

La Revolución Industrial Digital

Inteligencia artificial,
derechos humanos y debido proceso

¿Qué hay detrás de la promesa tecnológica?

Sergio J. Cuarezma Terán
José Coronel De Trinidad



UNIVERSIDAD JUÁREZ
AUTÓNOMA DE TABASCO
"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

La Revolución Industrial Digital

Inteligencia artificial, derechos humanos y debido proceso¹

¿QUÉ HAY DETRÁS DE LA PROMESA
TECNOLÓGICA?

Sergio J. Cuarezma Terán
José Coronel De Trinidad

1. Trabajo de investigación presentado en el 4º Congreso Internacional “Inteligencia artificial y derechos humanos: retos globales para la abogacía en la era digital”, celebrado del 19 al 23 de julio de 2026, Villahermosa, Tabasco, México, organizado por la Federación Mexicana de Colegios de Abogados, A.C. (FEMECA), el Instituto Universitario de Yucatán (IUDY), sede Tabasco, México, el Instituto de Estudio e Investigación Jurídica (INEJ), Nicaragua, el Instituto Internacional de Estudio e Investigación Jurídica (IINEJ), Afiliado a la Fundación de Ciudad del Saber, Panamá, y la Universidad Juárez Autónoma de Tabasco, México.

Equipo editorial

Autores : Sergio J. Cuarezma Terán
José Coronel De Trinidad
Vicerrector de Investigación : Gustavo A. Arocena
Director de Investigación : Diego Cuarezma Zapata
Jefe de edición : Alicia Casco Guido
Diseño de portada : Christell Ponce Vargas

ISBN: 978-99924-21-65-9

Todos los derechos reservados conforme a la Ley

© INEJ, 2026

El INEJ es una institución de Educación Superior, que contribuye al desarrollo humano, institucional, social y económico de la nación nicaragüense y de la región, a través de la investigación científica, los estudios de educación continua y de postgrados; creado por la Ley No. 604/2006, aprobada el 26 de octubre de 2006 y publicada en La Gaceta, Diario Oficial, No. 229, del día 24 de noviembre de 2006, República de Nicaragua. Inscrito, registrado y acreditado en la Secretaría Técnica para Atención a las Universidades (SETEC), Nicaragua, y miembro activo de la Agencia Centroamericana de Acreditación de Postgrado (ACAP), Tegucigalpa, Honduras.

www.inej.net
info@inej.net

A

José Luis González Martínez.

Índice

Presentación	9
1. Introducción: la tecnología nunca llega sola	27
2. De la mecanización a la sociedad algorítmica	31
3. ¿Quién financia la revolución industrial digital?	37
4. ¿Cuáles son los intereses que impulsan esta transformación?	55
5. ¿Qué tipo de ser humano se está configurando?	61
6. Inteligencia artificial y sistema de justicia	67
7. Derechos humanos en la sociedad algorítmica	79
8. El debido proceso frente a decisiones algorítmicas	87
9. Garantías no negociables para una justicia asistida por inteligencia artificial	93
10. América Latina y el riesgo de una dependencia algorítmica	105
11. De la eficiencia a la legitimidad	111
12. La abogacía ante la inteligencia artificial: competencia, independencia y responsabilidad	115
13. A manera de conclusión: poner la inteligencia al servicio de la humanidad	123
Referencias	127

Presentación

La inteligencia artificial ya no es una promesa reservada a un futuro distante. Hoy interviene en la forma en que buscamos información, trabajamos, nos comunicamos, consumimos, aprendemos y tomamos decisiones, y empieza a integrarse, con distinta intensidad, en la administración pública, la seguridad, la investigación penal, la valoración de riesgos y la actividad jurisdiccional. Ese avance suele describirse con un lenguaje de progreso: rapidez, precisión, eficiencia, automatización, personalización. Detrás de esas palabras, sin embargo, hay preguntas que el entusiasmo tecnológico rara vez contesta: ¿quién diseña los sistemas que empiezan a organizar aspectos esenciales de nuestra vida, con qué datos se entrenan y quién financia su desarrollo? ¿Qué intereses orientan sus finalidades, quién obtiene los beneficios y quién carga con los errores?

La obra *La Revolución Industrial Digital. Inteligencia artificial, derechos humanos y debido*

proceso: ¿Qué hay detrás de la promesa tecnológica? nace de la necesidad de formular esas preguntas sin prejuicios, pero también sin ingenuidad: no rechaza la innovación ni presenta la tecnología como una amenaza inevitable, pero tampoco celebra cada novedad como si la sola modernización garantizara justicia, bienestar o democracia. Su apuesta es más exigente: entender la inteligencia artificial como una construcción económica, política, social y jurídica, cuyos efectos dependen de decisiones humanas concretas, que determinan su diseño, su financiación, su contratación, su uso y su control.

