser concebida como una herramienta auxiliar dentro del proceso penal. Esto significa que puede contribuir a la investigación, al análisis de evidencia y al trabajo pericial, pero no debe sustituir la prueba legalmente practicada ni desplazar la valoración judicial. Su función es apoyar, no decidir; orientar, no condenar; procesar información, no reemplazar la convicción racional del juez.

El riesgo de considerar la IA como prueba autónoma absoluta radica en la sobrevaloración tecnológica. Cuando un resultado se presenta con lenguaje matemático, porcentajes, gráficos o términos técnicos, puede generar una apariencia de objetividad superior. Sin embargo, esa apariencia no elimina la posibilidad de error, sesgo, manipulación, limitaciones metodológicas o uso inadecuado de datos.

Santiago de León (2026) sostiene que la inteligencia artificial debe entenderse como herramienta de apoyo para la labor judicial y no como sustituto de la función jurisdiccional, porque el juez mantiene la responsabilidad de valorar la prueba, interpretar el derecho y adoptar la decisión final dentro del proceso. Esta idea resulta plenamente aplicable al proceso penal, donde la decisión judicial no puede delegarse en una herramienta automatizada.

En materia probatoria, la IA puede generar resultados útiles, pero esos resultados no deben confundirse con certeza penal. Un algoritmo puede sugerir coincidencias, detectar patrones o clasificar información, pero la responsabilidad penal exige prueba suficiente, legal, contradicha y valorada conforme a la sana crítica. La predicción algorítmica no equivale a hecho probado.

Esta advertencia es especialmente importante en casos de reconocimiento facial, análisis predictivo, detección de patrones criminales o clasificación automática de indicios. En estos escenarios, el sistema puede producir un resultado que oriente la investigación,

ISBN: 978-631-6557-82-7

pero no puede constituir por sí solo fundamento suficiente para atribuir responsabilidad penal. La IA debe operar como un punto de partida investigativo o como apoyo pericial, pero no como conclusión judicial definitiva.

Tabla 13 Función auxiliar de la IA frente a la prueba penal

Función de la IA	Utilidad dentro del proceso penal	Límite jurídico necesario
Identificación de patrones	Relacionar datos, hechos, lugares o personas	No convertir patrones en responsabilidad penal automática
Análisis de imágenes o videos	Detectar objetos, rostros, movimientos o alteraciones	Exigir validación pericial y revisión humana
Procesamiento de documentos	Clasificar información y ubicar datos relevantes	Verificar fuente, autenticidad y pertinencia
Apoyo a pericias informáticas	Recuperar archivos, analizar metadatos o reconstruir eventos	Documentar metodología, software y margen de error
Detección de deepfakes	Advertir posibles manipulaciones audiovisuales	Corroborar con otros medios técnicos y periciales

La tabla muestra que la utilidad de la IA depende de su función concreta. En todos los casos, su valor procesal requiere un límite jurídico: validación pericial, control humano, explicación metodológica, cadena de custodia, autenticidad y contradicción. Sin estos controles, el resultado algorítmico pierde fuerza probatoria y puede convertirse en un riesgo para las garantías procesales.

3.3 Fuente de prueba, medio de prueba, evidencia digital y resultado algorítmico

Para ubicar correctamente la inteligencia artificial dentro del proceso penal es necesario distinguir cuatro conceptos: fuente de prueba, medio de prueba, evidencia digital y resultado algorítmico.

ISBN: 978-631-6557-82-7

La fuente de prueba es el elemento, persona, objeto, dato o situación de donde proviene la información sobre un hecho. Puede ser una persona que presenció un delito, un documento, un dispositivo electrónico, una cámara, una conversación, una huella, una fotografía o una base de datos. La fuente existe antes de su incorporación formal al proceso.

El medio de prueba es el mecanismo jurídico mediante el cual esa información ingresa al proceso. En el sistema penal ecuatoriano, los medios de prueba son el documento, el testimonio y la pericia (COIP, 2014, art. 498). Por ello, aunque la realidad tecnológica sea amplia, la incorporación procesal debe adecuarse a las categorías previstas por la ley.

La evidencia digital comprende información almacenada, procesada o transmitida mediante sistemas tecnológicos. El COIP define el contenido digital como todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que pueda ser sometido a tratamiento informático (COIP, 2014, art. 500). Esta definición es suficientemente amplia para incluir archivos, registros, metadatos, comunicaciones, imágenes, audios, videos, bases de datos y otros elementos informáticos.

El resultado algorítmico, en cambio, es la conclusión generada por un sistema de IA a partir del procesamiento de datos. Puede consistir en una clasificación, coincidencia, predicción, alerta, reconstrucción, puntuación de riesgo, detección de anomalía o identificación de patrón. Este resultado no debe confundirse con la evidencia original. Es una inferencia generada mediante una herramienta tecnológica.

Furingo (2025) plantea una distinción relevante al señalar que, en la evidencia electrónica, los datos almacenados en dispositivos electrónicos constituyen la evidencia misma, mientras que en la IA los datos son la entrada que el algoritmo utiliza para generar inferencias que pueden servir como evidencia (p. 117). Esta diferencia resulta esencial para evitar confundir el archivo original con la conclusión producida por el sistema.

ISBN: 978-631-6557-82-7

Tabla 14 Diferencias entre fuente, medio, evidencia digital y resultado algorítmico

Concepto	Definición funcional	Ejemplo	Tratamiento procesal
Fuente de prueba	Origen de la información sobre el hecho	Teléfono celular, cámara, servidor, testigo	Debe ser identificada, preservada y vinculada al caso
Medio de prueba	Vía legal de incorporación al proceso	Documento, testimonio o pericia	Debe ajustarse al COIP
Evidencia digital	Información almacenada, procesada o transmitida tecnológicamente	Video, audio, metadato, correo electrónico, chat	Requiere técnicas forenses y cadena de custodia
Resultado algorítmico	Inferencia producida por IA a partir de datos	Coincidencia facial, patrón detectado, alerta de manipulación	Requiere validación técnica, pericial y contradicción

La tabla permite advertir que la IA no elimina las categorías tradicionales del derecho probatorio, sino que obliga a reinterpretarlas frente a nuevas formas de información. El proceso penal no debe aceptar el resultado algorítmico de manera aislada, sino conectarlo con la fuente original, el medio probatorio correspondiente y el procedimiento técnico que permitió su generación.

3.4 Aplicaciones probatorias de la IA en imágenes, audios, videos, documentos y metadatos

La inteligencia artificial tiene múltiples aplicaciones probatorias en el análisis de evidencia digital. Su utilidad aparece especialmente en casos donde el volumen, complejidad o formato de la información supera la capacidad de revisión manual de los operadores humanos.

En el análisis de imágenes, la IA puede identificar objetos, rostros, placas vehiculares, ubicaciones, patrones visuales, alteraciones o coincidencias entre archivos. En

ISBN: 978-631-6557-82-7

materia penal, esto puede servir para examinar cámaras de seguridad, fotografías extraídas de dispositivos, imágenes de redes sociales o registros visuales de una escena del hecho.

En el análisis de audios, puede emplearse para transcribir conversaciones, comparar voces, detectar ediciones, identificar ruido de fondo o clasificar fragmentos relevantes. Sin embargo, cualquier conclusión sobre identidad de voz o autenticidad de un audio debe ser tratada con cautela, porque puede estar afectada por calidad de grabación, interferencias, edición o generación sintética.

En el análisis de videos, la IA puede apoyar la detección de movimientos, objetos, personas, vehículos, alteraciones, cortes o manipulaciones. También puede facilitar la revisión de largas horas de grabación, permitiendo ubicar momentos relevantes para la investigación. No obstante, un video analizado por IA debe conservar su archivo original, sus metadatos y su trazabilidad técnica.

En el análisis documental, la IA puede clasificar grandes cantidades de archivos, buscar palabras clave, detectar coincidencias semánticas, identificar patrones financieros o relacionar información dispersa. Esta función es especialmente útil en delitos económicos, corrupción, lavado de activos, delincuencia organizada y fraude.

Los metadatos también tienen especial valor probatorio. Pueden indicar fecha de creación, ubicación, dispositivo utilizado, modificaciones, rutas de archivo, autoría técnica o historial de transmisión. La IA puede ayudar a procesar metadatos en grandes volúmenes, pero su interpretación requiere conocimientos especializados.

Santiago de León (2026) advierte que la evidencia digital presenta características particulares que la distinguen de la prueba tradicional, entre ellas su naturaleza intangible, su alta capacidad de almacenamiento, la posibilidad de ser copiada sin alterar el original y su susceptibilidad a modificaciones si no se preserva adecuadamente. Por ello, su obtención, preservación, análisis y presentación requieren técnicas especializadas y protocolos que garanticen autenticidad, integridad, confiabilidad y cadena de custodia.

El COIP también exige tratamiento técnico para el contenido digital. Según el artículo 500, el análisis, valoración, recuperación y presentación del contenido digital

ISBN: 978-631-6557-82-7

almacenado en dispositivos o sistemas informáticos debe realizarse mediante técnicas digitales forenses (COIP, 2014, art. 500). Esta regla es central para el uso de IA, porque impide que el análisis tecnológico se realice de manera improvisada o sin metodología verificable.

Tabla 15 Aplicaciones de IA sobre distintos tipos de evidencia digital

Tipo de evidencia	Aplicación de IA	Riesgo principal	Control requerido
Imágenes	Identificación de rostros, objetos o alteraciones	Falsos positivos o manipulación visual	Pericia, comparación técnica y archivo original
Audios	Transcripción, comparación de voz o detección de edición	Suplantación de voz o baja calidad del audio	Análisis acústico especializado
Videos	Detección de movimientos, objetos o deepfakes	Edición, cortes o generación sintética	Revisión forense y metadatos
Documentos	Clasificación, búsqueda semántica o relación de datos	Errores de extracción o contexto incompleto	Revisión humana y validación documental
Metadatos	Identificación de origen, fecha, ubicación o modificaciones	Alteración o interpretación incorrecta	Preservación técnica y cadena de custodia

La tabla evidencia que la IA puede aportar eficiencia en el análisis de diversos formatos, pero cada aplicación presenta riesgos específicos. Por ello, el uso de IA no debe desplazar la intervención pericial ni la revisión humana. Su utilidad depende de que los resultados sean verificables, reproducibles y explicables.

ISBN: 978-631-6557-82-7

3.5 Reconocimiento facial, biometría, geolocalización y videovigilancia

El reconocimiento facial, la biometría, la geolocalización y la videovigilancia son algunas de las aplicaciones más sensibles de la inteligencia artificial en materia penal. Su utilidad investigativa es evidente, pero también lo son sus riesgos para la intimidad, la protección de datos, la igualdad y la presunción de inocencia.

El reconocimiento facial permite comparar una imagen o video con una base de datos para identificar posibles coincidencias. Puede utilizarse en cámaras de seguridad, aeropuertos, espacios públicos, redes sociales o archivos policiales. Sin embargo, el resultado de una coincidencia facial no equivale a identificación plena. Debe ser tratado como un indicio técnico sujeto a verificación.

La biometría incluye datos asociados a características físicas, fisiológicas o conductuales. En Ecuador, la Ley Orgánica de Protección de Datos Personales define el dato biométrico como un dato personal único relacionado con características físicas, fisiológicas o conductuales que permite o confirma la identificación única de una persona, como imágenes faciales o datos dactiloscópicos (LOPDP, 2021, art. 4). Esta definición demuestra que el uso penal de biometría involucra datos personales de alta sensibilidad.

La geolocalización permite ubicar a una persona, dispositivo o vehículo en un espacio y tiempo determinados. Puede obtenerse de teléfonos móviles, aplicaciones, antenas, GPS, vehículos, cámaras o registros de plataformas digitales. Aunque puede ser útil para reconstruir hechos, también puede afectar gravemente la privacidad si se obtiene sin base legal suficiente o sin control judicial.

La videovigilancia asistida por IA permite analizar grandes cantidades de grabaciones, identificar movimientos, objetos, patrones de comportamiento o coincidencias biométricas. Su uso puede aportar datos relevantes en investigaciones penales, pero también puede derivar en vigilancia masiva o perfilamiento indebido si se aplica de forma indiscriminada.

Herrera Mamarandi, Gordón Lucero y Gutierrez Romero (2026) señalan que la identificación facial automática se ha vuelto relevante en la investigación forense

ISBN: 978-631-6557-82-7

contemporánea, aunque persisten debates sobre su estandarización metodológica, su apoyo científico y la posibilidad de considerarla evidencia concluyente. Esta observación es importante porque el reconocimiento facial puede ser útil, pero no debe tener valor concluyente sin corroboración.

En consecuencia, estas herramientas deben someterse a controles reforzados. Es necesario identificar el sistema utilizado, la base de datos consultada, la calidad de la imagen, el porcentaje de coincidencia, el margen de error, las condiciones de captura, los sesgos conocidos del sistema y la intervención humana realizada en el análisis.

