

UNIVERSIDAD TÉCNICA DE AMBATO FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES CARRERA DE DERECHO

Tema:

¨La protección de identidad de los administradores de justicia en los delitos de alta peligrosidad mediante el uso de la IA¨

Trabajo de Titulación previo a la obtención del Título de Abogada.

Autora: María Belén López Villagrán

Tutora: PhD. Eliana del Rocío Rodríguez Salcedo

Ambato - Ecuador

2026

APROBACION DEL TUTOR

Yo, PhD. Eliana del Roció Rodríguez Salcedo con cedula de identidad No. I 804126686, en mi calidad de Tutora del Proyecto de lnvestigaci6n sobre el tema: **"LA PROTECCION DE IDENTIDAD DE LOS ADMINISTRADORES DE JUSTICIA EN LOS DELITOS DE ALTA PELIGROSIDAD MEDIANTE EL USO DE LA** IA", desarrollado por María Belén López Villagrán, de la Carrera de Derecho, modalidad presencial, considero que dicho informe investigativo reúne los requisitos, tanto técnicos como científicos y corresponde a las normas establecidas en el Instructivo del Reglamento para la Titulaci6n de Grado en la Universidad Técnica de Ambato.

Por lo tanto, autorizo la presentaci6n del mismo ante el organismo pertinente, para que sea sometido a evaluaci6n por los profesores calificadores designados por el H. Consejo Directivo de la Facultad.

Ambato, 02 de diciembre 2025

TUTORA



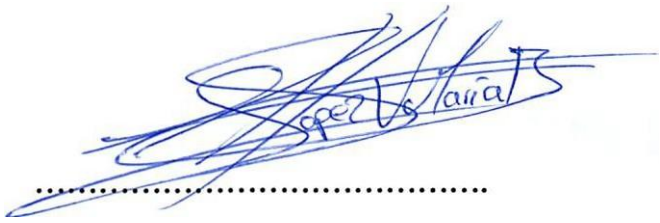
PhD. Eliana del Rocío Rodríguez Salcedo
C.I.: 1804126686

AUTORIA DEL TRABAJO DE TITULACION

Yo, María Belén López Villagrán con cedula de identidad N$_{0.}$ 1804038394, tengo a bien indicar que los criterios emitidos en el Proyecto de Investigación, bajo el tema: **"LA PROTECCION DE IDENTIDAD DE LOS ADMINISTRADORES DE JUSTICIA EN LOS DELITOS DE ALTA PELIGROSIDAD MEDIANTE EL USO DE LA** IA", también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autora de este Proyecto de Investigación.

Ambato, 02 de diciembre 2025

AUTORA



……

María Belén López Villagrán

C.I: 180403839-4

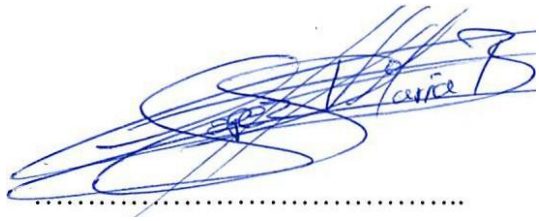
DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de este Proyecto de Investigaci6n, un documento disponible para su lectura, consulta y procesos de investigaci6n.

Cedo los derechos en línea patrimoniales de mi Proyecto de Investigaci6n, con fines de difusi6n publica; además apruebo la reproducci6n de este Proyecto de Investigaci6n, dentro de las regulaciones de la universidad, siempre y cuando esta reproducci6n no suponga una ganancia econ6mica potencial; y se realice respetando mis derechos de autora.

Ambato, 02 de diciembre 2025

AUTORA



María Belén López Villagrán

C.I: 180403839-4

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el Proyecto de Investigación, sobre el tema**: "LA PROTECCIÓN DE IDENTIDAD DE LOS ADMINISTRADORES DE JUSTICIA EN LOS DELITOS DE ALTA PELIGROSIDAD MEDIANTE EL USO DE LA IA"**, elaborado por María Belén López Villagrán, estudiante de la Carrera de Derecho, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Jurisprudencia y Ciencias Sociales y Auditoría de la Universidad Técnica de Ambato.

Ambato, …… 2026

_____

Título. Nombre Apellido
PRESIDENTE

_____

Título. Nombre Apellido
MIEMBRO CALIFICADOR

_____

Título. Nombre Apellido
MIEMBRO CALIFICADOR

DEDICATORIA

Le agradezco a Dios por sus bendiciones en cada circunstancia que se me ha presentado en este camino de formación profesional. A mi familia que nunca me dejaron sola y siempre estuvieron para apoyarme.

A mi padre Oswaldo López que siempre me brinda su fuerza para luchar día a día.

También dedico a mi madre Aida Villagrán que desde el cielo está conmigo cuidándome para que no me rinda y siga luchando por mis sueños.

A mi tutora la PhD. Eliana del Rocío Rodríguez Salcedo por su guía para lograr el desarrollo de este trabajo con éxito. A mis docentes que siempre estuvieron para brindarme sus enseñanzas, sus consejos, conocimientos y a mi Universidad Técnica de Ambato por abrirme las puertas y permitirme formarme en ella. Muchas gracias.

AGRADECIMIENTO

La presente tesis la dedico en primer lugar a Dios y a mi familia, por ser mi apoyo e inspiración para seguir adelante; son a quienes les dedico todo mi esfuerzo y sacrificio.

A mi padre Oswaldo López por ser mi gran apoyo desde un inicio y en especial porque desde hace un tiempo atrás es padre y madre, ya que mi madre partió de esta vida terrenal. A mi madre Aida Villagrán que, aunque no está presente físicamente, sé y aseguro que me cuida y me brinda todas sus bendiciones para seguir adelante y no truncarme la vida por su ausencia.

ÍNDICE GENERAL DE CONTENIDOS

CONTENIDO **PÁGINA**

PORTADA. i

APROBACIÓN DEL TUTOR. ii

AUTORÍA DEL TRABAJO DE TITULACIÓN. iii

DERECHOS DE AUTOR. iv

APROBACIÓN DEL TRIBUNAL DE GRADO v

DEDICATORIA vi

AGRADECIMIENTO vii

ÍNDICE GENERAL DE CONTENIDOS viii

ÍNDICE DE TABLAS x

RESUMEN EJECUTIVO xi

ABSTRACT xii

CAPÍTULO I. MARCO TEÓRICO 1

1.1.1. Antecedentes históricos 1

1.1.2. Antecedentes jurisprudenciales 3

1.1.3. Jueces sin rostro 5

1.2. Antecedentes doctrinarios 9

1.2.1. Anonimización 9

1.2.2. Datos personales 13

1.2.3. Inteligencia Artificial en la Justicia 15

1.2.4. Protección de identidad 24

1.2.5. Ciberseguridad 26

1.2.6. Debido proceso 27

1.2.7. Seguridad judicial 30

1.3. Antecedentes normativos 31

1.3.1. Constitución de la República del Ecuador 31

1.3.2. Ley Orgánica de Protección de Datos Personales 32

1.4. Objetivos 35

1.4.1. Objetivo General 35

1.4.2. Objetivos Específicos 35

CAPÍTULO II. MARCO METODOLÓGICO 37

2.2. Metodología 38

2.2.1. Enfoque 39

2.2.2. Modalidades de investigación – Tipo de investigación 40
2.2.3. Nivel 42
2.2.4. Métodos 43
2.2.5. Técnicas de investigación 45
2.2.6. Instrumento de investigación 46
2.2.7. Población 47
2.2.8. Muestra 48
CAPÍTULO III.....49
3.1. Análisis de los resultados.....49
3.1.1. Anonimización y técnicas de protección de datos 49
3.1.2. Inteligencia artificial en justicia y protección de datos.....58
3.1.3. Marco normativo y contexto ecuatoriano 66
3.2. Discusión 77
3.3. Conclusiones.....87
CAPÍTULO IV. 87
3.4. Recomendaciones.....88
ANEXOS 90

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

Tabla 1. Comparativa de jueces sin rostro en Ecuador.....67

Tabla 2. *Comparativa de casos.* 79

RESUMEN EJECUTIVO

Ecuador ha atravesado en los últimos años una crisis de seguridad marcada por el incremento de la violencia ejercida por el crimen organizado contra el sistema judicial, lo que ha debilitado la confianza institucional y generado riesgos directos para fiscales y jueces. El objetivo principal de esta investigación fue analizar la protección tecnológica que fortalezca la labor de los operadores de justicia sin afectar las garantías procesales. La metodología aplicada correspondió a un enfoque cualitativo con componentes analíticos y prospectivos, sustentado en la revisión documental, el análisis de casos recientes y la evaluación comparativa de sistemas de protección judicial en otros países de la región. Los resultados evidenciaron la existencia de una fuerte asimetría tecnológica entre el Estado y las organizaciones criminales, así como la carencia de protocolos interinstitucionales eficaces para prevenir ataques y amenazas. A partir de este diagnóstico, se elaboró un análisis basado en la revisión bibliográfica acerca de la pertinencia de la anonimización mediante el uso de inteligencia artificial para los denominados jueces sin rostro, adaptadas a las condiciones del contexto ecuatoriano. Se concluye que la implementación de este modelo no solo puede garantizar la seguridad de fiscales y jueces, sino también contribuir al fortalecimiento del Estado de derecho y a la consolidación de la confianza ciudadana en la administración de justicia.

PALABRAS CLAVE: crimen organizado, seguridad judicial, inteligencia artificial, Estado de derecho, Ecuador.

ABSTRACT

In recent years, Ecuador has experienced a security crisis marked by increased violence perpetrated by organized crime against the judicial system, which has weakened institutional trust and generated direct risks for prosecutors and judges. The main objective of this research was to analyze technological protection that strengthens the work of justice officials without compromising procedural guarantees. The methodology applied was a qualitative approach with analytical and prospective components, supported by a documentary review, an analysis of recent cases, and a comparative evaluation of judicial protection systems in other countries in the region. The results revealed a strong technological asymmetry between the State and criminal organizations, as well as a lack of effective inter-institutional protocols to prevent attacks and threats. Based on this diagnosis, an analysis was developed based on a literature review on the relevance of anonymization through the use of artificial intelligence for so-called faceless judges, adapted to the conditions of the Ecuadorian context. It is concluded that the implementation of this model can not only guarantee the safety of prosecutors and judges, but also contribute to strengthening the rule of law and consolidating citizen confidence in the administration of justice.

KEY WORDS: organized crime, judicial security, artificial intelligence, rule of law, Ecuador

CAPÍTULO I.
MARCO TEÓRICO

1.1. Antecedentes

Para la construcción del marco contextual de esta investigación, se han recopilado sistemáticamente antecedentes nacionales que evidencian la gravedad de la situación de seguridad que enfrentan los operadores de justicia en Ecuador. Los estudios documentan la alarmante frecuencia de amenazas y ataques, estableciendo una clara correlación entre el manejo de casos de alta peligrosidad y el incremento del riesgo personal para jueces y fiscales. Estos trabajos, junto con reportes de organismos como la ONU cuantifican el problema y analizan críticamente la insuficiencia de las medidas de protección tradicionales, señalando la imperiosa necesidad de explorar soluciones tecnológicamente avanzadas y estructurales para garantizar su seguridad e imparcialidad.

De forma complementaria, el examen de antecedentes a nivel internacional muestra un número creciente de estudios y experiencias en torno al uso de la inteligencia artificial para resguardar la identidad dentro del sistema judicial. Investigaciones como las de Rivero y Chinarro (2024) detallan el desarrollo y la implementación de sistemas automatizados de anonimización de documentos judiciales mediante técnicas de procesamiento de lenguaje natural. Asimismo, se han analizado modelos comparados, los cuales sirven como referentes valiosos para evaluar la viabilidad, los beneficios y los desafíos ético-jurídicos de implementar soluciones similares en el contexto específico del sistema legal ecuatoriano.

1.1.1. Antecedentes históricos

La legislación sobre Inteligencia Artificial (*AI Act*), promulgada en Europa en 2024, define un marco regulatorio novedoso que categoriza los sistemas de IA utilizados para la gestión de justicia como de alto riesgo, lo que requiere supervisión humana y transparencia. Sin embargo, esta normativa deja fuera de este análisis a las denominadas tecnologías auxiliares (como la anonimización de documentos judiciales), a pesar de que su aplicación generalizada presenta desafíos y riesgos propios que también merecerían ser regulados. Esta discrepancia demuestra el esfuerzo de balancear la innovación tecnológica con las garantías procesales, lo que posibilita a los Estados miembros utilizar medidas como la pseudonimización automatizada sin poner en riesgo la autonomía del poder judicial.

La automatización de los sistemas de pseudonimización y anonimización es,

según Terzidou (2023), una de las aplicaciones más alentadoras de la inteligencia artificial. Para ocultar y descubrir información privada en los registros judiciales, estos sistemas utilizan métodos de aprendizaje automático y procesamiento del lenguaje natural (PLN). De acuerdo con una investigación de la Comisión Europea, más de la mitad de los Estados miembros de la UE están implementando acciones para proteger el anonimato tanto de las decisiones judiciales como el de los jueces y fiscales en situaciones de riesgo moderado.

Estos sistemas no solo hacen más sencillos los procedimientos administrativos, sino que además reducen las equivocaciones humanas al gestionar información crítica. Simultáneamente, las cámaras de seguridad inteligentes que incorporan análisis de riesgos y reconocimiento facial suponen un progreso en la seguridad física. Al combinar información en tiempo real de redes sociales, cámaras y bases de datos policiales, estos sistemas pueden detectar conductas sospechosas (como amenazas en foros oscuros o vigilancia). Asimismo, tienen la capacidad de alertar a las autoridades antes de que un ataque suceda. No obstante, se deben usar con estrictas medidas de protección para impedir que se vulneren sin justificación la privacidad de los funcionarios o de los ciudadanos.

Además, la modernización de la identidad digital en los sistemas judiciales mediante blockchain[1] o cifrado homomórfico[2] fortalece la seguridad de las comunicaciones institucionales. Estas tecnologías no solo protegen contra ciberataques, sino que permiten verificar la autenticidad de documentos sin exponer datos sensibles, un avance crucial en casos donde la infiltración de redes criminales en sistemas estatales es una amenaza latente.

Según Andrade, Toapanta, Bano y Gómez (2024), en su artículo “Un enfoque de la inteligencia artificial para la protección de datos personales sustentado en la base legal” en el escenario contemporáneo, marcado por el avance de la criminalidad organizada y la sofisticación de delitos como el narcotráfico, el terrorismo o la corrupción sistémica, la protección de la identidad de jueces, fiscales y demás operadores jurídicos se ha convertido en un imperativo para preservar la integridad de los sistemas judiciales.

[1] Cadena de bloques.
[2] El cifrado homomórfico es una técnica avanzada de criptografía que permite realizar operaciones matemáticas con datos encriptados sin necesidad de descifrarlos previamente.

Los funcionarios encargados del deber de velar por el Estado de derecho están expuestos a amenazas que ponen en gran peligro sus vidas, así como las de sus familiares, y que, además, sirven para sabotear la autonomía del poder judicial y mantener la impunidad. En este contexto, la inteligencia artificial (IA) se presenta como un socio estratégico, que proporcionará herramientas innovadoras diseñadas para proteger la seguridad de su anonimato y seguridad.

Delgado y Espinoza (2024) sostienen en su artículo "Impacto de la Inteligencia Artificial en el Derecho a la Intimidad y Protección de Datos Personales" que los progresos tecnológicos, que incluyen desde algoritmos de anonimización hasta sistemas predictivos de amenazas, están reconfigurando los paradigmas de protección institucional. Ser capaz de propiciar respuestas más rápidas y flexibles a grupos de actores criminales que operan con recursos muy sofisticados. Esta evaluación estudia el cambio que la inteligencia artificial provocará en la administración de riesgos judiciales, particularmente en los casos donde develar quién es responsable de la justicia pueda tener efectos irreversibles.

La protección de la identidad en el ámbito judicial está fundamentada en los principios del derecho internacional de los derechos humanos, que han sido aprobados por organizaciones como la CIDH y el Consejo de Derechos Humanos de las Naciones Unidas. Estas entidades han indicado que instrumentos como el cifrado y el anonimato no son solo necesarios para asegurar la privacidad, sino también otros derechos asociados, como la libertad de expresión y la seguridad individual. El caso Escher contra Brasil (2009) tiene importancia también, porque la Corte Interamericana extendió el concepto de privacidad para incluir metadatos y elementos del proceso comunicativo, estableciendo una pauta que se utilizaría para proteger los datos de fiscales y jueces cuya información podría caer en manos de organizaciones delictivas.

1.1.2. Antecedentes jurisprudenciales

De acuerdo con Terzidou (2023), proyectos como ANOPPI[3] en Finlandia ilustran el potencial de la IA para la protección judicial. Y este nuevo sistema emplea algoritmos de aprendizaje automático para clasificar información personal en forma de frases o

[3] El proyecto ANOPPI (Anonimización y Protección de Identidades en el Sistema Judicial) es una iniciativa tecnológico-legal que busca desarrollar e implementar un sistema de inteligencia artificial especializado para proteger la identidad de jueces, fiscales y otros operadores de justicia.

alusiones indirectas que puedan revelar la identidad de un juez y las partes en litigio. Un proyecto similar en Austria está analizando millones de documentos judiciales históricos para entrenar modelos que identifiquen patrones lingüísticos relacionados con funcionarios en riesgo. Pero incluso en estos casos se pueden encontrar señales: la exclusión inicial de jueces y fiscales en los procesos de anonimización ya revela un choque entre seguridad y transparencia, especialmente en aquellos países en los que el crimen organizado afecta directamente a los agentes de justicia.

Estas tecnologías enfrentan barreras de implementación en varios niveles. Por un lado, la falta de datos judiciales que estén digitalizados y estandarizados reduce la posibilidad de entrenar algoritmos; por el otro, las técnicas nuevas de reidentificación de datos, que fusionan información que ha sido anonimizada con información de código abierto, ponen en riesgo la anonimización. En el ámbito de la ética, la inteligencia artificial plantea el reto de proteger las identidades sin comprometer la transparencia, un equilibrio necesario para poder exigir responsabilidades. Si la información llega a manos inapropiadas, el hecho de depender de plataformas tecnológicas privadas para crear estas herramientas podría generar conflictos de intereses o poner en riesgo la estrategia.

Cárdenas y Molano (2021), en su artículo científico, abordaron el tema de la aplicación de la inteligencia artificial como una herramienta para la toma de decisiones judiciales. El objetivo general de su estudio fue resolver las interrogantes sobre la utilidad, la factibilidad de implementación y las consecuencias de incorporar sistemas jurídicos expertos en este ámbito. Como resultado de su investigación académica, determinaron que la participación de la IA tiene como principal implicación un aumento significativo de la seguridad jurídica, derivado de una mayor confianza en el sistema judicial y una administración de justicia más rápida.

Concluyeron que, si bien estas ventajas pueden justificar los costos de su aplicación, la responsabilidad final de las decisiones judiciales debe recaer siempre en el juez humano, quien es irreemplazable en el análisis del caso concreto. Este estudio sienta una base crucial para la investigación, pues el incremento de la seguridad jurídica y la confianza que se observa es un soporte esencial para argumentar a favor de la puesta en marcha de la IA en situaciones altamente peligrosas.

Precisamente, la protección de la identidad de los jueces mediante el uso de estas

herramientas puede ser un factor determinante para lograr ese clima de confianza y eficacia, al blindar al administrador de justicia de represalias, permitiéndole ejercer sus funciones con mayor imparcialidad y libertad, tal como lo sugiere la conclusión sobre la irreemplazable función humana asistida por tecnología.

En su artículo científico, Rivero y Chinarro (2024) exploraron el uso de sistemas de inteligencia artificial en la judicatura, en énfasis en la dicotomía entre su función de asistencia al juez y la posibilidad de que lo sustituya, así como en los aspectos técnicos y medioambientales involucrados. Su objetivo fue examinar las posturas doctrinales y las adoptadas por diversos países, destacando el papel de la Unión Europea. Los resultados del estudio analizan dos modelos: el de sustitución, aplicado en China con los "*Smart Courts*",[4] y el de asistencia, utilizado en Estados Unidos con el algoritmo COMPAS. La conclusión enfatiza la importancia de un enfoque multidisciplinario que, además de los avances tecnológicos, tenga en cuenta las consecuencias éticas y medioambientales para asegurar que la IA se implemente de manera responsable y sostenible en el sistema judicial.

La investigación de Rivero Silva y Chinarro Vadillo es directamente relevante al ofrecer un marco comparativo de modelos de implementación. Para el tema de la protección de la identidad, el modelo de asistencia (como el algoritmo COMPAS) se presenta como el más viable y ético, donde la IA no reemplaza al juez, pero sí optimiza y protege el proceso. Por ejemplo, podría gestionar y enmascarar digitalmente la identidad del juez en entornos virtuales, analizar evidencia de forma remota y segura, y generar borradores de resoluciones que oculten estilos escriturales identificables, todo dentro de un enfoque multidisciplinar que priorice la seguridad del administrador de justicia sin comprometer la tutela judicial efectiva.

1.1.3. Jueces sin rostro

Para la seguridad judicial en la época digital, es fundamental un enfoque holístico. Esto requiere el desarrollo de marcos normativos adaptables que, sin obstaculizar la innovación, definan protocolos para el uso ético de la inteligencia artificial, con auditorías independientes y estándares de ciberseguridad incluidos. En segundo lugar, se debe invertir en infraestructura digital para que los sistemas sean interoperables entre

[4] Cortes inteligentes

jurisdicciones y crear depósitos de datos anónimos para obtener algoritmos más exactos. Es indispensable que los operadores jurídicos sean capacitadores en el uso de herramientas tecnológicas para garantizar que la implementación no se vea comprometida.

El Consejo de la Judicatura, en 2024, tomó la decisión de constituir el Tribunal de Garantías Penales y la Unidad Judicial con el objetivo de combatir el crimen organizado. Ambas entidades tienen su sede en Quito y su jurisdicción se extiende por todo el país. Estas recientes instancias están compuestas por magistrados especializados en delitos complejos, tales como el tráfico de drogas a gran escala, la financiación del terrorismo, el enriquecimiento ilícito, el terrorismo, la delincuencia organizada y el lavado de activos.

Según información recopilada por Merino, Guilcapi y Defas (2024), la creación de estas unidades fue acompañada por reformas legales orientadas a fortalecer la capacidad institucional para enfrentar estas amenazas de forma más efectiva. En paralelo, durante 2022 se realizaron 74 allanamientos vinculados a delitos de terrorismo y crimen organizado, donde se incautaron drogas, explosivos, armas y otros bienes ilícitos, reflejando la magnitud de la problemática y la necesidad de acciones coordinadas.

Frente a la persistente violencia y las amenazas directas contra funcionarios judiciales, se ha planteado en Ecuador la necesidad de implementar la figura de jueces sin rostro, inspirada en modelos de otros países que buscan proteger la identidad y la integridad de quienes enfrentan casos de crimen organizado. Aunque aún no existe en Ecuador una ley específica que regule de manera integral esta figura, la Ley Orgánica Reformatoria al Código Orgánico de la Función Judicial de 2020 ya contempla la posibilidad de aplicarla en situaciones de extrema violencia y amenazas.

Aunado a ello, Portilla, Romero, Chugá y Rodríguez (2024) manifiestan que estudios y encuestas realizadas entre magistrados y abogados muestran un respaldo unánime a esta propuesta: el 100% de los abogados consultados apoyan la implementación de jueces sin rostro como una garantía estatal necesaria para proteger la imparcialidad y seguridad de los operadores de justicia. Se ha recomendado incluso su inclusión en la Constitución como un mecanismo que refuerce la administración de justicia ante el avance del crimen organizado. En conjunto, la situación revela una amenaza grave al Estado de derecho y evidencia la urgencia de adoptar medidas

institucionales y legales que aseguren la protección efectiva de quienes sostienen la estructura judicial del país.

Uno de los retos más importantes para los sistemas de justicia en la época moderna, sobre todo en aquellas naciones donde el crimen organizado ha llegado a grados preocupantes de sofisticación y penetración estatal, es garantizar la identidad segura de quienes operan en la justicia cuando se trata de casos muy complejos. Este asunto va más allá del ámbito meramente operativo y encarna una cuestión de seguridad nacional y de mantenimiento del Estado de derecho. Se erosionan los fundamentos del contrato social, que son la base de las democracias, cuando los custodios de la administración de justicia se ven sometidos a presiones, amenazas o asaltos directos (Ramírez & Alvarado, 2025).

En el contexto ecuatoriano, la situación es especialmente grave debido a la convergencia de varios factores: la expansión de los cárteles del narcotráfico a nivel mundial, el sistema de corrupción crónica en sectores concretos del aparato judicial y la falta de capacidad del sistema para salvaguardar adecuadamente a sus propios funcionarios en los tribunales. Los números de agresiones a jueces y fiscales son solamente una pequeña parte visible de un fenómeno más profundo y estructural.

Mejía (2024), en un artículo publicado en Universidad y Sociedad, investigó la importancia de la figura de jueces sin rostro en Ecuador como mecanismo de protección para los administradores de justicia frente a las organizaciones criminales. Utilizando una metodología cualitativa, no experimental y descriptiva que incluyó análisis documental y entrevistas, el estudio tuvo como objetivo analizar la relevancia de esta figura jurídica. Los hallazgos establecieron que es necesario instaurar un sistema de seguridad para los jueces, sugiriendo en particular la utilización de jueces anónimos en casos de crimen organizado. La investigación señala que, al resguardar a los encargados de administrar justicia, se fomenta un ambiente más seguro para el personal judicial y la población en general, y se robustece la institucionalidad.

El estudio establece un vínculo claro entre la seguridad de los administradores de justicia y la fortaleza institucional, lo cual es la piedra angular del tema de investigación. La recomendación concreta de implementar la figura de "jueces sin rostro" para casos de alta peligrosidad sienta un precedente crucial sobre el cual se puede construir la propuesta de utilizar IA como herramienta tecnológica avanzada para implementar de manera

segura, eficiente y transparente este anonimato judicial, yendo más allá de las medidas de protección físicas tradicionales.