El recorrido del libro va de la historia de las revoluciones industriales a los desafíos concretos que la inteligencia artificial plantea al debido proceso, y deja una idea clara: la tecnología nunca llega sola. Cada revolución industrial reorganiza el trabajo, el capital, el territorio y el poder. La máquina de vapor modificó la producción y la disciplina laboral; la electricidad hizo posible la fabricación en masa; la informática convirtió la información en un recurso productivo central. La revolución digital actual no se limita a automatizar tareas: produce conclusiones, clasifica personas, anticipa comportamientos y convierte la decisión en un resultado reproducible a gran escala.

Ese recorrido histórico desemboca en la llamada cuarta revolución industrial y en la propuesta de una quinta revolución centrada en la persona, la sostenibilidad y la resiliencia. Pero ¿basta con llamar “humana” a una transformación para que lo sea? Difícilmente puede hablarse de centralidad de la persona cuando el trabajador está vigilado de forma permanente, el ciudadano queda reducido a una puntuación, o las decisiones esenciales dependen de sistemas que nadie logra explicar. Estas interrogantes atraviesan el texto entero y obligan a distinguir entre el lenguaje que acompaña a la innovación y las condiciones reales en que esa innovación se incorpora a la sociedad.

Uno de los aportes centrales del texto está, precisamente, en mirar la inteligencia artificial desde su economía política. Los sistemas contemporáneos necesitan capital, semiconductores, nube, centros de datos, electricidad, minerales, información y trabajo humano en volúmenes considerables. Ese desarrollo tecnológico no ocurre en un espacio abstracto: ocurre dentro de una infraestructura material y financiera que controlan, en buena medida, actores con capacidades desiguales, entre ellos grandes corporaciones, fondos de inversión, proveedores de cómputo, Estados, universidades, trabajadores de datos y millones de usuarios, todos dentro de una ca-

dena global cuyos beneficios y costos se reparten de forma muy desigual.

La pregunta por el financiamiento, entonces, no es un asunto secundario. Saber quién aporta los recursos permite entender quién fija prioridades, define estándares y decide qué problemas merecen atención. Un sistema pensado para publicidad, comercio o servicios financieros puede prometer ganancias inmediatas; una herramienta para traducir resoluciones judiciales a lenguas indígenas, fortalecer la defensa pública o acercar la justicia a comunidades alejadas, en cambio, difícilmente resulta atractiva para el mercado. ¿Debe el interés público limitarse a comprar lo que las empresas consideran rentable, o le corresponde al Estado definir prioridades, financiar bienes digitales públicos y orientar la innovación hacia necesidades sociales concretas?

Junto al capital visible, conviene reconocer otros financiamientos menos evidentes. Los datos que producen las personas alimentan modelos y sistemas de predicción; el trabajo de quienes etiquetan, corrigen, moderan y verifican contenidos sostiene la aparente autonomía de muchas plataformas; los centros de datos consumen energía, agua, suelo y minerales, y determinados territorios cargan con costos ambientales que rara vez

aparecen en el discurso de la innovación. Así, la nube deja de ser una realidad inmaterial y queda vinculada a infraestructuras, comunidades y recursos concretos: ¿quiénes permanecen invisibles cuando llamamos “inteligente” a un sistema, y qué costos laborales, sociales y ambientales se ocultan detrás de una respuesta inmediata?

Los intereses que impulsan esta transformación son varios. Las empresas buscan rentabilidad, crecimiento y control de mercado; los Estados persiguen productividad, seguridad, capacidad de vigilancia y autonomía estratégica; las instituciones públicas intentan reducir demoras y mejorar servicios; los usuarios quieren herramientas rápidas y accesibles. Ninguno de estos objetivos es necesariamente ilegítimo. El problema aparece cuando los intereses con mayor capacidad económica se presentan como si coincidieran automáticamente con el interés general: cuando pocos actores controlan los datos, la infraestructura, los modelos y los canales de distribución, terminan diseñando el entorno en el que ciertas conductas se vuelven más visibles, más probables o más rentables.

El trabajo no se limita, entonces, a preguntar qué máquinas estamos construyendo, sino qué idea de ser humano queda incorporada en ellas.

Para calcular, un sistema convierte la realidad en variables: historial, ubicación, consumo, relaciones, antecedentes, productividad, tiempos de respuesta, patrones de movimiento. Esa representación puede ser útil, pero nunca equivale a la persona completa. El riesgo aparece cuando el perfil estadístico desplaza al sujeto concreto y la probabilidad empieza a tratarse como identidad: surge el ser humano puntuado, predecible, optimizado y administrado. ¿Qué ocurre con la libertad cuando cada conducta deja una huella capaz de convertirse en consecuencia, y con la dignidad cuando una biografía compleja queda reducida a una clasificación?

Este planteamiento conduce al núcleo jurídico del trabajo: la relación entre inteligencia artificial, derechos humanos y sistema de justicia. Ahí aparece una distinción decisiva entre tecnologías instrumentales y tecnologías funcionales. Las primeras facilitan tareas como la búsqueda jurisprudencial, la transcripción, la traducción, la anonimización o la organización documental. Las segundas influyen directamente en decisiones que pueden afectar derechos: estiman riesgos, priorizan sospechosos, sugieren medidas, valoran patrones o proponen el sentido de una resolución. Cuanto más cerca está una herramienta de la li-

bertad, la culpabilidad o la pena, más intensos deben ser los controles jurídicos que la acompañan.