Tabla 16 Herramientas biométricas y exigencias probatorias

Herramienta	Posible utilidad penal	Riesgo jurídico	Exigencia probatoria
Reconocimiento facial	Identificar posibles coincidencias en imágenes o videos	Falsos positivos, sesgo racial o mala calidad de imagen	Pericia, margen de error y corroboración externa
Huellas dactilares asistidas por IA	Comparar impresiones latentes con bases de datos	Error de comparación o mala calidad de muestra	Validación por experto forense
Geolocalización	Ubicar dispositivo o persona en tiempo y espacio	Vigilancia indebida o afectación a privacidad	Base legal, autorización judicial y trazabilidad
Videovigilancia inteligente	Analizar grabaciones extensas o detectar eventos	Perfilamiento o identificación errónea	Conservación del video original y análisis pericial

La tabla permite observar que estas herramientas no deben ser rechazadas automáticamente, pero tampoco aceptadas sin control. Su uso procesal exige una relación directa con los hechos investigados, respeto a la legalidad, tratamiento adecuado de datos personales, validación técnica y posibilidad de contradicción por la defensa.

ISBN: 978-631-6557-82-7

3.6 Deepfakes, ciberdelincuencia, delitos económicos e identificación de patrones criminales

La inteligencia artificial también tiene relevancia en el análisis de deepfakes, ciberdelincuencia, delitos económicos e identificación de patrones criminales. Estos campos evidencian que la IA puede ser tanto una herramienta para cometer delitos como un instrumento para investigarlos.

Los deepfakes son contenidos audiovisuales sintéticos o manipulados mediante técnicas de inteligencia artificial. Pueden consistir en videos falsos, imágenes alteradas, voces clonadas o simulaciones altamente realistas. En el proceso penal, representan un desafío porque pueden ser utilizados para fabricar evidencia, desacreditar pruebas legítimas, extorsionar, suplantar identidades o afectar la reputación de personas.

Santiago de León (2026) advierte que las herramientas capaces de crear imágenes, audios o videos falsos con alto grado de realismo dificultan la verificación de autenticidad de la evidencia digital presentada en procesos judiciales. Esto obliga a los tribunales a adoptar criterios más rigurosos de admisión y valoración probatoria. Esta reflexión es especialmente relevante para el sistema penal, porque la autenticidad audiovisual ya no puede presumirse simplemente por la apariencia del archivo.

En materia de ciberdelincuencia, la IA puede apoyar la detección de intrusiones, recuperación de archivos eliminados, análisis de malware, identificación de direcciones IP, reconstrucción de eventos digitales, análisis de comunicaciones y clasificación de grandes volúmenes de datos. Estas herramientas son útiles en investigaciones de acceso no autorizado, fraude informático, explotación sexual en línea, phishing, ransomware o delitos contra la intimidad.

En delitos económicos y financieros, la IA puede identificar movimientos inusuales, redes de transferencias, patrones de lavado de activos, relaciones entre empresas, facturación irregular o comportamientos atípicos en bases de datos. No obstante, los patrones financieros detectados mediante IA deben ser interpretados cuidadosamente, porque una anomalía estadística no equivale necesariamente a conducta delictiva.

ISBN: 978-631-6557-82-7

La identificación de patrones criminales también puede ser útil en investigaciones de delincuencia organizada, corrupción, tráfico ilícito, trata de personas o delitos seriales. La IA puede relacionar hechos aparentemente aislados, detectar coincidencias de modus operandi o establecer vínculos entre sujetos y eventos. Sin embargo, existe el riesgo de que la correlación sea confundida con causalidad. El proceso penal exige hechos probados, no simples asociaciones estadísticas.

Tabla 17 IA frente a delitos digitales y patrones criminales

Ámbito	Utilidad de la IA	Riesgo probatorio	Criterio jurídico de control
Deepfakes	Detectar manipulación de imagen, audio o video	Confundir contenido falso con evidencia auténtica	Pericia audiovisual y verificación de metadatos
Ciberdelincuencia	Recuperar archivos, analizar malware o reconstruir eventos	Atribución errónea de autoría digital	Corroboración técnica y nexo causal
Delitos económicos	Detectar transacciones atípicas o redes financieras	Convertir anomalías en presunción de delito	Análisis contable, financiero y jurídico
Patrones criminales	Relacionar hechos, lugares o modus operandi	Criminalización por perfil o asociación estadística	Prueba individualizada y valoración conjunta

La tabla muestra que la IA puede ser especialmente útil en investigaciones complejas, pero también evidencia que sus resultados deben ser interpretados con prudencia. La detección de patrones no sustituye la prueba individualizada de responsabilidad penal. La información producida por IA debe ser corroborada con otros elementos probatorios.

ISBN: 978-631-6557-82-7

3.7 Necesidad de validación técnica, pericial y jurídica de los resultados generados por IA

La validación de los resultados generados por inteligencia artificial constituye una condición indispensable para su uso en el proceso penal. Esta validación debe realizarse en tres niveles: técnico, pericial y jurídico.

La validación técnica exige verificar el funcionamiento del sistema utilizado. Esto incluye identificar el software, versión, proveedor, modelo, datos de entrada, parámetros, margen de error, condiciones de uso, limitaciones y nivel de aceptación técnica. No basta con afirmar que la herramienta es "inteligente" o "avanzada"; debe demostrarse que el sistema es adecuado para la finalidad probatoria concreta.

Furingo (2025) sostiene que una prueba generada por IA solo puede reconocerse como evidencia científica si el algoritmo cumple criterios de verificabilidad, revisión por pares, margen de error, estándares de desarrollo y aceptación dentro de la comunidad científica (pp. 118-119). Esta afirmación permite trasladar al campo de la IA exigencias propias de la prueba científica, especialmente cuando el resultado pretende influir en la decisión judicial.

La validación pericial implica que un experto explique el procedimiento, los datos utilizados, las técnicas aplicadas, los resultados obtenidos y las limitaciones del análisis. En materia de IA, el perito adquiere una función esencial porque debe traducir la complejidad técnica a un lenguaje comprensible para el juez y para las partes. Furingo (2025) destaca que, en pruebas de IA, un experto debe explicar las técnicas y métodos utilizados, especialmente cuando se trata de conceptos abstractos como algoritmos (p. 121).

La validación jurídica, finalmente, exige que el resultado cumpla las reglas procesales de admisibilidad, legalidad, pertinencia, cadena de custodia, contradicción y valoración racional. El COIP establece que la cadena de custodia se aplica a elementos físicos o contenido digital para garantizar autenticidad, identidad y estado original, incluyendo las condiciones y personas que intervienen en la recolección, envío, manejo, análisis y conservación (COIP, 2014, art. 456). Asimismo, dispone que la valoración de la prueba debe considerar legalidad, autenticidad, cadena de custodia y aceptación científica y

ISBN: 978-631-6557-82-7

técnica de los principios en que se fundamenten los informes periciales (COIP, 2014, art. 457).

Estas reglas son decisivas para la IA probatoria. Si un resultado algorítmico no puede ser explicado, no se conoce su metodología, no existe cadena de custodia sobre los datos, no se sabe qué sistema fue empleado o no puede ser contradicho por la defensa, su valor probatorio debe ser limitado o incluso excluido, según la gravedad de la afectación.

Tabla 18 Niveles de validación de resultados generados por IA

Nivel de validación	Pregunta central	Elementos que deben verificarse
Técnica	¿El sistema funciona de manera fiable para el propósito utilizado?	Software, versión, datos, parámetros, margen de error y metodología
Pericial	¿Un experto puede explicar y defender el resultado?	Informe técnico, explicación oral, limitaciones y respuesta a contradicción
Jurídica	¿El resultado puede ingresar y valorarse válidamente en el proceso?	Legalidad, pertinencia, cadena de custodia, contradicción y motivación

La tabla resume la triple exigencia que debe cumplir la IA probatoria. La validez técnica no basta si no existe control pericial; y la explicación pericial no basta si la obtención o incorporación procesal fue ilegal. El resultado algorítmico solo puede tener fuerza probatoria cuando supera los tres niveles de validación.

3.8 Conclusión del capítulo

La inteligencia artificial puede desempeñar un papel importante como herramienta probatoria en el proceso penal, especialmente en el análisis de evidencia digital, imágenes, videos, audios, documentos, metadatos, datos biométricos, geolocalización, ciberdelincuencia, delitos económicos y detección de deepfakes. Sin embargo, su utilidad técnica no equivale automáticamente a validez jurídica.

ISBN: 978-631-6557-82-7

El análisis desarrollado permite afirmar que la IA no debe ser considerada un medio de prueba autónomo ni una fuente absoluta de verdad. En el sistema ecuatoriano, sus resultados deben ingresar al proceso mediante los medios de prueba reconocidos por el COIP: documento, testimonio o pericia. En la mayoría de casos, su tratamiento adecuado requerirá prueba pericial, especialmente cuando sea necesario explicar metodología, datos, algoritmos, margen de error, fiabilidad y limitaciones.

La distinción entre fuente de prueba, medio de prueba, evidencia digital y resultado algorítmico resulta fundamental. La fuente puede ser un dispositivo, archivo, cámara, base de datos o registro; el medio de prueba es la vía legal de incorporación; la evidencia digital es la información tecnológica relevante; y el resultado algorítmico es la inferencia producida por la IA. Confundir estas categorías puede generar errores de admisibilidad y valoración.

La IA puede fortalecer la investigación penal, pero también puede afectar garantías si se utiliza sin control. Por ello, los resultados generados mediante sistemas inteligentes deben someterse a validación técnica, pericial y jurídica. Deben ser explicables, auditables, trazables, sometidos a cadena de custodia, discutibles por la defensa y valorados racionalmente por el juez.

En definitiva, la inteligencia artificial puede contribuir a la actividad probatoria penal solo si permanece subordinada al derecho. La tecnología no reemplaza la prueba; la procesa, la organiza o la analiza. La decisión sobre su valor corresponde al juez, bajo las reglas de la sana crítica, el debido proceso y la presunción de inocencia.

CAPÍTULO IV.

Admisibilidad, fiabilidad y desafíos jurídicos de la prueba asistida por inteligencia artificial

ISBN: 978-631-6557-82-7

CAPÍTULO IV.

4 Admisibilidad, fiabilidad y desafíos jurídicos de la prueba asistida por inteligencia artificial

La admisibilidad de la prueba asistida por inteligencia artificial constituye uno de los problemas más complejos del proceso penal contemporáneo. La dificultad no radica únicamente en determinar si un resultado generado o procesado mediante IA puede ser incorporado al juicio, sino en establecer en qué condiciones jurídicas, técnicas y procesales puede ser considerado válido, fiable y respetuoso de las garantías del debido proceso.

En el proceso penal, la prueba no puede ser admitida solo porque resulte útil para esclarecer un hecho. Su incorporación exige legalidad, pertinencia, utilidad, conducencia, autenticidad, integridad, cadena de custodia y posibilidad de contradicción. En el caso de la prueba asistida por IA, estos requisitos adquieren mayor relevancia, porque los resultados algorítmicos pueden provenir de sistemas opacos, modelos no auditados, datos incompletos, bases sesgadas o procedimientos técnicamente difíciles de comprender para jueces, fiscales, defensores y víctimas.

La inteligencia artificial puede ayudar a detectar patrones, analizar grandes volúmenes de información, examinar audios, videos, imágenes, metadatos, documentos digitales o incluso advertir posibles manipulaciones mediante deepfakes. Sin embargo, esa utilidad técnica no implica aceptación automática. En materia penal, el uso de IA debe superar un control reforzado, pues su resultado puede influir en decisiones que afecten la libertad personal, la presunción de inocencia, la intimidad, la protección de datos personales y el derecho a la defensa.

Este capítulo analiza los criterios de admisibilidad, fiabilidad y control jurídico de la prueba asistida por inteligencia artificial. Para ello se examinan los requisitos generales de admisión probatoria, la legalidad en la obtención de datos, la pertinencia y utilidad del resultado algorítmico, la fiabilidad técnica, el margen de error, el control de sesgos, la explicabilidad, la trazabilidad, la auditoría, la cadena de custodia digital y los principales

ISBN: 978-631-6557-82-7

riesgos procesales derivados de falsos positivos, opacidad, discriminación y sobrevaloración tecnológica.

La incorporación de inteligencia artificial al ámbito probatorio penal exige un examen riguroso de admisibilidad y fiabilidad. No basta con que el sistema tecnológico produzca un resultado aparentemente útil o técnicamente sofisticado; dicho resultado debe cumplir condiciones jurídicas y técnicas que permitan su incorporación legítima al proceso. En este sentido, la prueba asistida por IA debe ser analizada a partir de criterios como la legalidad en la obtención de la información, la pertinencia respecto de los hechos investigados, la utilidad procesal, la autenticidad del dato, la fiabilidad técnica del sistema, la explicabilidad del método, la trazabilidad del procedimiento, la posibilidad de contradicción, la cadena de custodia y la valoración judicial motivada.