Gallegos (2023), su investigación se enfocó en examinar la viabilidad de un sistema de jueces sin rostro en Ecuador para juzgar delitos de delincuencia organizada, garantizando que su aplicación no viole derechos esenciales como el derecho a un debido proceso y la imparcialidad. Mediante el uso de métodos científicos como entrevistas y encuestas a especialistas, los resultados fueron contundentes: el 100% de los consultados aprobó que el Estado garantice la seguridad de los magistrados en estos casos, y el 100% coincidió en que un juez amenazado no puede actuar con imparcialidad, un hallazgo respaldado por el 75% de los juristas entrevistados. La investigación concluye que Ecuador debe adoptar esta figura para salvaguardar la integridad de los jueces, evitar la coacción sobre su imparcialidad y así garantizar la correcta aplicación de justicia.

La abrumadora aprobación de los expertos hacia medidas de protección estatales subraya la urgencia social y legal del tema. La conclusión a favor de implementar la figura provee un respaldo académico sólido. El reto que se deriva de esta necesidad de proteger la identidad sin vulnerar el derecho a la defensa es precisamente donde el uso de la IA se presenta como la solución innovadora. La tecnología podría, por ejemplo, enmascarar la identidad del juez en audiencias virtuales mediante distorsión de voz y video, o gestionar el acceso a la información sensible del caso, al implementar el anonimato que propone Gallegos Mancero mientras se registra digitalmente todo el proceso para garantizar su transparencia y control posterior.

Cuarán, y Sánchez (2025), en una publicación científica, examinaron los efectos que tiene en la seguridad jurídica y el debido proceso la incorporación de jueces sin rostro en la legislación ecuatoriana. A través de un enfoque cualitativo, descriptivo y utilizando métodos como el histórico-lógico, la revisión bibliográfica y el derecho comparado (con lecciones de Colombia), el estudio identificó que esta medida puede chocar con principios como la publicidad, la imparcialidad y el derecho a una defensa plena. Los hallazgos indican que su implementación directa violaría garantías constitucionales e internacionales. Sin embargo, los autores reconocen la apremiante necesidad de elevar las medidas de protección para los jueces debido al auge del crimen organizado, concluyendo que cualquier solución debe equilibrar cuidadosamente la seguridad judicial con la preservación de los derechos procesales y la confianza en el sistema.

Esto introduce una advertencia necesaria sobre los riesgos que conlleva la figura de los jueces anónimos para las garantías del debido proceso, contrastando el marco de la investigación al presentar ambas caras de la moneda. La advertencia de los autores sobre la posible violación de derechos no invalida la necesidad de protección, sino que exige encontrar un punto de equilibrio. Es precisamente en esta brecha donde el uso de la IA encuentra su mayor potencial y justificación. La tecnología podría ser la herramienta que permita lograr ese equilibrio, por ejemplo, mediante algoritmos que garanticen el anonimato del juez hacia las partes y el público, pero permitiendo un control auditable y restringido de su identidad por un comité superior o un sistema de verificación algorítmica para garantizar la trazabilidad y evitar abusos, reconciliando así la seguridad del juez con la transparencia del sistema que preocupa a los autores.

1.2. Antecedentes doctrinarios

1.2.1. Anonimización

La anonimización es un procedimiento de carácter legal y técnico que busca impedir la identificación o reidentificación de individuos a través de la alteración o eliminación de su información (Terzidou, 2023). Esta práctica, en el terreno jurídico, representa la base de la protección de jueces, fiscales y testigos en un ambiente muy peligroso, sobre todo debido a las amenazas del crimen organizado. A través del uso de algoritmos avanzados, procesamiento de lenguaje natural y métodos de aprendizaje automático que ocultan datos sensibles en documentos procesales, se asegura la transparencia del sistema y la seguridad de los operadores judiciales.

Conforme a lo anterior, la anonimización es un proceso técnico y legal que se ha diseñado para proteger los derechos esenciales de las personas que están involucradas, ya sea directa o indirectamente, en los actos del sistema judicial. Consistir en eliminar, cambiar o reemplazar la información personal que se encuentre en las resoluciones de los tribunales (sentencias, autos, providencias o escritos del proceso) para evitar que personas ajenas a estos documentos puedan identificar a los individuos que allí aparecen (Agencia Española de Protección de Datos, 2022).

Esta práctica no solo está justificada porque es necesario proteger la privacidad de las personas, sino también porque la ley tiene el deber de proteger los datos personales, sobre todo cuando se trata de información delicada. En este sentido, la anonimización se considera una protección esencial para evitar la revictimización, el estigma o cualquier

tipo de daño colateral que pueda surgir de la divulgación no controlada de documentos judiciales.

Este procedimiento sigue una lógica de dos vías: por un lado, promueve la publicidad de los actos jurisdiccionales como principio fundamental del Estado de derecho, lo que garantiza que los ciudadanos, académicos, periodistas y otros actores sociales interesados puedan consultar las decisiones del poder judicial; por otro lado, garantiza que dicha publicidad no infrinja la dignidad ni otros derechos esenciales de las personas implicadas, sobre todo los que se encuentran en situaciones vulnerables (Poder Judicial de Chile, 2022).

La importancia de ese equilibrio se hace evidente, en particular, en situaciones de violencia de género, crímenes sexuales, casos que implican a personas menores de edad o con discapacidad, víctimas de trata y protección a testigos. La pérdida de anonimato al dar a conocer datos privados puede tener un impacto desastroso en su seguridad, su integridad psicosocial y su vida diaria. Por esta razón, la anonimización se ha transformado en una política transversal para proteger los datos personales hoy en día.

La anonimización judicial, de acuerdo con Viguri (2022), en términos prácticos, hace referencia al tratamiento de datos que son identificables como información que no posibilita la identificación de un individuo a través de una perspectiva asociativa o indirecta. Los datos que necesitan tratamiento comprenden, entre otros, nombres completos, números de identificación (como RUC, cédula o pasaporte), direcciones específicas, fechas de nacimiento, números telefónicos y vehiculares, direcciones electrónicas, nombres de usuario y datos biométricos.

Todos estos elementos son susceptibles de revelar o facilitar la identidad de una persona, por lo que deben ser excluidos o modificados cuidadosamente. La normativa suele eximir de la anonimización a entidades públicas y personas jurídicas, ya que su identificación no compromete derechos individuales, así como ciertos datos estructurales del expediente judicial, como el número de causa, que permiten su trazabilidad sin violar la privacidad de las partes.

Asimismo, la anonimización puede clasificarse en dos grandes enfoques según su grado de cobertura: total y parcial. La total es aquella en la que se eliminan o modifican todos los datos personales de los individuos naturales mencionados en el documento judicial, sin importar su rol procesal, con excepción de los operadores de justicia (jueces, fiscales, defensores públicos) cuando actúan en el ejercicio de sus funciones. Esta

modalidad proporciona el mayor nivel de protección, aunque puede limitar la utilidad del documento si se requiere una contextualización más precisa.

Por su parte, la anonimización parcial selecciona determinados sujetos para el tratamiento de sus datos, generalmente en atención a criterios de vulnerabilidad o confidencialidad, como menores, víctimas o testigos, permitiendo mantener visibles otros datos relevantes para el análisis jurídico o estadístico. Esta forma exige un mayor juicio técnico y ético, ya que implica decisiones discriminadas sobre quién debe ser protegido y por qué (Poder Judicial de Chile, 2022).

Las técnicas utilizadas para anonimizar documentos judiciales son múltiples y se deben aplicar con base en protocolos previamente establecidos por los sistemas judiciales o por las entidades encargadas de publicar las resoluciones. Entre estas técnicas se encuentran la supresión directa de datos (eliminación del contenido sensible), la pseudonimización (reemplazo de nombres por iniciales o códigos alfanuméricos), la generalización (sustitución de datos específicos por categorías generales), y la perturbación (introducción de pequeñas alteraciones irreversibles en los datos).

Es fundamental que estas técnicas aseguren la imposibilidad de reidentificar a las personas, incluso combinando la información con otros documentos públicos. Por ello, se debe realizar una evaluación de riesgo de reidentificación antes de publicar los textos. Además, los procesos de anonimización que están automatizados deben tener en cuenta las validaciones hechas a mano, porque los sistemas que procesan el lenguaje podrían no contar con datos sensibles, no estructurados o implosivos.

La finalidad última de la anonimización judicial no reduce la protección más abstracta de los datos; se ubica en un contexto más extenso que incluye el respeto a los derechos individuales y la obligación de honrar la accesibilidad de la información pública. El método posibilita que los periodistas, investigadores, estudiantes y organizaciones de la sociedad civil analicen las decisiones judiciales de un modo que no pone en riesgo la privacidad de los sujetos implicados en el proceso y que, a la vez, no exige al sistema judicial revelar innecesariamente a los ciudadanos (Guerrero, 2020).

Normalmente, la responsabilidad de llevar a cabo esta anonimización es de los departamentos técnicos de los tribunales, pero también puede recaer en las oficinas de transparencia, las unidades de tecnología judicial y, en ocasiones, hasta en las editoriales que publican artículos académicos o divulgativos donde se aplica la jurisprudencia. Estos actores tienen que estar adecuadamente capacitados y operar siguiendo estrictos estándares legales y éticos. En este marco, la anonimización judicial es una forma

concreta de cooperación entre el sistema judicial y la protección de la privacidad, así como de fomento de una justicia que sea transparente, accesible y digna del respeto humano.

Su rigor ayuda no solo a evitar perjuicios que provengan de la exposición subsidiaria de datos personales, sino también a promover una cultura de derechos en la cual la protección del individuo informado es vista no como un impedimento, sino como un componente que garantiza un sistema organizado democráticamente (Villares, 2022). Hoy en día, cuando el acceso a las sentencias por internet y la digitalización de los expedientes son cada vez más comunes, se vuelve imperativo anonimizar los órganos judiciales. Esto es fundamental para garantizar que el acceso a la justicia no se convierta en un nuevo ámbito de violación a los derechos básicos.

La eliminación del nombre de los jueces que intervienen en el proceso y la adopción de decisiones en procedimientos judiciales no es común ni está establecida como un estándar en los sistemas de jurisdicciones jurídicas comparadas o referenciales. En la práctica, las leyes relacionadas con la protección de datos personales y los principios que rigen el desempeño jurisdiccional coinciden en que los nombres y otras informaciones de identificación de los jueces deben ser publicados correctamente en las resoluciones judiciales, magistrados o tribunales que desempeñan dicha función. Esto se fundamenta en la legitimidad de las instituciones y los principios democráticos, pues el poder judicial, al actuar con imparcialidad y transparencia, está bajo mecanismos de control social. Estos controles se realizan exactamente a través de la transparencia y la divulgación pública de las operaciones (Cano, 2020).

Que el juez que emite una resolución sea visible no solo garantiza el principio de publicidad de la justicia, sino también fortalece la rendición de cuentas del sistema judicial ante los ciudadanos. Conocer qué juez o tribunal ha intervenido en un caso específico permite efectuar un análisis crítico y objetivo acerca de la imparcialidad, la coherencia y el fundamento de las decisiones judiciales; esto es esencial para mantener la confianza ciudadana en la administración judicial. Los jueces no suelen estar protegidos por esta salvaguarda debido a su rol público, que los expone a un grado de visibilidad institucional más elevado que el de las partes del proceso (los testigos, peritos o víctimas), cuya información probablemente sea anonimizada para salvaguardar su privacidad y prevenir la revictimización.

La estrategia general de anonimización de información en el sector judicial determina que el propósito principal del procesamiento de datos es evitar que se

identifique a personas que no ocupan roles centrales dentro del aparato estatal. Por lo tanto, sus datos relativos a jueces, magistrados, fiscales, defensores públicos y abogados que intervienen en un procedimiento judicial se llevan a cabo en el ejercicio de sus competencias profesionales en todo momento, excepto la anonimidad.

Esto no es simplemente una excepción, sino una respuesta a la lógica de que la divulgación de este grupo de actores tiene sus propias justificaciones, en virtud de su rol institucional y su deber de ser transparentes. El ejercicio de la judicatura implica emitir decisiones de gran importancia pública, y en ese caso, el que las emite debe firmar y fechar la decisión para asegurar la trazabilidad del proceso jurídico y la función de rendición de cuentas (Mark et al., 2021).

Sin embargo, la norma prevé excepciones en situaciones con un alto grado de particularidad y justificación. En situaciones excepcionales, si existen amenazas verificadas a la integridad personal del juez, cuando esté envuelto en litigios de alto riesgo, o haya sido blanco de ataques a la integridad de una persona destacada, o cuando haya habido antecedentes de agresiones contra el personal judicial, el organismo responsable podrá permitir que la información del magistrado sea omitida o se mantenga anónima parcialmente. Las medidas excepcionales deben implementarse con la mayor cautela y justificación posible, garantizando que su uso no se transforme en un método para debilitar el control sobre el ejercicio de la justicia en su nombre, ni en una opción que niegue al ciudadano el derecho a decidir quién administra justicia en su lugar (Bobek, 2019).

1.2.2. Datos personales

Se considera información personal a los datos que permiten identificar o identificar a alguien, como su nombre, dirección, números de teléfono o incluso referencias indirectas. Su implementación en este campo debe llevarse a cabo con especial precaución, ya que las organizaciones criminales podrían emplearlos para hostigar o amenazar al personal del sistema judicial. El propósito de las obligaciones establecidas en la Ley Orgánica de Protección de Datos Personales (2021) en Ecuador es asegurar la privacidad y resguardo de la información personal. Esto incluye la pseudonimización, el cifrado y la anonimización de esa información. Estos deberes protegen los derechos esenciales de privacidad y seguridad y garantizan que no se pueda acceder a la información sin autorización.

El principio de confidencialidad establece que quienes están a cargo de los datos

personales, en su mayoría del sector privado y público, tienen el deber estricto de no revelar dichos datos, evitar el acceso no autorizado y no emplear la información para propósitos no permitidos. Este deber no es solamente legal, sino también ética: a quien le toca, entre otras cosas, la custodia de información personal tiene un deber ético a su cargo: cuidarla como un bien valioso y personal. En la práctica, esto implica actualmente medidas de seguridad correspondientes, que pueden varían desde controles de acceso físico o electrónico hasta protocolos de manejo de los datos sensibles.

La confidencialidad pretende, en definitiva, proteger la intimidad de las personas, evitar que extraños no autorizados obtengan información que se puede utilizar en su menoscabo y asegurar que los datos se traten con confidencia en instituciones que recibieron y administra datos personales. Es, por tanto, un deber continuo que se extiende incluso más allá del fin de la relación laboral de los servidores públicos, quienes deben respetar el secreto profesional en todo momento.

El principio de minimización, por su parte, plantea la necesidad de actuar con mesura y proporcionalidad en el tratamiento de datos. No se trata de recolectar información de manera indiscriminada o preventiva "por si acaso" pudiera servir en el futuro, sino de limitar la recolección y el almacenamiento estrictamente a los datos que son necesarios para cumplir con la finalidad previamente definida y comunicada al titular (Mendoza, 2023).

En otras palabras, si cierta información no es indispensable para prestar un servicio o cumplir una función pública específica, no debe pedirse ni conservarse. Este principio busca reducir riesgos asociados a la acumulación excesiva de datos, como filtraciones masivas o usos indebidos, y promueve prácticas más eficientes y responsables. En contextos como el gobierno electrónico, donde la digitalización facilita la captura y el cruce de grandes volúmenes de información, la minimización resulta especialmente importante para evitar la creación de bases de datos innecesariamente extensas y peligrosas para la privacidad de los ciudadanos.

El principio de finalidad completa y fortalece estas obligaciones al de determinar que los datos personales solo pueden utilizarse para los fines legítimos, específicos y determinados que produjo su recopilación. Por lo tanto, quien tenga sus datos debe ser consciente con claridad para qué se están empleando y se le ha indicado el uso, el

encargado del tratamiento está obligado a cumplir ese fin sin alterar el uso a otros fines no comunicados o incompatibles (Roldán, 2021).

Ejemplo de ello son los datos recopilados para actividades estadísticas, a estos no les pueden ser destinados a fines comerciales y sin que se esté basado en una nueva legitimación legal o en el consentimiento del titular. Este principio requiere una planificación reflexiva de los procedimientos de recogida de datos y es una defensa de la transparencia de la relación entre las instituciones y el ciudadano. Además, establece un marco para controlar y limitar el poder de las entidades que recolectan datos, evitando que se produzcan situaciones de vigilancia indebida o usos arbitrarios de la información.

En Ecuador, estos principios están consagrados en la Ley Orgánica de Protección de Datos Personales (LOPDP), promulgada en 2021, la cual se inspira en estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. La legislación ecuatoriana recoge de forma explícita los principios de confidencialidad, minimización y finalidad, y obliga tanto a entidades públicas como privadas a respetarlos mediante la adopción de políticas, procedimientos y controles técnicos y organizativos adecuados. La ley también establece que el responsable de los datos tiene derecho a ser informado acerca de la transparencia y determina que debe comunicarse a la titular información fundamental sobre el procesamiento, como la identidad del responsable, los fines del tratamiento y la posibilidad de compartir los datos con terceros.

Para asegurar la aplicación de estos principios la LOPDP prevé la creación de una Autoridad de Protección de Datos de datos responsables de que se cumpla la normativa, de investigar los incumplimientos y sancionar a quienes violen los derechos de los titulares. Además, establece la obligación de implementar medidas de seguridad que sean proporcionales al riesgo del tratamiento, con el objetivo de prevenir filtraciones, pérdidas o accesos no autorizados que puedan comprometer la privacidad de las personas. La legislación ecuatoriana, así, intenta establecer un ambiente de confianza en la gestión de datos personales, salvaguardando los derechos esenciales de los ciudadanos y reforzando un alto nivel de transparencia y responsabilidad en el manejo público y privado de información.

1.2.3. Inteligencia Artificial en la Justicia

La inteligencia artificial (IA), en el marco judicial, es un instrumento estratégico para la modernización de los sistemas de protección y la gestión de riesgos. Las herramientas que se basan en inteligencia artificial tienen el potencial de optimizar la ciberseguridad institucional, el reconocimiento de patrones riesgosos y la anonimización de las sentencias. Sin embargo, es necesario equilibrar la innovación que ha sido puesta en marcha con garantías procesales para evitar situaciones de empleo sesgado o poco claro (Balcells, 2020).

La inteligencia artificial también juega un papel fundamental en la predicción de sentencias judiciales y en brindar sugerencias personalizadas, ya que es capaz de examinar enormes cantidades de datos históricos y descubrir patrones en los acontecimientos pasados. Estos sistemas son capaces, a través de modelos predictivos, de acercarse a un resultado específico en contextos de arbitraje, litigio o audiencia. Por lo tanto, son de gran ayuda para abogados, litigantes y mediadores que quieren tener en cuenta los factores positivos y negativos antes de tomar una decisión trascendental. Este tipo de análisis no reemplaza el trabajo valorativo e interpretativo de los jueces. Más bien, es una herramienta estratégica que permite elaborar argumentos y tomar decisiones informadas, además de disminuir la incertidumbre en el proceso (Rosero, 2025).

En materia de optimización y transparencia la IA ofrece herramientas para localizar zonas críticas como cuellos de botella y atrasos en el manejo de expedientes o en la convocatoria a audiencias, permitiendo reorganizar los recursos y hacer más eficiente el sistema judicial. Además de que a través de algoritmos que registran y explican el proceso de análisis por el que se llega a una recomendación o predicción se asegura la transparencia y la coherencia en las decisiones, contribuyendo al hecho de que las resoluciones sean más claras y verificables para las partes interesadas como para la sociedad en general. Esto de este modo que se refuerza la confianza social en la administración de justicia.

En la parte de apoyo a jueces y magistrados los sistemas de inteligencia artificial se comportan como asistentes expertos, criticar de expedientes largos, organizar la información principal, referenciando precedentes relevantes y advertir los aspectos jurídicos más importantes de la causa. De esta manera los operadores de justicia pueden ahorrar tiempo en tareas de revisión documental y centrarse en el análisis dogmático, sin ceder al control humano, fundamental en todas las etapas claves, por la conjuración del

cristal rocoso de la parcialidad y, sobre todo, del imperativo de los principios procesales.

Por último, la IA ayuda a la desconexión y anonimización y protección de datos en el ámbito jurisdiccional mediante técnicas que suprimen u ocultan datos personales sensible dentro de documentos legales, sentencias o bases de datos evitando que quede el registro de la identidad de los individuos involucrados. Además, también gestiona la información cumpliendo con altos estándares de seguridad digital impidiendo accesos no autorizados y saliendo de riesgos de infracción o uso de malas acciones a la información. Esto es especialmente relevante en un escenario en el que la adopción de responsabilidad para manejar datos personales no es únicamente un asunto de principios éticos, sino también una obligación legal basada en normativas nacionales e internacionales de protección de datos.

En el ámbito judicial la inteligencia artificial lo que ofrece es un conjunto de herramientas tecnológicas plurales cada una correspondiente a funciones determinadas y con alcances diversos, todos ellos implementados con el fin de llegar a las diferentes fases del proceso jurisdiccional. Su puesta en práctica no obstante va más allá de lo técnica y requiere una implementación estrictamente orientada a la respetuosa observancia de los derechos y garantías fundamentales como la transparencia, la imparcialidad, publicidad de los actos procesales, protección de datos personales y de supervisión humana continua.

A este marco de garantías pretenden ordenarlo con arbitrar que el uso de la IA aumenta la justicia y no comprometa su autoridad, sin sesgos de errores o slips que comprometa la validez de las decisiones. La adecuada selección del tipo de IA que haya de implementarse estará determinada no sólo por la fase procesal en la que se hayan de aplicar, sino también por la configuración del asunto y por las particulares demandas de cada proceso.

Entre las modalidades más importante se encuentran la IA de automatización que viene desarrollado para llevar a cabo de una manera rápida y precisa tareas administrativas y documentales. Este tipo de sistemas facilita la revisión de decenas de expedientes y la gestión digital de archivos legales, genera informes iniciales, clasifica peticiones procesales y logra tramitar solicitudes como la concesión de justicia gratuita. Al aliviar los esfuerzos operativos, la automatización libera enfoques y recursos para que jueces y demás estructuras puedan enfocarse en el análisis real de los casos legales.

Otra de las categorías en ver aumento son los asistentes virtuales o chatbots[5] legales, que se presentan como vías de comunicación interactivo para que ciudadanos y profesionales del derecho tengas la orientación. Estos sistemas pueden brindar información general de trámites, calmar dudas recurrentes, orientar en la presentación de documentos, prestan un primer mejor nivel de asesoría jurídica. Su contribución es fundamental para incrementar el acceso a la justicia mediante la disminución de la congestión en las oficinas judiciales y la optimización de la experiencia del usuario del sistema.

Del mismo modo, los sistemas de análisis forense y EDI (de pruebas electrónicas) cuentan con perfiles especializados en el estudio y procesamiento de grandes cantidades de pruebas digitales, como documentos electrónicos, vídeos, grabaciones e imágenes. Estos sistemas ayudan a las investigaciones, identifican información importante y reportan de forma objetiva sobre valoraciones que apoyen el trabajo judicial. Es más sencillo identificar elementos de prueba que podrían ser pasados por alto al analizar datos únicos manualmente, gracias a su capacidad para examinar información compleja y multimodal.

Por otra parte, están los algoritmos de predicción judicial, que son técnicas de aprendizaje automático cuyo propósito es anticipar el desenlace futuro de un juicio o una sentencia y asesorar en relación con riesgos, como la posibilidad de reincidencia en un asunto penal o la ausencia de sanción en un litigio civil. Aunque no es preciso usarlas, se consideran estas previsiones un instrumento útil para definir estrategias legales e incluir componentes analíticos que optimizan el proceso de toma de decisiones humanas. La IA generativa es un progreso innovador porque posibilita que se hagan de manera automática documentos, currículos y estudios legales. También juega un papel clave en la investigación tecnológica. Además, puede ser útil para anonimizar datos y proteger así la información personal y asegurar

Detectar patrones se ha vuelto una herramienta sumamente útil para identificar similitudes y conexiones entre precedentes, casos, peticiones y decisiones. Esta habilidad permite que los criterios judiciales sean coherentes, que se encuentren de manera efectiva los precedentes y que se formulen argumentos legales más firmes. La combinación de

[5] Programa informático que simula una conversación con usuarios finales humanos

tecnologías de inteligencia artificial, que operan bajo la supervisión humana y en el contexto de procesos de garantía, está lista para revolucionar cómo funciona el sistema, mejorando su eficiencia, fiabilidad y accesibilidad.

En las etapas tempranas del proceso, la inteligencia artificial se comporta como un potente potenciador de la capacidad gerencial. Los sistemas de recepción y clasificación electrónicas y automatizadas posibilitan la rápida inscripción de expedientes, la obtención de información relevante a través del tratamiento del lenguaje natural y OCR, así como la realización de una evaluación inicial sobre el origen y la experiencia. Estas herramientas hacen posible la gestión de las solicitudes de asistencia jurídica gratuita mediante formatos inteligentes que facilitan inspeccionar requisitos previos, identificar vacíos y clasificar los casos según su urgencia.

No obstante, esta automatización conlleva también ciertos peligros específicos, por ejemplo: la adopción de decisiones equivocadas al principio, debidas a prejuicios en los modelos de clasificación; o la marginación de individuos con escaso grado de alfabetización digital. Por lo tanto, su uso tiene que asegurar la apertura de los principios nuevos, notificar a las partes sobre el empleo de la IA y proporcionar procesos simples para pedir la revisión de cualquier decisión fundamentada en automatización.

En el transcurso de la investigación y la valoración de pruebas, la IA pliega sus capacidades analíticas en su aspecto más espectacular técnico: sistemas analíticos forenses digitales pueden extraer metadatos, reconstruir trayectorias temporales, imputar comunicaciones y detectar secciones de alteraciones en archivos; algoritmos de visión por computadora procesan imágenes y grabaciones analizando datos, objetos o eventos relevantes, al tratarse de procesos automatizados que comportan ejercicios más rigurosos que cualquier observación humana.

Estas capacidades precisamente aceleran el orden estatuto un montón el anglo-fase probatoria y a fuerza contraria se pueden hallar conexión que fueron fatídica de cifraría manualmente. Pero la validez de estos resultados depende de protocolos de buena custodia de la cadena digital, validación tecnológica de algoritmos (incluyendo pruebas contra deepfakes[6] y manipulaciones), documentación completa de los procesos de

[6] Video, imagen o audio creado o modificado con inteligencia artificial para mostrar a personas reales o ficticias haciendo o diciendo algo que nunca hicieron.

extraído y la necesidad de exhibir la revisión humana en la prueba interpretativa, de forma que peritos y operadores judiciales puedan contextualizarlos, certificar la integridad de la información y hacer que los sofisticados métodos usados sean descritos en audiencia (González, 2023).