Incluso una herramienta aparentemente administrativa puede adquirir poder decisorio. Un sistema que ordena expedientes puede empezar a señalar cuáles son “urgentes”, y esa prioridad termina influyendo en la asignación de recursos y, en definitiva, en la posibilidad real de investigar, acusar o defender. Por esta razón, el control no debería activarse solo cuando aparece la decisión final: tiene que extenderse al diseño, la selección de datos, la adquisición, la contratación, la configuración, la actualización y el retiro del sistema. Una tecnología puede cambiar de función sin que nadie lo note, y una institución puede terminar delegando poder sin haber discutido públicamente esa delegación.

En el ámbito penal, los riesgos adquieren una intensidad particular. La policía predictiva tiende a reproducir los lugares y grupos que históricamente han sido más vigilados; el reconocimiento facial genera falsos positivos con consecuencias graves; el análisis masivo de datos permite construir perfiles íntimos a partir de información dispersa; y la inteligencia artificial generativa produce textos, imágenes o audios verosímiles que dificultan establecer la autenticidad de la prue-

ba. Frente a estas posibilidades, el libro deja una advertencia esencial: la capacidad técnica de recopilar, combinar o inferir información no equivale, por sí misma, a una autorización jurídica para hacerlo.

Los derechos humanos, en la sociedad algorítmica, se examinan aquí desde una perspectiva amplia. La dignidad exige tratar a la persona como sujeto y no como objeto de administración; la privacidad protege no solo secretos, sino la posibilidad misma de vivir sin observación constante; la igualdad obliga a mirar los resultados y no solo variables aparentemente neutrales; la libertad de expresión requiere transparencia y mecanismos de reclamo frente a sistemas que organizan lo que vemos; y la democracia necesita ciudadanos capaces de formar opiniones sin manipulación oculta. De ahí que la regulación de la inteligencia artificial no pueda reducirse a una cuestión de consumo o eficiencia empresarial: cuando están en juego libertades, oportunidades y acceso a derechos, el problema es constitucional.

El debido proceso ocupa un lugar central en esta discusión. Su función histórica ha sido contener el poder, y esa necesidad no desaparece cuando el poder se expresa mediante una interfaz, una puntuación o una recomendación automática. Al

contrario: se vuelve más urgente, porque la automatización puede ocultar al autor de la decisión, dispersar responsabilidades y dar una apariencia de inevitabilidad. ¿Cómo se defiende una persona frente a un resultado que desconoce, o cómo impugna una clasificación si no sabe qué datos se usaron? ¿Cómo existe igualdad de armas cuando una parte cuenta con expertos y sistemas complejos, mientras la otra solo recibe una conclusión revestida de autoridad científica?

El libro responde a estas preguntas con los componentes de un debido proceso adecuado a las decisiones algorítmicas. La persona debe ser informada, de antemano, de que se usó una herramienta y de la función concreta que cumplió; tiene que existir trazabilidad para identificar la versión del sistema y reconstruir su operación; las razones deben ser comprensibles y permitir conocer los datos, factores y límites relevantes; la defensa debe poder cuestionar la calidad de la información, la validez del modelo y su margen de error; y toda decisión debe quedar bajo la responsabilidad de una autoridad humana con competencia, tiempo, información y poder real para apartarse del resultado tecnológico.

El control humano, insiste el texto, no puede consistir en una firma al final de un procedi-

miento automático: una supervisión meramente formal no impide la obediencia algorítmica. El juez, el fiscal, el defensor, el abogado o el funcionario deben examinar críticamente la herramienta, contrastarla con el resto de la información y motivar su propia conclusión. Deben poder, además, suspender su uso cuando el sistema falle, opere fuera del contexto para el que fue validado o produzca resultados incompatibles con el derecho. La última palabra tiene que pertenecer a una persona jurídicamente responsable, no porque el juicio humano sea infalible, sino porque el Estado de derecho exige razones, contradicción y responsabilidad.

El capítulo dedicado a las garantías no negociables formula, sobre esa base, condiciones concretas para una justicia asistida por inteligencia artificial: base legal clara, finalidad definida, evaluaciones de impacto sobre derechos humanos, registros públicos de los sistemas utilizados, prohibición de decisiones penales exclusivamente automatizadas, validación científica independiente y local, calidad y trazabilidad de los datos, explicaciones suficientes, auditorías periódicas, seguridad, contratación pública que preserve la soberanía institucional, responsabilidad identificable, límites reforzados frente a tecnologías de vigilan-

cia, recursos efectivos, reparación y formación crítica de los operadores jurídicos.