En este contexto, la siguiente figura resume los principales criterios de admisibilidad y fiabilidad que deben observarse para que la prueba asistida por inteligencia artificial pueda ser utilizada válidamente dentro del proceso penal, en armonía con las garantías del debido proceso y la sana crítica judicial.

Figura 4 Criterios de admisibilidad y fiabilidad de la prueba asistida por IA

ISBN: 978-631-6557-82-7

4.1 Criterios de admisibilidad de la prueba asistida por IA

La admisibilidad probatoria es el primer filtro jurídico que permite determinar si un elemento puede ingresar válidamente al proceso penal. En el caso de la prueba asistida por inteligencia artificial, este filtro debe ser particularmente riguroso, porque no se trata de una prueba tradicional, sino de un resultado que puede haber sido producido mediante sistemas automatizados, modelos estadísticos, aprendizaje automático o herramientas de análisis digital.

En el sistema penal ecuatoriano, la prueba debe estar vinculada con los hechos materia del proceso y con la responsabilidad penal que se pretende demostrar. El Código Orgánico Integral Penal establece que la finalidad de la prueba es llevar a la o al juzgador al convencimiento sobre los hechos, las circunstancias de la infracción y la responsabilidad de la persona procesada (COIP, 2014, art. 453). Por tanto, una prueba asistida por IA solo debe ser admitida si contribuye de manera legítima y concreta al esclarecimiento de hechos penalmente relevantes.

La admisibilidad exige, en primer lugar, legalidad. El resultado generado por IA no puede provenir de datos obtenidos ilícitamente, de accesos no autorizados, de vulneraciones a la intimidad, de interceptaciones ilegales, de tratamientos indebidos de datos personales o de manipulaciones de evidencia digital. La utilidad investigativa no sanea la ilicitud de origen.

En segundo lugar, exige pertinencia. El resultado algorítmico debe guardar relación directa o indirecta con el hecho investigado. No sería admisible, por ejemplo, incorporar análisis masivos de datos personales si estos no tienen conexión real con el objeto del proceso. El uso de IA no puede convertirse en una excusa para ampliar ilimitadamente la investigación penal.

En tercer lugar, exige utilidad. La prueba debe aportar información relevante y no simplemente repetir datos ya conocidos o generar resultados innecesarios. La sofisticación tecnológica no equivale a utilidad procesal. Un informe asistido por IA puede ser técnicamente complejo y, aun así, procesalmente inútil si no contribuye a esclarecer el hecho.

ISBN: 978-631-6557-82-7

En cuarto lugar, exige conducencia. El medio utilizado debe ser idóneo para demostrar aquello que se pretende acreditar. Un sistema de reconocimiento facial puede servir para orientar una hipótesis investigativa, pero no necesariamente para demostrar de manera concluyente la identidad de una persona. Una herramienta de IA puede detectar patrones financieros, pero eso no equivale automáticamente a probar lavado de activos, fraude o corrupción.

La admisibilidad exige posibilidad de contradicción. Si las partes no pueden conocer, examinar y discutir el origen de los datos, el método utilizado, el sistema aplicado y las limitaciones del resultado, la prueba asistida por IA pierde legitimidad procesal. La contradicción no puede reducirse a discutir una conclusión ya cerrada por una máquina.

Tabla 19 Criterios mínimos de admisibilidad de prueba asistida por IA

Criterio	Pregunta de control	Exigencia procesal
Legalidad	¿Los datos y resultados fueron obtenidos conforme a la Constitución y la ley?	Excluir elementos obtenidos con vulneración de derechos
Pertinencia	¿El resultado se relaciona con los hechos materia del proceso?	Evitar análisis masivos o irrelevantes
Utilidad	¿El resultado aporta información necesaria para el caso?	Impedir prueba redundante o innecesaria
Conducencia	¿La IA es idónea para demostrar lo que se pretende probar?	Evitar inferencias técnicas desproporcionadas
Contradicción	¿Las partes pueden examinar y cuestionar el resultado?	Garantizar acceso suficiente a metodología, datos y pericia

La tabla muestra que la admisibilidad de la prueba asistida por IA no puede depender solo de su novedad tecnológica. Cada resultado debe superar controles jurídicos concretos. La IA puede facilitar el análisis probatorio, pero no elimina las exigencias propias del proceso penal.

ISBN: 978-631-6557-82-7

4.2 Legalidad en la obtención de datos y evidencias digitales

La legalidad en la obtención de datos constituye el punto de partida de toda prueba asistida por inteligencia artificial. Los sistemas inteligentes trabajan con información: imágenes, videos, audios, textos, metadatos, registros de ubicación, datos biométricos, comunicaciones, archivos, bases de datos o patrones de comportamiento. Si esos datos fueron obtenidos de manera ilícita, el resultado producido por la IA queda contaminado desde su origen.

El principio de exclusión probatoria impide que el Estado obtenga ventajas procesales a partir de vulneraciones de derechos. En materia penal, la obtención de evidencia digital puede implicar acceso a dispositivos electrónicos, cuentas personales, comunicaciones privadas, servidores, sistemas informáticos, redes sociales, bases de datos institucionales o información sensible. Cada uno de estos supuestos exige base legal suficiente y, cuando corresponda, autorización judicial.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos reconoce valor jurídico a los mensajes de datos. Su artículo 2 dispone que “los mensajes de datos tendrán igual valor jurídico que los documentos escritos” y que su eficacia, valoración y efectos se someten a la ley y su reglamento (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, art. 2). Esta regla es relevante porque permite reconocer valor jurídico a la información digital, pero no elimina la necesidad de verificar su origen, integridad y legalidad.

La misma ley establece que, cuando se requiera presentar o conservar información en su forma original, este requisito se cumple con un mensaje de datos si puede comprobarse que ha conservado la integridad de la información desde que fue generado por primera vez en su forma definitiva (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, art. 7). Esta disposición resulta especialmente útil para el proceso penal, porque conecta el valor jurídico del mensaje de datos con la integridad de su contenido.

En el ámbito de la IA probatoria, la legalidad no se limita al archivo final. También debe examinarse el origen de los datos utilizados para producir el resultado. Por ejemplo, si una herramienta de IA analiza rostros, debe determinarse si las imágenes fueron obtenidas

ISBN: 978-631-6557-82-7

lícitamente; si analiza comunicaciones, debe verificarse si existió autorización legal; si procesa datos biométricos, debe revisarse si el tratamiento cumple las normas de protección de datos; y si examina metadatos, debe establecerse si su extracción respetó derechos fundamentales.

La legalidad también exige proporcionalidad. No todo tratamiento de datos es admisible por el solo hecho de servir a una investigación penal. El Estado debe justificar la necesidad de acceder a determinada información, demostrar su relación con el caso y evitar afectaciones excesivas a personas no vinculadas con el proceso. La IA incrementa este riesgo porque permite analizar información masiva con gran rapidez, lo que puede facilitar investigaciones invasivas si no existen límites claros.

Por tanto, una prueba asistida por IA será legalmente admisible solo si los datos de entrada fueron obtenidos conforme a la Constitución, la ley y las garantías procesales. Si los datos son ilícitos, el resultado algorítmico no debe ingresar al proceso o debe ser excluido, según corresponda.

4.3 Pertinencia, utilidad y conducencia del resultado generado por IA

La pertinencia, utilidad y conducencia son criterios que permiten evitar que la prueba asistida por IA se convierta en una fuente de información excesiva, confusa o desvinculada del caso penal. Estos criterios cumplen una función de racionalización probatoria.

La pertinencia exige que el resultado generado por IA se relacione con los hechos investigados. En un proceso penal no se puede incorporar cualquier dato por el simple hecho de haber sido procesado tecnológicamente. Una herramienta de IA puede detectar relaciones, coincidencias o patrones, pero esos resultados deben tener conexión real con la infracción investigada y con la posible responsabilidad de la persona procesada.

La utilidad exige que el resultado aporte algo relevante. Si el informe algorítmico no contribuye a aclarar los hechos, no permite contrastar una hipótesis o no añade información significativa, su incorporación puede ser innecesaria. En materia de IA, este criterio es importante porque existe el riesgo de presentar grandes cantidades de datos procesados que impresionen por volumen, pero que no tengan verdadera relevancia probatoria.

ISBN: 978-631-6557-82-7

La conducencia exige idoneidad. El resultado debe ser apto para demostrar el hecho que se pretende probar. Por ejemplo, una herramienta de análisis de voz puede aportar información sobre similitudes acústicas, pero no necesariamente demostrar identidad plena. Un sistema de detección de deepfake puede advertir señales de manipulación, pero no determinar por sí solo la autoría de la falsificación. Un algoritmo de análisis financiero puede identificar operaciones atípicas, pero no demostrar automáticamente dolo o participación criminal.

Santiago de León (2026) señala que la jurisprudencia latinoamericana ha comenzado a desarrollar criterios sobre admisibilidad, autenticidad y valoración de la prueba digital, destacando tres ejes: autenticidad, cadena de custodia y valor probatorio. Esta sistematización permite sostener que la prueba digital, incluida la asistida por IA, requiere un control que vaya más allá de la simple admisión formal.

La prueba asistida por IA también debe ser valorada dentro del conjunto probatorio. Un resultado aislado puede orientar, pero no necesariamente acreditar. La responsabilidad penal exige una construcción probatoria integral. Por ello, los resultados algorítmicos deben ser corroborados con otros medios de prueba, como testimonios, documentos, pericias, registros técnicos, informes forenses o evidencia material.

Tabla 20 Diferencia entre pertinencia, utilidad y conducencia en la prueba asistida por IA

Criterio	Alcance	Ejemplo aplicado a IA
Pertinencia	Relación con los hechos investigados	Un análisis de metadatos es pertinente si se relaciona con fecha, lugar o autoría del hecho
Utilidad	Aporte real al esclarecimiento del caso	Una clasificación automatizada es útil si permite identificar información relevante no conocida
Conducencia	Idoneidad para demostrar lo que se pretende probar	Un sistema facial puede orientar identificación, pero requiere corroboración pericial

ISBN: 978-631-6557-82-7

La tabla permite diferenciar tres exigencias que suelen confundirse. Una prueba puede ser pertinente, pero no útil; o útil, pero no conducente para demostrar una afirmación específica. En IA probatoria, esta distinción es esencial para evitar la sobrevaloración de resultados técnicos.

4.4 Fiabilidad técnica, margen de error y control de sesgos algorítmicos

La fiabilidad técnica es uno de los requisitos más importantes para valorar la prueba asistida por inteligencia artificial. Un resultado algorítmico solo puede tener relevancia probatoria si el sistema utilizado es confiable para el propósito específico para el cual fue empleado. No basta con afirmar que una herramienta es moderna, avanzada o ampliamente utilizada. Debe demostrarse que funciona adecuadamente en el contexto concreto del caso.

La fiabilidad exige identificar el software utilizado, su versión, el proveedor, el modelo, los parámetros aplicados, los datos de entrada, la metodología de análisis, los criterios de salida y las limitaciones conocidas. También debe indicarse si el sistema fue entrenado con datos adecuados, si ha sido validado, si existen estudios sobre su rendimiento y si ha sido sometido a auditorías o pruebas independientes.

En materia de prueba científica, Furingo (2025) recoge criterios de validez que resultan útiles para la prueba asistida por IA: la técnica debe ser verificable, haber sido publicada y sometida a revisión por pares, especificar margen de error y estándares de desarrollo, y gozar de aceptación en la comunidad científica. Aunque estos criterios no son una regla legal ecuatoriana expresa, ofrecen un marco razonable para evaluar la fiabilidad de sistemas inteligentes utilizados con finalidad probatoria.

El margen de error es particularmente relevante. Todo sistema de IA puede equivocarse. Un reconocimiento facial puede producir falsos positivos; una herramienta de transcripción puede alterar el sentido de una conversación; un sistema de detección de deepfake puede no identificar una manipulación sofisticada; un algoritmo de clasificación puede asignar erróneamente relevancia a un dato. Si el margen de error no se conoce o no se informa, el juez y las partes no pueden valorar adecuadamente la fuerza del resultado.

ISBN: 978-631-6557-82-7

El control de sesgos también es indispensable. Los sistemas de IA aprenden de datos. Si esos datos reflejan desigualdades, errores históricos, prácticas discriminatorias o falta de representatividad, el sistema puede reproducir o amplificar esos sesgos. En materia penal, esto puede traducirse en identificaciones erróneas, perfilamientos indebidos, vigilancia selectiva o afectación desproporcionada a determinados grupos.

La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO advierte que las tecnologías de IA pueden incorporar y exacerbar sesgos, generando discriminación, desigualdad, exclusión y afectaciones a derechos humanos y libertades fundamentales (UNESCO, 2021). Esta advertencia debe ser trasladada al proceso penal, donde un sesgo algorítmico no es solo un problema técnico, sino una posible vulneración de garantías procesales.