Recogiendo la gestión y tramitación del expediente, la IA nutre los sistemas de gestión procesal para mejorar la carga redistribución, el control de plazos y orden documental. Automatizar es posible clasificar textos, destinar los expedientes a despachos o competencias jurisdiccionales correspondientes según criterios objetivos, enviar recordatorios automáticos de vencimiento de plazos procesales y enviar notificaciones electrónicas a las partes.

Hacia un nivel más avanzado, modelos predictivos de demanda de carga de trabajo facilitan la planificación de personas y audiencias y la reasignación de audiencias para ahorrar tráfico mientras se les toma a los asistentes de resumen automático los hechos y los puntos jurídicos principales para preparar audiencias. Para que estos beneficios pasen a ser una mayor eficacia real sin la pérdida de derechos, es necesario la implementación de fuertes controles de acceso, registros de auditoría que documenten todas las intervenciones algorítmicas, políticas de retención y eliminación de datos y procedimientos para ser revertidas o corregidas dichas asignaciones por razones de equidad o especialidad del caso.

Cuando se llega a la resolución y sentencia, la IA puede tener función de apoyo sofisticada mediante algoritmos de análisis prospectivo que, basados en jurisprudencia y datos histórico estima rangos probables de resultado, hasta rangos de tipicidad del padecimiento o, en cualquier caso, relación directa o indirecta con el caso reproducido. Estas previsiones incorporan un elemento estadístico y comparativo de las asociaciones y vacíos de las variables jurídicas como parte de un grupo de herramientas operativas para capacitar a jueces y litigantes. Aun así, su naturaleza correlacional pide precaución, las recomendaciones no deben reemplazar la apreciación jurídica individualizada (Lima et al., 2023).

Por eso, en la fase decisoria cualquier uso de IA debe sujetarse a normas de explicabilidad (por la que se pueda entender cómo se produjo la recomendación), de trazabilidad (registro exhaustivo de todos los datos y versiones del modelo), y de

supervisión humana vinculante, asegurando que la decisión final sea del juez y exigible en sede de contiendas judiciales. Además, los sistemas utilizados deben ser objeto de auditorías por mandato y pruebas que identifiquen sesgos u impactos desproporcionados sobre grupos protegidos, garantizando así coherencia y legitimidad en el ámbito de la administración de justicia (Contini, 2019).

En la materia del asesoramiento y la ayuda al usuario los chatbots y asistentes inteligentes basados en IA amplían el acceso a la información procesal y orientación práctica para particulares y profesionales. Estos registros pueden orientar en la cumplimentación de los formularios, informar a plazos y requisitos, dar plantillas de escritos o incluso ayudar a redactar intervenciones básicas, con disponibilidad las 24h del día y con habilidades multilingües y accesibilidad para personas con discapacidad.

Su contribución es especialmente importante para litigantes desprotegidos porque a la vez que reduce las barreras que impiden a estas personas iniciar una demanda. En cualquier caso, es preciso clarificar: los asistentes deben dejar claro que no reemplazan la asesoría jurídica profesional, proporcionar opciones para derivar a atención humana y garantizar la confidencialidad de las comunicaciones mediante encriptación y políticas de privacidad que limiten el uso y la reutilización de los datos.

En todas estas etapas se evidencian una serie de dificultades y reclamaciones transversales que meritan más profundización. La gobernanza de datos se vuelve indispensable: lo primero que hay que hacer es dejado claro orígenes, calidad y consentimiento para que la información pueda ser manejada, establecer medidas de minimización y anonimización cuando proceda, mantener controles para evitar reidentificación no autorizada (Lima et al., 2023).

A la hora de los derechos fundamentales, las apps tienen que pasar a estar sujetas a evaluaciones de impacto algorítmico que mediten riesgos de privacidad, de igualdad y de tramitación procedente, han de estos remedios y tribunales ante decisiones automatizadas, y en los diseños técnicos han de insertar medidas de corrección para el sesgo, pruebas de equidad, y estrategias de monitoreo continuo para detectar la deriva del modelo (m*odel drift*).[7] Desde la organización, poner en marcha la IA requiere formación

[7] Disminución de la precisión de un modelo de aprendizaje automático con el tiempo debido a cambios en los datos del mundo real que ya no coinciden con los datos históricos con los que fue entrenado

para jueces, funcionarios y peritos; protocolos de concesión que hagan que haya una documentación técnica (*model cards*,[8] *data statements*[9]); y políticas públicas que delimiten el uso, transparencia proactiva, y responsabilidad institucional (Cumbre Judicial Iberoamericana, 2023).

Una vez llegados al camino de implementación es aconsejable seguir una estrategia gradual, fundada sobre proyectos piloto evaluados externamente con indicadores precisos de impacto procedimental y derechos y con participación ciudadana para legitimar los criterios de priorización y los mecanismos de salvaguardia. Por ello, la IA puede revolucionar componentes operativos y analíticos del proceso judicial a través de la aceleración de trámites, la gestión más eficiente de prueba y la expansión de la accesoria la justicia sin comprometer la neutralidad, la publicidad y la protección de las garantías procesales que fundan al Estado de derecho.

Una vez llegados al camino de implementación es aconsejable seguir una estrategia gradual, fundada sobre proyectos piloto evaluados externamente con indicadores precisos de impacto procedimental y derechos y con participación ciudadana para legitimar los criterios de priorización y los mecanismos de salvaguardia. Por ello, la IA puede revolucionar componentes operativos y analíticos del proceso judicial a través de la aceleración de trámites, la gestión más eficiente de prueba y la expansión del acceso a la justicia sin comprometer la neutralidad, la publicidad y la protección de las garantías procesales que fundan a el Estado de derecho (Lavin et al., 2024).

A partir de ella, la transparencia es un pilar fundamental para hacer compatible el uso de la IA en procesos judiciales. Significa que cualquiera puede intervenir, analizar o sugerir producido por sistemas de algoritmos debe constar en el expediente, visible y accesible a jueces, partes y, cuando sea el caso, públicos. Esto va más allá de una mera anotación genérica de que se utilizó IA, metiendo contenido como metadatos o informes en los que se describa el tipo de herramienta utilizada, los criterios de análisis, las fuentes de datos utilizadas y los límites conocidos del sistema.

La transparencia procesal no se trata solo de un formalismo: permite que el juez pueda efectuar una revisión sustantiva sobre el valor probatorio o consultivo de la

[8] Documento conciso que acompaña a los modelos de aprendizaje automático.
[9] Declaración breve incluida en una publicación científica que informa al lector sobre la ubicación y las condiciones para acceder a los datos que respaldan los resultados del estudio

intervención tecnológica, así como a las partes se les proporcione la materia de la que pueda precisar para cuestionar, complementar o contextualizar esos resultados. Además, proporciona auditorías externas e independientes y control externo, evitando la "caja negra" algorítmica que podría socavar la confianza pública.

En términos de imparcialidad equidad el desafío está en evitar sesgos algorítmicos que replican o agraven discriminación preexistente si es por contenido de datos de entrada o si es error en diseño o si es aplicación de criterios estadísticos inapropiados. En el ámbito judicial donde predomina el principio de igualdad procesal, cualquier sesgo se traducirá en trato desigual entre las partes o en discriminación a grupos históricamente marginados. Por eso es necesario que se realicen auditorías periódicas de equidad, pruebas de definitivo no discriminación y corrección, mediatizada por medias automáticas o manuales de sesgo detectado. Asimismo, los algoritmos deben ser transparentes, para así poder distinguir si sus decisiones están influenciadas por factores irrelevantes o ilegítimos para el motivo. La neutralidad tecnológica no es inducida: es producto de una programación deliberada, un entrenamiento asistido por supervisión, una supervisión continua.

El principio de publicidad de las decisiones judicial, incluso aquellas que la Justicia ha tenido en cuenta con asistencia tecnológica, debe ser accesible y transparente para las partes y para la sociedad, excepto en aquellos supuestos en los que la ley establezca limitaciones por razones de seguridad, protección de víctimas o secreto profesional (Lavin et al., 2024). Esto significa que, si es utilizada IA en el proceso decisorio o de valoración probatoria debe decirlo en la sentencia o resolución, además de la explicación de cómo incurrió en el razonamiento final del juez. Esta demanda además de garantizar participación ciudadana y transparencia fortalece la confianza en la justicia, demostrando que la tecnología es un complemento y no una sustitución de la toma de decisiones humanas.

La protección de la privacidad y de datos personales es otro de los pilares clave, puesto que en muchas ocasiones la IA judicial trata con datos sensible como los del salón médico, de órdenes de persecución policiales, correos personales, antecedentes penales, etc. Para proteger este derecho hay que implementar mecanismos de anonimización y pseudonimización de la información, protocolos de encriptación, control riguroso de accesos y políticas de retención y destrucción segura de los mismos al cesar su propósito

procesal. La protección no es solamente tecnológica, sino también, legal: debe basarse en la normativa nacional de protección de datos y estándares internacionales, evitando que ningún perfil de tratamiento supere lo necesario para el fin justificante. Asimismo, se debe incluir la capacidad de las partes a acceder a cuáles han sido los datos que ha tratado la IA y bajo qué criterios (Rosero, 2025).

El principio de legalidad y supervisión humana significa que a la IA no le está permitido operar fuera de marcos legales ni reemplazar el juicio crítico de un juez o tribunal. Este dictamen implica que un uso de la tecnología tiene que estar en los marcos legales claros, tenga respeto por las garantías del debido proceso y en su nivel final de toma de decisiones, la intervención esté decidida por un operador humano. La supervisión no puede tener un contenido solo formal debe incluir un juicio activo en el que el juez piense si la propuesta mecanicista es compatible con el marco legal con los hechos probados y con el principio de justicia. Lo de la IA, en este contexto, es una herramienta de ayuda, pero la toma de decisiones sigue siendo humana y jurídicamente responsable (Lima et al., 2023).

Por otro lado, para que el empleo de estos sistemas sea responsable, es necesaria una regulación sólida, con normativas claras acerca de su creación, desarrollo, supervisión y auditoría. Es imprescindible que haya mediaciones que impidan la usurpación de funciones judiciales, detecten y contrarresten sesgos, y además posibiliten la trazabilidad y la explicación detallada de cada intervención tecnológica.

Si no existe una regulación específica o si los controles se ejecutan de manera demasiado permisiva, la legitimidad del sistema judicial corre el riesgo de verse en peligro. Esto puede dar lugar a circunstancias de trato desigual, violación de derechos fundamentales o falta de transparencia. Por ende, es fundamental que las políticas públicas respalden la implementación de la inteligencia artificial en el sistema judicial, controles y protocolos técnicos para asegurar que haya coherencia entre salvaguardar las libertades procesales y la innovación tecnológica.

1.2.4. Protección de identidad

Es esencial resguardar la identidad de los operadores de justicia para asegurar un Estado de Derecho y una judicatura autónoma. El *doxing*,[10] el espionaje digital y la

[10] El acto de recopilar y publicar información privada e identificable de una persona en internet sin su

divulgación de datos privados son peligros que buscan amedrentar o cooptar a los jueces y fiscales. En esta línea, serán necesarios sistemas completos que incorporen el anonimato de archivos, la codificación de las conversaciones y los mecanismos de protección digital. La aplicación de estas acciones, en combinación con modificaciones en la ley y capacitación especializada, hará posible prevenir agresiones y mejorar la confianza que los ciudadanos tienen en el manejo de justicia (Veronese & Nunes, 2021).

Es pertinente mencionar el principio de transparencia que se encuentra en el Artículo 12 del Código Orgánico Administrativo (2017): "Art. 12.- Principio de transparencia." De acuerdo con este Código y la ley, los individuos tendrán acceso a la información pública y de interés general, así como a los registros, expedientes y archivos administrativos. Esta norma enfatiza la relación entre el acceso a la información pública y el principio de transparencia que debe regir las acciones del Estado. Así, la definición que da el Artículo 5 de la LOTAIP es más adecuada.

Según esto, se considera información pública a cualquier documento que esté en poder de las instituciones públicas (o privadas mencionadas en la ley) y que no tenga en cuenta su formato. También a aquellos documentos cuya responsabilidad recaiga sobre estas entidades o que hayan sido elaborados con fondos estatales. Esta idea se completa con el principio que está en la letra a) del artículo 4 de la ley pertinente, el cual establece que los ciudadanos tienen la propiedad de la información pública. El acceso a la información debe ser garantizado por el Estado y las instituciones privadas que tienen los archivos públicos.

En relación con la difusión de la información que gestionan las entidades públicas, el Artículo 7 de la ley representó un progreso importante al requerir a estas entidades que divulguen en sus sitios web, por motivos de transparencia, la estructura organizativa, los nombres de sus autoridades, el directorio institucional, las retribuciones económicas, los planes y programas implementados, la base legal bajo la cual opera cada entidad, los horarios para atender al público, así como su dirección y números telefónicos y otras formas de acceso disponibles para el público en general; además de los formularios necesarios para presentar solicitudes o reclamaciones.

Este fue un procedimiento verdaderamente revolucionario, ya que antes era casi

consentimiento.

un misterio o incluso un "secreto de Estado" que los ciudadanos supieran información sobre el funcionamiento, las actividades, los planes, los puestos de trabajo, la clase de documentación y otros aspectos de una institución específica. Pedir estos datos significaba largos y complejos trámites burocráticos para conseguir la información requerida.

Sin embargo, hoy en día también es necesario seguir un proceso administrativo para acceder a la información, como se explicará más adelante, siendo pertinente reiterar que la administración pública se basa en satisfacer las necesidades de las personas y el interés general. Por lo tanto, su adecuado ejercicio requiere especialmente que se cumplan las normas individuales o generales. Para ello, existe un procedimiento administrativo ajustado a dichas normativas.

1.2.5. Ciberseguridad

La ciberseguridad en el campo judicial significa implementar acciones técnicas y organizativas para proteger los sistemas y la información de accesos no autorizados, filtraciones o ciberataques (Parlamento Europeo, 2024). En Ecuador, la ausencia de protocolos estandarizados y los sistemas detallados generan vulnerabilidades que son aprovechadas por el crimen organizado. Para proteger la infraestructura digital y la información delicada de los operadores de justicia, son esenciales estrategias como el control predictivo de riesgos utilizando inteligencia artificial, la vigilancia inteligente y el cifrado homomórfico.

De acuerdo con Rodríguez-Márquez (2021), los sistemas judiciales contemporáneos custodian datos de extrema sensibilidad que incluyen expedientes judiciales completos, información personal de ciudadanos, correspondencia institucional reservada y documentos legales que, de ser comprometidos, podrían destruir vidas, alterar sentencias o socavar la credibilidad de la administración de justicia. Esta protección se ha convertido en un imperativo ante la creciente sofisticación de las amenazas cibernéticas que apuntan específicamente a las instituciones de justicia.

En los últimos años se ha observado un incremento alarmante de ciberataques dirigidos contra instituciones judiciales en múltiples jurisdicciones a nivel global. Estas ofensivas digitales se manifiestan mediante *ransomware*[11] que secuestra sistemas,

[11] Tipo de software malicioso (malware) que cifra los archivos de un equipo o sistema y exige un pago.

campañas de *phishing* dirigidas a funcionarios judiciales, filtración masiva de datos sensibles e incluso operaciones de ciberguerra entre estados-nación. Esta tendencia evidencia la vulnerabilidad crítica de las infraestructuras digitales judiciales, particularmente en un contexto de transformación digital acelerada donde la digitalización masiva de expedientes y servicios judiciales ha expandido exponencialmente la superficie de ataque disponible para delincuentes informáticos (Morán, 2021). Cada nuevo sistema digital implementado representa una potencial puerta de entrada que, si no está adecuadamente protegida, pone en riesgo no solo la privad de las personas sino la propia integridad funcional del sistema judicial.

Frente a este panorama de amenazas, Cáceres (2017) indica que la formación especializada del capital humano emerge como una línea de defensa primordial. La capacitación continua de personal judicial, administrativo y técnico en materia de ciberseguridad se ha vuelto tan crucial como la implementación de tecnologías avanzadas. Técnicas como la inteligencia de fuentes abiertas (OSINT) permiten identificar proactivamente amenazas, proteger evidencias digitales críticas para los procesos judiciales y responder de manera efectiva ante incidentes de seguridad. Además, la naturaleza compleja de estos desafíos demanda perfiles profesionales multidisciplinarios que combinen conocimientos jurídicos profundos con competencias técnicas especializadas, creando así equipos capaces de entender tanto el marco legal como los aspectos tecnológicos de la ciberseguridad judicial.

El marco normativo y la gestión estratégica de la ciberseguridad representan otro eje esencial para la protección efectiva de los sistemas judiciales. La ausencia o insuficiencia de marcos legales modernos específicamente diseñados para delitos informáticos en numerosas jurisdicciones, sumada a la crónica falta de inversión en infraestructuras de seguridad robustas, crea vulnerabilidades sistémicas difíciles de mitigar. Se requiere desarrollar políticas de seguridad comprehensivas, establecer centros de operaciones de seguridad (SOC) especializados, actualizar normativas obsoletas y fomentar la cooperación internacional para fortalecer las defensas judiciales frente a ataques transnacionales. Solo mediante este enfoque integral puede garantizarse la continuidad operativa y mantener la confianza ciudadana en la administración de justicia (Pérez, 2021).

1.2.6. Debido proceso

Para asegurar que el asunto se resuelva de manera imparcial, para proteger los derechos de las partes y para dar a conocer las acciones del procedimiento, el debido proceso se convierte en un principio esencial en la administración de la justicia (Bodero et al., 2024). La implementación de tecnologías, especialmente en el caso de la inteligencia artificial (IA), viola este principio por problemas significativos. Los parámetros de cifrado o anonimización no tendrían que ser obstáculos que limiten el ingreso a la documentación accesible y a la transparencia. Por lo tanto, se implementan procedimientos que mantienen en secreto la identidad de los roles de riesgo sin poner en peligro las garantías del proceso, logrando así un balance entre la protección y una justicia abierta y responsable.

Sin embargo, enfocándonos un poco más en las pautas de valoración probatoria que se presentaron en el capítulo anterior. Es necesario cuestionarnos si estos principios básicos son compatibles con la aplicación de IA en el contexto de la justicia penal. Como es sabido, estos derechos están directamente conectados: la dignidad humana, la paz, así como el resguardo de las minorías y de los grupos más vulnerables o débiles (Carbonell, 2007, p. 73-75). Es por ello por lo que, se debe tener una especial consideración al momento que se aborden causas que involucren a grupos minoritarios de la sociedad. Pues históricamente se ha invisibilizado su participación a nivel político y jurídico. Existen precedentes de sistemas de inteligencia artificial que han atentado contra la presunción de inocencia.

Un ejemplo es el sistema Compas, en el que la agencia de noticias independiente Propública examinó las calificaciones de riesgo otorgadas a más de 7.000 individuos detenidos en Broward, Florida, durante 2013 y 2014. Luego, determinó el número de personas acusadas por nuevos delitos en los dos años posteriores, lo que corresponde al mismo parámetro empleado por quienes desarrollaron el algoritmo. La puntuación demostró ser muy poco confiable para predecir los crímenes violentos: solamente el 20% de los individuos a quienes se pronosticó que perpetrarían delitos violentos lo hicieron.

Cuando se tuvo en cuenta una amplia gama de delitos, incluidos delitos menores como conducir con una licencia vencida, el algoritmo fue algo más preciso que lanzar una moneda al aire. De los que se consideró probable que reincidieran, el 61 por ciento fueron arrestados por cualquier delito posterior en un plazo de dos años. Además, encontramos diferencias raciales notables. El algoritmo erróneamente predijo a quién volvería a

delinquir, con una proporción similar de acusados negros y blancos, aunque de formas muy distintas (Angwin et al., 2016).

El precedente presentado nos demuestra que no solamente se está emitiendo un juicio de valor sobre los ciudadanos sin que se determine su culpabilidad ante una autoridad competente, sino que también ese juicio de valor en múltiples casos a resultado erróneo. Si bien, existen pocos incidentes en el que un sesgo prejuicio algorítmico haya generado una vulneración a la presunción de inocencia, al ser los sistemas de inteligencia artificial predictivos, siempre existe el riesgo de que este se produzca. Por ello los usuarios del sistema tienen una responsabilidad para con los beneficiarios de la administración de justicia, pues a ellos les corresponde corregir y prevenir la existencia de estos sesgos y prejuicios.

Roa y Sanabria-Moyano (2022) describen algunas de las cualidades que comparten los sistemas predictivos de inteligencia artificial. Por ejemplo, en lo que respecta a los algoritmos predictivos del riesgo, son patrones matemáticos fundamentados en la automatización del procedimiento de predecir el comportamiento de una persona mediante un score (puntaje) que establece su nivel de riesgo. Se emplean en los procedimientos de toma de decisiones, como por ejemplo para implementar medidas cautelares o después de la condena en un proceso judicial. Por ejemplo, los algoritmos mencionados respaldan las actividades policiales mediante datos automatizados en tiempo real sobre las zonas donde se deben desplegar operaciones de policía.

Conforme a ello, incluso se han utilizado sistemas de inteligencia artificial predictivos para determinar si se le debe otorgar o no a una persona medidas alternativas a la pena privativa de la libertad. Uno de ellos es el PSA (*Public Safety Assessment*),[12] que ha sido empleado para establecer si el procesado puede seguir en libertad hasta la fase de juicio, considerando el grado de riesgo de reincidencia o no comparecencia en la audiencia del juicio. El LSI-R (*Level of Service Inventory-Revised*) es otro algoritmo que se utiliza para predecir riesgos,[13] que se aplica en las salidas y la libertad condicional de los acusados; aquí, la ponderación se basa en factores como los antecedentes penales, el lugar donde reside, la educación, el trabajo, el ocio, la familia y problemas relacionados

[12] Herramienta de evaluación de riesgos utilizada por los jueces en muchos lugares de Estados Unidos para ayudarlos a tomar decisiones sobre si liberar o no a un acusado antes de su juicio.
[13] Herramienta de evaluación actuarial que se utiliza en el sistema de justicia penal para medir los factores de riesgo y las necesidades criminógenas de los delincuentes.

con alcohol o drogas, así como actitudes personales y emocionales.

Por otro lado, se encuentra el algoritmo HART (*Harm Assessment Risk Tool*),[14] su función consiste en anticipar el grado de riesgo de que las personas cometan delitos en un periodo de dos años, utilizando elementos como la edad, el sexo y el historial delictivo. Este algoritmo contribuye a establecer si un individuo con bajo riesgo puede ser enviado por los agentes policiales a un programa de rehabilitación llamado *Checkpoint*[15] (Roa y Sanabria-Moyano, 2022).

Este uso ajeno a las labores de apoyo y redacción podría llegar a ser el punto de no retorno desde el cual la IA se volvería incompatible con los principios del procedimiento penal. El juicio previo que se ejecuta incluso podría terminar influyendo en el criterio de un juez al momento de resolver sobre la situación de un procesado privado de la libertad. Potencialmente este rango de vulneración podría expandirse hasta principios como el principio de duda razonable. Gracias a los ejercicios de estos sistemas aplicados en Estados Unidos existen evidencias de que estos sistemas no son exactos, tienen un muy amplio rango de error, y son vulnerables a la producción de sesgos algorítmicos, frente a la limitada información que se le puede ofrecer al sistema de procesamiento de datos.

1.2.7. Seguridad judicial

La seguridad judicial va más allá de la protección física de funcionarios, abarcando también la integridad de sus datos, la independencia institucional y la capacidad del Estado para imponer el orden legal. Amenazas como el narcotráfico y la corrupción sistémica han expuesto las limitaciones de los mecanismos tradicionales, haciendo indispensable un enfoque integral. Esto incluye reformas legales, inversión tecnológica y cambios culturales que promuevan la adopción de IA, sistemas de alerta temprana y protocolos de anonimización, consolidando un modelo de justicia resiliente frente a la criminalidad organizada (Ramírez & Alvarado, 2025).

Rodríguez-Márquez (2021) señala que la integridad y autonomía de los administradores de justicia dependen cada vez más de su seguridad en el entorno digital,

[14] Algoritmo de inteligencia artificial que evalúa el riesgo de que una persona reincida, cometa crímenes violentos o desaparezca.
[15] Punto de control que permite monitorear, verificar o guardar el estado de un sistema o proceso en un momento dado

un aspecto que ha adquirido una relevancia crítica ante el aumento de las amenazas tanto físicas como virtuales. La protección judicial ya no se limita a la seguridad física de las instalaciones o las personas, sino que se extiende a la preservación de su independencia decisoria y al resguardo de su información personal y profesional frente a ciberataques, fugas de datos, hostigamiento en línea y campañas de desprestigio orquestadas a través de plataformas digitales. Este entorno ha hecho necesario desarrollar marcos de seguridad integrales que aborden tanto los riesgos tradicionales como los emergentes.

Entre los peligros digitales más significativos a los que se enfrentan los jueces se encuentran el acceso ilícito a sistemas que contienen expedientes o datos sensibles, la suplantación de identidad en redes sociales con el fin de perjudicar su credibilidad o manipular sus resoluciones, el acoso mediante mensajes intimidatorios y campañas de desinformación, así como la vigilancia encubierta de sus actividades digitales para obtener ventaja o ejercer presión indirecta (Bustamante & Marín, 2021). Estos riesgos exigen no solamente medidas técnicas avanzadas, sino también una capacitación continua en ciberseguridad dirigida a los operadores judiciales, la implantación de autenticación multifactorial y cifrado de comunicaciones, protocolos ágiles de respuesta ante incidentes y evaluaciones periódicas de vulnerabilidades en los sistemas utilizados.

1.3. Antecedentes normativos

1.3.1. Constitución de la República del Ecuador

El artículo 66 de la Constitución de la República del Ecuador (2008), consagra una serie de derechos esenciales que establecen la dignidad del ser humano y la existencia en términos de autonomía y seguridad. En particular, el apartado 3 establece que se posee potestad a la integridad personal de manera amplia, incluyendo dimensiones morales, psicológicas, físicas y sexuales. Este derecho supone que nadie debe ser sometido a circunstancias o daños innecesarios que tengan el potencial de perjudicar su físico, su bienestar mental, su moralidad o su libre determinación en términos sexuales. Este aspecto es especialmente relevante en el campo legal. Si una sentencia muestra datos sensibles de un individuo, especialmente en circunstancias de abuso, agresión o crímenes de naturaleza sexual, tal divulgación podría ser vista como una novedosa manera de afectar su integridad, aunque esta vez a nivel institucional.