Estas garantías no son obstáculos al progreso: son las condiciones que distinguen una herramienta al servicio de la justicia de una forma automatizada de arbitrariedad. Cuando están en juego la libertad, la reputación, la presunción de inocencia o la posibilidad de ejercer la defensa, la rapidez no puede sustituir a la legalidad. Del mismo modo, el secreto empresarial no puede convertirse en una barrera absoluta frente al derecho de contradicción. Una institución pública no debería contratar aquello que no es capaz de comprender, auditar, explicar o detener.

América Latina recibe también una mirada particular. La región necesita modernizar sistemas judiciales marcados por demoras, desigualdad territorial, limitaciones presupuestarias y barreras de acceso. La inteligencia artificial puede ayudar a ordenar expedientes, traducir información, mejorar búsquedas y acercar servicios, pero aceptar modelos contruidos con datos, lenguas y prácticas de otros contextos puede generar errores sistemáticos y nuevas dependencias. ¿Estamos preparados para importar sistemas sin importar también sus sesgos, y puede hablarse de soberanía judicial cuando los datos, las licencias

y la capacidad de auditoría dependen enteramente de proveedores externos?

La dependencia algorítmica, sostiene el libro, no se supera con discursos vacíos, sino fortaleciendo instituciones, ciencia, educación, infraestructura y cooperación regional. La modernización no debería crear dos justicias: una rápida para quien dispone de conectividad, equipos y conocimientos, y otra precaria para quien queda fuera de los circuitos digitales. América Latina necesita políticas propias, repositorios jurídicos abiertos, formación interdisciplinaria, compras transparentes y capacidad pública para entender lo que contrata. La inclusión digital no consiste solo en dar acceso a una plataforma; supone garantizar que todas las personas puedan comprender, usar y cuestionar la tecnología en condiciones de igualdad.

El debate, propone la obra, debería desplazarse de la eficiencia hacia la legitimidad. Resolver más casos en menos tiempo puede ser valioso, pero la justicia no es una fábrica de decisiones: una respuesta rápida puede ser injusta, una predicción correcta en promedio puede perjudicar gravemente a una persona concreta, y una fórmula uniforme puede reproducir con gran precisión una desigualdad histórica. La legitimidad no vie-

ne solo del resultado, sino también del procedimiento: ser oído, conocer la acusación, discutir la prueba, entender las razones y recurrir ante una autoridad independiente. Desde esta perspectiva, la eficiencia solo es legítima cuando está al servicio de la tutela judicial efectiva.

La abogacía ocupa igualmente un espacio decisivo en esta transformación, y el texto rechaza la idea de que el profesional del derecho se convierta en un simple usuario de respuestas automáticas. La inteligencia artificial puede facilitar búsquedas, comparar argumentos, organizar evidencia y preparar borradores, pero cada resultado que entra al proceso se convierte en una afirmación humana. Por eso subsisten los deberes de verificación, diligencia, veracidad, lealtad, confidencialidad y respeto al tribunal: un abogado no puede atribuir al sistema una cita inexistente, una norma derogada, una confusión de hechos o la exposición indebida de datos personales.

La competencia tecnológica, sin embargo, no debería convertirse en un privilegio reservado a grandes despachos o instituciones con más recursos. Si una fiscalía cuenta con laboratorios, analistas y sistemas avanzados, mientras la defensa pública carece de medios para examinar esos resultados, la innovación termina profundizando la

desigualdad de armas. Por eso los colegios profesionales, las universidades y las instituciones de justicia deben impulsar formación, guías, repositorios de incidentes, criterios de contratación y mecanismos de asistencia. El futuro de la abogacía no será de quien obedezca mejor a la máquina ni de quien pretenda ignorarla, sino de quien combine conocimiento jurídico, comprensión tecnológica e independencia profesional.

Esta obra propone leer la revolución industrial digital no como un destino inevitable, sino como un proceso abierto a decisiones democráticas. Sus páginas no ofrecen una respuesta simplista ni una lista de prohibiciones generales, sino un método de análisis: preguntar quién financia, quién diseña, qué datos se utilizan, qué riesgos se toleran, quién puede impugnar, quién responde y quién conserva la última palabra. Ese método permite reconocer los beneficios de la innovación sin renunciar al deber de examinar sus estructuras de poder y sus efectos sobre la persona.

Al comenzar la lectura conviene mantener abiertas algunas preguntas: ¿queremos una tecnología que amplíe la capacidad humana, o una que convierta al ser humano en objeto permanente de medición? ¿Aceptaremos decisiones rápidas aunque no puedan explicarse, y permitiremos que

la protección de contratos privados limite el derecho de defensa? ¿Estaremos dispuestos a fortalecer nuestras instituciones para que puedan auditar, corregir y detener sistemas defectuosos, y qué papel corresponde a jueces, fiscales, defensores, universidades, colegios profesionales y ciudadanía en la construcción de una justicia digital legítima?