Tabla 21 Elementos de fiabilidad técnica en prueba asistida por IA

Elemento	Pregunta de control	Relevancia procesal
Identificación del sistema	¿Qué herramienta, versión y proveedor fueron utilizados?	Permite verificar origen y características del análisis
Metodología	¿Cómo se procesaron los datos?	Permite revisar si el procedimiento fue adecuado
Datos de entrada	¿Qué información fue analizada?	Permite controlar legalidad, pertinencia y calidad
Margen de error	¿Cuál es la tasa de error conocida?	Permite medir fuerza probatoria del resultado
Sesgos	¿El sistema presenta riesgos de discriminación o falsos positivos?	Protege igualdad y presunción de inocencia
Validación externa	¿El sistema ha sido probado o auditado?	Refuerza confiabilidad técnica

La tabla sintetiza los elementos mínimos que deberían revisarse antes de atribuir valor probatorio a un resultado asistido por IA. Sin esta información, la prueba se vuelve opaca y su valoración puede convertirse en un acto de confianza injustificada en la tecnología.

ISBN: 978-631-6557-82-7

4.5 Explicabilidad, trazabilidad, auditoría y reproducibilidad del procedimiento

La explicabilidad, trazabilidad, auditoría y reproducibilidad son requisitos esenciales para que una prueba asistida por IA pueda ser sometida a contradicción y valoración racional. Estos criterios permiten abrir la "caja negra" tecnológica y transformar un resultado algorítmico en un objeto procesal discutible.

La explicabilidad implica que el funcionamiento general del sistema y el camino seguido para obtener el resultado puedan ser comprendidos por las partes y por el juez en un nivel suficiente. No significa que todos los operadores jurídicos deban dominar programación, estadística o ciencia de datos; significa que el perito debe poder explicar qué hizo la herramienta, con qué datos, bajo qué parámetros, con qué limitaciones y con qué grado de confianza.

La trazabilidad supone que el procedimiento pueda reconstruirse desde el inicio hasta el resultado final. En materia de prueba digital, esto incluye identificar la fuente original, el momento de recolección, el método de extracción, las personas que intervinieron, los sistemas utilizados, los archivos generados, las modificaciones realizadas y los mecanismos de preservación. Sin trazabilidad, no es posible verificar si el resultado corresponde realmente al dato original.

La auditoría permite revisar el sistema o el procedimiento aplicado. Puede ser interna o externa, previa o posterior, técnica o institucional. En el proceso penal, la auditoría resulta fundamental cuando se pretende utilizar herramientas que influyen en la identificación de personas, la autenticidad de evidencia, la reconstrucción de hechos o la evaluación de patrones.

La reproducibilidad exige que, bajo condiciones equivalentes, el procedimiento pueda ser replicado para verificar si produce resultados similares. Este criterio es importante para evitar que la prueba dependa de una operación irrepetible, no documentada o técnicamente incontrolable. Si el resultado no puede reproducirse o verificarse, su valor probatorio debe ser limitado.

ISBN: 978-631-6557-82-7

La UNESCO sostiene que los sistemas de IA utilizados en contextos sensibles, como la aplicación de la ley y el sistema judicial, deben contar con mecanismos de supervisión adecuados y salvaguardias para garantizar derechos humanos, Estado de derecho, independencia judicial y supervisión humana (UNESCO, 2021). Esta orientación permite afirmar que la explicabilidad y la auditoría no son simples exigencias técnicas, sino garantías procesales.

En materia penal, un resultado no explicable puede afectar el derecho de defensa. La defensa no puede contradecir aquello que no puede conocer ni comprender. Si el sistema no permite identificar los datos utilizados, los criterios aplicados o las razones del resultado, la contradicción se vuelve ilusoria.

Tabla 22 Requisitos de control técnico-procesal

Requisito	Función	Consecuencia de su ausencia
Explicabilidad	Permite comprender el resultado	Debilita la contradicción y la defensa
Trazabilidad	Permite reconstruir el procedimiento	Afecta autenticidad e integridad
Auditoría	Permite revisar sistema y metodología	Impide control independiente
Reproducibilidad	Permite verificar el resultado	Reduce fiabilidad probatoria
Supervisión humana	Evita automatización decisoria	Riesgo de delegar funciones judiciales en la máquina

Esta tabla permite observar que la prueba asistida por IA requiere un control integral. El problema no se resuelve únicamente con presentar un informe final. Es necesario documentar todo el procedimiento, permitir su revisión y asegurar que el resultado sea comprensible y discutible.

ISBN: 978-631-6557-82-7

4.6 Cadena de custodia digital y preservación de la evidencia tecnológica

La cadena de custodia digital es uno de los principales mecanismos para garantizar la autenticidad, integridad y trazabilidad de la evidencia tecnológica. En el contexto de la inteligencia artificial, su importancia aumenta porque los sistemas inteligentes suelen trabajar con archivos digitales, metadatos, bases de datos, imágenes, audios, videos, documentos electrónicos o registros informáticos que pueden ser alterados, duplicados, comprimidos, editados o manipulados.

El COIP establece que la cadena de custodia se aplica a elementos físicos o contenido digital materia de prueba, con el fin de garantizar su autenticidad, identidad y estado original, así como las condiciones, personas y cambios que intervienen en su recolección, envío, manejo, análisis y conservación (COIP, 2014, art. 456). Esta regla es fundamental para cualquier prueba asistida por IA, porque permite verificar que los datos analizados corresponden efectivamente a la fuente original.

La cadena de custodia inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Esta continuidad permite demostrar que la evidencia no fue alterada indebidamente. En evidencia digital, ello implica preservar el archivo original, documentar copias forenses, identificar dispositivos, registrar hashes, conservar metadatos, evitar modificaciones y controlar el acceso a los soportes tecnológicos.

El COIP también establece que el análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos debe realizarse mediante técnicas digitales forenses (COIP, 2014, art. 500). Esta disposición es decisiva, porque la prueba digital no debe ser manipulada de manera informal. Su tratamiento exige herramientas, procedimientos y personal especializado.

Los Manuales, Protocolos, Instructivos y Formatos del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses reconocen un área específica de cadena de custodia e incluyen un instructivo para el manejo de indicios y/o evidencia digital (Fiscalía General del Estado, 2014). Este tipo de instrumentos es relevante porque

ISBN: 978-631-6557-82-7

permite trasladar las reglas legales a procedimientos prácticos de recolección, preservación y análisis.

En el caso de evidencia generada o manipulada mediante IA, como deepfakes, la cadena de custodia digital cumple una función adicional: permite comparar el archivo presentado con su fuente original, revisar metadatos, detectar alteraciones, establecer condiciones de obtención y verificar si el contenido fue sometido a análisis técnico adecuado. Adriano-Caiza, Marfetan-Marfetan y Machado-Maliza (2025) sostienen que la cadena de custodia digital prevista en los artículos 456 y 457 del COIP constituye el principal mecanismo de verificación de autenticidad frente a evidencias deepfake.

Tabla 23 Cadena de custodia digital aplicada a prueba asistida por IA

Fase	Actuación necesaria	Finalidad
Recolección	Identificar dispositivo, archivo, ubicación y condiciones de obtención	Determinar origen de la evidencia
Preservación	Crear copia forense, conservar original y registrar hash	Evitar alteración del contenido
Documentación	Registrar custodios, fechas, herramientas y procedimientos	Asegurar trazabilidad
Análisis	Utilizar técnicas digitales forenses y herramientas verificables	Garantizar fiabilidad técnica
Presentación	Explicar metodología, resultados y limitaciones en juicio	Permitir contradicción y valoración

La tabla muestra que la cadena de custodia digital no es una formalidad. Es el mecanismo que conecta la evidencia original con el resultado presentado en juicio. Sin cadena de custodia, la prueba tecnológica pierde fuerza y puede generar dudas razonables sobre su autenticidad o integridad.

ISBN: 978-631-6557-82-7

4.7 Riesgos procesales: falsos positivos, opacidad, discriminación y sobrevaloración tecnológica

La prueba asistida por inteligencia artificial presenta riesgos procesales específicos que deben ser enfrentados desde el derecho probatorio. Entre los más relevantes se encuentran los falsos positivos, la opacidad, la discriminación algorítmica y la sobrevaloración tecnológica.

Los falsos positivos ocurren cuando un sistema identifica erróneamente una coincidencia. En materia penal, este riesgo es especialmente grave. Un sistema de reconocimiento facial puede asociar incorrectamente el rostro de una persona con una imagen de videovigilancia; una herramienta de detección de voz puede sugerir una coincidencia equivocada; un sistema de análisis financiero puede clasificar como sospechosa una operación legítima; o un detector de deepfakes puede identificar manipulación donde no existe. Estos errores pueden orientar indebidamente la investigación o influir en la valoración judicial.

La opacidad algorítmica impide conocer cómo se produjo el resultado. Si el sistema opera como una caja negra, las partes no pueden examinar la calidad de los datos, los criterios de procesamiento, el margen de error o las razones de la conclusión. Esta opacidad afecta directamente la contradicción y el derecho a la defensa.

La discriminación algorítmica se produce cuando el sistema genera resultados diferenciados por sesgos presentes en los datos o en el diseño del modelo. En el proceso penal, este riesgo puede afectar la igualdad ante la ley y la presunción de inocencia, especialmente si se utilizan herramientas predictivas, biométricas o de perfilamiento.

La sobrevaloración tecnológica surge cuando jueces, fiscales o partes atribuyen a la IA un grado de certeza superior al que realmente posee. El hecho de que un resultado sea producido por un sistema automatizado no significa que sea infalible. La tecnología puede errar, sesgarse, depender de datos defectuosos o producir inferencias no justificadas.

Adriano-Caiza et al. (2025) advierten que el COIP carece de regulación específica sobre evidencias generadas con inteligencia artificial y que existe una brecha significativa

ISBN: 978-631-6557-82-7

entre el avance tecnológico deepfake y la capacidad institucional ecuatoriana de detección. Esta observación evidencia que el sistema penal enfrenta una tensión entre innovación tecnológica y suficiencia normativa.

Santiago de León (2026) también señala que la jurisprudencia latinoamericana tiende a reconocer la validez de la prueba digital, pero exige autenticidad, integridad, peritajes informáticos, sana crítica y supervisión humana. Esta tendencia resulta útil para el sistema ecuatoriano, porque permite adoptar una posición equilibrada: no rechazar la prueba tecnológica, pero tampoco aceptarla sin controles.

Tabla 24 Riesgos procesales de la prueba asistida por IA y respuestas jurídicas

Riesgo procesal	Manifestación	Respuesta jurídica
Falsos positivos	Coincidencias erróneas en rostro, voz, patrones o datos	Exigir margen de error, pericia y corroboración
Opacidad	Imposibilidad de conocer cómo se obtuvo el resultado	Exigir explicabilidad y auditoría
Discriminación	Resultados sesgados contra grupos o personas	Evaluar sesgos y datos de entrenamiento
Sobrevaloración tecnológica	Aceptar el resultado como verdad automática	Aplicar sana crítica y motivación reforzada
Debilidad institucional	Falta de protocolos específicos sobre IA	Crear estándares técnicos y jurídicos de admisión

La tabla resume los riesgos que justifican un control reforzado. La inteligencia artificial puede ser útil, pero sus resultados deben ser tratados con prudencia. En materia penal, el error tecnológico no es un simple problema operativo; puede traducirse en una imputación injusta, una medida cautelar indebida o una condena errónea.

4.8 Conclusión del capítulo

La admisibilidad y fiabilidad de la prueba asistida por inteligencia artificial exige un análisis jurídico y técnico riguroso. No basta con que la herramienta sea útil, novedosa o eficiente. En el proceso penal, todo resultado generado o procesado mediante IA debe

ISBN: 978-631-6557-82-7

someterse a controles de legalidad, pertinencia, utilidad, conducencia, autenticidad, integridad, cadena de custodia, fiabilidad técnica, explicabilidad, trazabilidad, auditoría y contradicción.

El marco ecuatoriano ofrece bases normativas importantes, especialmente en el COIP, la Ley de Comercio Electrónico y los instrumentos de cadena de custodia. Sin embargo, todavía existen vacíos específicos respecto al uso de inteligencia artificial como herramienta probatoria, particularmente frente a sistemas opacos, reconocimiento facial, deepfakes, análisis predictivo y procesamiento automatizado de datos.

La cadena de custodia digital y las técnicas forenses constituyen mecanismos indispensables para preservar la autenticidad e integridad de la evidencia tecnológica. No obstante, en el caso de IA, estos mecanismos deben complementarse con exigencias adicionales: identificación del sistema utilizado, explicación metodológica, margen de error, control de sesgos, reproducibilidad, auditoría y validación pericial.

Los riesgos procesales son significativos. Falsos positivos, opacidad, discriminación algorítmica y sobrevaloración tecnológica pueden afectar la presunción de inocencia, el derecho a la defensa, la igualdad de armas y la motivación judicial. Por ello, la prueba asistida por IA no debe ser tratada como prueba concluyente por sí misma, sino como un elemento técnico sujeto a corroboración y valoración conjunta.