Por lo tanto, la anonimización no solo es requerida, sino que además se considera una herramienta indispensable para proteger el derecho a la integridad. Además, el inciso en cuestión determina que se tiene derecho a vivir sin violencia. Este derecho incluye no

solo la violencia física, sino también otras formas de violencia que pueden surgir de una exposición inapropiada mediante documentos públicos, como la simbólica, mediática o psicológica. En este contexto, la anonimización resguarda particularmente a individuos en condición de vulnerabilidad, como son los niños, las niñas, las mujeres, los adolescentes, los adultos mayores y las personas con discapacidades.

Esto se alinea con el deber irrenunciable del Estado de prevenir, erradicar y sancionar cualquier manifestación de violencia. Dicha obligación tiene su fundamento directo en la Constitución, la cual, en su Artículo 66, reconoce y garantiza una serie de derechos esenciales. Entre ellos, se consagra el derecho a la integridad personal en sus dimensiones física, psíquica, moral y sexual, así como el derecho a una vida libre de violencia tanto en el espacio público como en el privado. Es precisamente a raíz de estos derechos que el Estado está constitucionalmente compelido a adoptar todas las medidas necesarias para combatir la violencia en todas sus formas, al mismo tiempo que debe garantizar el derecho a la intimidad personal y familiar.

Asimismo, el numeral 20 del artículo 66 establece el derecho a la intimidad personal y familiar, derecho que cobra una importancia trascendental en los procesos judiciales, en los que, a menudo, se ventilan aspectos sumamente privados de la vida de los individuos: relaciones familiares, enfermedades, prácticas sexuales, conflictos económicos, entre otros. El principio de publicidad de los fallos judiciales no debe interpretarse como una autorización para vulnerar la intimidad de los ciudadanos. La anonimización judicial representa el mecanismo técnico y jurídico mediante el cual se resguarda este derecho, permitiendo la difusión de decisiones judiciales sin divulgar elementos que identifiquen directamente a las personas involucradas. La protección de la intimidad no es simplemente una cuestión de discreción: es un mandato constitucional y una condición para el pleno ejercicio de los derechos humanos en el ámbito de la justicia.

1.3.2. Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales (2021), por su parte, constituye el instrumento jurídico fundamental que regula el uso y tratamiento de los datos personales en Ecuador. Su artículo 2 define el ámbito de aplicación material y especifica que esta normativa aplica al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizado o no. Esto incluye, sin duda, las sentencias judiciales que se emiten en formato digital o físico, y que pueden ser almacenadas, procesadas y difundidas por diferentes órganos del Estado.

De acuerdo con el Artículo 2, sobre el ámbito de aplicación material, esta ley regula el tratamiento de datos personales sin importar el tipo de soporte en el que se encuentren, ya sea automatizado o no, así como cualquier uso posterior de los mismos. Se establece que son de acceso público y pueden ser tratados los datos de contacto de profesionales, así como la información de comerciantes, representantes, socios, accionistas de empresas y servidores públicos.

Esta permisibilidad está condicionada a que los datos se refieran estrictamente al ejercicio de sus actividades laborales, profesionales, comerciales o funciones públicas. Los datos que se pueden tratar bajo esta premisa incluyen nombres y apellidos, el puesto o funciones que desempeñan, direcciones postales o electrónicas y números de teléfono de carácter profesional. Adicionalmente, y específicamente para los servidores públicos, también se consideran de acceso público y, por lo tanto, susceptibles de tratamiento, el historial y la situación actual de sus declaraciones patrimoniales y de sus remuneraciones (Ley Orgánica de Protección de Datos Personales, 2021, artículo 2).

Si bien se establece una excepción en los casos de tratamiento de datos por parte de entidades estatales en funciones penales, esta excepción no significa una carta blanca para vulnerar los derechos fundamentales. La misma norma impone el cumplimiento obligatorio de los estándares internacionales en materia de derechos humanos y los principios de legalidad, proporcionalidad y necesidad.

En consecuencia, es imperativo que el manejo de la información, incluso en el contexto de causas penales y datos judiciales, se realice con sumo cuidado y respeto. El objetivo fundamental debe ser minimizar los riesgos de identificar o exponer indebidamente a las personas implicadas. Para lograr esto, una herramienta clave es la anonimización, definida legalmente como la aplicación de medidas destinadas a impedir la identificación o la reidentificación de una persona natural, sin que esto requiera esfuerzos desproporcionados (Ley Orgánica de Protección de Datos Personales, 2021, artículo 4).

El artículo 4 de la misma ley describe el proceso de anonimización como un conjunto de medidas con el propósito de evitar que una persona natural sea identificada o reidentificada sin que se requiera un esfuerzo excesivo. Esta definición es fundamental para comprender que la anonimización no se limita a suprimir nombres, sino que consiste en adoptar una perspectiva integral para impedir que una persona sea individualizada por la combinación de diferentes datos. Esto quiere decir que en el ámbito judicial deben eliminarse no únicamente los nombres completos, sino también otras cosas como las

fechas exactas de nacimiento, las direcciones específicas, las relaciones familiares o detalles singulares del caso que puedan conducir a identificar a los implicados. La finalidad es lograr un verdadero anonimato, que permita publicar la sentencia sin comprometer la privacidad de quienes participaron en el proceso.

De acuerdo con el Artículo 7, el tratamiento de datos personales se considera legítimo y lícito cuando se da alguna de las condiciones que allí se establecen. Una de estas condiciones, señalada en el punto 4, es que dicho tratamiento esté fundamentado en el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos que le hayan sido conferidos al responsable del tratamiento.

Estos poderes deben derivarse de una competencia específica que le haya sido atribuida por una norma legal, es decir, una ley. Sin embargo, este ejercicio no es absoluto, ya que está sujeto a varios requisitos: debe cumplir con los estándares internacionales de derechos humanos aplicables a la materia, respetar los principios establecidos en esta ley y actuar siempre bajo los criterios de legalidad, proporcionalidad y necesidad (Ley Orgánica de Protección de Datos Personales, 2021, artículo 7).

De acuerdo con el artículo 7, el tratamiento de datos personales se considera lícito y legítimo bajo ciertas condiciones, siendo una de ellas la que se fundamenta en el interés público o en el ejercicio de potestades públicas establecidas por la ley. En este contexto, la administración de justicia, al ser un servicio público esencial, requiere por su propia naturaleza transparencia y estar sujeto al escrutinio y supervisión ciudadana. No obstante, no se justifica el interés público si se divulgan indiscriminadamente datos personales.

Esta misma norma establece que el interés mencionado debe tener como base los principios de proporcionalidad, necesidad y legalidad. En otras palabras, solo se puede divulgar información privada si es absolutamente indispensable para satisfacer el interés público; esto supone que no se debe divulgar información adicional que permita la identificación de las personas. En este marco, la anonimización aparece como una medida equitativa que posibilita la publicidad judicial sin poner en riesgo los derechos básicos.

Art. 37.- Seguridad de datos personales: 1) Métodos de anonimización, pseudonimización o encriptación de información personal (Ley Orgánica de Protección de Datos Personales, artículo 37, 2021).

El artículo 37 instaura la protección de datos como un principio fundamental, imponiendo a los organismos que los tratan, incluida la justicia, la obligación de adoptar medidas organizativas y técnicas adecuadas al grado de confidencialidad de los datos. Ejemplos de estas medidas son el cifrado, la pseudonimización y la anonimización. Dicha

regulación es de especial trascendencia en el contexto del sistema de información judicial, donde las resoluciones deben ser gestionadas conforme a criterios técnicos que garanticen que no ocurran accesos, usos o filtraciones inapropiados de datos personales. Asimismo, la regulación requiere una perspectiva preventiva fundamentada en el análisis de riesgos. Esto significa que es necesario evaluar el posible efecto que tendrá la divulgación de un fallo sobre los derechos de las partes implicadas incluso antes de su publicación.

El principio de seguridad en el tratamiento de datos personales exige que, tal como lo establece el artículo 38 sobre medidas de seguridad en el sector público, los protocolos gubernamentales de seguridad de la información integren todas las acciones necesarias para gestionar dichos datos. Esto incluye la capacidad de enfrentar cualquier riesgo, amenaza o vulnerabilidad, así como incidentes de acceso no autorizado, pérdida, alteración, destrucción o divulgación, ya sea accidental o ilícita (Ley Orgánica de Protección de Datos Personales, 2021).

El artículo 38 complementa el anterior, universalizando las obligaciones de seguridad en el sector público. Todas las instituciones, incluidas las judiciales, deben implementar medidas específicas para prevenir riesgos, amenazas, accesos no autorizados u otros tipos de pérdida o distorsión de datos. Esto apoya el requisito de anonimato en el caso de que el objeto de un fallo pueda tender a absolver la identidad de las personas en riesgo o poner en peligro su seguridad. En un entorno donde la tecnología puede ser utilizada para realizar la difusión de información de forma masiva e inmediata, esta predisposición exige que los datos de carácter personal incluidos en la sentencia sean debidamente salvaguardados mediante el uso de protocolos bien construidos y eficientes.

1.4. Objetivos

1.4.1. Objetivo General

Analizar la protección de la identidad de los administradores de justicia en los delitos de alta peligrosidad mediante el uso de la IA.

1.4.2. Objetivos Específicos

1. Identificar el marco jurídico que regula la protección de la identidad de los administradores de justicia en delitos de alta peligrosidad.
2. Describir los riesgos y amenazas que enfrentan en la protección de identidad los administradores de justicia en los delitos de alta peligrosidad.

3. Caracterizar experiencias internacionales en el uso de IA para la protección de funcionarios judiciales y extraer buenas prácticas adaptables al contexto ecuatoriano.

CAPÍTULO II.
MARCO METODOLÓGICO

2.1. Materiales

En la organización y análisis crítico del conjunto documental, los registros bibliográficos fueron esenciales para el progreso de la investigación. El objetivo de estos registros fue documentar, de manera sistemática y estandarizada, la información esencial de cada fuente, incluyendo el título, la fecha en que se publicó, la editorial institucional y el lugar donde están las bases de datos (por ejemplo, SciELO o Scopus), además de un compendio de sus aportes conceptuales y empíricos.

Es un formato que compara y contrasta de manera estricta las regulaciones internacionales (incluida la Ley Europea de Inteligencia Artificial), nacionales (como la Ley Orgánica de Protección de Datos Personales del Ecuador) y decisiones paradigmáticas, junto con estudios de caso sobre sistemas judiciales de anonimización. La estructuración de datos en los registros permitió rastrear la línea argumentativa y hallar las lagunas entre los argumentos, lo que facilitó la intersección analítica de variables éticas, técnicas y legales vinculadas a cuestiones cualitativas (Arias y Covinos, 2021).

El método bibliográfico fue clave, ya que permitió realizar un estudio sistemático de documentos escritos en el campo de la protección de la identidad. Este análisis incluyó informes técnicos, literatura académica, registros institucionales y regulaciones. En consecuencia, se evaluaron los documentos más importantes utilizando matrices de clasificación: las resoluciones fundamentales, la Ley Europea de Inteligencia Artificial, los procedimientos para anonimizar y las investigaciones científicas vinculadas a la ciberseguridad. Se intentó identificar fallas en la legislación, las pautas técnicas y las tendencias de ciberseguridad.

Este método, de acuerdo con Hernández et al. (2018), posibilita la comparación y el aislamiento de los datos objetivos acerca de los marcos regulatorios, en relación con las realidades que aparecen en los informes técnicos y los conceptos teóricos. Para ejemplificar, se examinó la discrepancia entre las leyes vigentes en materia de protección de datos y su aplicación concreta en relación con delitos organizados, a partir de estudios de caso, investigaciones publicadas e informes de organizaciones. El objetivo de la revisión bibliográfica fue sintetizar el conocimiento técnico y académico actual, así como

seleccionar referencias indexadas en repositorios de datos como SciELO y Scopus, y también informes de organismos (CIDH, ONU).

Este proceso no solo situó la investigación en el contexto de los debates globales, sino que además reveló una nueva dirección, que es la aplicación de blockchain para garantizar que los registros anonimizados permanezcan inalterables. Para investigar vivencias particulares mediante fichas de sistematización, se utilizaron como corolario los estudios de caso en Finlandia (ANOPPI) y en Colombia (los jueces sin rostro).

Los costos, las tecnologías empleadas, el impacto sobre la seguridad del operador y los dilemas éticos son algunas de las variables que se volvieron a introducir. Se evidenciaron en las comparaciones entre casos patrones que pueden ser generalizados, como el vínculo entre la financiación estatal y el triunfo de una solicitud, o los riesgos que suponen para la transparencia de los sistemas automatizados de anonimización. Este método proporciona evidencias empíricas de manera indirecta, lo que llevó a sugerir sugerencias que podrían ser aplicadas en otras áreas judiciales.

2.2. Metodología

La metodología de la investigación científica se entiende como el conjunto de procedimientos sistemáticos, racionales y críticos empleados para obtener conocimiento nuevo, verificable y válido acerca de un fenómeno determinado. Su finalidad es garantizar la objetividad del proceso investigativo, permitiendo que los resultados obtenidos sean comprobables y replicables. Según Arias y Covinos (2021), la metodología constituye el camino ordenado que guía al investigador desde la formulación del problema hasta la interpretación de los resultados, con el propósito de contribuir al avance del conocimiento científico.

La metodología de la investigación jurídica, por su parte, se define como el conjunto de métodos, técnicas y procedimientos que permiten el estudio sistemático del derecho, tanto en su dimensión normativa como en su aplicación práctica. Su objetivo es interpretar, analizar y evaluar el ordenamiento jurídico, los principios y las instituciones legales, con el fin de comprender su alcance, validez y coherencia dentro del sistema jurídico. De acuerdo con Mila et al. (2021), la metodología jurídica no se limita a la descripción de las normas, sino que busca explicar su significado, finalidad y relación con la realidad social, política y ética que las sustenta.

2.2.1. Enfoque

El enfoque de investigación constituye la perspectiva fundamental, tanto en lo epistemológico como en lo metodológico, que se adopta para examinar un fenómeno. Esta postura define de manera global la naturaleza de los datos a recopilar, las técnicas para su análisis y el marco para la interpretación de los hallazgos. En este sentido, el enfoque actúa como una guía teórica que permite al investigador adoptar una postura coherente frente al objeto de estudio, ya sea desde una visión cuantitativa, cualitativa o mixta (Hernández et al., 2018).

El enfoque cualitativo se caracteriza por centrarse en la comprensión profunda de los fenómenos sociales, jurídicos o humanos desde la perspectiva de los sujetos involucrados. Busca interpretar significados, experiencias, contextos y procesos en lugar de cuantificar variables o establecer relaciones numéricas. Se fundamenta en la observación, el análisis de documentos, el discurso y la interpretación de la realidad (Baena, 2019).

Se eligió una metodología cualitativa debido a que tiene la habilidad de proporcionar un enfoque de múltiples dimensiones sobre el fenómeno en cuestión. Así, gracias al uso de la inteligencia artificial (IA), fue factible examinar con mayor profundidad los elementos tectónicos vinculados a la conservación de la identidad, incluyendo sus dimensiones, que abarcan cuestiones prácticas, éticas y legales en el campo judicial. Contrario al enfoque cuantitativo, la metodología cualitativa se fundamenta en datos y medidas estadísticas, según Hernández et al. (2018).

Así, es posible analizar los retos, las posturas y las vivencias de los principales actores: magistrados, fiscales, legisladores y especialistas en ciberseguridad. Se realizó un estudio exhaustivo de las normativas, tanto nacionales como internacionales, relacionadas con la implementación de tecnologías emergentes en el sistema judicial, para garantizar así una visión integral. Además, el objetivo de este procedimiento fue examinar las leyes, las normas, las políticas institucionales y los precedentes judiciales actuales para identificar lagunas legales y estudiar la viabilidad de implementar soluciones fundamentadas en inteligencia artificial.

Se revisaron de nuevo los análisis de casos y la información técnica acerca de experiencias anteriores ligadas a la seguridad de los funcionarios públicos, lo cual permitió realizar comparaciones entre las condiciones legales y tecnológicas en diferentes contextos.

Para ofrecer sugerencias útiles a las instituciones judiciales y los legisladores, el estudio

también incluyó un enfoque práctico. Este propósito incluyó tanto la identificación del problema como las soluciones a medio y corto plazo (Romero et al., 2022).

Siguiendo este enfoque, se empleó una metodología comparativa que analizó los sistemas de protección judicial en países con dificultades semejantes. Se incluyeron los métodos de protección cifrada de la justicia tanto en España como en Colombia, además del sistema ANOPPI de Finlandia, que emplea inteligencia artificial para encubrir la identidad de los fiscales y testigos. Los casos de estudio tienen el potencial de mostrar prácticas óptimas que, teniendo en cuenta la infraestructura tecnológica disponible, las culturas organizacionales y la legislación vigente, podrían implementarse en Ecuador.

Se implementó un enfoque de revisión sistemática con el fin de crear una sólida base teórica, la cual posibilitó identificar, examinar y resumir estudios previos sobre la inteligencia artificial en el ámbito de la protección de datos en el sistema judicial. Se emplearon directivas estandarizadas con el fin de reducir los sesgos. El análisis de contenido de documentos regulatorios y textos vinculados a la política pública en torno a la privacidad y la tecnología dentro del poder judicial, que revelaron una discrepancia entre lo legislado y lo practicado, fue útil para completar esta estrategia.

Asimismo, se empleó un método sistemático que reconoce que la aplicación de la inteligencia artificial en la protección judicial no es un proceso aislado, sino que está relacionada con los demás elementos del sistema judicial. Este método incluyó examinar de qué manera estas tecnologías impactan principios esenciales como la privacidad, la transparencia y el debido proceso, así como también su relación recíproca con la ciberseguridad institucional. La perspectiva holística de la estrategia posibilitó anticipar potenciales contradicciones en términos operativos y regulatorios, para asegurar que las soluciones planteadas sean efectivas y cuenten con un respaldo ético (Mila et al., 2021).

2.2.2. Modalidades de investigación – Tipo de investigación

El tipo de investigación se refiere a la naturaleza y características del estudio que se realiza, así como al propósito que persigue dentro del proceso científico. Determina el nivel de profundidad, el alcance y las estrategias empleadas para abordar el objeto de estudio. Según Hernández et al. (2018), el tipo de investigación orienta el diseño metodológico y define la manera en que se obtendrán, analizarán e interpretarán los datos, garantizando así la coherencia entre los objetivos planteados y los métodos utilizados. En este sentido, la elección del tipo de investigación depende de la naturaleza del problema, los recursos disponibles y los resultados esperados.

La investigación bibliográfica y documental consiste en el examen, análisis y síntesis de información proveniente de fuentes escritas, impresas o digitales, con el fin de fundamentar teóricamente un problema de estudio y construir un marco de referencia sólido. Según Baena (2019), este tipo de investigación implica la revisión sistemática y crítica de documentos tales como libros, artículos científicos, leyes, reglamentos, informes institucionales y bases de datos especializadas, permitiendo obtener un conocimiento actualizado y verificable del tema tratado.

Se llevó a cabo el análisis desde una perspectiva bibliográfica y documental, la cual se consideró adecuada para examinar la situación del arte en relación con la protección judicial mediante la colaboración sistemática y crítica de la inteligencia artificial (Mila et al., 2021). La metodología posibilitó la revisión de una amplia gama de documentos, entre ellos regulaciones internacionales como la Ley de Inteligencia Artificial de la Unión Europea. Esta ley establece por primera vez un marco normativo para la creación de sistemas éticos en crímenes organizados. También se incluyen informes de entidades especializadas, como la Corte Interamericana de Derechos Humanos y las Naciones Unidas, que han registrado detalladamente las tendencias violentas contra el personal judicial.

Los recursos académicos que se añaden están indexados además en bases de datos de gran impacto (ejemplo: Web of Science, SciELO y Scopus) y se centran en las aplicaciones específicas de la inteligencia artificial en los sistemas judiciales. Los informes que abordan las iniciativas de anonimización judicial en el país (y otras con problemáticas parecidas) se encuentran en esta lista, lo cual hace que la presentación de propuestas sea situacional.

El periodo documental fue más allá de ser un mero proceso de recopilación de fuentes y se transformó en una etapa analítica que ha representado los diferentes marcos requeridos para esclarecer el problema en toda su amplitud (Arias & Covinos, 2021). Con esta estrategia, fue posible comparar el probable avance tecnológico con la normativa en vigor en Ecuador y determinar no solo los espacios de innovación, sino también las posibles contradicciones en la regulación. Todo esto se mantiene a partir del análisis de sentencias paradigmáticas que han delineado la jurisprudencia en relación con el balance entre la jurisprudencia de seguridad y las garantías primordiales.

2.2.3. Nivel

El nivel investigativo hace referencia al grado de profundidad con el que se aborda el objeto de estudio dentro del proceso de investigación científica. Este nivel determina el tipo de conocimiento que se busca alcanzar ya sea exploratorio, descriptivo, explicativo o correlacional y orienta las estrategias metodológicas que se aplicarán. Según Arias y Covinos (2021), el nivel de investigación define la relación entre el investigador y el fenómeno analizado, estableciendo el alcance del estudio y la forma en que se describen, interpretan o explican las variables o dimensiones involucradas. En síntesis, el nivel investigativo delimita el alcance epistemológico y metodológico del trabajo científico.

El nivel **exploratorio** se caracteriza por abordar temas poco estudiados o novedosos, con el propósito de obtener una comprensión preliminar del fenómeno y establecer las bases para futuras investigaciones. Este nivel no pretende ofrecer resultados concluyentes, sino identificar tendencias, relaciones o elementos significativos que orienten nuevas líneas de análisis. De acuerdo con Baena (2019), la investigación exploratoria permite familiarizarse con problemáticas emergentes, formular hipótesis iniciales y definir categorías de análisis, especialmente cuando el objeto de estudio carece de antecedentes suficientes o se encuentra en desarrollo.

El nivel descriptivo, por su parte, busca detallar con precisión las características, comportamientos o manifestaciones de un fenómeno determinado. Su propósito es ofrecer una representación objetiva y ordenada de la realidad estudiada, sin establecer relaciones causales. Según Hernández et al. (2018), la investigación descriptiva permite caracterizar hechos, procesos o situaciones, proporcionando información clara y sistematizada que sirva como base para el análisis y la interpretación posterior.

El presente estudio se llevó a cabo en dos niveles interdependientes, lo que ayudó a examinar de manera integral los puntos de vista relacionados con la línea de investigación en políticas públicas, derecho y sociedad. Para empezar, el nivel descriptivo llevó a cabo un examen crítico de las políticas vigentes relacionadas con la defensa de los titulares de justicia. Esto incluye tanto las acciones ordinarias que llevan a cabo los gobiernos como sus restricciones en la práctica.

La investigación ha revelado que las leyes actuales sobre la protección de testigos, la privacidad de datos y los marcos regulatorios no son suficientes ante las nuevas amenazas digitales, tales como el asalto a los tribunales electrónicos o el ataque del

Internet de las cosas (IoT). Se identificaron vacíos en la normativa que requerían una revisión inmediata de las políticas en el área correspondiente mediante un estudio comparativo de estándares y casos nacionales e internacionales, incluidos los Principios de Bangalore.

El nivel exploratorio, además, investiga los efectos socio jurídicos que resultan de la implementación de soluciones fundamentadas en inteligencia artificial. Este estudio evidenció correlaciones relevantes entre el grado de adopción tecnológica y la disminución de amenazas, así como entre la ocurrencia de delitos de alto riesgo y las pautas de riesgo asociadas con los funcionarios que participan en el sistema judicial.

El estudio pasó del campo abstracto al plantear una política regulatoria flexible que tenía como objetivo armonizar la innovación tecnológica con la seguridad democrática. El proceso de investigación no solo detectó las brechas en los modelos tradicionales de protección, sino que también produjo datos empíricos que respaldan las modificaciones institucionales gracias a la combinación de componentes del derecho, la tecnología y las políticas.

Su aplicabilidad en el ámbito social es evidenciada por su habilidad para cumplir con las exigencias concretas de una justicia equitativa y segura, al mismo tiempo que se adapta a metas como el ODS 16, que fomenta la paz, la justicia y el fortalecimiento de las instituciones. La metodología utilizada también posibilitó la elaboración de sugerencias que se podrían implementar en diferentes escenarios, como los sistemas judiciales de América Latina y Europa, para alcanzar un balance entre la transparencia, el resguardo de los derechos esenciales y la eficacia institucional.

2.2.4. Métodos

El método de investigación constituye el conjunto ordenado de procedimientos, técnicas y estrategias que orientan el proceso científico hacia la obtención de conocimiento verificable. Representa el camino lógico que el investigador sigue para alcanzar los objetivos del estudio, garantizando coherencia entre el marco teórico, los instrumentos empleados y los resultados obtenidos. Según Hernández et al. (2018), el método científico es un sistema de reglas que guían la observación, el análisis y la interpretación de los fenómenos, con el propósito de asegurar la validez, fiabilidad y objetividad de las conclusiones. En el ámbito jurídico y social, los métodos de

investigación no solo buscan describir o explicar, sino también interpretar y valorar los procesos normativos, institucionales y éticos que estructuran la realidad.

El método analítico metodológico consiste en descomponer el objeto de estudio en sus partes esenciales para examinar cada una de ellas con mayor profundidad y precisión. Este método permite distinguir los componentes fundamentales de un fenómeno, establecer relaciones entre ellos y reconstruir una visión integral basada en el conocimiento de sus elementos. De acuerdo con Arias y Covinos (2021), el método analítico posibilita el estudio detallado de los factores que configuran la realidad investigada, proporcionando una comprensión más rigurosa y crítica de su estructura interna.

El método analítico metodológico divide el tema en sus componentes esenciales para examinarlo con mayor profundidad, distinguiéndolo en sus elementos éticos, tecnológicos y legales. Para realizar este análisis, se utilizaron métodos como el uso de algoritmos para procesar el lenguaje natural y ocultar la identidad en documentos judiciales, así como las leyes actuales sobre la privacidad de las decisiones judiciales (Arias y Covinos, 2021). Después de este pormenorizado análisis, se aplicaron los resultados a la teoría. En ella, se determinaron sugerencias concretas acerca de cómo diseñar sistemas de inteligencia artificial que respeten los principios de las reglas fundamentales del derecho.