Esperamos que estas interrogantes acompañen al lector a lo largo del texto, y que cada capítulo se comprenda como una invitación a deliberar. La promesa tecnológica merece ser examinada, no adorada ni temida. La inteligencia artificial puede contribuir a corregir demoras, facilitar información, ampliar capacidades y apoyar tareas complejas, pero su incorporación solo será compatible con una sociedad democrática cuando permanezca visible, discutible, auditable y subordinada al derecho. Detrás de cada dato hay una historia; detrás de cada expediente, una vida; y detrás de cada decisión, una responsabilidad que ninguna tecnología puede asumir por nosotros.

Esta convicción, que inspira y recorre toda la investigación, se encuentra estrechamente vinculada con la misión académica de las instituciones desde las cuales ha sido desarrollada. En el Instituto de Estudio e Investigación Jurídica (INEJ),

de Nicaragua, y en el Instituto Internacional de Estudio e Investigación Jurídica (IINEJ), afiliado a la Fundación Ciudad del Saber, Panamá, la investigación científica constituye una función esencial y permanente. Ambos institutos se conciben como centros de producción, pensamiento, reflexión y difusión del conocimiento en las ciencias jurídicas, políticas y sociales, comprometidos con el estudio riguroso de los desafíos que plantea la realidad contemporánea. Desde esta perspectiva, existe la convicción de que solo mediante el conocimiento crítico, sistemático y científicamente fundamentado de esa realidad es posible formular acciones concretas orientadas a su transformación, desarrollo y mejoramiento. La elaboración de trabajos como el que ahora se presenta responde, precisamente, a ese compromiso institucional de generar conocimientos capaces de contribuir al fortalecimiento del derecho, de las instituciones democráticas y de la protección efectiva de la dignidad humana.

Finalmente, expresamos nuestro agradecimiento a las instituciones que hicieron posible el 4.º Congreso Internacional “Inteligencia artificial y derechos humanos: retos globales para la abogacía en la era digital”, espacio académico en el que se presentó esta investigación: la Federación Mexicana de Colegios de Abogados, A. C.

(FEMECA); el Instituto Universitario de Yucatán (IUDY), sede Tabasco, la Universidad Juárez Autónoma de Tabasco, México, el Instituto de Estudio e Investigación Jurídica (INEJ), Nicaragua y el Instituto Internacional de Estudio e Investigación Jurídica (IINEJ), afiliado a la Fundación Ciudad del Saber, Panamá. Su compromiso con el diálogo jurídico, la cooperación académica y la formación profesional ha permitido abrir un debate imprescindible sobre el lugar que deben ocupar la dignidad humana, los derechos fundamentales y el debido proceso en la era digital.

Sergio J. Cuarezma Terán

José Coronel De Trinidad

Managua, Nicaragua, 21 de julio de 2026

Resumen

La revolución industrial digital suele presentarse como un proceso inevitable, guiado por la innovación y destinado a ampliar las capacidades humanas. Esa descripción queda incompleta cuando se omiten las estructuras económicas, políticas, laborales y materiales que hacen posible la inteligencia artificial. Los sistemas contemporáneos requieren capital, centros de datos, semiconductores, electricidad, minerales, trabajo humano, información y decisiones públicas. Este trabajo examina quién financia la cuarta revolución industrial y la propuesta de una quinta revolución industrial, qué intereses convergen en su desarrollo y qué modelo de relación entre la persona, la máquina y el poder público se está configurando. Desde esa economía política de la inteligencia artificial, se analizan sus efectos sobre la dignidad, la privacidad, la igualdad, la autonomía, la democracia y el debido proceso, con especial atención al sistema de justicia penal y a la justicia digital. La tesis sostiene que la tecnología puede contribuir a

una administración de justicia más accesible, ordenada y oportuna, pero solo cuando permanece subordinada a la Constitución, a los derechos humanos y a una decisión humana responsable, motivada, revisable y abierta a contradicción. La pregunta decisiva no es cuánto puede hacer la inteligencia artificial, sino qué estamos dispuestos a permitirle hacer con la libertad, la reputación y el destino de las personas. La investigación combina reflexión jurídica, análisis crítico de literatura especializada, normas recientes e informes oficiales, evitando citas textuales extensas y privilegiando una redacción propia.

Palabras clave: revolución industrial digital; inteligencia artificial; poder económico; derechos humanos; debido proceso; justicia penal; vigilancia; explicabilidad; control humano.

Abstract. The digital industrial revolution is often presented as an inevitable process driven by innovation and aimed at expanding human capabilities. That account remains incomplete when it overlooks the economic, political, labor, and material structures that make artificial intelligence possible. Contemporary systems depend on capital, data centers, semiconductors, electricity, minerals, human labor, information, and public policy choices. This paper examines who finances

the fourth industrial revolution and the proposal for a fifth industrial revolution, which interests shape their development, and what model of relationship among persons, machines, and public power is emerging. From this political economy of artificial intelligence, the paper analyzes the effects of algorithmic systems on dignity, privacy, equality, autonomy, democracy, and due process, with particular attention to criminal justice and digital justice. Its central thesis is that technology may contribute to a more accessible, orderly, and timely administration of justice only when it remains subordinate to constitutional principles, human rights, and a responsible human decision that is reasoned, reviewable, and open to challenge. The decisive question is not how much artificial intelligence can do, but what we are willing to allow it to do with people's liberty, reputation, and future. The study combines legal reflection, critical analysis of specialized literature, recent regulations, and official reports, while avoiding extensive quotations and favoring original argumentation.