En definitiva, la inteligencia artificial puede fortalecer el sistema penal si se utiliza como herramienta auxiliar, transparente y controlada. Pero puede convertirse en una amenaza si se presenta como verdad automática, si no puede ser explicada, si no se conserva adecuadamente la evidencia original o si impide la contradicción efectiva de las partes. La admisibilidad de la IA probatoria debe construirse sobre una regla básica: ninguna tecnología puede estar por encima del debido proceso.

CAPÍTULO V.

Garantías procesales, valoración judicial y protocolo para el uso de IA probatoria

ISBN: 978-631-6557-82-7

CAPÍTULO V.

5 Garantías procesales, valoración judicial y protocolo para el uso de IA probatoria

La incorporación de inteligencia artificial en el sistema penal no puede analizarse únicamente desde la perspectiva de la eficiencia investigativa o de la modernización tecnológica. Su utilización dentro de la actividad probatoria exige una evaluación estricta desde las garantías procesales, especialmente cuando los resultados generados por sistemas algorítmicos pueden influir en la imputación, acusación, admisión de prueba, valoración judicial o motivación de una sentencia penal.

En los capítulos anteriores se ha sostenido que la inteligencia artificial debe ser entendida como una herramienta probatoria auxiliar y no como una fuente autónoma de verdad. Esta afirmación adquiere especial importancia en este capítulo, porque el centro del análisis ya no es solamente la utilidad de la IA, sino las condiciones que deben cumplirse para que su uso no vulnere el derecho a la defensa, la contradicción probatoria, la igualdad de armas, la protección de datos personales, la presunción de inocencia, la motivación judicial y la prohibición de decisiones penales automatizadas.

El sistema penal se legitima no solo por su capacidad para investigar y sancionar delitos, sino por su obligación de hacerlo dentro de límites constitucionales. La inteligencia artificial puede contribuir al análisis de grandes volúmenes de datos, a la detección de patrones, a la identificación de manipulación digital, al reconocimiento de elementos audiovisuales y al apoyo de informes periciales. Sin embargo, cuando su funcionamiento es opaco, no auditado, sesgado o difícilmente explicable, puede convertirse en un riesgo para la justicia penal.

El presente capítulo desarrolla las garantías procesales que deben observarse frente al uso de IA probatoria. Se analiza el derecho a la defensa, la contradicción, la igualdad de armas, la protección de datos personales, la prueba pericial asistida por IA, el interrogatorio y contrainterrogatorio técnico, la sana crítica, la duda razonable, la motivación judicial

ISBN: 978-631-6557-82-7

reforzada, la supervisión humana y, finalmente, se propone un protocolo básico para jueces, fiscales, defensores y peritos.

5.1 Derecho a la defensa, contradicción probatoria e igualdad de armas

El derecho a la defensa constituye una garantía esencial del proceso penal. Su finalidad es impedir que una persona sea sometida a una decisión judicial sin haber tenido oportunidad real de conocer, discutir y refutar los del error del sistema, sino también de la imposibilidad de controlarlo.

Tabla 25 Garantías mínimas de defensa frente a prueba asistida por IA

Garantía	Exigencia concreta	Finalidad procesal
Acceso a la información técnica	Conocer sistema, versión, datos, metodología y parámetros	Preparar defensa material y técnica
Contradicción probatoria	Interrogar al perito y cuestionar el resultado	Evitar aceptación automática de la IA
Igualdad de armas	Permitir revisión independiente o pericia de parte	Equilibrar el debate entre acusación y defensa
Tiempo razonable	Otorgar plazo suficiente para analizar informes complejos	Evitar indefensión técnica
Explicación comprensible	Traducir el resultado técnico a lenguaje jurídico claro	Permitir valoración judicial y contradicción efectiva

La tabla muestra que la defensa frente a prueba asistida por IA no puede ser meramente formal. Para que exista contradicción real, la defensa debe poder comprender el resultado, identificar sus debilidades y presentar argumentos técnicos o jurídicos en contra. La IA no puede convertirse en una barrera de conocimiento que impida el ejercicio efectivo del derecho de defensa.

ISBN: 978-631-6557-82-7

5.2 Protección de datos personales, intimidad y límites frente a la vigilancia masiva

La inteligencia artificial depende del tratamiento de datos. En el sistema penal, estos datos pueden incluir imágenes faciales, huellas, registros de voz, ubicación, comunicaciones, metadatos, videos, documentos, perfiles de comportamiento, información financiera, datos sensibles o datos biométricos. Por ello, el uso de IA probatoria debe someterse no solo a reglas penales, sino también a criterios de protección de datos personales, intimidad y proporcionalidad.

La Ley Orgánica de Protección de Datos Personales reconoce derechos vinculados al acceso, decisión y protección sobre la información personal. En el contexto penal, esto resulta especialmente relevante porque la investigación puede requerir datos personales para esclarecer hechos; sin embargo, ese acceso debe estar sometido a legalidad, necesidad y proporcionalidad. La persecución penal no puede justificar tratamientos indiscriminados o masivos de información personal.

La propia ley reconoce el derecho del titular a ser informado sobre la existencia y forma de hacer efectivos derechos como acceso, eliminación, rectificación, actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas (LOPDP, 2021, art. 12). Aunque el proceso penal tiene particularidades propias, esta regla refleja una preocupación jurídica fundamental: las decisiones automatizadas pueden afectar derechos y, por tanto, requieren control.

La elaboración de perfiles también presenta riesgos relevantes. Cuando un sistema de IA clasifica a una persona según patrones, conductas esperadas, ubicación, relaciones o riesgos, puede generar sospechas basadas en probabilidades y no en hechos individualmente probados. Esto es especialmente peligroso en materia penal, porque puede conducir a vigilancia selectiva, estigmatización o criminalización anticipada.

La protección de datos personales no impide toda investigación tecnológica. Lo que exige es que el tratamiento de datos sea legítimo, necesario, proporcional, limitado a la finalidad investigativa y controlado por autoridad competente. Si se utiliza IA para analizar

ISBN: 978-631-6557-82-7

información de personas no vinculadas al proceso, grandes bases de datos o registros biométricos, el control debe ser más estricto.

La UNESCO (2021) advierte que la transparencia y explicabilidad son condiciones importantes para proteger derechos humanos, y que la falta de transparencia puede afectar la posibilidad de impugnar decisiones basadas en sistemas de IA. Esta orientación se conecta directamente con la protección de datos, porque una persona no puede cuestionar un tratamiento automatizado si desconoce su existencia, finalidad o impacto.

Tabla 26 Riesgos de protección de datos en IA probatoria

Tipo de dato o tratamiento	Riesgo procesal	Garantía necesaria
Datos biométricos	Identificación errónea o vigilancia masiva	Legalidad, autorización y control pericial
Geolocalización	Reconstrucción invasiva de movimientos	Necesidad, proporcionalidad y control judicial
Comunicaciones digitales	Afectación a intimidad y secreto comunicacional	Base legal y autorización cuando corresponda
Perfilamiento algorítmico	Criminalización por patrones de conducta	Prohibición de inferir responsabilidad penal por perfil
Bases de datos masivas	Inclusión de personas no relacionadas con el proceso	Minimización y finalidad específica

La tabla permite observar que la protección de datos no es un tema accesorio, sino un componente central de la prueba asistida por IA. Cuando un sistema procesa información personal para producir un resultado probatorio, el juez debe verificar no solo la utilidad del resultado, sino también la legalidad y proporcionalidad del tratamiento.

ISBN: 978-631-6557-82-7

5.3 Prueba pericial asistida por IA: metodología, datos, parámetros y resultados

La prueba pericial es el medio más adecuado para incorporar al proceso penal resultados complejos generados o analizados mediante inteligencia artificial. Esto se debe a que la IA requiere explicación técnica, validación metodológica y traducción del conocimiento especializado a un lenguaje comprensible para el juez y las partes.

El COIP establece que los peritos deben ser profesionales expertos en el área, especialistas titulados o con conocimientos, experiencia o experticia en la materia, acreditados por el Consejo de la Judicatura (COIP, 2014, art. 511). Esta exigencia resulta fundamental en casos de IA, porque no cualquier operador informático está en capacidad de explicar algoritmos, modelos de aprendizaje automático, análisis de metadatos, reconocimiento facial, detección de deepfakes o procesamiento automatizado de evidencia digital.

El informe pericial debe contener, como mínimo, lugar y fecha de realización del peritaje, identificación del perito, descripción y estado de la persona u objeto peritado, técnica utilizada, fundamentación científica, ilustraciones gráficas cuando correspondan, conclusiones y firma (COIP, 2014, art. 511). En el caso de prueba asistida por IA, estos requisitos deben ampliarse funcionalmente para incluir información sobre el sistema utilizado, versión, proveedor, parámetros, datos de entrada, margen de error, limitaciones y posibilidad de reproducción.

La metodología debe estar claramente descrita. No basta con afirmar que “se utilizó inteligencia artificial”. Esa expresión es demasiado general. El informe debe precisar si se usó reconocimiento facial, análisis de voz, procesamiento de lenguaje natural, detección de manipulación audiovisual, clasificación automatizada de documentos, análisis predictivo o extracción de metadatos. Cada técnica tiene alcances, riesgos y limitaciones distintas.

Los datos utilizados también deben estar identificados. El perito debe explicar qué archivos fueron analizados, de dónde provienen, cómo fueron obtenidos, si se conservaron íntegros, si existe cadena de custodia, si se trabajó sobre copias forenses y si los datos fueron modificados, comprimidos o transformados durante el análisis.

ISBN: 978-631-6557-82-7

Los parámetros del sistema son igualmente relevantes. En muchos sistemas de IA, pequeñas variaciones en los parámetros pueden modificar los resultados. Por ello, el informe debe describir los criterios de configuración utilizados y justificar su pertinencia técnica.

Finalmente, los resultados deben ser expuestos con cautela. Un perito no debe presentar un resultado algorítmico como certeza absoluta si el sistema solo genera probabilidad, coincidencia o indicio técnico. La conclusión pericial debe distinguir entre hallazgos objetivos, inferencias técnicas, márgenes de error y limitaciones del análisis.

Tabla 27 Contenido mínimo recomendado para informes periciales asistidos por IA

Elemento del informe	Contenido recomendado	Justificación
Identificación del sistema	Nombre, versión, proveedor y tipo de IA utilizada	Permite verificar la herramienta aplicada
Datos analizados	Fuente, formato, origen y cadena de custodia	Permite controlar legalidad e integridad
Metodología	Procedimiento técnico seguido	Permite reproducibilidad y contradicción
Parámetros	Configuración, umbrales y criterios técnicos	Permite evaluar la confiabilidad del resultado
Margen de error	Tasa de error conocida o limitaciones del sistema	Permite valorar fuerza probatoria
Resultados	Hallazgos, inferencias y conclusiones	Evita confundir probabilidad con certeza
Limitaciones	Riesgos, restricciones y condiciones del análisis	Permite valoración prudente

La tabla permite construir un estándar mínimo para informes periciales asistidos por IA. Su finalidad no es burocratizar la pericia, sino asegurar que el resultado pueda ser comprendido, auditado y discutido. En materia penal, la falta de claridad metodológica puede traducirse en indefensión.

ISBN: 978-631-6557-82-7

5.4 Interrogatorio, contrainterrogatorio y contradicción técnica del informe pericial

El informe pericial no debe ser valorado como un documento aislado. En el proceso penal, la pericia adquiere verdadera fuerza en la audiencia, cuando el perito sustenta oralmente sus conclusiones y responde al interrogatorio y contrainterrogatorio de los sujetos procesales. Esta dinámica es esencial para la contradicción probatoria.

El COIP dispone que los peritos deben comparecer a la audiencia de juicio, sustentar oralmente sus informes y contestar los interrogatorios de las partes (COIP, 2014, art. 511). Esta regla es particularmente importante en pruebas asistidas por IA, porque la audiencia permite transformar un informe técnico complejo en un debate comprensible y controlable.

El interrogatorio directo permite que la parte que presenta la pericia aclare el objeto del análisis, la metodología utilizada, la idoneidad del perito, los datos examinados, el funcionamiento de la herramienta y las conclusiones alcanzadas. En el caso de IA, el interrogatorio debe evitar respuestas generales. El perito debe explicar concretamente qué hizo la herramienta y qué hizo el experto humano.

El contrainterrogatorio cumple una función garantista. Permite cuestionar la fiabilidad del sistema, la calidad de los datos, la cadena de custodia, la falta de auditoría, el margen de error, los sesgos, las limitaciones metodológicas, la ausencia de reproducibilidad o la interpretación excesiva de los resultados. En materia de IA, el contrainterrogatorio debe dirigirse tanto al procedimiento técnico como a la conclusión jurídica que se pretende derivar de él.

La contradicción técnica puede exigir la participación de peritos de parte o consultores especializados. La defensa no siempre podrá cuestionar adecuadamente un informe de IA sin apoyo técnico. Por ello, el juez debe garantizar condiciones razonables para que la defensa pueda analizar el informe, preparar preguntas y, de ser necesario, solicitar una pericia independiente.