El método teórico-deductivo se fundamenta en la aplicación del razonamiento lógico para derivar conclusiones particulares a partir de principios generales o hipótesis previamente formuladas. Este enfoque parte de postulados teóricos, los contrasta con evidencias empíricas y, posteriormente, deduce interpretaciones o soluciones aplicables al fenómeno en estudio. Según Baena (2019), este método permite integrar la teoría con la observación de la realidad, garantizando que las conclusiones tengan una base lógica y sustentada.

El método teórico-deductivo comienza con la formulación de hipótesis específicas, que luego se contrastan con datos obtenidos empíricamente. Por su parte, el método histórico-crítico estudió la sucesión cronológica de cómo los sistemas de protección de la justicia han progresado, comenzando con los más antiguos basados en guardias armados y continuando con las soluciones digitales. Por ejemplo, este debate permitió manifestar la tristeza por la lentitud de los procedimientos para regular la

inteligencia en regiones como Latinoamérica, en contraposición a la rapidez y flexibilidad con que actúan las organizaciones criminales.

El método hermenéutico se centra en la interpretación crítica y comprensiva de textos, discursos y normas, con el propósito de descubrir su significado profundo dentro de un contexto histórico, social o filosófico. En el campo jurídico, este método permite desentrañar la intención normativa y el sentido ético de las disposiciones legales. Según Hernández et al. (2018), la hermenéutica implica un diálogo entre el texto y el intérprete, donde la comprensión surge de la interacción entre la tradición jurídica y los desafíos contemporáneos.

El método hermenéutico fue empleado para examinar críticamente los textos jurídicos y éticos más significativos (como la RGPD o las resoluciones de tribunales internacionales), no solamente con su redacción como punto de atención, sino también teniendo en cuenta su esencia dentro del contexto de la revolución tecnológica. Simultáneamente, el análisis histórico examinó la manera en que los delincuentes se beneficiaron de las falacias de los reguladores durante la década pasada, lo que muestra cómo han cambiado los crímenes contra la privacidad judicial**.**

2.2.5. Técnicas de investigación

Las técnicas de investigación constituyen los procedimientos operativos empleados para obtener, registrar y analizar la información necesaria dentro del proceso científico. Representan las acciones concretas que permiten aplicar los métodos de investigación, garantizando la validez y confiabilidad de los resultados. Según Arias y Covinos (2021), las técnicas son los medios prácticos que el investigador utiliza para acceder a los datos, ya sea mediante la observación, la entrevista, el análisis de documentos o cualquier otro recurso empírico que facilite la comprensión del fenómeno estudiado.

En el presente estudio se aplicaron técnicas de investigación de carácter documental, orientadas al examen sistemático y crítico de fuentes escritas y normativas. Estas técnicas se centraron principalmente en la observación documental y el análisis de contenido, adecuadas a la naturaleza cualitativa y jurídica de la investigación. La observación documental consistió en el estudio detallado de diversas fuentes secundarias, como libros especializados, artículos científicos, informes institucionales, normas jurídicas, tratados internacionales y sentencias relevantes. Este procedimiento permitió

identificar los elementos doctrinarios y normativos que sustentan la discusión sobre la inteligencia artificial aplicada al ámbito judicial y su vinculación con la protección de los derechos fundamentales.

Por su parte, el análisis de contenido se empleó como técnica transversal para interpretar de manera rigurosa los textos revisados, identificando categorías recurrentes, vacíos normativos y tendencias doctrinarias relevantes para el objeto de estudio. De acuerdo con Baena (2019), esta técnica permite descomponer la información textual en unidades significativas, revelando las estructuras conceptuales y los patrones argumentativos presentes en el discurso jurídico.

Asimismo, se utilizó el fichaje como instrumento auxiliar de recolección y organización de información, lo que posibilitó clasificar de forma sistemática los datos obtenidos de las fuentes revisadas libros, artículos científicos, informes institucionales y documentos legales para construir un marco conceptual sólido y coherente. En conjunto, estas técnicas favorecieron la integración de perspectivas teóricas, normativas y prácticas, permitiendo desarrollar un análisis exhaustivo basado en un corpus documental amplio y diverso, coherente con los objetivos planteados en la investigación.

De manera complementaria, se aplicó la técnica comparativa, lo que permitió contrastar el tratamiento doctrinal y normativo del fenómeno analizado en diferentes contextos jurídicos. Dicho procedimiento favoreció la identificación de semejanzas y divergencias en cuanto a la aplicación de principios, la adopción de medidas de protección y el uso de tecnologías emergentes en el ámbito judicial. Estas técnicas de investigación documental se articularon con un criterio de exhaustividad y rigor académico, garantizando que la construcción teórica se fundamentara en fuentes pertinentes, actuales y de reconocido valor científico.

2.2.6. Instrumento de investigación

Los instrumentos de investigación son los medios o recursos específicos que el investigador emplea para recopilar, registrar, organizar y sistematizar la información necesaria en el desarrollo del estudio. Constituyen el soporte técnico que permite aplicar las técnicas seleccionadas, garantizando la fiabilidad y precisión de los datos obtenidos. Según Hernández et al. (2018), los instrumentos son las herramientas que transforman la observación o el análisis en información verificable, facilitando la interpretación y el procesamiento de los resultados de manera estructurada y coherente. En el ámbito de la

investigación jurídica y documental, estos instrumentos adquieren especial relevancia, ya que posibilitan el manejo riguroso de grandes volúmenes de información proveniente de fuentes normativas, doctrinarias y jurisprudenciales, asegurando su adecuada clasificación y análisis crítico.

Las fichas nemotécnicas o fichas bibliográficas son instrumentos de registro y organización de información provenientes de diversas fuentes, cuyo propósito es almacenar de forma sistemática y ordenada los datos esenciales de los documentos consultados. Estas fichas pueden contener citas textuales, paráfrasis, resúmenes, comentarios críticos o referencias normativas, y permiten mantener un control eficiente sobre los materiales utilizados durante la investigación. De acuerdo con Baena (2019), las fichas bibliográficas son una herramienta metodológica que facilita la recuperación de información relevante, apoyando tanto la elaboración del marco teórico como la argumentación analítica del estudio.

Los instrumentos utilizados correspondieron principalmente a matrices de análisis documental diseñadas para la organización, clasificación y síntesis de la información recopilada. Estas matrices permitieron registrar de manera ordenada los datos extraídos de la literatura, diferenciando entre el contenido general y específico de cada fuente, así como identificando su relevancia en el marco del problema de investigación (Arias & Covinos, 2021). El uso de fichas bibliográficas constituyó un apoyo metodológico esencial, ya que facilitaron el almacenamiento de citas textuales, referencias normativas y comentarios analíticos que sirvieron de base para la elaboración del marco teórico y jurídico.

Adicionalmente, se implementaron guías de revisión bibliográfica que aseguraron la coherencia entre los objetivos de la investigación y las fuentes consultadas. Estas guías establecieron criterios de selección como actualidad, pertinencia, validez académica y aplicabilidad al contexto ecuatoriano, lo que garantizó un análisis riguroso y sistemático. En conjunto, los instrumentos de investigación empleados posibilitaron un manejo eficiente y ordenado del material documental, reforzando la validez interna de los resultados obtenidos y asegurando la consistencia del desarrollo investigativo.

2.2.7. Población

En investigación, la población se define como el conjunto total de elementos, personas, documentos o unidades de análisis que poseen características comunes y que

son objeto de estudio. Representa el universo sobre el cual se pretende generalizar los resultados o comprender las dinámicas del fenómeno investigado. Según Hernández et al. (2018), la población comprende todos los casos posibles que cumplen con los criterios previamente establecidos por el investigador, siendo la base a partir de la cual se selecciona la muestra y se estructuran los procedimientos de análisis.

Los actores técnicos, legales e institucionales que se han incluido en la investigación pertenecen a una población de estudio vinculada directa o indirectamente con la salvaguarda de la identidad de las autoridades judiciales al usar inteligencia artificial en situaciones peligrosas. En esta muestra tomaron parte experiencias en políticas públicas, ciberseguridad y derecho digital, así como integrantes del sistema de justicia ecuatoriano. Asimismo, se añadieron documentos de la institución, informes técnicos y marcos regulatorios a nivel nacional e internacional que son relevantes o tienen un impacto en la aplicación de tecnologías emergentes dentro del ámbito judicial.

2.2.8. Muestra

La muestra se entiende como el subconjunto representativo de la población que se selecciona para ser estudiado de manera directa. Su propósito es facilitar el análisis sin perder la validez ni la generalización de los resultados obtenidos. Según Arias y Covinos (2021), la muestra constituye una parte del universo total que conserva las características esenciales de la población, permitiendo desarrollar un estudio más profundo y focalizado. En investigaciones cualitativas o documentales, la muestra se determina en función de criterios teóricos, de relevancia y pertinencia, más que por la cantidad de elementos seleccionados.

La muestra abarcó varios documentos estratégicos, entre los que se encuentran normas clave (la Ley de Protección de Datos Personales de Ecuador y la Ley de Inteligencia Artificial de la Unión Europea), así como fallos y casos prácticos que demuestran el uso mundial de las tecnologías para lograr un anonimato judicial. Con el objetivo de asegurar la trazabilidad y la coherencia en el proceso de recopilación y análisis de documentos, se implementó el modelo PRISMA; sin embargo, este modelo fue ajustado a las condiciones específicas del marco legal y cualitativo.

CAPÍTULO III.
RESULTADOS Y DISCUSIÓN

3.1. Análisis de los resultados

3.1.1. Anonimización y técnicas de protección de datos

La anonimización constituye una estrategia técnica y jurídica que busca impedir la identificación o reidentificación de una persona natural a partir de la información contenida en resoluciones o expedientes judiciales. En el contexto ecuatoriano, la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021) la define como el procedimiento mediante el cual se aplica un conjunto de medidas que imposibilitan la identificación de los titulares de datos, salvo que se realicen esfuerzos desproporcionados. Esta definición se articula con principios de legalidad, proporcionalidad y necesidad, lo que obliga a ponderar la publicidad judicial con la protección de la intimidad.

De este modo, la anonimización trasciende la mera supresión de nombres, al incluir la detección de información indirecta como fechas, lugares o relaciones familiares que pueda servir como vector de reidentificación (Bobek, 2019). En la práctica, se dispone de diversas técnicas de protección de datos que pueden aplicarse en los documentos judiciales. Entre ellas destacan la supresión de identificadores, la pseudonimización,[16] la generalización de valores y la perturbación de la información (Agencia Española de Protección de Datos, 2022).

Protocolos jurisdiccionales como el del Poder Judicial de Chile (2022) contemplan modalidades de anonimización parcial o total, según el nivel de riesgo y la vulnerabilidad de las partes. Estas técnicas deben acompañarse de criterios estandarizados que aseguren consistencia, garantizando la protección de víctimas, testigos o funcionarios judiciales sin sacrificar la utilidad mínima de los documentos para fines de revisión, control social o investigación académica (Cano, 2020).

El desarrollo reciente de la anonimización automatizada mediante algoritmos de procesamiento de lenguaje natural (PLN) y sistemas de reconocimiento de entidades nombradas ha permitido abordar el tratamiento masivo de resoluciones judiciales (Mark

[16] La pseudonimización es una técnica de protección de datos que sustituye los identificadores directos de una persona, como su nombre o dirección, por seudónimos (como códigos o números únicos) para proteger la privacidad.

et al., 2021; Terzidou, 2023). Estas herramientas pueden identificar y reemplazar nombres, direcciones o referencias contextuales de manera sistemática; sin embargo, presentan limitaciones asociadas a falsos positivos, omisiones y vulnerabilidades frente a técnicas de reidentificación (Contini, 2019). Por ello, la automatización debe entenderse como un apoyo complementario dentro de un esquema "*human-in-the-loop*",[17] en el cual la validación manual y la auditoría periódica resultan imprescindibles para reducir riesgos (Cárdenas & Martínez, 2021).

Más allá de las intervenciones textuales, las medidas criptográficas representan un componente central de la protección. El cifrado de bases de datos, la autenticación robusta y técnicas avanzadas como el cifrado holomórfico permiten procesar información sensible sin exponerla en claro (Andrade, Toapanta, Bano, & Gómez, 2024). Estas soluciones deben integrarse con políticas de control de accesos, registros de trazabilidad y auditorías de integridad, de modo que se garantice no solo la confidencialidad de la información, sino también la rendición de cuentas institucional (Roldán, 2021).

Finalmente, la anonimización requiere una evaluación sistemática del riesgo de reidentificación, que contemple escenarios de cruce de datos con fuentes abiertas o minería de información en redes sociales. Modelos como el *k-anonymity*[18] o la *differential privacy*[19] ofrecen marcos útiles para medir los niveles de riesgo, aunque la normativa subraya que el riesgo cero es inalcanzable (Viguri, 2022). En consecuencia, las instituciones judiciales deben establecer protocolos organizativos claros, con unidades responsables de la aplicación de estas técnicas, capacitación continua de su personal y mecanismos de control externo que aseguren transparencia y confianza ciudadana en los procesos de anonimización (Mejía, 2024; Guerrero, 2020).

Las técnicas de protección de datos y anonimización basadas en inteligencia artificial constituyen un avance decisivo en la gestión segura de información en entornos donde se manejan datos sensibles, como los ámbitos judiciales, administrativos y sanitarios. A través de la aplicación de modelos algorítmicos sofisticados, es posible

[17] Enfoque que integra la intervención humana en un proceso de toma de decisiones de una máquina o un sistema de inteligencia artificial.
[18] Propiedad de privacidad en un conjunto de datos que se utiliza para proteger la identidad de las personas cuando se comparten datos.
[19] Marco matemático que proporciona una garantía rigurosa de que la inclusión o exclusión de la información de un individuo en un conjunto de datos no afectará de forma significativa el resultado de un análisis estadístico.

garantizar que la identidad de las personas se mantenga resguardada frente a intentos de exposición indebida, logrando así un equilibrio entre el uso intensivo de información para fines legítimos y la salvaguarda de los derechos fundamentales vinculados a la privacidad. La IA aporta un componente de automatización y precisión que supera en muchos casos las técnicas tradicionales de anonimización, puesto que no solo actúa eliminando o enmascarando identificadores directos, sino que además es capaz de anticipar riesgos de reidentificación al detectar patrones complejos que los humanos difícilmente podrían prever (Medina, 2025).

Una de las aplicaciones más destacadas es la anonimización automática, en la cual algoritmos avanzados pueden procesar grandes volúmenes de información, identificando de manera inmediata nombres, direcciones, números de identificación y otros datos personales. Estos algoritmos utilizan procedimientos como el enmascaramiento, la generalización o la perturbación para transformar los datos de modo que conserven su utilidad en el análisis, pero sin que sea posible vincularlos a individuos concretos. A diferencia de los métodos manuales, la IA aporta rapidez y una reducción significativa del margen de error, lo que resulta crucial en contextos donde se manejan miles de expedientes, como ocurre en tribunales o instituciones públicas.

La desidentificación inteligente es otro aporte fundamental, pues el aprendizaje automático permite detectar no solo la información sensible de manera explícita, sino también aquella que podría servir indirectamente para reidentificar a una persona. Esto se logra gracias a la capacidad de los modelos para identificar patrones, correlaciones y relaciones entre atributos, ajustando automáticamente los parámetros de anonimización según el nivel de riesgo presente en cada conjunto de datos. De esta manera, se incrementa la seguridad en situaciones en que la simple eliminación de nombres no es suficiente, dado que combinaciones como edad, lugar de residencia y ocupación podrían bastar para inferir la identidad de alguien.

Igualmente, relevante es la generación de datos sintéticos, una técnica que recurre a modelos generativos de IA para crear información artificial que conserva las propiedades estadísticas de los datos originales, pero que no pertenece a ningún individuo real. Este método resulta particularmente valioso en la investigación científica, la capacitación de algoritmos o la elaboración de estadísticas públicas, ya que posibilita análisis confiables sin comprometer la privacidad de los sujetos. De este modo, los

investigadores o instituciones pueden trabajar con grandes bases de datos simuladas que reflejan tendencias y comportamientos, al mismo tiempo que cumplen estrictamente con las obligaciones legales de confidencialidad.

A ello se suma la evaluación automatizada del riesgo de reidentificación, mediante herramientas capaces de medir la probabilidad de que un conjunto de datos previamente anonimizado pueda ser revertido para revelar identidades. Estos sistemas no solo alertan sobre las vulnerabilidades detectadas, sino que también sugieren medidas adicionales, como el refuerzo de técnicas de enmascaramiento o la reducción de la granularidad en ciertos campos de información. En un entorno donde la capacidad tecnológica para cruzar y combinar datos es cada vez más poderosa, contar con mecanismos que midan en tiempo real el nivel de exposición se convierte en un requisito indispensable para mantener estándares sólidos de protección.

El procesamiento automatizado de documentos mediante técnicas de procesamiento de lenguaje natural representa otra dimensión del uso de IA en este ámbito. Estas herramientas no solo identifican y bloquean datos personales en sentencias judiciales, correos electrónicos o expedientes administrativos, sino que además pueden clasificarlos, estructurarlos y resguardarlos en sistemas seguros, reduciendo la posibilidad de filtraciones involuntarias. Junto a ello, metodologías como el aprendizaje federado permiten entrenar modelos sin necesidad de trasladar los datos fuera de sus entornos de origen, lo que minimiza riesgos de fuga al mantener la información bajo control local y descentralizado (Pérez Y. , 2025).

La privacidad diferencial se ha consolidado como un estándar de referencia, aplicando “ruido” matemático a los datos con el objetivo de garantizar que los resultados de análisis agregados no puedan descomponerse para identificar a sujetos individuales. Este mecanismo, combinado con la detección automática de atributos indirectos, refuerza las barreras frente a intentos de inferencia indebida. En este último caso, la IA se emplea para identificar relaciones no evidentes entre variables que podrían permitir la deducción de una identidad, proponiendo correcciones que neutralicen tales riesgos antes de que los datos sean compartidos o utilizados.

Pese a su sofisticación, estas técnicas no están exentas de retos. La evolución constante de las capacidades de cómputo y de los métodos de análisis implica que lo que

hoy puede considerarse un conjunto de datos suficientemente anonimizado podría no serlo en el futuro. Los riesgos de reidentificación se transforman al mismo ritmo que avanza la tecnología, por lo que es necesario complementar la aplicación de IA con controles humanos, auditorías constantes y marcos normativos claros que regulen la manera en que se implementan estas soluciones. Asimismo, la dimensión ética no puede soslayarse, ya que el tratamiento de información personal exige un compromiso institucional con la transparencia, la rendición de cuentas y la protección efectiva de los derechos de los ciudadanos.

En la actualidad, estas técnicas representan el estado del arte en protección de datos y encuentran aplicación creciente en sectores como la justicia, la salud y la regulación pública. Los tribunales pueden publicar sentencias anonimizadas sin comprometer la integridad de los expedientes, los hospitales pueden compartir datos clínicos para fines de investigación sin poner en riesgo a los pacientes, y los organismos reguladores pueden elaborar informes basados en datos sensibles sin temor a exponer a individuos. De esta forma, la inteligencia artificial se convierte en un aliado indispensable no solo en la automatización de procesos, sino también en la consolidación de un marco institucional que respete la privacidad como un derecho fundamental en la era digital.

Las técnicas de anonimización automática se sustentan hoy en modelos de reconocimiento de entidades y en arquitecturas de lenguaje que van mucho más allá de los antiguos patrones basados en expresiones regulares. Estos modelos entrenados sobre corpus[20] representativos y afinados para dominios jurídicos o clínicos cuando corresponde detectan no solo nombres y números de identificación, sino también referencias indirectas: apellidos compuestos, menciones contextuales, referencias temporales que acotan identidades, e incluso frases que actúan como identificadores implícitos (Hernández et al., 2025).

La aplicación práctica combina pasos previos al procesamiento (como la normalización y corrección de errores de OCR en documentos escaneados), una fase de detección y clasificación de entidades sensibles con modelos entrenados o afinados ad hoc, y finalmente transformaciones compatibles con los objetivos analíticos (enmascaramiento consistente, generalización de valores, perturbación estadística). En la

[20] Un Corpus en el ámbito de la inteligencia artificial se refiere a una colección estructurada de textos escritos o grabaciones orales que se utilizan para entrenar y evaluar modelos de aprendizaje automático.

fase de transformación se debe decidir cuidadosamente si la operación es reversible o irreversible para cada atributo, pues transformar nombres por pseudónimos consistentes permite seguimiento longitudinal sin reidentificación, mientras que la perturbación irreversible favorece la protección, pero sacrifica trazabilidad; esa dicotomía exige políticas claras y trazabilidad de los cambios aplicados.

La desidentificación inteligente implica además que el sistema no aplique reglas estáticas, sino que evalúe dinámicamente el riesgo de reidentificación según el contexto de uso. Esto se consigue mediante modelos de riesgo que ponderan la rareza de combinaciones de atributos, la disponibilidad de fuentes externas que pudieran cruzarse y la sensibilidad del dominio. En la práctica, los modelos de *machine learning* pueden asignar puntajes de riesgo a registros o campos y activar distintos niveles de anonimización: desde una leve generalización hasta la supresión completa, pasando por la creación de campos sintetizados.

Este enfoque adaptativo requiere calibración continua: los parámetros de anonimización deben ajustarse con base en métricas de utilidad de los datos y en pruebas de ataque (simulaciones de *linkage* con fuentes públicas), de modo que la protección no sea decorativa sino efectiva frente a amenazas reales. Además, la desidentificación inteligente integra metadatos sobre el tratamiento aplicado, conservando un registro que permite auditorías y la reversión controlada cuando la ley o la investigación lo exijan bajo estrictas garantías.

La generación de datos sintéticos es una herramienta poderosa para conjugar protección y capacidad analítica, pero no exenta de complejidades técnicas. Los modelos generativos modernos como redes antagónicas generativas (GANs), *autoencoders* variacionales (VAEs) o modelos de difusión aprenden las distribuciones conjuntas de los atributos y producen observaciones que mantienen correlaciones y propiedades estadísticas útiles para análisis agregados o para entrenar modelos predictivos. No obstante, la calidad de los datos sintéticos debe evaluarse bajo dos prismas: fidelidad estadística y riesgo de fuga.

La fidelidad exige que los datos sintéticos reproduzcan estructuras relevantes (distribuciones marginales, correlaciones, relaciones temporales), mientras que el riesgo de fuga obliga a verificar que el modelo no haya memorizado registros reales que puedan

ser regenerados y reidentificados. Las estrategias de mitigación incluyen el empleo de privacidad diferencial durante el entrenamiento, la inclusión de penalizaciones contra la memorización y pruebas de membresía que comparen similitudes entre muestras reales y sintéticas. Solo combinando evaluaciones rigurosas de utilidad y privacidad podrá un repositorio sintético convertirse en una alternativa viable a la apertura o al intercambio de datos reales.

La evaluación automatizada del riesgo de reidentificación debe concebirse como un proceso cuantitativo y replicable. Existen métricas clásicas que siguen siendo útiles para diagnosticar vulnerabilidades: k-anonymity, que mide cuántos registros comparten un mismo perfil de atributos; *l-diversity*, que exige diversidad en atributos sensibles para evitar que una *equivalence class* revele una característica; y *t-closeness*, que compara distribuciones para evitar inferencias estadísticas.

Sin embargo, estas métricas son parámetros diagnósticos y no soluciones por sí mismas: un análisis de riesgo moderno debe simular escenarios de ataque reales, considerando las bases de datos que un adversario podría usar para hacer linkage y empleando técnicas de aprendizaje para estimar probabilidades de reidentificación. Esa evaluación operacional incorpora tanto pruebas offline como monitoreo continuo tras la liberación o uso restringido de datos, midiendo indicadores de riesgo con umbrales definidos por la política institucional y obligando a contramedidas automáticas cuando se superan niveles preestablecidos.

El aprendizaje federado ofrece un modelo arquitectónico para entrenar con datos distribuidos sin centralizarlos, pero su correcta implantación exige medidas complementarias porque no es una panacea por sí misma. En una configuración federada, los nodos locales calculan actualizaciones del modelo que se agregan de forma segura por un servidor central o mediante protocolos de agregación segura; sin embargo, las actualizaciones pueden filtrar información sensible por medio de ataques de inversión o inferencia sobre gradientes.

Por eso, la práctica avanzada combina federación con protección por privacidad diferencial a nivel de gradiente, agregación segura criptográfica y técnicas de compresión/privacidad para reducir la exposición. Además, la heterogeneidad de los datos (no-IID) en entornos reales implica desafíos de convergencia y sesgo, lo que obliga a

diseñar esquemas de agregación robustos, ajustes de hiperparámetros[21] conscientes del dominio y evaluaciones de equidad para que los modelos no reproducen desigualdades presentes en subconjuntos geográficos o demográficos.

La privacidad diferencial, como paradigma teórico y práctico, aporta garantías cuantificables que ayudan a medir la pérdida de privacidad en términos matemáticos. El parámetro conocido como épsilon resume la magnitud de la privacidad: valores más pequeños implican mayor protección, pero también mayor ruido y menor precisión en los resultados. En implementaciones reales se aplican mecanismos como Laplace o Gaussiano para perturbaciones en funciones agregadas, y se controlan la composición de múltiples consultas para no exceder el presupuesto de privacidad.

En ambientes judiciales o sanitarios, esto exige una aproximación pragmática: definir qué consultas requieren alta fidelidad y cuáles pueden tolerar ruido, documentar el presupuesto de privacidad asignado a cada proceso y auditar el uso acumulado. La privacidad diferencial también puede aplicarse de forma local (perturbando datos antes de salir del origen) o centralizada, y su elección condiciona la arquitectura y el reparto de responsabilidades entre los custodios de los datos y los analistas.

En el tratamiento de documentos legales y expedientes, las técnicas de procesamiento de lenguaje natural permiten automatizar la detección y la redacción de información sensible, pero enfrentan retos propios del lenguaje jurídico: ambigüedad, referencias implícitas, nombres institucionales que se solapan con nombres personales y la presencia de anotaciones o firmas en formatos no estructurados. Por eso, una solución operativa robusta combina modelos de NLP finos con *workflows* de revisión humana por muestreo y herramientas de visualización que permitan a redactores verificar el resultado.