Keywords: digital industrial revolution; artificial intelligence; economic power; human rights; due process; criminal justice; surveillance; explainability; human control.

1. Introducción: la tecnología nunca llega sola

Cada época ha construido una imagen de su máquina. La máquina de vapor fue asociada con el progreso industrial; la electricidad, con la producción en masa; la computadora, con la sociedad de la información. Hoy, la inteligencia artificial aparece rodeada de una promesa todavía más ambiciosa: conocer, anticipar y decidir. Ya no se limita a ejecutar una orden visible. Clasifica rostros, recomienda contenidos, detecta patrones, redacta documentos, estima riesgos, prioriza expedientes y propone respuestas. En el sistema penal puede ayudar a ordenar evidencia, identificar conexiones y reducir demoras. También puede convertir una sospecha en una puntuación, una correlación en un indicio y un perfil estadístico en una decisión que afecte la libertad.

La discusión, por tanto, no puede agotarse en preguntar si la inteligencia artificial es buena o mala. Una tecnología no posee por sí sola un pro-

grama moral. Sus efectos dependen de quién la diseña, con qué datos se entrena, qué problema pretende resolver, quién paga su desarrollo, quién recibe sus beneficios y quién soporta sus errores. Detrás de cada sistema hay decisiones sobre costos, precisión, velocidad, tolerancia al riesgo y distribución del poder. Cuando esas decisiones se trasladan a la justicia, dejan de ser asuntos meramente técnicos y se convierten en cuestiones constitucionales.

Conviene formular desde el inicio una pregunta incómoda: ¿qué hay detrás de todo esto? La respuesta más seria no es un nombre propio ni una organización secreta. Detrás hay una red compuesta por empresas tecnológicas, fondos de inversión, proveedores de nube, fabricantes de semiconductores, Estados, universidades, ejércitos, organismos reguladores, trabajadores de datos y millones de usuarios que producen información. Sus intereses no son idénticos. Algunos buscan rentabilidad; otros, ventaja estratégica; otros, soberanía tecnológica; otros, mejores servicios públicos. Precisamente por esa diversidad, el problema no consiste en descubrir una voluntad única, sino en comprender qué intereses terminan imponiéndose cuando la capacidad de financiar, computar y acumular datos se concentra en pocos actores.

La justicia no puede mirar este proceso desde la distancia. Si el sistema judicial adopta herramientas que no comprende, contrata servicios que no puede auditar o acepta secretos empresariales frente al derecho de defensa, corre el riesgo de trasladar una parte de la soberanía jurisdiccional hacia infraestructuras privadas. En ese momento, la innovación deja de ser una ayuda y comienza a convertirse en una forma de dependencia. El desafío de nuestro tiempo consiste en aprovechar la capacidad de la tecnología sin permitir que la lógica de la eficiencia vacíe de contenido a la dignidad, la igualdad de armas, la presunción de inocencia y el derecho a una decisión motivada.

La promesa tecnológica llega acompañada de un vocabulario cuidadosamente elegido: optimización, precisión, personalización, predicción. Cada palabra parece describir una mejora indiscutible. Sin embargo, cuando esas expresiones entran en un tribunal, deben traducirse al lenguaje de las garantías. Optimizar puede significar reducir el tiempo de escucha; personalizar puede convertirse en perfilar; predecir puede terminar anticipando responsabilidad; automatizar puede ocultar quién decidió. El jurista no debe rechazar el lenguaje técnico, pero tampoco puede permitir que ese lenguaje desplace las preguntas propias del derecho.

Antonio D'Aloia ha descrito la inteligencia artificial como un hecho social que atraviesa la vida individual, la democracia, la administración y la justicia. Esta dimensión impide tratarla como una herramienta aislada. Un sistema algorítmico se integra en instituciones que ya poseen desigualdades, rutinas y formas de ejercer autoridad. Por ello, la misma aplicación puede producir consecuencias distintas según el contexto. Un buscador jurisprudencial puede ampliar el conocimiento de un tribunal bien dotado y, al mismo tiempo, profundizar la distancia respecto de una defensa pública que carece de acceso, formación o capacidad de cómputo (D'Aloia, 2025).

La cuestión tampoco consiste en conservar intactas prácticas judiciales deficientes. La congestión, la demora, la pérdida de expedientes, la falta de información y las barreras territoriales afectan derechos desde mucho antes de la inteligencia artificial. La justicia digital puede ofrecer respuestas valiosas mediante expedientes electrónicos, comunicaciones seguras, firma electrónica y audiencias a distancia. Ahora bien, modernizar no significa trasladar la antigua burocracia a una pantalla ni sustituir el razonamiento por una recomendación automática. La transformación merece ese nombre cuando mejora el acceso sin empobrecer el proceso.