Los Manuales, Protocolos, Instructivos y Formatos del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses destacan que la preparación

ISBN: 978-631-6557-82-7

de la defensa técnica del informe pericial en audiencia es una fase fundamental, pues no solo se trata de dar cuenta del contenido literal del informe, sino de exponer los alcances de la investigación y la opinión profesional con manejo teórico (Fiscalía General del Estado, 2014). Esta idea puede aplicarse plenamente a la IA probatoria: el perito debe explicar no solo el resultado, sino el proceso.

Tabla 28 Preguntas guía para contradicción técnica de prueba asistida por IA

Área de control	Preguntas sugeridas
Idoneidad del perito	¿Cuál es su formación específica en IA, informática forense o análisis digital?
Sistema utilizado	¿Qué herramienta se usó, qué versión y con qué validación técnica?
Datos de entrada	¿De dónde provienen los datos y cómo se preservó su integridad?
Metodología	¿El procedimiento puede ser reproducido por otro experto?
Margen de error	¿Cuál es la tasa de error conocida y cómo afecta el resultado?
Sesgos	¿El sistema ha sido evaluado frente a sesgos o falsos positivos?
Conclusión	¿El resultado es certeza, probabilidad, coincidencia o simple indicio?

La tabla tiene una función práctica: orientar el debate procesal. En casos de IA probatoria, el juez, el fiscal y la defensa deben evitar que la audiencia se limite a ratificar el informe. La audiencia debe servir para examinar críticamente la prueba, revelar sus límites y permitir una valoración racional.

5.5 Sana crítica, duda razonable y motivación judicial reforzada

La valoración judicial de la prueba asistida por IA debe realizarse conforme a la sana crítica, la presunción de inocencia y el estándar de duda razonable. El juez no puede aceptar un resultado algorítmico por su sola apariencia técnica. Debe examinar su legalidad, autenticidad, cadena de custodia, fiabilidad, aceptación científica, contradicción y relación con el conjunto probatorio.

ISBN: 978-631-6557-82-7

El COIP establece que la valoración de la prueba debe considerar legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales (COIP, 2014, art. 457). Esta regla ofrece una base clara para valorar prueba asistida por IA. Si el sistema utilizado no posee aceptación técnica suficiente, no ha sido explicado o no permite contradicción, su valor probatorio debe ser reducido.

La duda razonable adquiere especial importancia cuando existen resultados tecnológicos no concluyentes. Un reconocimiento facial con margen de error relevante, un detector de deepfake no validado, una inferencia basada en datos incompletos o un análisis algorítmico opaco no pueden servir como fundamento suficiente de condena. La responsabilidad penal exige prueba robusta, no sospechas tecnificadas.

La motivación judicial también debe ser reforzada. Cuando el juez valora prueba asistida por IA, debe explicar por qué considera fiable el resultado, cómo fue incorporado, qué garantías se respetaron, qué objeciones formuló la defensa, cómo fueron respondidas y de qué manera se relaciona la prueba tecnológica con los demás elementos del proceso.

La Corte Constitucional del Ecuador, en la sentencia 1158-17-EP/21, estableció que una argumentación jurídica suficiente debe contar con una estructura mínimamente completa, integrada por fundamentación normativa suficiente y fundamentación fáctica suficiente (Corte Constitucional del Ecuador, 2021, sentencia No. 1158-17-EP/21). Este estándar es relevante para la IA probatoria, porque una sentencia que valore resultados algorítmicos debe explicar tanto las normas aplicables como los hechos y elementos técnicos que justifican su valoración.

En materia penal, la motivación debe ser especialmente cuidadosa cuando la prueba tecnológica incide en la identificación de una persona, la autenticidad de evidencia digital, la reconstrucción de hechos o la existencia de patrones. La decisión judicial no puede limitarse a señalar que “el sistema determinó” o “la IA concluyó”. El juez debe motivar por qué ese resultado es confiable y suficiente dentro del conjunto probatorio.

ISBN: 978-631-6557-82-7

Tabla 29 Elementos de motivación judicial reforzada en prueba asistida por IA

Elemento	Pregunta que debe responder la sentencia
Legalidad	¿La prueba fue obtenida conforme a la Constitución y la ley?
Autenticidad	¿Se acreditó que el archivo, dato o resultado corresponde al original?
Cadena de custodia	¿Se preservó adecuadamente la evidencia digital?
Fiabilidad técnica	¿El sistema utilizado es confiable y aceptado técnicamente?
Contradicción	¿La defensa pudo cuestionar el resultado y al perito?
Corroboración	¿El resultado fue confirmado por otros elementos probatorios?
Duda razonable	¿El resultado supera las dudas planteadas por la defensa?

La tabla muestra que la motivación judicial frente a IA probatoria debe ser concreta. No basta con una referencia genérica a la prueba pericial. El juez debe demostrar que comprendió el alcance técnico del resultado y que lo valoró de manera crítica, no automática.

5.6 Prohibición de decisiones penales automatizadas y necesidad de supervisión humana

Uno de los límites más importantes frente al uso de inteligencia artificial en el sistema penal es la prohibición de decisiones penales automatizadas. La IA puede asistir, ordenar información, sugerir coincidencias, detectar patrones o apoyar pericias, pero no puede sustituir la decisión humana de fiscales, jueces o tribunales.

La decisión penal exige responsabilidad institucional, valoración jurídica, análisis de garantías, motivación y control público. Un sistema automatizado no puede asumir responsabilidad ética ni jurídica por la privación de libertad de una persona. Tampoco puede ponderar adecuadamente circunstancias humanas, contextuales, probatorias y normativas con la legitimidad que corresponde a la función judicial.

La UNESCO (2021) establece que siempre debe ser posible atribuir responsabilidad ética y jurídica a personas físicas o entidades jurídicas existentes durante el ciclo de vida de

ISBN: 978-631-6557-82-7

los sistemas de IA. Además, señala que los sistemas de IA nunca deben reemplazar la responsabilidad final de los seres humanos ni su obligación de rendir cuentas. Este principio es plenamente aplicable al proceso penal.

La supervisión humana no debe ser simbólica. No basta con que una persona apruebe automáticamente lo que el sistema propone. La supervisión debe ser significativa, es decir, debe incluir capacidad real de revisión, comprensión, corrección, rechazo y explicación del resultado. Si el operador humano se limita a confirmar la conclusión de la IA sin análisis crítico, la supervisión se convierte en una formalidad.

La prohibición de decisiones automatizadas también se vincula con la Ley Orgánica de Protección de Datos Personales, que reconoce el derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas (LOPDP, 2021, art. 12). En materia penal, este principio debe tener una lectura aún más estricta: ninguna imputación, acusación, medida cautelar, sentencia o valoración decisiva puede fundarse exclusivamente en resultados automatizados.

Esto no impide el uso de IA en el proceso penal. Lo que impide es delegar la responsabilidad decisoria. La IA puede ser una herramienta de apoyo a la investigación o a la pericia, pero la decisión debe permanecer bajo control humano, jurídico y judicial.

Tabla 30 Diferencia entre asistencia tecnológica y decisión automatizada

Uso permitido	Uso prohibido o altamente riesgoso
IA como apoyo para organizar evidencia	IA como fundamento exclusivo de imputación
IA como herramienta auxiliar del perito	IA sustituyendo la explicación pericial
IA para detectar posibles patrones	IA atribuyendo responsabilidad penal por perfil
IA para alertar sobre manipulación digital	IA determinando autenticidad sin revisión humana
IA como insumo para valoración judicial	IA reemplazando la motivación del juez

ISBN: 978-631-6557-82-7

La tabla permite diferenciar entre un uso legítimo y un uso incompatible con el debido proceso. El problema no es la tecnología en sí, sino la delegación indebida de funciones humanas esenciales en un sistema automatizado.

5.7 Propuesta de protocolo para jueces, fiscales, defensores y peritos

La ausencia de regulación específica sobre inteligencia artificial probatoria obliga a construir criterios mínimos de actuación para los operadores del sistema penal. Estos criterios no sustituyen la necesidad de una reforma normativa, pero pueden servir como protocolo básico de control jurídico y técnico.

El protocolo debe partir de una idea central: toda prueba asistida por IA debe ser tratada como prueba tecnológica compleja. Por tanto, requiere control de legalidad, identificación del sistema, documentación metodológica, preservación de evidencia digital, validación pericial, contradicción efectiva y motivación judicial reforzada.

En este sentido, la Figura 5 sintetiza las fases mínimas que deberían observarse para que el uso de inteligencia artificial como apoyo probatorio sea compatible con el debido proceso, la defensa, la contradicción y la valoración judicial motivada.

ISBN: 978-631-6557-82-7

Figura 5 Protocolo garantista para el uso de IA como apoyo probatorio

Como se observa en la figura, el uso de IA probatoria no debe iniciar directamente con el procesamiento tecnológico, sino con la definición de la finalidad probatoria y la verificación de una base legal suficiente. Posteriormente, deben documentarse el sistema utilizado, los parámetros aplicados, los controles de calidad, la intervención pericial y las posibilidades reales de contradicción por parte de la defensa. Solo después de cumplir estas fases el resultado puede ser valorado judicialmente conforme a la sana crítica.

Tabla 31 Protocolo general para el uso de IA como herramienta probatoria penal

Etapa	Acción requerida	Responsable principal
Identificación	Precisar qué sistema de IA se utilizó, versión, proveedor y finalidad	Fiscalía / perito

ISBN: 978-631-6557-82-7

Legalidad	Verificar origen lícito de datos y autorización cuando corresponda	Fiscalía / juez
Preservación	Conservar evidencia original, copias forenses, metadatos y cadena de custodia	Sistema forense / Fiscalía
Metodología	Documentar procedimiento, parámetros, margen de error y limitaciones	Perito
Acceso	Permitir a la defensa conocer información técnica suficiente	Fiscalía / juez
Contradicción	Garantizar interrogatorio, contrainterrogatorio y pericia de parte si procede	Juez
Valoración	Analizar legalidad, autenticidad, fiabilidad, corroboración y duda razonable	Juez
Motivación	Explicar por qué se admite o valora el resultado algorítmico	Juez

Esta tabla resume el protocolo mínimo que debería aplicarse en procesos penales donde se utilice IA como herramienta probatoria. Su finalidad es evitar que los resultados tecnológicos ingresen al proceso sin control suficiente.

Desde la perspectiva de los jueces, el protocolo exige verificar la legalidad de la obtención de datos, controlar la admisibilidad, garantizar contradicción, exigir explicación pericial, valorar el margen de error y motivar de forma reforzada. El juez no debe asumir que un resultado es fiable por haber sido producido mediante IA.

Desde la perspectiva de los fiscales, el protocolo exige documentar desde el inicio el uso de herramientas inteligentes. La Fiscalía debe conservar la evidencia original, registrar la cadena de custodia, identificar el sistema utilizado, justificar su necesidad, preservar los datos de entrada y presentar peritos capaces de explicar el procedimiento.

Desde la perspectiva de los defensores, el protocolo exige revisar la legalidad de la obtención de datos, cuestionar la cadena de custodia, solicitar información técnica, preparar contrainterrogatorio especializado, pedir pericias independientes cuando sea necesario y advertir al juez sobre sesgos, opacidad o falta de reproducibilidad.

ISBN: 978-631-6557-82-7

Desde la perspectiva de los peritos, el protocolo exige claridad metodológica. El perito debe explicar qué sistema se utilizó, cómo funciona de manera general, qué datos fueron procesados, qué limitaciones existen, cuál es el margen de error y qué nivel de certeza puede atribuirse al resultado. El perito no debe presentar inferencias algorítmicas como verdades absolutas.

Tabla 32 Obligaciones diferenciadas por operador procesal

Operador	Obligaciones frente a IA probatoria
Juez	Controlar admisibilidad, garantizar contradicción y motivar valoración
Fiscalía	Obtener datos legalmente, preservar evidencia y presentar pericia suficiente
Defensa	Cuestionar legalidad, fiabilidad, sesgos, metodología y cadena de custodia
Perito	Explicar técnica, datos, parámetros, margen de error y limitaciones
Instituciones forenses	Actualizar protocolos, capacitar personal y fortalecer capacidades técnicas

La tabla evidencia que el control de la IA probatoria no corresponde a un solo actor. Se trata de una responsabilidad distribuida. El sistema penal solo puede utilizar IA de manera legítima si todos los operadores cumplen funciones de control, documentación, contradicción y valoración.

5.8 Conclusión del capítulo

La inteligencia artificial puede contribuir al sistema penal únicamente si se encuentra subordinada a las garantías procesales. Su uso no debe debilitar el derecho a la defensa, la contradicción, la igualdad de armas, la protección de datos personales, la motivación judicial ni la presunción de inocencia. Por el contrario, mientras más compleja sea la tecnología utilizada, mayor debe ser el nivel de control jurídico, técnico y judicial.