Asimismo, la interoperabilidad entre sistemas requiere normalizar metadatos, conservar trazabilidad de redacciones y asegurar que los documentos anonimizados conserven la integridad probatoria cuando se necesite su uso público. La existencia de errores en OCR o en la segmentación del texto debe contemplarse explícitamente en los controles de calidad, con métricas de *recall* y precisión sobre la detección de entidades

[21] Los hiperparámetros son configuraciones externas que se establecen antes de entrenar un modelo de aprendizaje automático y que controlan el proceso de entrenamiento

sensibles y procesos de remediación rápida para corregir falsos negativos que comprometan la privacidad.

Las medidas técnicas deben integrarse en un marco organizacional y jurídico que garantice cumplimiento y responsabilidad. La adopción de controles de acceso estrictos, cifrado en tránsito y en reposo, registros de auditoría inmutables, gestión de llaves y políticas claras de retención y minimización de datos son imprescindibles. Complementariamente, los procesos de evaluación de impacto sobre la protección de datos (DPIA) y la existencia de comités de gobernanza con expertos legales, técnicos y representantes de usuarios son prácticas que aseguran que las decisiones sobre anonimización respondan a criterios de proporcionalidad y necesidad. La transparencia sobre los métodos aplicados, sin revelar mecanismos que pudieran facilitar ataques, además de la publicación de resúmenes técnicos y métricas de performance, contribuye a la confianza pública y a la legitimidad de los esfuerzos de protección.

Los desafíos técnicos y éticos evolucionan con rapidez: técnicas de reidentificación cada vez más sofisticadas, externalización de datos a terceros proveedores y el hecho de que los datos anonimizados pueden adquirir valor comercial que motive ataques hacen indispensable un ciclo continuo de evaluación, actualización y auditoría. En términos prácticos, esto implica crear pipelines de anonimización que incorporen pruebas automatizadas de regresión, ejercicios periódicos de "*red teaming*" para poner a prueba las defensas, y procesos de parcheo y actualización de modelos y sistemas. La capacitación del personal, el establecimiento de acuerdos contractuales con proveedores que incluyan cláusulas de privacidad y auditabilidad, y la participación ciudadana en la definición de políticas de apertura de datos son elementos complementarios que fortalecen la resiliencia institucional.

Finalmente, la aproximación más efectiva es siempre multicapa: no basta con una sola técnica o herramienta, sino que la protección real se construye combinando anonimización automática, desidentificación inteligente, generación controlada de datos sintéticos, evaluaciones cuantitativas de riesgo, arquitecturas de aprendizaje federado cuando convenga, y la adopción de privacidad diferencial en las consultas críticas, todo ello bajo un paraguas de gobernanza, auditoría y responsabilidad ética.

Esta estrategia permite no solo reducir la probabilidad de exposición indebida, sino también mantener la utilidad de los datos para la investigación, la elaboración de políticas y la administración pública. Si lo considera útil, señor, puedo transformar este análisis en un plan operativo paso a paso para implantar una solución en un tribunal, hospital o agencia regulatoria, incluyendo un pipeline técnico, métricas de aceptación, y un esquema de gobernanza y auditoría que asegure la aplicabilidad práctica de estas ideas.

3.1.2. Inteligencia artificial en justicia y protección de datos

La incorporación de la inteligencia artificial (IA) en los sistemas de justicia constituye uno de los debates más complejos y actuales en la intersección entre tecnología y derecho. El potencial de estas herramientas radica en su capacidad para procesar grandes volúmenes de información, identificar patrones relevantes y asistir en la toma de decisiones judiciales (Lima, Fuentes, & Martins, 2023). En este sentido, la IA puede contribuir a la eficiencia procesal, la reducción de tiempos y la mejora en la gestión de expedientes, pero su uso plantea desafíos sustantivos respecto de la protección de los datos personales y la preservación de los derechos fundamentales de las partes involucradas en un proceso judicial (Rivero & Chinarro, 2024).

El interés en el uso de la IA en la justicia se ha multiplicado a partir de experiencias comparadas. En Brasil, por ejemplo, el sistema Víctor del Supremo Tribunal Federal ha mostrado la viabilidad de aplicar algoritmos de clasificación para agilizar la tramitación de casos (Lima et al., 2023). Sin embargo, estos avances tecnológicos deben ser acompañados de marcos normativos sólidos que prevengan la vulneración de derechos y aseguren transparencia en los procesos de decisión automatizada. Como lo subraya la Unión Europea en su Ley de Inteligencia Artificial (Parlamento Europeo, 2024), resulta imprescindible regular el uso de la IA en sectores de alto impacto, incluyendo la justicia, para garantizar proporcionalidad y responsabilidad institucional.

En el caso ecuatoriano, la discusión sobre IA se articula con la necesidad urgente de fortalecer la seguridad de fiscales, jueces y operadores de justicia, quienes enfrentan amenazas del crimen organizado. La IA puede convertirse en una herramienta para reforzar la protección de datos sensibles de estos funcionarios mediante mecanismos de anonimización automatizada, predicción de amenazas y detección de patrones de riesgo en comunicaciones digitales (Andrade, Toapanta, Bano, & Gómez, 2024). La aplicación

de IA en este contexto no se limita a la gestión documental, sino que se proyecta como un mecanismo de ciberseguridad judicial orientado a prevenir ataques e infiltraciones.

No obstante, el uso de IA en los sistemas judiciales genera cuestionamientos éticos y jurídicos. Diversos autores advierten sobre el riesgo de que los algoritmos introduzcan sesgos, afecten la imparcialidad judicial o creen una "opacidad algorítmica" incompatible con los principios de publicidad y motivación de las decisiones (Balcells, 2020; Contini, 2019). Este problema se agrava en contextos donde las instituciones carecen de infraestructura tecnológica suficiente o de protocolos de supervisión adecuados. Por tanto, la discusión sobre IA en justicia no puede disociarse del debate sobre responsabilidad, explicabilidad y control humano en el uso de estas tecnologías (Cárdenas & Martínez, 2021).

Desde una perspectiva de protección de datos, la IA ofrece tanto oportunidades como riesgos. Por un lado, puede reforzar la protección mediante la detección automatizada de información personal en sentencias o expedientes, reduciendo errores humanos en la anonimización (Terzidou, 2023). Por otro, el uso de algoritmos sobre grandes bases de datos judiciales abre la puerta a potenciales vulneraciones, ya que los sistemas requieren entrenamiento con información sensible que podría ser mal gestionada o filtrada. Por esta razón, organismos como la Agencia Española de Protección de Datos (2022) insisten en la necesidad de aplicar principios de minimización y proporcionalidad en el uso de datos para sistemas de IA.

La implementación de IA en justicia también exige adaptaciones normativas nacionales. En Ecuador, la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021) establece obligaciones claras en torno al tratamiento de datos sensibles y a los procesos de anonimización. Sin embargo, todavía no incorpora una regulación específica sobre decisiones asistidas por IA en el ámbito judicial. Este vacío legal representa un desafío, ya que el despliegue de estas tecnologías debe alinearse con el marco constitucional de protección de derechos, en particular con el principio de debido proceso y la tutela judicial efectiva (Asamblea Nacional Constituyente del Ecuador, 2008).

Los debates doctrinarios reflejan posiciones divergentes. Algunos sostienen que la IA puede fortalecer el acceso a la justicia al facilitar la resolución de casos menores o

estandarizados (Cumbre Judicial Iberoamericana, 2023). Otros, en cambio, consideran que su introducción podría debilitar la independencia judicial y convertir los tribunales en meros ejecutores de decisiones automatizadas (Rivero & Chinarro, 2024). Este dilema exige analizar la IA como un instrumento de apoyo, y no de sustitución, manteniendo siempre al juez como garante último de la legalidad y los derechos fundamentales (Cárdenas & Martínez, 2021).

En la práctica comparada, se observa un énfasis en la IA como herramienta de apoyo a la gestión judicial, más que como mecanismo de decisión. Por ejemplo, en España y Argentina se han desarrollado proyectos de IA destinados a la clasificación de expedientes y al control de tiempos procesales, sin que los algoritmos reemplacen la valoración de pruebas o la aplicación del derecho (Lavin, Cristallo, Sánchez, & Corvalán, 2024). Estos casos ilustran cómo la IA puede incorporarse progresivamente al sistema judicial, priorizando eficiencia sin sacrificar garantías.

La cuestión de la explicabilidad (*explainability*)[22] es fundamental en este debate. Los sistemas de IA empleados en la justicia deben ser auditables y comprensibles para jueces, abogados y ciudadanos. De lo contrario, se corre el riesgo de que las decisiones se basen en "cajas negras" que atenten contra la transparencia procesal (Mark et al., 2021). En este sentido, la academia ha propuesto el desarrollo de algoritmos explicables (XAI, por sus siglas en inglés) que permitan identificar las razones detrás de una clasificación o predicción, asegurando control judicial sobre el proceso tecnológico (Rosero, 2025).

En virtud de ello, la convergencia entre inteligencia artificial, justicia y protección de datos obliga a los Estados a diseñar políticas integrales que articulen aspectos técnicos, jurídicos y éticos. La IA no puede concebirse como una solución aislada, sino como parte de una estrategia más amplia que incluya ciberseguridad, formación especializada de jueces y fiscales, y cooperación internacional en el ámbito de derechos digitales (Guerrero, 2020; Mejía, 2024). Solo a través de este enfoque multidimensional será posible garantizar que la IA contribuya a fortalecer la justicia y el Estado de derecho, sin poner en riesgo los derechos fundamentales de las personas.

[22] Capacidad de un modelo de IA para describir y justificar sus resultados y decisiones de una manera que los humanos puedan entender.

La inteligencia artificial se proyecta como un recurso esencial para garantizar la protección de la identidad en contextos judiciales de alto riesgo, particularmente en el caso de los jueces sin rostro. Su incorporación en este ámbito no solo responde a la necesidad de resguardar la vida e integridad de los operadores de justicia, sino que también contribuye a fortalecer la legitimidad de los procesos penales al blindarlos frente a posibles presiones externas, amenazas o intentos de intimidación. La capacidad de la IA para automatizar, robustecer y auditar los procedimientos de anonimización convierte a esta tecnología en un aliado estratégico en la consolidación de un sistema judicial seguro y confiable.

Dentro de sus aplicaciones concretas, la inteligencia artificial puede intervenir en la gestión y procesamiento de documentos judiciales, eliminando cualquier elemento que comprometa la confidencialidad de los jueces. Esto incluye desde el borrado de metadatos invisibles para el ojo humano hasta la pseudonimización de información sensible, de manera que las resoluciones o expedientes carezcan de huellas que permitan rastrear al responsable de una decisión. La automatización de estos procesos reduce el margen de error humano y aporta un nivel adicional de rigurosidad en la protección, garantizando que la información difundida sea plenamente depurada antes de llegar al dominio público.

Asimismo, los algoritmos avanzados permiten generar identificadores anónimos y alias seguros que sustituyen la verdadera identidad de los jueces, construyendo capas adicionales de resguardo. Estos mecanismos no se limitan a un acto inicial de encriptación o sustitución de datos, sino que se actualizan periódicamente, verificando que no existan correlaciones indirectas o patrones que conduzcan a la reidentificación. De esta forma, la IA no solo oculta la identidad en un momento puntual, sino que asegura un monitoreo constante y adaptativo frente a nuevas técnicas de rastreo digital que podrían surgir con el tiempo (Andrade et al., 2024).

El papel del procesamiento de lenguaje natural es igualmente crucial, pues posibilita un análisis minucioso de textos para detectar nombres, referencias personales o estructuras narrativas que, de manera inadvertida, podrían desvelar la identidad del juez. Al reemplazar automáticamente dichos elementos por alternativas genéricas o codificadas, se garantiza que las resoluciones judiciales mantengan su valor jurídico y argumentativo sin comprometer la seguridad del magistrado. Este tipo de filtrado

inteligente constituye un puente entre la transparencia de las decisiones judiciales y la necesidad imperiosa de proteger la vida de quienes las emiten.

Otro aspecto relevante es el uso de algoritmos de auditoría y monitoreo que, asistidos por inteligencia artificial, se encargan de rastrear la circulación de la información y detectar vulnerabilidades. Estos sistemas pueden identificar intentos de acceso indebido, filtraciones accidentales o patrones de uso sospechosos que pudieran anticipar un riesgo de exposición. La ventaja reside en que la IA no se limita a un rol reactivo, sino que cumple una función preventiva al generar alertas tempranas, permitiendo que las instituciones judiciales adopten medidas inmediatas para reforzar la seguridad de los datos comprometidos.

La implementación de estas herramientas exige un marco normativo sólido que articule la protección de datos personales con los principios constitucionales vinculados a la administración de justicia. La inteligencia artificial, al servicio del anonimato judicial, debe operar bajo criterios de confidencialidad, integridad y disponibilidad de la información, asegurando que su uso no vulnere derechos fundamentales ni debilite la transparencia institucional. En este sentido, el despliegue tecnológico debe complementarse con mecanismos de control humano que supervisen la correcta aplicación de los algoritmos y garanticen un equilibrio entre eficacia técnica y respeto a los principios jurídicos.

La supervisión humana constituye, de hecho, un requisito indispensable para evitar riesgos asociados al sesgo algorítmico o a la sobreexposición de datos. Sin una adecuada intervención de operadores jurídicos especializados, la IA podría generar reidentificaciones involuntarias o incurrir en errores que comprometan la finalidad del anonimato. De allí la importancia de establecer protocolos auditables que permitan verificar cada etapa del proceso, asegurando que la tecnología no actúe como un ente autónomo incontrolado, sino como una herramienta integrada a la lógica institucional de la justicia.

En definitiva, la inteligencia artificial ofrece un abanico de soluciones que abarcan desde la automatización de la anonimización hasta el monitoreo constante y la generación de alertas en tiempo real. Estas capacidades no solo elevan el nivel técnico de la protección otorgada a los jueces sin rostro, sino que también fortalecen la resiliencia del

proceso penal frente a amenazas graves provenientes de organizaciones criminales o actores con poder de intimidación. Al garantizar el resguardo de la identidad de los jueces, la IA se erige como un componente esencial para preservar la independencia judicial, la confianza ciudadana y la seguridad del Estado de derecho.

En términos técnicos, la estrategia más robusta parte de un diseño por capas: un primer nivel de defensa automatizado se encarga de la identificación y eliminación de trazas directas de identidad; un segundo nivel emplea técnicas criptográficas y de gestión de claves para garantizar que cualquier pseudónimo o identificador pueda ser administrado con seguridad; y un tercer nivel provee auditoría, monitorización y gobernanza para equilibrar la protección con la rendición de cuentas. Este enfoque en profundidad reconoce que la anonimización no es un único acto puntual, sino un proceso continuo que debe incorporarse al ciclo de vida de la información judicial desde la ingestión del expediente hasta su publicación y archivo.

La detección y clasificación de información susceptible de levantar la anonimización a un juez es el primer cuello de botella técnico y requiere una combinación de herramientas. Los sistemas deben integrar OCR de alta calidad para documentos escaneados, reconocimiento de entidades (NER) entrenado en dominios jurídicos para localizar nombres, cargos, referencias geográficas y cualquier metadato incrustado en archivos digitales. A ello se suman reglas heurísticas y detección difusa para capturar variantes y errores tipográficos, así como módulos de correlación que identifiquen patrones indirectos, por ejemplo, estilos de firma, referencias a resoluciones anteriores o frases idiosincrásicas que podrían, en conjunto, facilitar la reidentificación.

Es importante subrayar que la medición de la eficacia de estos módulos se realiza mediante métricas de clasificación (precisión, exhaustividad y F1) y, sobre todo, mediante pruebas adversariales[23] que simulan ataques reales de vinculación y reidentificación. Una vez detectada la información sensible, la transformación debe sopesar dos objetivos en tensión: preservar la integridad jurídica y probatoria del contenido y, al mismo tiempo, eliminar las señales que permitan vincular el documento con una persona concreta.

[23] Las pruebas adversariales implican intentar de forma proactiva "romper" una aplicación proporcionándole datos que probablemente generen resultados problemáticos.

Entre las técnicas habituales aparecen la pseudonimización mediante alias rotativos, el enmascaramiento irreversible (*hashing* en contextos donde no se requerirá recuperación), la tokenización con almacenamiento de mapeos en bóvedas cifradas y la redacción controlada de pasajes susceptibles de revelar identidad. En casos donde el estilo de redacción pueda revelar autoría (riesgo de estilometría), se pueden aplicar transformaciones de texto que preserven la argumentación y la ratio decidendi, pero neutralicen rasgos estilísticos siempre bajo revisión humana para evitar alterar el sentido jurídico.

Además, para estadísticas o informes agregados, la incorporación de técnicas de privacidad diferencial ofrece una capa matemática de protección frente a ataques de inferencia, aunque su empleo en documentos jurídicos exige cuidado porque introduce ruido que puede afectar interpretaciones sensibles. La seguridad del sistema en su conjunto depende críticamente de la arquitectura de despliegue y de la gestión de claves. Los mapeos entre identidad real y alias deben custodiarse con controles de acceso estrictos, aislamiento de funciones y, preferiblemente, técnicas de *escrow* multiparte donde nunca una sola entidad tenga el control absoluto.

El uso de módulos de seguridad de hardware (HSM), enclaves seguros o soluciones de cifrado homomórfico para operaciones concretas puede reducir la superficie de ataque. Asimismo, existen decisiones de diseño importantes entre operar en entornos *on-premises* o en la nube: la primera opción reduce la dependencia de terceros y la exposición, mientras que la segunda puede ofrecer escalabilidad; la elección debe derivarse de una evaluación de riesgo, la criticidad del caso y el marco jurídico aplicable. En todos los casos, la integridad de las resoluciones publicadas debería asegurarse con firmas digitales inmutables que acrediten que el texto difundido es la versión autorizada y anonimizadas aprobada por el órgano correspondiente.

Los riesgos de reidentificación obligan a contemplar vectores sofisticados. La recolección masiva de datos en fuentes abiertas (redes sociales, noticias, registros públicos) permite realizar ataques de *linkage* que combinan mínimos fragmentos de información para revelar identidades. La estilometría y los modelos de atribución autoral modernos representan otra amenaza: algoritmos capaces de correlacionar patrones de redacción con autores conocidos.

A nivel de IA, los modelos entrenados con datos sensibles pueden sufrir fugas por ataques de extracción o por inferencias de membresía; por ello, las organizaciones deberían evitar entrenar con datos sin depuración y, cuando sea necesario usar aprendizaje automático, aplicar técnicas de entrenamiento con privacidad diferencial, limitar el acceso a los modelos y someterlos a pruebas de membresía e inversión. La mitigación de estos riesgos pasa por una combinación de prevención (minimizar y tratar datos antes del uso), detección (monitoreo continuo y pruebas red team) y respuesta (procedimientos de contingencia y revocación de publicaciones cuando se detecte un incidente).

La gobernanza y las salvaguardias judiciales son igualmente críticas: la anonimización no puede transformarse en un escudo para la opacidad institucional ni en un obstáculo para la rendición de cuentas. Por ello, debe establecerse un marco normativo que determine qué tipos de procesos justifican el secreto de identidad, quién puede solicitar la revelación de *mapping* bajo qué condiciones y mediante qué garantías, y qué órganos de control supervisan la aplicación de las técnicas.

La adopción de registros de auditoría inmutables, con acceso restringido y trazabilidad criptográfica, permite que tanto auditores internos como comités independientes verifiquen que la anonimización se aplicó correctamente y que los mapeos sólo se han utilizado conforme al debido proceso. En términos operativos, esto requiere políticas claras sobre retención, eliminación segura de mapeos y la existencia de protocolos de emergencia para revelar identidades a autoridades competentes mediante órdenes judiciales explícitas y procedimientos de control judicial.

También es esencial atender las limitaciones éticas y de derechos humanos que emergen. La protección de la identidad debe equilibrarse con el principio de publicidad de la función jurisdiccional y el derecho de las partes y de la sociedad a conocer motivaciones y responsables. Si la técnica desplaza el deber de transparencia, se socava la confianza pública. Por ello, cualquier sistema técnico debe acompañarse de políticas que expliquen públicamente los criterios que justifican el anonimato, los límites temporales de la protección y los mecanismos de supervisión que impiden abusos. Asimismo, es necesario formar al personal judicial y administrativo sobre los riesgos y las prácticas correctas: la tecnología solo es tan buena como las personas que la gestionan.

Desde la perspectiva de aseguramiento de calidad, la implementación debe incluir pruebas de vulnerabilidad continuas, pruebas de reidentificación por terceros independientes, ejercicios de "red-team" donde expertos intenten romper el anonimato y auditorías periódicas sobre sesgos algorítmicos. Se deben definir umbrales de aceptación técnica, por ejemplo, tasas de detección mínima para NER y límites de riesgo residual aceptables calculados sobre escenarios adversariales y someter el sistema a revisiones independientes antes de su uso en casos críticos. Igualmente, cualquier modelo de IA deberá contar con documentación exhaustiva sobre el conjunto de entrenamiento, las transformaciones aplicadas y los límites conocidos del sistema (*model cards y data sheets para datasets*), de modo que los responsables judiciales conozcan sus capacidades y limitaciones.

Finalmente, la introducción de IA para anonimizar jueces sin rostro debe concebirse como un proyecto interdisciplinario que integre expertos en derecho, informática forense, criptografía, privacidad de datos, ética y seguridad operativa. No existe una solución puramente tecnológica que sea suficiente por sí sola; la eficacia real reside en una combinación de buen diseño técnico, controles legales, transparencia sobre criterios y mecanismos de supervisión y una cultura institucional orientada al cumplimiento y a la protección de los derechos fundamentales. La IA puede elevar considerablemente el nivel de protección y reducir riesgos, pero siempre dentro de un marco donde la rendición de cuentas, la revisión humana y la evaluación continúa del riesgo ocupen un lugar central.

3.1.3. Marco normativo y contexto ecuatoriano

En el Ecuador, la discusión en torno a la adopción de la figura de jueces sin rostro se ha intensificado debido a la escalada de violencia vinculada a la delincuencia organizada y al aumento del poder de estructuras criminales con capacidad real de intimidar e incluso atentar contra la vida de jueces, fiscales y otros operadores de justicia. Este escenario ha abierto un debate profundo sobre la necesidad de implementar medidas extraordinarias que fortalezcan la independencia judicial y aseguren que los procesos penales de alto impacto no se vean paralizados o distorsionados por la presión ejercida por grupos delictivos (Acuña et al., 2025).

La naturaleza del fenómeno criminal en Ecuador marcado por carteles internacionales, mafias locales y estructuras armadas que operan en cárceles y territorios

urbanos ha transformado las condiciones en las que los jueces desempeñan sus funciones, al punto de que la administración de justicia se percibe amenazada no solo por la corrupción, sino también por el miedo y la coacción. En este sentido, los jueces sin rostro aparecen como un mecanismo destinado a reducir esa vulnerabilidad, permitiendo que quienes tienen la responsabilidad de juzgar delitos complejos lo hagan con la certeza de que su identidad y seguridad estarán debidamente protegidas.

Los estudios realizados en 2024 y 2025, a nivel académico y en sectores especializados de la práctica judicial, han confirmado la viabilidad de implementar esta figura sin necesidad de reformar de manera profunda la Constitución ecuatoriana. En efecto, se sostiene que los principios ya vigentes dentro del sistema jurídico permiten justificar la medida, siempre y cuando se regule bajo parámetros claros de excepcionalidad, proporcionalidad y temporalidad. La experiencia comparada refuerza este argumento: Colombia, en la década de los noventa, implementó jueces sin rostro frente al embate del narcotráfico y la amenaza de grupos armados, lo que permitió avanzar en procesos judiciales que de otro modo hubieran sido inviable por el altísimo riesgo para la vida de los jueces.

Perú, en un contexto similar, utilizó este mecanismo para juzgar a miembros de Sendero Luminoso y del MRTA, logrando procesar a líderes terroristas que, de haber conocido la identidad de sus jueces, habrían atentado contra ellos o sus familias. Estos antecedentes internacionales son considerados en Ecuador como una referencia clara de que la figura puede ser eficaz, siempre que se la diseñe de manera compatible con las garantías fundamentales.

Tabla 1.

Comparativa de jueces sin rostro en Ecuador

Aspecto	**Colombia**	**Perú**	**Lecciones para Ecuador**
Delitos aplicables	Narcotráfico, crimen organizado, terrorismo	Terrorismo interno (Sendero Luminoso, MRTA)	Limitar la figura a delitos de alto riesgo, evitando aplicación generalizada. IA puede identificar

			automáticamente los procesos que cumplen criterios de riesgo.
Publicidad de procesos	Anonimato del juez frente a las partes, pero registros completos y confidenciales	Jueces anónimos, supervisión de comité especial dentro del Poder Judicial	Garantizar transparencia funcional mediante registros auditables por instancias superiores; la IA puede generar trazabilidad automatizada y verificable de actuaciones.
Debido proceso y derecho a la defensa	Derecho a recusar y control institucional de imparcialidad mantenido mediante tribunales superiores	Comité especial revisa conflictos de interés y supervisa imparcialidad de manera confidencial	Establecer canales seguros de recusación y revisión, apoyados por IA, para mantener garantías procesales incluso con anonimato.
Imparcialidad judicial	Supervisión por órganos superiores evita percepciones de parcialidad	Comité confidencial asegura imparcialidad y coherencia de fallos	IA puede monitorear patrones de decisiones y alertar posibles sesgos, reforzando imparcialidad objetiva.
Motivación de las decisiones	Jueces obligados a fundamentar fallos; registros auditables	Fallos motivados y revisables por comité confidencial	IA puede documentar el razonamiento judicial paso a paso, garantizando

			motivación clara y auditabilidad.
Proporcionalidad y temporalidad	Medida excepcional, aplicada solo en contextos de alto riesgo	Excepcional y temporal, nunca regla general	Definir criterios estrictos de excepción y límites temporales; IA puede ayudar a vigilar cumplimiento de estos criterios.
Seguridad jurídica y legalidad	Regulación específica y protocolos internos	Regulación y supervisión interna para evitar arbitrariedad	Establecer marco normativo claro que respalde la medida; IA como soporte técnico, no sustituto del juez, asegurando legalidad y consistencia.
Riesgos mitigados	Amenazas físicas a jueces, paralización de procesos por crimen organizado	Represalias violentas, cuestionamientos de imparcialidad	Minimizar riesgo de ataques y garantizar continuidad judicial, mientras se preservan derechos fundamentales mediante supervisión y trazabilidad tecnológica.