La tesis de este trabajo se sitúa, por tanto, lejos de dos posiciones cómodas. La primera celebra toda innovación como si la novedad fuera una fuente de legitimidad. La segunda responde con prohibiciones generales que ignoran beneficios verificables. Entre ambas existe una tarea más exigente: separar usos auxiliares de usos decisivos, identificar riesgos concretos, definir garantías antes del despliegue y conservar una autoridad pública capaz de comprender, auditar y detener el sistema. Esa tarea no puede quedar en manos exclusivas de desarrolladores, proveedores o consultores; pertenece al debate constitucional.

2. De la mecanización a la sociedad algorítmica

Las revoluciones industriales no son simples sucesiones de inventos. Cada una reorganiza el trabajo, el capital, el territorio y la autoridad. La primera revolución industrial substituyó progresivamente la fuerza humana y animal por la energía mecánica; concentró la producción en la fábrica y consolidó nuevas relaciones entre propiedad, trabajo y disciplina. La segunda incorporó la electricidad, el petróleo, la química y la producción en serie, mientras la gran corporación adquiría una capacidad económica desconocida. La tercera introdujo la electrónica, la informática y las telecomunicaciones, haciendo de la información un recurso productivo central. El derecho respondió lentamente a cada una: primero protegió la propiedad y el contrato; después reconoció la desigualdad material y desarrolló el derecho laboral, la seguridad social y nuevas jurisdicciones; finalmente, comenzó a regular los datos, las comunicaciones y la prueba electrónica.

La llamada cuarta revolución industrial describe la convergencia de sistemas ciberfísicos, inteligencia artificial, internet de las cosas, robótica, biotecnología y análisis masivo de datos. Su rasgo distintivo no es únicamente que las máquinas ejecuten tareas, sino que los sistemas produzcan inferencias y adapten su comportamiento a partir de datos. En este entorno, la frontera entre lo físico y lo digital se vuelve porosa: los dispositivos observan el mundo, los modelos lo traducen en variables y las plataformas responden mediante decisiones automatizadas o recomendaciones que orientan la conducta humana.

Sin embargo, la expresión cuarta revolución industrial también cumple una función narrativa. Presenta un conjunto heterogéneo de cambios como una etapa coherente e inevitable. Esa narrativa puede ser útil para ordenar el debate, pero también puede ocultar opciones políticas. Nada obliga a que la digitalización se organice alrededor de plataformas cerradas, vigilancia comercial o concentración de infraestructura. Esas son formas históricas concretas de financiar y gobernar la innovación, no consecuencias naturales de la técnica.

La denominada quinta revolución industrial, o Industria 5.0, requiere todavía mayor cautela. No

existe un consenso histórico que permita afirmar que la humanidad ya ha ingresado en una quinta revolución distinta. En buena medida, se trata de una propuesta normativa impulsada, entre otros actores, por la Comisión Europea para orientar la industria hacia tres objetivos: centralidad de la persona, sostenibilidad y resiliencia. La idea pretende corregir los excesos de una automatización centrada exclusivamente en productividad y situar el bienestar del trabajador en el núcleo del proceso productivo (Comisión Europea, 2021). Más que anunciar una época consumada, Industria 5.0 expresa una disputa por el sentido de la tecnología.

Esa disputa es decisiva. Una colaboración entre humanos y máquinas puede significar que la tecnología libere tiempo, reduzca tareas peligrosas y amplíe capacidades. También puede significar que el trabajador sea vigilado minuto a minuto, evaluado por métricas opacas y obligado a adaptarse al ritmo de un sistema. La palabra colaboración no resuelve el problema de poder. Para saber si la quinta revolución es verdaderamente humana, debemos preguntar quién fija los objetivos, quién puede detener el sistema, quién impugna sus resultados y quién conserva la última palabra.

2.1. De la automatización de tareas a la producción de inferencias

Conviene distinguir la automatización tradicional de los sistemas que aprenden patrones a partir de datos. Una regla informática puede ordenar expedientes por fecha o verificar si falta una firma. Un modelo de aprendizaje automático, en cambio, puede clasificar documentos según semejanzas, estimar probabilidades o recomendar prioridades. La diferencia no es meramente técnica. En el primer caso, la regla suele ser visible y estable; en el segundo, el comportamiento depende del conjunto de entrenamiento, de las variables seleccionadas y de decisiones estadísticas que pueden resultar difíciles de explicar a la persona afectada.

La inteligencia artificial generativa introduce otra capa. No se limita a clasificar: produce texto, imagen, audio o código con apariencia de coherencia. En la práctica jurídica puede resumir expedientes, preparar borradores y localizar argumentos. También puede inventar referencias, mezclar hechos o presentar como segura una respuesta incierta. Su fluidez crea un riesgo particular: el error ya no aparece como una falla evidente, sino como una afirmación bien redactada. El deber profesional exige verificar cada resulta-

do y evitar que la comodidad convierta una sugerencia en una fuente.