ISBN: 978-631-6557-82-7

El derecho a la defensa exige acceso suficiente a la información técnica que sustenta el resultado algorítmico. La contradicción probatoria exige que el perito explique el procedimiento y responda al interrogatorio y contrainterrogatorio. La igualdad de armas exige que la defensa pueda cuestionar la prueba en condiciones razonables. La protección de datos exige que el tratamiento de información personal sea legal, necesario, proporcional y limitado a la finalidad del proceso.

La prueba pericial asistida por IA debe ser clara, verificable y metodológicamente suficiente. El informe debe identificar la herramienta utilizada, los datos procesados, los parámetros aplicados, el margen de error, las limitaciones y las conclusiones. En audiencia, el perito debe sostener técnicamente su informe y permitir que las partes lo cuestionen.

La valoración judicial debe realizarse conforme a la sana crítica y al estándar de duda razonable. El juez no puede aceptar resultados algorítmicos como verdad automática. Debe motivar de manera reforzada por qué considera fiable la prueba, cómo fue obtenida, cómo se preservó, cómo fue contradicha y cómo se relaciona con el conjunto probatorio.

Finalmente, ninguna decisión penal debe ser automatizada. La IA puede asistir al sistema penal, pero no reemplazar la responsabilidad humana. La decisión sobre la libertad, responsabilidad o inocencia de una persona debe permanecer en manos de jueces y operadores jurídicos sometidos a la Constitución, la ley, la motivación y el control público.

ISBN: 978-631-6557-82-7

Conclusiones generales

La inteligencia artificial representa una de las transformaciones tecnológicas más relevantes para el sistema penal contemporáneo. Su capacidad para procesar grandes volúmenes de información, identificar patrones, analizar evidencia digital, examinar imágenes, audios, videos, documentos y metadatos permite advertir su utilidad en la investigación criminal y en la gestión probatoria. Sin embargo, su incorporación al proceso penal no puede ser comprendida únicamente desde la eficiencia, sino desde su compatibilidad con el debido proceso, la defensa, la contradicción, la presunción de inocencia y la valoración racional de la prueba.

La inteligencia artificial no debe ser considerada una prueba autónoma ni una fuente absoluta de verdad. Su naturaleza jurídica dentro del proceso penal debe entenderse como herramienta auxiliar de análisis, procesamiento, clasificación o interpretación de información. En consecuencia, los resultados generados mediante sistemas inteligentes deben ingresar al proceso a través de los medios probatorios reconocidos por el ordenamiento jurídico, principalmente la prueba documental, el contenido digital y la prueba pericial.

La prueba penal mantiene una función garantista dentro del Estado constitucional de derechos y justicia. Su finalidad no consiste únicamente en reconstruir hechos, sino en hacerlo mediante procedimientos lícitos, controlables y respetuosos de los derechos fundamentales. Por ello, ninguna herramienta tecnológica puede justificar la flexibilización de garantías procesales ni la admisión de elementos obtenidos con vulneración de derechos.

La utilización de inteligencia artificial en materia probatoria exige un control reforzado de admisibilidad. No basta con que el resultado algorítmico sea útil o técnicamente sofisticado; debe cumplir condiciones de legalidad, pertinencia, utilidad, conducencia, autenticidad, integridad, fiabilidad técnica y posibilidad efectiva de contradicción. La innovación tecnológica no elimina los requisitos clásicos de la prueba penal, sino que obliga a aplicarlos con mayor rigor.

ISBN: 978-631-6557-82-7

La legalidad en la obtención de datos constituye un requisito esencial. Los sistemas de IA trabajan con información que puede incluir datos personales, biométricos, comunicaciones, metadatos, imágenes, registros de ubicación y otros elementos sensibles. Si los datos de entrada fueron obtenidos ilícitamente, el resultado producido por la herramienta tecnológica también queda afectado en su legitimidad procesal.

La cadena de custodia digital es un elemento indispensable para preservar la autenticidad e integridad de la evidencia tecnológica. En pruebas asistidas por IA, no solo debe conservarse el resultado final, sino también la fuente original, los datos analizados, las copias forenses, los metadatos, las herramientas utilizadas, los parámetros aplicados y las personas que intervinieron en el procedimiento. Sin trazabilidad, la prueba digital pierde confiabilidad.

La fiabilidad técnica de los sistemas de inteligencia artificial debe ser demostrada y no presumida. Todo resultado algorítmico debe estar acompañado de información suficiente sobre el software utilizado, versión, proveedor, metodología, datos de entrada, margen de error, limitaciones, sesgos posibles y validación técnica. En materia penal, el desconocimiento de estos aspectos puede afectar gravemente la defensa y la valoración judicial.

La opacidad algorítmica constituye uno de los principales desafíos jurídicos de la IA probatoria. Cuando las partes no pueden conocer cómo se produjo un resultado, la contradicción se vuelve meramente formal. Por ello, la explicabilidad, la auditoría, la reproducibilidad y la supervisión humana deben ser condiciones mínimas para admitir y valorar pruebas asistidas por inteligencia artificial.

Los sesgos algorítmicos representan un riesgo directo para la igualdad, la presunción de inocencia y la imparcialidad del proceso penal. Si los sistemas de IA son entrenados con datos incompletos, discriminatorios o históricamente sesgados, pueden reproducir errores institucionales, generar falsos positivos o reforzar prácticas de vigilancia selectiva. Por tanto, el control de sesgos debe formar parte del análisis de admisibilidad y valoración probatoria.

ISBN: 978-631-6557-82-7

La prueba pericial cumple una función central en la incorporación de resultados generados o asistidos por IA. El perito no debe limitarse a presentar la conclusión del sistema, sino explicar la metodología aplicada, los datos procesados, los parámetros utilizados, el margen de error, las limitaciones y el alcance real del resultado. La pericia debe permitir que el juez y las partes comprendan la prueba, la cuestionen y la valoren racionalmente.

El derecho a la defensa exige que la persona procesada y su defensa técnica tengan acceso suficiente a la información necesaria para cuestionar la prueba asistida por IA. La defensa no puede controvertir eficazmente un resultado algorítmico si desconoce el sistema utilizado, los datos ingresados, el procedimiento aplicado o las limitaciones de la herramienta. En consecuencia, el uso de IA en el proceso penal debe garantizar igualdad de armas y contradicción efectiva.

La valoración judicial de la prueba asistida por inteligencia artificial debe realizarse conforme a la sana crítica y al estándar de duda razonable. El juez no puede aceptar un resultado tecnológico por su sola apariencia científica o por la autoridad técnica del sistema utilizado. Debe analizar su legalidad, autenticidad, cadena de custodia, fiabilidad, contradicción, corroboración y relación con el conjunto probatorio.

La motivación judicial debe ser reforzada cuando se valoren pruebas asistidas por IA. La sentencia debe explicar de manera clara por qué se consideró admisible y fiable el resultado algorítmico, cómo fue preservada la evidencia, qué objeciones presentó la defensa, cómo fueron resueltas y de qué manera ese elemento se relaciona con las demás pruebas. Una decisión que se limite a aceptar la conclusión de la IA sin análisis crítico resulta incompatible con el debido proceso.

La inteligencia artificial no puede sustituir la decisión judicial ni la responsabilidad humana dentro del sistema penal. La función de juzgar exige valoración jurídica, análisis contextual, motivación, ponderación de garantías y responsabilidad institucional. Por ello, la IA puede asistir al juez, al fiscal, al defensor o al perito, pero no reemplazar su función ni convertirse en fundamento exclusivo de una decisión penal.

ISBN: 978-631-6557-82-7

El uso de inteligencia artificial predictiva en materia penal debe ser tratado con especial cautela. Las predicciones, perfiles de riesgo o patrones estadísticos no pueden equipararse a prueba individualizada de responsabilidad penal. Una persona no puede ser investigada, acusada o condenada con base exclusiva en probabilidades algorítmicas, perfiles automatizados o asociaciones estadísticas.

Las evidencias deepfake constituyen un desafío probatorio especialmente relevante. La posibilidad de crear o manipular imágenes, audios y videos mediante inteligencia artificial obliga a fortalecer los mecanismos de autenticación, análisis forense, cadena de custodia digital y pericia especializada. La apariencia de realidad de un archivo audiovisual ya no puede ser suficiente para atribuirle valor probatorio sin verificación técnica.

El marco jurídico ecuatoriano cuenta con bases importantes para regular la prueba tecnológica, especialmente en materia de debido proceso, medios de prueba, contenido digital, cadena de custodia, valoración probatoria, mensajes de datos y protección de datos personales. Sin embargo, todavía existen vacíos específicos sobre el uso de inteligencia artificial en el proceso penal, particularmente respecto a reconocimiento facial, deepfakes, análisis predictivo, auditoría algorítmica y decisiones automatizadas.

La ausencia de regulación específica sobre IA probatoria no implica que su uso esté prohibido, pero sí exige mayor prudencia judicial. Mientras no exista una normativa especializada, los jueces, fiscales, defensores y peritos deben aplicar de manera estricta los principios constitucionales, las reglas probatorias vigentes, los estándares de prueba digital, la protección de datos personales y las garantías del debido proceso.

El sistema penal ecuatoriano necesita desarrollar protocolos específicos para el uso de inteligencia artificial como herramienta probatoria. Estos protocolos deben establecer reglas sobre identificación del sistema utilizado, documentación de datos de entrada, preservación de evidencia digital, auditoría, aplicabilidad, margen de error, control de sesgos, validación pericial, acceso de la defensa y motivación judicial.

La inteligencia artificial puede fortalecer la justicia penal si se utiliza con transparencia, control humano, responsabilidad institucional y respeto a los derechos fundamentales. Su valor no reside en sustituir al derecho, sino en servirle. La tecnología

ISBN: 978-631-6557-82-7

solo será legítima dentro del proceso penal si contribuye al esclarecimiento de los hechos sin sacrificar las garantías que protegen a la persona frente al poder punitivo del Estado.

En definitiva, la inteligencia artificial como herramienta probatoria plantea una tensión entre innovación tecnológica y garantías procesales. La respuesta jurídica no debe ser el rechazo absoluto ni la aceptación acrítica. El camino adecuado consiste en construir un modelo de uso responsable, controlado y garantista, donde la IA pueda apoyar la investigación penal y el análisis probatorio, pero siempre subordinada a la Constitución, la ley, la pericia, la contradicción, la motivación judicial y la dignidad humana.

ISBN: 978-631-6557-82-7

Referencias bibliográficas

- Adriano-Caiza, B. P., Marfetan-Marfetan, V. D. R., & Machado-Maliza, M. E. (2025). Evidencias deepfake en sistema penal ecuatoriano: reconocimiento, autenticidad y aceptación probatoria en juicios. *Verdad y Derecho. Revista Arbitrada de Ciencias Jurídicas y Sociales, 4*(Especial), 325–343. https://doi.org/10.62574/r083dh53
- Asamblea Constituyente. (2008). *Constitución de la República del Ecuador*. Registro Oficial No. 449, 20 de octubre de 2008. Última modificación: 25 de enero de 2021.
- Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal, COIP*. Registro Oficial Suplemento No. 180, 10 de febrero de 2014. Última modificación: 17 de febrero de 2021.
- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Quinto Suplemento No. 459, 26 de mayo de 2021.
- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732.
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 77–91.
- Congreso Nacional del Ecuador. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. Registro Oficial Suplemento No. 557, 17 de abril de 2002. Última reforma: Quinto Suplemento del Registro Oficial No. 525, 27 de agosto de 2021.
- Consejo de Europa. (2024). *Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho*. El Consejo de Europa identifica este convenio como el primer tratado internacional jurídicamente vinculante sobre IA, derechos humanos, democracia y Estado de derecho.

ISBN: 978-631-6557-82-7

- Corte Constitucional del Ecuador. (2021, 20 de octubre). *Sentencia No. 1158-17-EP/21. Caso Garantía de la motivación*.
- Corte Interamericana de Derechos Humanos. (2009). *Caso Barreto Leiva vs. Venezuela. Fondo, reparaciones y costas. Sentencia de 17 de noviembre de 2009*.
- Corte Interamericana de Derechos Humanos. (2015). *Caso Ruano Torres y otros vs. El Salvador. Fondo, reparaciones y costas. Sentencia de 5 de octubre de 2015*.
- Citron, D. K. (2008). Technological due process. *Washington University Law Review, 85*(6), 1249–1313.
- Ferrer Beltrán, J. (2007). *La valoración racional de la prueba*. Marcial Pons.
- Fiscalía General del Estado. (2014). *Manuales, protocolos, instructivos y formatos del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses*. Registro Oficial Suplemento No. 318, 25 de agosto de 2014.
- Furingo, C. I. (2025). La inteligencia artificial: ¿innovación o amenaza para las garantías procesales en la justicia penal? *Revista de Derecho UNED, 36*, 101–131.
- Gascón Abellán, M. (2010). *Los hechos en el derecho: Bases argumentales de la prueba* (3.ª ed.). Marcial Pons.
- González Lagier, D. (2005). *Quaestio facti: Ensayos sobre prueba, causalidad y acción*. Palestra.
- Herrera Mamarandi, D. A., Gordón Lucero, B. J., & Gutierrez Romero, D. P. (2026). Uso de la inteligencia artificial en la investigación criminal y el derecho penal ecuatoriano: retos procesales, probatorios y éticos. *Polo del Conocimiento, 11*(6), 823–838. https://doi.org/10.23857/pc.v11i6.11796
- National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce. El marco AI RMF de NIST se utiliza como referencia para gestión de riesgos, confiabilidad y gobernanza de sistemas de IA.
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2022). *Recomendación sobre la ética de la inteligencia artificial*. UNESCO.