Fuente. Elaboración propia.

El tema más sensible en el debate ecuatoriano ha sido la compatibilidad entre la protección de la identidad de los jueces y el respeto al debido proceso y a los derechos de las partes. Críticos de la figura han planteado que ocultar la identidad del juez podría ser visto como un obstáculo para garantizar la transparencia, la publicidad de los juicios y el derecho a conocer a quien decide sobre la libertad o la culpabilidad de un individuo. Sin embargo, la doctrina mayoritaria y los análisis judiciales realizados en el país han respondido que esta medida no necesariamente implica la vulneración de tales garantías, siempre que se establezcan mecanismos paralelos de control, como la posibilidad de

impugnación, la revisión por tribunales colegiados y la supervisión estricta de las decisiones judiciales.

La clave, entonces, está en configurar un diseño normativo que permita equilibrar el derecho de defensa con la necesidad de proteger la vida de los jueces, asegurando que el anonimato no se convierta en un instrumento de arbitrariedad, sino en una herramienta de protección legítima frente a riesgos concretos y extraordinarios. La percepción dentro de la comunidad jurídica ecuatoriana se inclina de manera decidida hacia la aceptación de esta figura. En investigaciones recientes, el 100% de los abogados encuestados manifestó que consideran los jueces sin rostro una medida indispensable para el contexto actual del país, caracterizado por una escalada de violencia que ha alcanzado niveles inéditos en su historia contemporánea.

Este consenso se explica porque los profesionales del derecho reconocen que la independencia judicial no se limita a la ausencia de presiones políticas o económicas, sino que también exige la protección física de quienes administran justicia. Si un juez no puede actuar libremente por temor a represalias contra él o su familia, el derecho mismo pierde eficacia, y el sistema de justicia se convierte en un terreno fértil para la impunidad. De ahí que la implementación de jueces sin rostro sea vista no como un privilegio para los jueces, sino como una garantía para la sociedad en su conjunto, en tanto asegura que los procesos penales se desarrollen con imparcialidad y continuidad.

No obstante, y pese al consenso doctrinal y técnico, hasta la fecha no se han producido reformas normativas que institucionalicen esta figura en Ecuador. La ausencia de modificaciones a nivel constitucional o de leyes orgánicas implica que la figura de jueces sin rostro no tiene un marco regulatorio claro que habilite su aplicación en los procedimientos penales ordinarios. Esta carencia refleja, por un lado, la prudencia del legislador ante las tensiones que podrían surgir con el marco de derechos humanos y, por otro, una falta de voluntad política para enfrentar de manera frontal un problema cuya urgencia ya es evidente. La doctrina, sin embargo, insiste en la necesidad de superar esta inercia legislativa y diseñar un sistema regulado que contemple las condiciones excepcionales de aplicación, los límites a su uso y los controles judiciales y constitucionales pertinentes.

La discusión sobre su implementación también pone de relieve una cuestión de fondo: el equilibrio entre seguridad y derechos fundamentales. El derecho constitucional ecuatoriano, al igual que el derecho internacional de los derechos humanos, establece principios que garantizan el debido proceso y el acceso a una justicia transparente. Sin embargo, también reconoce la necesidad de medidas excepcionales frente a circunstancias extraordinarias, siempre que estas se encuentren debidamente justificadas y limitadas en el tiempo (Portilla et al., 2024).

La figura de los jueces sin rostro se enmarca precisamente en esa tensión, donde la protección de la vida de los jueces y la preservación de la función judicial se erigen como valores que justifican una limitación parcial de la publicidad y transparencia de la identidad judicial. La doctrina insiste en que no se trata de un sacrificio desmedido de derechos, sino de una ponderación razonable para garantizar el bien mayor: la continuidad de la justicia en un entorno dominado por la criminalidad organizada.

Desde un punto de vista político y social, la adopción de jueces sin rostro también refleja una respuesta del Estado a la demanda ciudadana de enfrentar con firmeza al crimen organizado. En un contexto en que las cárceles ecuatorianas se han convertido en centros de operación de grupos armados y el poder del narcotráfico ha penetrado múltiples instituciones, la sociedad exige soluciones visibles y eficaces. La institucionalización de jueces sin rostro podría enviar un mensaje claro de que el Estado está dispuesto a proteger a sus funcionarios y a no ceder ante las amenazas del crimen, fortaleciendo así la confianza ciudadana en la justicia.

No obstante, este objetivo no debe desligarse de la responsabilidad de diseñar un marco legal que evite que la medida se convierta en una herramienta discrecional o permanente, lo cual podría socavar la legitimidad del sistema. En conclusión, la figura de jueces sin rostro en Ecuador representa una alternativa jurídicamente viable, socialmente necesaria y constitucionalmente admisible, pero que aún permanece en el terreno de la propuesta y no de la realidad normativa.

El marco jurídico ecuatoriano en materia de protección de datos y funcionamiento de la administración pública ha experimentado importantes avances en la última década, consolidando un andamiaje normativo que responde a las exigencias internacionales en derechos digitales. La Ley Orgánica de Protección de Datos Personales (Asamblea

Nacional del Ecuador, 2021) constituye el instrumento central, pues regula de manera integral el tratamiento, almacenamiento y transferencia de información personal en el país. Esta normativa reconoce los datos personales como un derecho autónomo y establece principios como licitud, finalidad y proporcionalidad, obligando tanto a entidades públicas como privadas a cumplir con estándares de seguridad en la gestión de información.

En paralelo, el Código Orgánico Administrativo (COA) (Asamblea Nacional del Ecuador, 2017) ofrece un soporte regulatorio complementario al fijar procedimientos y competencias para el manejo de datos dentro de la administración pública, reforzando la transparencia y la obligación de custodia responsable. Ambas normas se convierten en pilares de protección frente al riesgo de abuso o exposición indebida de datos en un contexto de creciente digitalización judicial.

Desde un plano constitucional, la Constitución de la República del Ecuador (Asamblea Nacional Constituyente del Ecuador, 2008) sienta las bases de los derechos fundamentales vinculados a la intimidad, el habeas data y la tutela judicial efectiva, garantizando que el manejo de información personal esté sometido a principios de proporcionalidad y necesidad. Este marco se articula con la Ley Orgánica de Transparencia y Acceso a la Información Pública (Congreso Nacional del Ecuador, 2004), que asegura el derecho de la ciudadanía a acceder a información pública, pero al mismo tiempo exige restricciones proporcionales para proteger datos sensibles.

La coexistencia de transparencia y protección de datos plantea un reto de equilibrio institucional: garantizar la publicidad de los actos judiciales sin exponer indebidamente a las partes involucradas. De esta manera, el marco normativo ecuatoriano persigue armonizar la apertura informativa con la salvaguarda de los derechos fundamentales en un entorno judicial cada vez más vulnerable frente a amenazas externas.

La incorporación de jueces sin rostro en el Ecuador, especialmente en un modelo apoyado por inteligencia artificial (IA) para garantizar el anonimato o para gestionar procesos judiciales sensibles, implica un análisis detallado de los principios y garantías constitucionales y procesales que podrían verse involucrados o eventualmente tensionados (Andrade et al., 2024). El punto central está en determinar cómo compatibilizar el marco de protección a la función judicial con los derechos

fundamentales reconocidos en la Constitución de 2008 y en los tratados internacionales de derechos humanos ratificados por el Estado ecuatoriano.

La publicidad de los procesos judiciales, reconocida en el artículo 168 de la Constitución de la República del Ecuador (2008), constituye una garantía esencial del Estado constitucional de derechos, orientada a que los juicios se desarrollen a la vista de las partes y, en general, de la sociedad, para evitar la opacidad y garantizar la confianza en la justicia. La introducción de jueces sin rostro supone, de manera inmediata, una restricción a este principio, pues la identidad de quienes imparten justicia no se revelaría públicamente.

Este límite podría parecer contrario a la transparencia procesal; sin embargo, debe subrayarse que la publicidad no es absoluta y admite excepciones cuando están en juego bienes jurídicos de alta relevancia, como la vida y seguridad de los jueces. Con el apoyo de la IA, sería posible compensar este déficit de visibilidad personal mediante la creación de sistemas que registren y archiven de forma íntegra las actuaciones y decisiones, de modo que, aunque la identidad del juez se mantenga en reserva, las motivaciones y razonamientos de sus fallos sean plenamente accesibles, verificables y auditables por las partes y órganos de control.

El derecho al debido proceso (artículo 76 de la Constitución) representa el eje transversal de toda la discusión. Dentro de este derecho se incluyen varias manifestaciones: el derecho a ser oído, a ejercer la defensa, a contar con un juez competente e imparcial, y a impugnar decisiones judiciales. El anonimato judicial podría generar tensiones con algunas de estas manifestaciones, en particular con la posibilidad de conocer al juez que dirige el proceso o de presentar recusaciones.

No obstante, la doctrina constitucional admite que el debido proceso puede articularse con medidas excepcionales siempre que exista proporcionalidad. Una implementación con apoyo de IA permitiría establecer canales de recusación y control a través de mecanismos institucionales en los que un comité o un órgano colegiado verifiquen la idoneidad del juez sin necesidad de revelar su identidad públicamente, asegurando que no existan vínculos de parcialidad o intereses indebidos. Así, el debido proceso se preserva, aunque se ejecute bajo modalidades innovadoras.

La imparcialidad judicial, consagrada en el artículo 172 de la Constitución, exige que los jueces actúen únicamente conforme a la Constitución, la ley y los principios de justicia, sin influencia de poderes externos. En el modelo de jueces sin rostro, el principal riesgo es que la opacidad en la identidad pueda generar sospechas de parcialidad o falta de independencia, lo que podría socavar la confianza de la ciudadanía en la administración de justicia.

En este punto, la IA puede convertirse en un aliado importante, pues su capacidad para registrar cada actuación, generar historiales transparentes y comparar patrones de razonamiento judicial permitiría que los fallos sean supervisados por instancias superiores y órganos de control, reforzando la idea de imparcialidad objetiva. No se trata de sustituir al juez por un algoritmo, sino de utilizar la tecnología como un mecanismo de apoyo para evitar desviaciones y asegurar que el anonimato no se traduzca en arbitrariedad.

El principio de motivación de las sentencias (artículo 76.7.l) constituye otra garantía fundamental. Toda decisión judicial debe ser clara, razonada y suficientemente argumentada, de forma que las partes comprendan por qué se ha resuelto de una u otra manera. El anonimato judicial en nada debería limitar este principio, siempre que se garantice la obligación de motivación. Con el apoyo de la IA, este deber podría reforzarse, ya que los sistemas tecnológicos permitirían registrar no solo el fallo final, sino también el proceso lógico y normativo seguido por el juez, facilitando la trazabilidad de las decisiones.

De esa forma, la garantía de motivación incluso podría fortalecerse bajo este modelo, ya que el escrutinio se desplazaría de la persona del juez hacia la calidad y coherencia de sus decisiones. La presunción de inocencia (artículo 76.2) es otro derecho que se ve indirectamente comprometido. La defensa podría alegar que, al desconocer la identidad del juez, se limita su capacidad de evaluar y cuestionar posibles sesgos, lo cual afectaría la equidad procesal.

Sin embargo, mientras el sistema garantice recursos de apelación, revisión y control judicial, esta garantía no se vulnera necesariamente. La IA puede ofrecer un valor añadido al asegurar que las decisiones se tomen con base en parámetros objetivos y con trazabilidad completa, reduciendo la posibilidad de que un fallo adverso se deba a factores subjetivos o externos. En este punto, el reto consiste en diseñar protocolos que demuestren

que el anonimato no afecta el juicio justo, sino que únicamente protege al juez frente a amenazas.

El derecho a la defensa y a la contradicción (artículo 76.7.a y b) es probablemente uno de los más delicados en este contexto. Los abogados defensores podrían alegar que, sin conocer al juez, su capacidad para cuestionar su imparcialidad o presentar recusaciones se ve disminuida. Para responder a este dilema, la implementación debería incluir mecanismos de verificación confidenciales gestionados por instituciones como el Consejo de la Judicatura, que puedan revisar en reserva la identidad del juez para descartar incompatibilidades o intereses.

De esta manera, la defensa no quedaría en estado de indefensión, pues tendría la seguridad de que existen filtros institucionales, aunque no pueda confrontar directamente al juez en lo personal. La IA aquí podría servir como un medio de verificación adicional, analizando posibles vínculos del juez con partes procesales o patrones de decisiones que puedan generar dudas razonables. La seguridad jurídica (artículo 82) y el principio de legalidad penal (artículo 76.3) demandan que toda restricción de derechos esté previamente establecida en la ley, sea clara y previsible, y se aplique conforme al principio de proporcionalidad.

Esto significa que la introducción de jueces sin rostro no podría implementarse de forma improvisada ni discrecional, sino únicamente mediante una reforma normativa expresa que establezca los supuestos excepcionales, las condiciones de aplicación, los órganos encargados de controlar la medida y los límites temporales. La IA, en este marco, no sustituiría la ley, pero sí podría garantizar que su aplicación sea coherente, verificable y uniforme, reduciendo el riesgo de discrecionalidad o abusos.

Finalmente, el principio de proporcionalidad, reconocido tanto en la Constitución como en la jurisprudencia de la Corte Constitucional, es central para evaluar la validez de esta figura. La proporcionalidad implica que la medida sea adecuada para alcanzar un fin legítimo (proteger la vida de los jueces y garantizar la continuidad de la justicia), necesaria en ausencia de alternativas menos restrictivas, y equilibrada, es decir, que el beneficio obtenido no sea inferior al sacrificio de derechos que genera.

En este sentido, los jueces sin rostro con apoyo de IA se justifican únicamente en contextos de alto riesgo relacionados con delincuencia organizada o terrorismo, y no en

procesos ordinarios. La medida debe ser estrictamente temporal y excepcional, y siempre sometida a control constitucional para evitar que se convierta en regla general. En síntesis, la figura de jueces sin rostro en Ecuador, con apoyo de inteligencia artificial, involucra directamente garantías como la publicidad, el debido proceso, la imparcialidad judicial, la motivación de las sentencias, la presunción de inocencia, el derecho a la defensa y la seguridad jurídica.

Todas estas garantías no serían necesariamente vulneradas si el diseño institucional establece un equilibrio entre protección de la vida de los jueces y preservación de los derechos de las partes. La IA podría convertirse en un soporte que brinde trazabilidad, control y transparencia técnica, siempre bajo la premisa de que las decisiones judiciales deben seguir siendo humanas, motivadas y sujetas a revisión en instancias superiores.

En el ámbito académico, los estudios recientes sobre la justicia ecuatoriana han resaltado la importancia de medidas excepcionales frente a la amenaza del crimen organizado. Cuarán y Sánchez (2025) examinan el concepto de “jueces sin rostro” como una estrategia normativa orientada a proteger la identidad de los operadores de justicia en casos de delincuencia organizada, destacando los dilemas que este mecanismo plantea en términos de seguridad jurídica y debido proceso. Según los autores, el anonimato de los jueces puede garantizar su integridad física, pero también puede tensionar el principio de publicidad de la justicia, lo que requiere un diseño normativo cuidadoso para no afectar las garantías constitucionales.

En la misma línea, Gallegos (2023) aporta evidencia empírica sobre la implementación práctica de esta figura en procesos vinculados a criminalidad organizada, identificando fortalezas y debilidades del modelo. Su estudio revela que, aunque la figura de jueces sin rostro busca reforzar la seguridad institucional, en la práctica enfrenta limitaciones operativas y críticas desde la perspectiva de los derechos humanos.

Este cuerpo normativo y doctrinario refleja un contexto ecuatoriano caracterizado por tensiones entre seguridad y garantías procesales, donde las medidas de protección incluyendo la anonimización de datos y la figura de jueces sin rostro deben evaluarse a la luz del marco constitucional y de las obligaciones internacionales en derechos humanos. Así, Ecuador se encuentra en la encrucijada de diseñar un sistema judicial que combine

transparencia, protección de datos y salvaguarda de los operadores de justicia, con el fin de asegurar tanto la legitimidad institucional como la efectividad en la lucha contra el crimen organizado.

Su implementación exigiría un diseño legal cuidadoso que garantice un uso limitado y controlado, orientado a contextos de alto riesgo relacionados con delincuencia organizada y terrorismo. La experiencia comparada demuestra que la medida puede ser efectiva y compatible con un Estado de derecho, siempre que se eviten excesos y se respeten los principios de proporcionalidad y excepcionalidad.

La ausencia de reformas concretas en el Ecuador no elimina la pertinencia del debate, sino que, por el contrario, evidencia la urgencia de avanzar hacia una legislación clara que permita blindar a los jueces frente a las amenazas del crimen organizado. En última instancia, la adopción de esta figura no solo se orienta a proteger a los operadores de justicia, sino a resguardar la integridad misma del sistema democrático, cuyo funcionamiento depende de que la justicia pueda actuar con independencia y sin miedo.

3.2. Discusión

Uno de los riesgos centrales identificados en la literatura es la influencia indebida de sistemas de IA sobre la actividad judicial, que puede materializarse en opacidad, sesgos y atribuciones de autoridad técnica que desplacen la responsabilidad humana. Contini (2019), en el marco de UNODC, advierte que la IA puede funcionar como un “caballo de Troya” si no existen salvaguardas jurídicas y técnicas adecuadas: algoritmos sin explicabilidad pueden condicionar prácticas administrativas y operativas, reducir márgenes de discrecionalidad informada y crear una aparente eficacia que en realidad encubre decisiones no auditables.

Esta problemática adquiere mayor riesgo en contextos donde el crimen organizado ya ejerce presión sobre el sistema judicial, pues la combinación de opacidad algorítmica y amenazas externas erosiona la trazabilidad y dificulta identificar responsables en caso de fallos o abusos (Contini, 2019). Vinculado a ello, la gestión de datos para entrenar modelos de IA genera vulnerabilidades concretas de privacidad y reidentificación. Rosero (2025) enfatiza que los sistemas de IA que manipulan pruebas electrónicas trabajan con metadatos y datos sensibles que, si no se someten a protocolos criptográficos robustos y

controles de acceso, pueden ser objeto de filtraciones o reidentificación mediante cruces con fuentes abiertas.

Además, la propia cadena de custodia digital exige estándares más altos: si se incorporan modelos de IA sin registros de versiones, sin registro de procedimientos de anonimización ni sin auditorías técnicas, se pone en riesgo la validez probatoria y la seguridad de los operadores judiciales (Rosero, 2025). Existen vacíos institucionales y normativos que dificultan la adopción segura de IA en la protección de identidad. A nivel nacional, muchas normas de protección de datos fueron diseñadas antes del auge de la IA y no contienen mandatos específicos sobre auditoría algorítmica, evaluaciones de impacto de privacidad para algoritmos, ni obligaciones de explicabilidad y registro técnico de modelos.

Esto crea una zona gris donde las instituciones pueden adoptar tecnologías sin criterios homogéneos de evaluación del riesgo, lo que, en situaciones de alta peligrosidad, puede traducirse en medidas de protección insuficientes o inconsistencia entre jurisdicciones (Asamblea Nacional del Ecuador, 2021; Parlamento Europeo, 2024). Desde el punto de vista organizativo, la falta de unidades técnicas especializadas y capacitación es otro vacío manifiesto.

Mejía (2024) propone la creación de estructuras institucionales dedicadas unidad de protección judicial y equipos técnicos mixtos que integren peritos en ciberseguridad, juristas y analistas de datos. Sin estas instancias, las decisiones sobre anonimización automatizada, cifrado homomórfico o políticas de acceso se diluyen entre áreas administrativas sin experticia, lo que aumenta el riesgo de implementaciones deficientes y de dependencia de proveedores externos sin control apropiado.

En términos de gobernanza de la tecnología, la ausencia de protocolos de evaluación y pruebas adversariales (*adversarial testing*)[24] para técnicas automatizadas de anonimización constituye un fallo crítico. El documento revisado resalta la necesidad de someter cualquier sistema a intentos controlados de reidentificación antes de su puesta en producción, y de documentar públicamente (sin revelar vulnerabilidades) los resultados de dichas pruebas para justificar la proporcionalidad de publicar resoluciones

[24] Las pruebas adversarias son un método para evaluar sistemáticamente un modelo de aprendizaje automático (ML) con el fin de aprender cómo se comporta cuando se le proporciona información maliciosa o dañina inadvertidamente.

anonimizadas. Sin dicha exigencia, la institución puede creer que ha mitigado riesgos que, en realidad, permanecen latentes y explotables por actores sofisticados.

En la esfera normativa internacional, las buenas prácticas son emergentes, pero ya existen marcos útiles: la AI Act de la UE (Parlamento Europeo, 2024) exige categorización de riesgo, supervisión humana y evaluación de impacto de derechos fundamentales para sistemas de alto riesgo condiciones aplicables al uso de IA en justicia; estas exigencias sirven como referencia para diseñar requisitos de implementación local. El documento aconseja que Ecuador adopte criterios similares, por ejemplo: obligatoriedad de evaluaciones de impacto algorítmico, registros técnicos, políticas de transparencia proactiva y obligaciones de auditoría por terceros independientes (Parlamento Europeo, 2024).

Tabla 2.

Comparativa de casos.

País	Propuesta	Fortalezas existentes	Contraste con Ecuador
Colombia	Políticas integrales de ciberseguridad y protocolos para protección de infraestructuras críticas; énfasis en formación y SOCs[25] locales (Cáceres, 2017).	Experiencias en fortalecimiento de infraestructuras y programas de capacitación en seguridad.	Ecuador necesita consolidar SOCs judiciales y formación especializada; falta coordinación nacional para ciberprotección judicial.
Brasil	Implementaciones a escala (sistemas de apoyo y automatización en tribunales como el sistema Víctor), con atención en eficiencia procesal y control	Capacidad técnica en algunos tribunales mayores; precedentes de uso de IA en gestión de expedientes.	Riesgo de replicar modelos sin salvaguardas: Ecuador necesita marcos de supervisión algorítmica y pruebas

[25] Sistema en un Chip (System on a Chip), circuito integrado que contiene todos los componentes principales de un sistema informático

	documental (Lima et al., 2023).		de impacto antes de adopción.
Finlandia	Proyectos piloto de anonimización automatizada (ANOPPI), uso de PLN[26] para detección de entidades y enmascaramiento con evaluación técnica (Terzidou, 2023).	Enfoques experimentales robustos y cultura de pruebas adversariales.	Ecuador carece de pilotos controlados y de protocolos de validación técnica para anonimización automática.
Unión Europea (UE)	AI Act: clasificación por riesgo, requerimientos de explicabilidad, supervisión humana y evaluaciones de impacto (Parlamento Europeo, 2024).	Marco regulatorio avanzado que obliga a controles estrictos para IA de alto riesgo.	Ecuador necesita incorporar mandatos parecidos (evaluación de impacto algorítmico, transparencia técnica) a su normativa nacional.
Ecuador	Ley de Protección de Datos (2021) y COA (2017) ofrecen base legal; iniciativas académicas proponen jueces sin rostro y soluciones basadas en IA (Gallegos, 2023; Cuarán & Sánchez, 2025).	Existe marco legal básico, conciencia institucional y estudios académicos que proponen soluciones; creación de unidades especializadas propuesta por la doctrina (Mejía, 2024).	Falta normativa específica sobre IA en justicia (auditoría algorítmica), ausencia de unidades técnicas consolidadas, escasez de pilotos validados, y recursos para desplegar cifrado homomórfico y protocolos de adversarial testing.

[26] Procesamiento de lenguaje natural: rama de la inteligencia artificial que permite a las computadoras entender, interpretar y generar lenguaje humano tanto hablado como escrito.

Fuente: Elaboración propia.

Desde la óptica preventiva, Merino, Guilcapi y Defas (2024) sostienen que políticas institucionales proactivas más que reactivas son clave para combatir el crimen organizado. Proponen integrar la protección de identidad dentro de una estrategia más amplia que incluya inteligencia institucional (OSINT), fortalecimiento de seguridad física y digital, protocolos interinstitucionales de intercambio seguro de información y líneas de coordinación con fuerzas del orden. La idea es que la IA sea una herramienta dentro de un sistema de prevención que reduzca la superficie de ataque y no un parche tecnocrático aislado (Merino, Guilcapi, & Defas, 2024).

En términos concretos de propuestas tecnológicas, el documento revisado recomienda medidas combinadas: anonimización automática supervisada, cifrado homomórfico para operaciones analíticas sobre datos sensibles, control de accesos por roles y registros inmutables de versiones (blockchain) para auditar cambios en documentos anonimizados. Estas soluciones técnicas deben acompañarse de marcos legales que definan responsabilidades, mecanismos de revisión y cauces de apelación en caso de errores de anonimización, además de políticas de retención que limiten la persistencia de datos sensibles (Andrade et al., 2024; Roldán, 2021).

En la esfera de confianza pública, es imprescindible promover transparencia responsable: publicar memorias técnicas que expliquen los criterios generales de anonimización y auditoría (sin revelar vulnerabilidades operativas), incluir controles ciudadanos y académicos en pilotos, y articular mecanismos de rendición de cuentas. El objetivo es evitar que medidas de protección se perciban como cortinas de humo para ocultar responsabilidad institucional; al contrario, deben reforzar la legitimidad del sistema. Mejía (2024) subraya que la confianza ciudadana es un componente clave para la sostenibilidad de las iniciativas tecnológicas de protección judicial.

Además, la hoja de ruta recomendada combina reformas normativas, inversión en capacidades técnicas y estrategia institucional: (a) actualizar la normativa para incluir exigencias de auditoría algorítmica y evaluación de impacto; (b) crear unidades técnicas y programas de formación continua; (c) establecer alianzas internacionales para intercambiar buenas prácticas (Finlandia, UE, Brasil, Colombia); y (e) asegurar fondos y gobernanza transparente que eviten dependencia tecnológica sin control. Solo una política

pública integral puede mitigar los riesgos identificados y cerrar los principales vacíos detectados en la revisión documental.