ISBN: 978-631-6557-82-7

- Organisation for Economic Co-operation and Development. (2024). *OECD AI Principles*. Los principios de IA de la OCDE fueron adoptados inicialmente en 2019 y actualizados en 2024.
- Parlamento Europeo y Consejo de la Unión Europea. (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial*. *Diario Oficial de la Unión Europea*, L, 2024/1689, 12 de julio de 2024.
- Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.
- Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4.ª ed.). Pearson.
- Santiago de León, E. G. (s. f.). *La prueba digital y la inteligencia artificial en los sistemas judiciales latinoamericanos: tendencias jurisprudenciales*. Universidad de San Carlos de Guatemala.
- Taruffo, M. (2011). *La prueba de los hechos* (4.ª ed.). Trotta.

SEMBLANZA DE AUTORES

LA INTELIGENCIA ARTIFICIAL COMO HERRAMIENTA PROBATORIA
EN EL SISTEMA PENAL: DESAFÍOS JURÍDICOS Y GARANTÍAS PROCESALES

ISBN: 978-631-6557-82-7

JULIO CESAR ROMERO AMORES

Guayaquil, Ecuador 21 de mayo de 1985

jromero@solutocg.com

https://orcid.org/0009-0000-1969-037X

Formación académica:

- Contador Público Autorizado
- Abogado.

Experiencia Profesional:

- Profesional con más de 25 años de trayectoria asesorando a empresas a nivel nacional, brindando soluciones integrales en los ámbitos contable, financiero, legal y tributario. A lo largo de su carrera ha acompañado a organizaciones de diversos sectores en la toma de decisiones estratégicas, el cumplimiento normativo y la optimización de sus procesos administrativos y legales.

Intereses y Áreas de Especialización:

- Docencia
- Sistemas
- Jurídico

Autor de la obra

ISBN: 978-631-6557-82-7

DAYANA ELIZABETH QUINTERO CEPEDA

Riobamba, Ecuador 05 de abril de 2000

daitaquinte@live.com

https://orcid.org/0000-0002-4140-1746

Formación académica:

- Abogada- Universidad de los Andes.
- Maestrante en Derecho Penal y Procesal - UNEMI

Experiencia Profesional:

- Procuradora Judicial de la ANT y CTE
- Asistente Técnico del Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y a Adolescentes Infractores de Ecuador (SNAI).
- Analista de Patrocinio en el área jurídica en el Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y a Adolescentes Infractores de Ecuador. Especialista en Comunicación Digital

Obras Publicadas:

- Restorative justice and its impact on juvenile offenders.
- La corrupción en la salud pública durante la pandemia en Ecuador

Intereses y Áreas de Especialización:

- Derecho Penal
- Derecho constitucional
- Contratación pública

Autor de la obra

ISBN: 978-631-6557-82-7

JONATHAN EDUARDO LÓPEZ POVEDA

Guayaquil, Ecuador 10 de mayo de 1992

info@lopezygomez.com

https://orcid.org/0009-0009-7058-4279

Formación académica:

- Ingeniero en Contabilidad y Auditoría C.P.A. por la Universidad Católica de Santiago de Guayaquil.
- Magíster en Administración de Empresas (MBA).
- Magíster en Gestión de Proyectos por la Universidad Casa Grande.
- Magíster en Gestión del Talento Humano por la Universidad Casa Grande.
- Especialista en Tributación por la Universidad Técnica Particular de Loja (UTPL).
- Especialista en Mediación por la Universidad Internacional del Ecuador (UIDE).
- Especialista en Mediación por el Centro de Arbitraje y Mediación de la Cámara de Economía Popular y Solidaria de Quito (CAMCEPSQ).
- Distinguido con el grado honorífico de Doctor Honoris Causa por la Universidad Gestalt de México.
- Distinguido con el grado honorífico de Doctor Honoris Causa por la Asociación de Magíster, Doctores y Postdoctores del Perú.

Experiencia Profesional:

- Socio Director de LOPEZ & GOMEZ S.A., firma especializada en servicios contables, auditoría, asesoría tributaria, consultoría financiera, cumplimiento corporativo y acompañamiento estratégico para empresas y emprendimientos.
- Tax Consultant de Advanced Audit Ecuador AAE Cía. Ltda., firma de auditoría y aseguramiento dedicada a servicios de auditoría financiera, auditoría tributaria, control interno, gestión de riesgos y cumplimiento normativo bajo estándares nacionales e internacionales.

ISBN: 978-631-6557-82-7

- Socio de LGLAWYERS S.A.S., bufete jurídico especializado en Derecho Tributario, Societario, Laboral, Civil y mecanismos alternativos de resolución de conflictos, brindando asesoría integral y representación legal a organizaciones y personas naturales.
- Socio de CAPIEMCORP S.A.S., empresa especializada en capacitación empresarial, formación ejecutiva, certificación de competencias laborales, desarrollo organizacional y fortalecimiento profesional para instituciones públicas, privadas y emprendedores.
- Asesor estratégico en materias contables, financieras, tributarias, societarias y de gestión empresarial.
- Especialista en Derecho Tributario, Societario y Laboral, con experiencia en planificación fiscal, cumplimiento normativo y estructuración corporativa.
- Consultor en implementación de Normas Internacionales de Información Financiera (NIIF), fortalecimiento del control interno y mejora de procesos organizacionales.
- Auditor interno de Sistemas Integrados de Gestión, con experiencia en diseño, implementación y evaluación de estándares ISO orientados a la mejora continua y la excelencia empresarial.

Obras Publicadas:

- Humanizar la Educación en Contextos Tecnológicos.
- Stare Decisis en la Era de la Inteligencia Artificial.
- Interpretación Jurídica Inteligente.
- Tributación en la Economía Digital en Ecuador.
- La Mediación como Mecanismo de Solución de Conflictos en Ecuador.
- Compliance Corporativo y Gestión Integral de Riesgos Empresariales.
- Fiscalidad de Plataformas Digitales, Influencers y Economía Colaborativa en Ecuador.
- Decisiones Financieras Inteligentes: Cómo Entender tus Números y Gestionar tu Negocio con KPIs, EBITDA y un Enfoque Basado en NIIF.
- Despertando Mentes: Estrategias Pedagógicas Innovadoras para Fomentar el Pensamiento Crítico en la Educación Superior.
- Derecho Penal Digital: Ciberdelitos, Inteligencia Artificial y Criminalidad en la Era Tecnológica.

ISBN: 978-631-6557-82-7

- Psicología del Dinero y Decisiones Financieras.

Intereses y Áreas de Especialización:

- Contabilidad y Auditoría.
- Tributación Nacional e Internacional.
- Derecho Tributario, Societario y Laboral.
- Mediación y Resolución Alternativa de Conflictos.
- Gestión de Proyectos.
- Gestión del Talento Humano.
- Normas Internacionales de Información Financiera (NIIF).
- Sistemas Integrados de Gestión e ISO.
- Inteligencia Artificial aplicada a los negocios y al derecho.
- Transformación Digital.
- Finanzas Corporativas.
- Educación y Capacitación Empresarial.
- Emprendimiento y Desarrollo Empresarial.
- Innovación, productividad y sostenibilidad organizacional.

ISBN: 978-631-6557-82-7

NATHALIE FERNANDA GÓMEZ SUÁREZ

Guayaquil, Ecuador 22 de julio de 1985

gerencia@lopezygomez.com

https://orcid.org/0009-0002-2227-7599

Formación académica:

- Ingeniera en Contabilidad y Auditoría C.P.A. por la Universidad Católica de Santiago de Guayaquil.
- Magíster en Administración de Empresas (MBA).
- Magíster en Gestión del Talento Humano.
- Especialista en Tributación por la Universidad Técnica Particular de Loja (UTPL).
- Especialista en Mediación por la Universidad Internacional del Ecuador (UIDE).
- Especialista en Mediación por el Centro de Arbitraje y Mediación de la Cámara de Economía Popular y Solidaria de Quito (CAMCEPSQ).
- Mediadora calificada por el Consejo de la Judicatura del Ecuador.
- Distinguida con el grado honorífico de Doctor Honoris Causa por la Universidad Gestalt de México.
- Distinguida con el grado honorífico de Doctor Honoris Causa por la Asociación de Magíster, Doctores y Postdoctores del Perú.

Experiencia Profesional:

- Socia Directora de LOPEZ & GOMEZ S.A., firma especializada en asesoría contable, tributaria, financiera y consultoría empresarial, liderando procesos de planificación fiscal, cumplimiento normativo, control financiero y acompañamiento estratégico para organizaciones de diversos sectores económicos.
- Socia de LGLAWYERS S.A.S., firma jurídica especializada en Derecho Tributario, Societario y Laboral, participando en la estructuración y evaluación de estrategias fiscales, cumplimiento corporativo y fortalecimiento legal-financiero de empresas y emprendimientos.

ISBN: 978-631-6557-82-7

- Tax Consultant de Advanced Audit Ecuador AAE Cía. Ltda., firma de auditoría y aseguramiento dedicada a servicios de auditoría financiera, auditoría tributaria, control interno, gestión de riesgos y cumplimiento normativo bajo estándares nacionales e internacionales.
- Más de veinte años de experiencia profesional en las áreas contable, tributaria, financiera y administrativa, brindando asesoría especializada a organizaciones de diversos sectores económicos.
- Especialista en planificación tributaria y estrategia fiscal, orientada a la optimización de la carga impositiva dentro del marco legal vigente, la mitigación de riesgos tributarios y el fortalecimiento del cumplimiento normativo empresarial.
- Amplia experiencia en supervisión, control y administración de procesos contables y tributarios, incluyendo la gestión integral de más de treinta cuentas corporativas.
- Experta en cumplimiento de obligaciones tributarias, revisión fiscal, elaboración y análisis de información financiera, conciliaciones tributarias y atención de requerimientos ante organismos de control.
- Experiencia en auditoría tributaria, revisión de cumplimiento fiscal, evaluación de riesgos y fortalecimiento de sistemas de control interno para la mejora de la gestión organizacional.
- Responsable de la implementación y fortalecimiento de procedimientos administrativos, controles financieros y mecanismos de supervisión orientados a la eficiencia operativa, transparencia y sostenibilidad empresarial.
- Asesora estratégica en materia contable, tributaria y financiera, contribuyendo a la toma de decisiones, el fortalecimiento patrimonial y el crecimiento sostenible de las organizaciones.

Obras Publicadas:

- Tributación en la Economía Digital en Ecuador.
- La Mediación como Mecanismo de Solución de Conflictos en Ecuador.
- Compliance Corporativo y Gestión Integral de Riesgos Empresariales.
- Fiscalidad de Plataformas Digitales, Influencers y Economía Colaborativa en Ecuador.
- Empresas Inteligentes y Gobernanza Corporativa en la Economía Digital: Transformación Organizacional, Innovación Empresarial y Desafíos Regulatorios Contemporáneos.

ISBN: 978-631-6557-82-7

- Modelos Empresariales Disruptivos y Sostenibilidad Corporativa: Nuevas Estructuras Organizacionales, Responsabilidad Estratégica y Competitividad Global.

Intereses y Áreas de Especialización:

- Contabilidad y Auditoría.
- Tributación Nacional e Internacional.
- Planificación Tributaria y Estrategia Fiscal.
- Cumplimiento Tributario y Normativo.
- Derecho Tributario.
- Mediación y Resolución Alternativa de Conflictos.
- Compliance Corporativo.
- Gestión Integral de Riesgos Empresariales.
- Gobierno Corporativo.
- Finanzas Empresariales.
- Control Interno.
- Gestión Administrativa y Financiera.
- Transformación Digital y Regulación Empresarial.
- Desarrollo Organizacional.
- Sostenibilidad y Competitividad Empresarial.

Autor de la obra

LA INTELIGENCIA ARTIFICIAL COMO HERRAMIENTA PROBATORIA EN EL SISTEMA PENAL:

DESAFÍOS JURÍDICOS Y GARANTÍAS PROCESALES

Una obra que examina los desafíos jurídicos y las garantías procesales frente al uso de la inteligencia artificial como herramienta probatoria en el proceso penal, desde una perspectiva crítica, doctrinaria y jurisprudencial.

DEBIDO PROCESO

PRUEBA DIGITAL

DERECHOS FUNDAMENTALES

ISBN 978-631-6557-82-7