La puesta en marcha de soluciones basadas en IA dentro de una jurisdicción debe comenzar por una base normativa sólida y por políticas internas precisas que definan obligaciones, límites y responsabilidades; sin un andamiaje legal claro que establezca los estándares de tratamiento, las finalidades legítimas, los criterios de minimización y los mecanismos de transparencia, cualquier despliegue técnico corre el riesgo de erosionar derechos fundamentales y de generar desconfianza pública.

Esa base normativa no solo debe codificar niveles mínimos de protección por ejemplo, cuándo procede la anonimización versus la pseudonimización, qué criterios permiten la divulgación de datos judiciales o sanitarios, o cómo documentar y auditar decisiones algorítmicas sino también requerir instrumentos procedimentales como evaluaciones de impacto de la protección de datos, registros de actividades de tratamiento y protocolos de rendición de cuentas algorítmica que conviertan principios generales en obligaciones operativas verificables.

A su vez, esa regulación debe articularse con estándares internacionales y buenas prácticas técnicas sin quedar prisionera de un formalismo excesivamente rígido: debe dejar margen para que las unidades técnicas adapten parámetros de anonimización y protocolos criptográficos a la naturaleza de los datos y a las amenazas emergentes, siempre dentro de umbrales de seguridad previamente acordados y auditables. Antes de cualquier operación técnica es clave realizar una matriz de riesgos que identifique vectores concretos de reidentificación, impacto en derechos y efectos colaterales sobre garantías procesales.

Esta evaluación debe ser tanto cualitativa como cuantitativa: hay que mapear qué atributos son sensibles, qué combinaciones pueden actuar como cuasi-identificadores, qué fuentes externas podrían usarse para linkage y qué escenarios adversos (desde errores de OCR hasta ataques de *scraping* y *linkage* masivo) son plausibles en la práctica. En términos operativos, esto exige realizar pruebas de enlace controladas, simulaciones de ataques de inferencia (*membership inference, model inversion*) y ejercicios de stress sobre modelos generativos para evaluar el riesgo de memorización.

Los resultados de esas pruebas alimentan decisiones sobre el tipo de técnica a emplear (pseudonimización consistente si se requiere trazabilidad longitudinal, anonimización irreversible si la trazabilidad no es necesaria) y condicionan parámetros técnicos críticos, entre ellos el presupuesto de privacidad en implementaciones con privacidad diferencial o el grado de perturbación aceptable en datos liberados para investigación.

Desde la perspectiva tecnológica, la jurisdicción debe adoptar una estrategia multicapa que combine técnicas de anonimización automática, controles criptográficos y arquitecturas de protección distribuida. En la capa de tratamiento de texto y documentos, los modelos de procesamiento de lenguaje natural (afinados al lenguaje jurídico y adaptados a las variantes locales) deben formar parte de pipelines que incluyan procesos previos robustos (corrección de OCR, normalización de nombres, detección de firmas y metadatos) y procesos posteriores de control de calidad supervisados por revisión humana por muestreo.

Para el intercambio y análisis de datos, los mecanismos de generación de datos sintéticos constituyen una alternativa potente para permitir investigación y desarrollo sin exponer registros reales; sin embargo, su implementación exige controles contra la memorización (regularización del entrenamiento, pruebas de similitud y penalizaciones por *overfitting*) y la aplicación, si procede, de privacidad diferencial durante el entrenamiento de los modelos generativos.

Complementariamente, técnicas criptográficas como el cifrado homomórfico, el cómputo multipartito seguro (MPC) o el uso de entornos de ejecución confiable (TEE) pueden proteger cálculos sobre datos sensibles cuando la privacidad diferencial no es viable por razones de precisión, siempre reconociendo que estas soluciones tienen costes computacionales y requisitos operativos que deben ponderarse frente a la urgencia y la escala de los procesos jurisdiccionales.

El aprendizaje federado aporta ventajas significativas para el sector judicial porque permite entrenar modelos colaborativos sin centralizar datos; no obstante, su adopción segura exige la incorporación de contramedidas específicas: es imprescindible aplicar privacidad diferencial sobre los gradientes, agrupar actualizaciones mediante agregación segura criptográfica y establecer límites de contribución y mecanismos de

clipping para minimizar fugas de información a través de gradientes. Además, la heterogeneidad de datos (no-IID) y los sesgos locales requieren mecanismos de evaluación que aseguren que los modelos no reproducen ni amplifican desigualdades regionales o demográficas; en la práctica, eso obliga a diseñar métricas de equidad, realizar pruebas de performance por subgrupos y crear procesos de ajuste que compensen datos escasos o no representativos en ciertas oficinas judiciales.

En definitiva, la federación debe entenderse como una capa arquitectónica dentro de una estrategia de privacidad que combine protección estadística, criptografía y gobernanza contractual. La privacidad diferencial, bien aplicada, proporciona garantías matemáticas sobre la magnitud de la divulgación de información individual, pero exige gestión cuidadosa del parámetro de privacidad (epsilon) y de su composición a lo largo del tiempo. En el ámbito jurisdiccional esto se traduce en decisiones prácticas: definir qué operaciones requieren alta fidelidad (por ejemplo, análisis estadísticos esenciales para políticas públicas o para detectar patrones delictivos) y cuáles pueden tolerar ruido; asignar presupuestos de privacidad por proyecto y monitorizar la "cuenta" de privacidad acumulada; y documentar de forma transparente esas decisiones para auditores y afectados.

En paralelo, las métricas clásicas de anonimización (k-anonymity, l-diversity, t-closeness) siguen siendo herramientas valiosas para diagnósticos iniciales, pero deben complementarse con evaluaciones de riesgo dinámicas que contemplen fuentes externas disponibles públicamente y la evolución tecnológica que facilita nuevos tipos de reidentificación. La gobernanza y los controles organizativos son tan determinantes como la tecnología. Es indispensable crear estructuras permanentes de gobierno de datos que incluyan equipos multidisciplinarios responsables de políticas y supervisión, comités de ética que revisen proyectos críticos, y unidades técnicas que aseguren la implementación, el mantenimiento y la auditoría de los modelos.

Estos órganos deben operar con protocolos claros de acceso (principio del menor privilegio), gestión de llaves, cifrado en tránsito y en reposo, trazabilidad inmutable de las operaciones sobre datos y registros de auditoría que permitan reconstruir decisiones y tratamientos. En el plano contractual, las adquisiciones tecnológicas deben incorporar cláusulas de privacidad obligatorias, derechos de auditoría, controles sobre subcontratistas y requisitos de interoperabilidad y portabilidad de modelos y metadatos;

además, los acuerdos de cooperación interinstitucional deben estipular responsabilidades claras sobre reidentificación, notificación de incidentes y corresponsabilidad en la implementación de medidas correctivas.

La transparencia y la explicabilidad no son meros adornos normativos; son instrumentos prácticos para preservar la legitimidad del sistema judicial. Documentar los criterios de diseño, los datos utilizados, los parámetros de anonimización y las métricas de utilidad permite a las partes afectadas comprender y, cuando corresponda, impugnar decisiones que afecten derechos.

En ese sentido, las jurisdicciones deberían publicar resúmenes técnicos accesibles, establecer canales de reclamación y revisión humana efectiva, y mantener ventanas de control que permitan a operadores judiciales supervisar, detener o revertir decisiones automatizadas cuando exista riesgo de error o vulneración de garantías procesales. La explicabilidad también debe orientarse según el interlocutor: informes técnicos detallados para auditores y resúmenes comprensibles para ciudadanos, y herramientas de visualización que faciliten la inspección por parte de juristas y peritos sin exigir conocimientos profundos de ciencia de datos.

La auditoría técnica e institucional debe ser continua y diversa en métodos para ser efectiva. Además de auditorías independientes periódicas, es aconsejable incorporar monitoreo en tiempo real de indicadores de riesgo, por ejemplo, métricas de *drift* en datos que puedan aumentar la reidentificación, detección de consultas anómalas, o alertas sobre patrones de uso que indiquen scraping y ejercicios proactivos como red-teaming y pruebas de penetración específicas de linkage.

Las auditorías deben evaluar no solo la robustez de los modelos sino también la eficacia de los procesos humanos que los rodean: formación del personal, procedimientos de revisión por muestreo, protocolos de escalamiento y capacidad de respuesta ante incidentes. Igualmente, es recomendable establecer procesos de "re-anonimización" y reglas para la retirada o revisión de *datasets* cuando cambien las condiciones de riesgo o se detecten vulnerabilidades.

Los aspectos éticos y de justicia son transversales y deben informar cada decisión técnica. Es esencial aplicar la prueba de proporcionalidad y necesidad para cada uso de IA en la jurisdicción: ¿es estrictamente necesario usar datos sensibles para lograr el fin

perseguido? ¿Se han explorado alternativas menos intrusivas? Asimismo, debe prestarse especial atención a los efectos sobre grupos vulnerables, evitando que automatizaciones replicantes de sesgos institucionales produzcan desigualdades en decisiones procesales o administrativas. Involucrar a comunidades afectadas en la definición de políticas de apertura y anonimización, y someter los proyectos de mayor impacto a revisiones éticas externas, contribuye a legitimar las decisiones y a incorporar perspectivas que los técnicos o legisladores podrían pasar por alto.

Desde el punto de vista operativo y de implementación, la adopción práctica debe seguir una hoja de ruta por fases: diagnóstico y priorización de casos de uso, pilotos controlados en entornos seguros, evaluación rigurosa de utilidad y privacidad, escalado progresivo con auditorías intermedias y finalmente integración definitiva acompañada de capacitación masiva y recursos de soporte. Cada fase debe incluir criterios de aceptación claros (KPIs técnicos y jurídicos), presupuestos de privacidad definidos, un plan de contingencia para incidentes y acuerdos de colaboración con instituciones académicas y proveedores que permitan transferir conocimiento y validar soluciones.

La cooperación regional e interinstitucional para compartir buenas prácticas, modelos de prueba y protocolos de interoperabilidad resulta además crucial para evitar duplicación de esfuerzos y para armonizar estándares en contextos transfronterizos. En suma, la implementación jurisdiccional de técnicas de protección de datos basadas en IA exige mucho más que la simple adopción de algoritmos: demanda una estrategia integrada que articule norma, tecnología, gobernanza, transparencia y ética, con procesos de evaluación de riesgo y auditoría permanentes.

Solo mediante un enfoque multicapa que combine anonimización técnica, protecciones criptográficas, privacidad diferencial cuando proceda, aprendizaje federado con salvaguardias, marcos contractuales sólidos, supervisión humana y participación ciudadana podrá una jurisdicción aprovechar la eficiencia y el potencial analítico de la IA sin sacrificar la protección de los derechos fundamentales ni la legitimidad del sistema de justicia. Si lo desea, señor, puedo convertir este análisis en un plan operativo detallado para un tribunal, hospital o agencia regulatoria que incluya prioridades temporales, *checklist* técnico-legal, métricas de aceptación y un esquema de gobernanza y auditoría para poner en marcha estas recomendaciones paso a paso.

CAPÍTULO IV.
CONCLUSIONES Y RECOMENDACIONES

3.3. Conclusiones

La protección de la identidad de los administradores de justicia en delitos de alta peligrosidad mediante el uso de inteligencia artificial se presenta como una solución viable y necesaria en el contexto ecuatoriano, donde la creciente violencia del crimen organizado ha expuesto las limitaciones de los mecanismos tradicionales de seguridad. La IA no solo permite implementar sistemas avanzados de anonimización y cifrado que protegen la identidad de jueces y fiscales, sino que también fortalece la imparcialidad y continuidad de los procesos judiciales, siempre que su aplicación se enmarque en un equilibrio entre innovación tecnológica y respeto a las garantías procesales.

El marco jurídico ecuatoriano, integrado por la Constitución de 2008, la Ley Orgánica de Protección de Datos Personales (2021) y el Código Orgánico Administrativo (2017), establece bases sólidas para la protección de la identidad de los operadores de justicia. Sin embargo, se evidencia una falta de regulación específica sobre el uso de IA en el ámbito judicial, lo que genera vacíos normativos que dificultan la implementación segura y estandarizada de herramientas tecnológicas para la protección de la identidad en casos de alta peligrosidad.

Los administradores de justicia en Ecuador enfrentan riesgos y amenazas crecientes que incluyen desde ataques físicos y amenazas directas hasta ciberataques, doxing y vigilancia digital por parte de organizaciones criminales. Estos riesgos no solo comprometen su seguridad personal y familiar, sino que también afectan la independencia judicial y la transparencia del sistema, poniendo en evidencia la urgencia de adoptar medidas tecnológicas y protocolos de ciberseguridad que superen las capacidades de los mecanismos de protección convencionales.

Las experiencias internacionales, como el sistema ANOPPI en Finlandia, los jueces sin rostro en Colombia y Perú, y la regulación de la IA en la Unión Europea, ofrecen valiosas lecciones y buenas prácticas adaptables al contexto ecuatoriano. Entre ellas destacan la anonimización automatizada, la auditoría algorítmica, la supervisión humana continuada y la integración de marcos éticos y legales que aseguren que el uso de la IA no vulnere derechos fundamentales, sino que fortalezca la seguridad judicial sin sacrificar la transparencia.

3.4. Recomendaciones

Se recomienda al Consejo de la Judicatura y a la fiscalía general del Estado desarrollar e implementar de manera prioritaria un “Sistema Integral de Protección de Identidad con IA”. Este sistema debería emplear técnicas avanzadas de anonimización de voz y video en audiencias, cifrado de extremo a extremo para comunicaciones y documentos sensibles, y el uso de plataformas seguras para la gestión de casos. Es crucial que, paralelamente, se elaboren protocolos éticos y guías de procedimiento que aseguren que el uso de estas tecnologías no menoscabe el derecho a la defensa, la publicidad de los procesos ni otras garantías procesales, estableciendo un comité de supervisión interdisciplinario que evalúe continuamente este equilibrio.

Es imperativo que la Asamblea Nacional, en coordinación con la Corte Constitucional y el Consejo de la Judicatura, impulse la creación de una “Ley Orgánica para el Uso de la Inteligencia Artificial en la Función Judicial”. Esta ley debe llenar los vacíos normativos existentes, estableciendo los principios, límites y salvaguardas para el desarrollo e implementación de herramientas de IA. La normativa debe especificar estándares técnicos para la anonimización y el cifrado, definir los derechos de los justiciables, regular la auditoría de los algoritmos y crear un registro público de los sistemas utilizados, asegurando así una implementación segura, estandarizada y respetuosa de los derechos fundamentales.

Se insta a las instituciones del sistema de justicia a adoptar de manera inmediata un “Protocolo de Ciberseguridad y Protección Digital para Operadores de Justicia”. Este protocolo debe ir más allá de la protección física tradicional e incluir medidas como: evaluaciones periódicas de riesgo digital, capacitación especializada en prevención de doxing y phishing, uso de herramientas de comunicación encriptadas, limpieza de datos personales en registros públicos en línea y la creación de una unidad de respuesta rápida ante ciberamenazas. El objetivo es construir un escudo tecnológico que proteja la integridad digital de jueces y fiscales, preservando así su independencia y la seguridad de sus familias.

Se recomienda que el Estado ecuatoriano, a través de la Secretaría de Innovación y en colaboración con el órgano judicial, diseñe un “Plan de Implementación Progresiva de IA Inspirado en Mejores Prácticas Internacionales”. Este plan debe analizar y adaptar modelos exitosos como el sistema ANOPPI de Finlandia para la gestión documental anónima, incorporar el principio de “jueces sin rostro” para casos selectos de alta peligrosidad siguiendo los parámetros de Colombia y Perú, y adoptar los estándares de la

UE en materia de auditoría algorítmica y supervisión humana. La clave reside en no copiar, sino en contextualizar estas experiencias, integrando desde el inicio un marco ético robusto y mecanismos de control que prevengan sesgos y aseguren la transparencia del sistema judicial.

ANEXOS

Anexo 1. Ficha de revisión bibliográfica

Tipo de Fuente	Autor	Año de publicación	País de origen	Contenido teórico General	Contenido teórico específico	Base de datos
Guía técnica	Agencia Española de Protección de Datos	2022	España / Singapur	Lineamientos sobre anonimización de datos	Técnicas de anonimización aplicadas en protección de datos	https://www.aepd.es/documento/guia-basica-anonimizacion.pdf
Artículo científico	Andrade, D.; Toapanta, M.; Bano, M.; Gómez, E.	2024	Ecuador	Inteligencia artificial y protección de datos	Propuesta de IA para garantizar privacidad según base legal ecuatoriana	https://doi.org/10.56712/latam.v5i4.2530
Libro	Arias, J.; Covinos, M.	2021	Perú	Metodología de investigación	Diseño de investigación y enfoques jurídicos	http://repositorio.concytec.gob.pe/handle/20.500.12390/2260
Norma jurídica	Asamblea Nacional Constituyente del Ecuador	2008	Ecuador	Constitución de la República	Derechos fundamentales y garantías judiciales	
Norma jurídica	Asamblea Nacional del Ecuador	2017	Ecuador	Código Orgánico Administrativo	Procedimientos administrativos y	https://www.gobiernoelectronico.gob.ec/wp-

					regulación del sector público	content/uploads/2020/11/COA.pdf
Norma jurídica	Asamblea Nacional del Ecuador	2021	Ecuador	Ley Orgánica de Protección de Datos Personales	Regulación de derechos de privacidad y tratamiento de datos	https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf
Capítulo de libro	Balcells, M.	2020	España	Uso de IA en justicia penal	Ventajas y riesgos del uso de IA en el sistema penal	https://dialnet.unirioja.es/servlet/libro?codigo=774981
Artículo científico	Bobek, M.	2019	Países Bajos	Protección de datos y anonimización	Aplicación de anonimización en decisiones judiciales	https://journals.sagepub.com/doi/abs/10.1177/1023263X19851628
Artículo científico	Bustamante, M.; Marín, J.	2021	Ecuador	Justicia digital y acceso a internet	Protección de datos personales en procesos judiciales digitales	https://doi.org/10.37768/unw.rid.02.01.001

Informe / Documento técnico	Cáceres, J.	2017	Colombia	Estrategia nacional de ciberseguridad	Marco de ciberdefensa y protección institucional	https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-1/2017_1_09_caceres_s.pdf
Artículo científico	Cano, Y.	2020	España	Seudonimización y anonimización	Aplicación en sentencias del orden jurisdiccional social	https://burjcdigital.urjc.es/items/d27b38f1-1524-4692-99fa-cde33e880f73
Artículo científico	Cárdenas, E.; Martínez, V.	2021	Brasil	IA en decisiones judiciales	Posibilidades de aplicación de IA en resolución de casos judiciales	https://doi.org/10.1590/2317-6172202101
Caso judicial	Corte IDH	2009	Brasil	Jurisprudencia internacional	Caso Escher y derechos humanos	https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf
Norma jurídica	Congreso Nacional del Ecuador	2004	Ecuador	Transparencia y acceso a información	Ley de acceso público y transparencia gubernamental	https://www.oas.org/juridico/pdfs/mesicic5_ecu_ane_cpccs

						_22_ley_org_tran_acc_inf_pub.pdf
Informe / Artículo	Contini, F.	2019	ONU / Internacional	IA y justicia	Riesgos de influencia indebida de IA en el poder judicial	https://www.unodc.org/dohadeclaration/es/news/2019/06/artificial-intelligence_-a-new-trojan-horse-for-undue-influence-on-judiciaries.html
Artículo científico	Cuarán, C.; Sánchez, D.	2025	Ecuador	Seguridad jurídica en Ecuador	Implementación de jueces sin rostro para protección judicial	http://revistacodigocientifico.itslosandes.net/index.php/1/article/view/935
Documento institucional	Cumbre Judicial Iberoamericana	2023	Iberoamérica	Aplicaciones de IA en Poder Judicial	Propuesta de uso de IA en tribunales	https://www.cumbrejudicial.org/sites/default/files/2023-08/Aplicaciones%20de%20Inteligencia%20Artificial%20en%20los%20Poder

						es%20Judiciales.pdf
Artículo científico	Delgado, J.; Espinoza, J.	2024	Ecuador	IA y privacidad	Impacto de IA en derechos de intimidad y protección de datos	https://doi.org/10.37811/cl_rcm.v8i5.14497
Tesis / Informe universitario	Gallegos, J.	2023	Ecuador	Jueces sin rostro	Implementación para juzgamiento de delitos de crimen organizado	https://dspace.uniandes.edu.ec/handle/123456789/16300
Libro / Informe	Gamboa, J.	2020	Colombia	Ciberseguridad	Protección de infraestructuras críticas y seguridad nacional	-
Artículo científico	González, I.	2023	España	IA generativa y ciberdelincuencia	Uso de IA para delitos digitales de género y deepfakes	https://doi.org/10.12795/IESTSCIENTIA.2023.i02.08
Artículo científico	Guerrero, B.	2020	Chile	Protección de datos judicial	Principio de publicidad vs privacidad en actuaciones judiciales	https://doi.org/10.5354/0719-2584.2020.54372
Libro	Hernández, R.; Fernández, C.; Baptista, P.	2018	Perú	Metodología de investigación	Técnicas y métodos aplicables a	https://www.esup.edu.pe/wp-content/uploads/20

					investigación científica	20/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodología%20Investigacion%20Cientifica%206ta%20ed.pdf
Artículo científico	Lavin, R.; Cristallo, J.; Sánchez, M.; Corvalán, J.	2024	Argentina	IA en procesos judiciales	Evaluación de asistencia tecnológica judicial	https://fund.ar/wp-content/uploads/2024/10/Fundar_Uso-de-inteligencia-artificial-en-los-procesos-judiciales_CC-BY-NC-ND-4.0-1.pdf
Artículo científico	Lima, V.; Fuentes, J.; Martins, A.	2023	Brasil	IA en decisiones judiciales	Sistema Victor del STF para apoyo en juicios	https://doi.org/10.5380/rinc.v10i2.92598
Artículo científico	Mark, G.; Nagy, D.; Vagi, R.; Pal, J.; Orosz, T.	2021	Internacional	Anonimización de documentos legales	Desafíos técnicos y problemas abiertos de anonimización	https://doi.org/10.5380/rinc.v10i2.92598

Artículo científico	Mejía, A.	2024	Ecuador	Protección judicial	Apoyo tecnológico a administradores de justicia	https://rus.ucf.edu.cu/index.php/rus/article/view/4785
Artículo científico	Mendoza, P.	2023	Ecuador	Protección de datos	Derechos humanos en gobierno electrónico	https://doi.org/10.47463/rj.v2i1.74
Artículo científico	Merino, F.; Guilcapi, V.; Defas, R.	2024	Ecuador	Sistema judicial	Reducción del crimen organizado mediante judicialización	https://doi.org/10.37811/cl_rcm.v8i2.11224
Artículo científico	Mila, F.; Yánez, K.; Mantilla, J.	2021	Ecuador	Metodología de investigación jurídica	Técnicas para estudio del derecho	https://pdfs.semanticscholar.org/3937/0c41102384bf0d2f245498722991b4756a64.pdf
Artículo científico	Morán, A.	2021	Ecuador	Ciberseguridad	Protección de infraestructuras críticas	https://doi.org/10.59794/rscd.2019.v5i5.pp73-85
Noticia / Reporte	Noroña, K.	2023	Ecuador	Ataques a funcionarios judiciales	Registro de ataques en 2023	https://gk.city/2023/01/30/ataques-funcionarios-judiciales-ecuador-2023/

Informe	Oficina del ACNUDH	2023	Internacional / Ecuador	Estado de derecho	Impacto de ataques al poder judicial ecuatoriano	https://www.ohchr.org/es/press-releases/2023/08/attacks-against-ecuadorian-judiciary-threaten-rule-law-warns-un-expert
Norma jurídica / Reglamento	Parlamento Europeo	2024	UE	Ley de Inteligencia Artificial	Regulación del uso de IA en Europa	https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689
Artículo científico	Pérez, J.	2021	España	Cibercriminalidad	Penalización y desafíos del derecho frente a delitos virtuales	https://ojs.ual.es/ojs/index.php/RIDJ/article/download/7063/5890
Norma jurídica / Protocolo	Poder Judicial de Chile	2022	Chile	Anonimización judicial	Procedimientos de anonimización de datos judiciales	https://www.pjud.cl/docs/download/57691

Artículo científico	Portilla, R.; Romero, M.; Chugá, J.; Rodríguez, E.	2024	Ecuador	Función judicial	Defensa de derechos constitucionales en procesos penales	https://doi.org/10.46377/dilemas.v12i1.4363
Artículo científico	Ramírez, M.; Alvarado, L.	2025	Ecuador	Jueces sin rostro	Alternativa contra intimidación del crimen organizado	https://doi.org/10.33996/revistalex.v9i28.297
Artículo científico	Rivero, S.; Chinarro, D.	2024	España	IA en judicatura	Dicotomía entre asistencia y sustitución en decisiones judiciales	https://dialnet.unirioja.es/servlet/articulo?codigo=9898129
Artículo científico	Rodríguez-Márquez, M.	2021	Colombia	Ciberseguridad judicial	Recomendaciones para justicia digital	https://revistas.uis.edu.co/index.php/revistauisingenierias/article/download/11485/11338/81854
Artículo científico	Roldán, F.	2021	Ecuador	Protección de datos	Consentimiento y finalidad en regulación de datos personales	https://doi.org/10.18272/ulr.v8i1.2184
Libro / Metodología	Romero, H.; Real, J.; Ordoñez, J.;	2022	Ecuador	Metodología de investigación	Aplicación en estudios jurídicos	https://doi.org/10.47606/ACVEN/ACLIB0017

	Gavino, G.; Saldarriaga, G.					
Artículo científico	Rosero, V.	2025	Ecuador	IA y prueba electrónica	Impacto de IA en evidencia digital	https://doi.org/10.33210/rci.v3i1.46
Artículo científico	Terzidou, K.	2023	Internacional	Anonimización automatizada	Automatización de anonimización de sentencias judiciales	https://doi.org/10.1145/3594536.3595151
Artículo científico	Veronese, A.; Nunes, A.	2021	Latinoamérica	IA y protección de datos	Marco jurídico y políticas integradoras de IA	https://doi.org/10.53857/MZBU2371
Artículo científico	Viguri, J.	2022	España	Anonimización de datos	Justicia y anonimización en administración judicial	https://dialnet.unirioja.es/descarga/articulo/8725051.pdf
Artículo científico	Villares, D.	2022	España	Anonimización judicial	Retos de digitalización y protección de datos en justicia	https://dialnet.unirioja.es/servlet/articulo?codigo=8744166