Rojas Rodríguez y Durán Alvarado muestran que la incorporación de IA al derecho penal abarca actividades muy diferentes: análisis de evidencia digital, clasificación de casos, reconocimiento facial, valoración de riesgos y apoyo a decisiones judiciales. Colocar todas bajo una sola etiqueta impide graduar las garantías. Una herramienta de búsqueda no merece el mismo tratamiento que un sistema que influye en una medida cautelar. La regulación debe atender la función, la intensidad de la intervención y el daño posible, no solo el nombre comercial de la tecnología (Rojas Rodríguez y Durán Alvarado, 2025).

2.2. La industrialización de la decisión

La primera industria transformó la energía; la actual transforma la decisión en un producto reproducible. Empresas y administraciones buscan convertir juicios antes dispersos en flujos estandarizados: ingreso de datos, puntuación, recomendación y respuesta. Este proceso puede reducir arbitrariedades cuando hace visibles criterios antes ocultos, pero también puede consolidarlas a gran escala. Una práctica discriminatoria aplicada por un funcionario afecta un conjunto limitado de ca-

sos; incorporada en una plataforma nacional, adquiere velocidad, alcance y apariencia científica.

La sociedad algorítmica no elimina la discrecionalidad. La desplaza. Alguien define la variable que contará como riesgo, el umbral que activará una alerta, el error que se considera tolerable y la población utilizada para validar el modelo. Estas elecciones suelen ocurrir antes de que el juez o el ciudadano vean el resultado. De ahí que el control jurídico deba comenzar en el diseño, la contratación y la selección de datos. Revisar únicamente la decisión final deja fuera una parte decisiva del poder.

3. ¿Quién financia la revolución industrial digital?

3.1. Capital privado, grandes corporaciones y fondos de inversión

El primer motor visible es el capital privado. El Informe AI Index 2026 de la Universidad de Stanford estima que la inversión privada en inteligencia artificial en Estados Unidos alcanzó 285.900 millones de dólares en 2025, mientras la inversión corporativa global en IA llegó a 581.700 millones. Las metodologías varían entre informes, pero la tendencia es inequívoca: el flujo de capital hacia modelos, chips, centros de datos, aplicaciones y empresas emergentes crece a una velocidad extraordinaria (Stanford HAI, 2026). La OCDE, por su parte, calcula que la inversión de capital de riesgo en empresas de IA recuperó en 2025 niveles cercanos a los máximos de 2021 y que la IA generativa captó 35.300 millones de dólares de capital de riesgo ese año (OCDE, 2026).

¿De dónde procede ese dinero? Una parte proviene de los beneficios acumulados por las grandes empresas tecnológicas. Otra llega por medio de fondos de capital de riesgo, fondos de pensiones, administradores de activos, capital privado y mercados bursátiles. El ciudadano puede estar financiando indirectamente esta expansión a través de sus ahorros, de su pensión o de fondos institucionales que invierten en compañías tecnológicas. Esto no significa que cada ahorrante conozca o apruebe cada uso de la IA. Significa que la arquitectura financiera convierte el ahorro social en capital disponible para proyectos cuya orientación queda, en gran medida, en manos de gestores y corporaciones.

La concentración es relevante. UNCTAD ha señalado que apenas cien empresas, principalmente de Estados Unidos y China, representaron alrededor del cuarenta por ciento del gasto mundial empresarial en investigación y desarrollo en 2022. El mismo informe advierte que la infraestructura, el talento y la capacidad de innovación en IA se concentran en unas pocas economías y corporaciones (UNCTAD, 2025). Cuando pocos actores controlan el cómputo, la nube, los modelos y las vías de distribución, no solo obtienen ventajas comerciales. También adquieren capaci-

dad para definir estándares, precios, condiciones de acceso y prioridades de investigación.

El AI Index 2026 confirma la magnitud de esta concentración. La inversión privada estadounidense en IA alcanzó 285.900 millones de dólares en 2025, mientras la inversión privada mundial llegó a 344.700 millones. Es decir, el desarrollo no se distribuye de manera uniforme: se agrupa alrededor de ecosistemas capaces de reunir capital, talento, chips, energía y mercados. La OCDE añade que las empresas de IA recibieron cerca del sesenta y uno por ciento del valor mundial del capital de riesgo en 2025. Estas cifras no anuncian por sí mismas un resultado político, pero muestran quién posee la capacidad de experimentar, comprar competidores y fijar ritmos de adopción (Stanford HAI, 2026; OCDE, 2026).

El financiamiento también determina qué problemas reciben atención. Un producto dirigido a publicidad, comercio o servicios financieros ofrece retornos inmediatos; una herramienta para traducir resoluciones en lenguas indígenas, asistir a personas privadas de libertad o fortalecer defensorías públicas puede carecer de un mercado atractivo. Si el interés público depende solo de la rentabilidad, las necesidades de quienes tienen menor capacidad de pago quedarán al

margen. El Estado no debe limitarse a comprar lo que el mercado ofrece: necesita definir prioridades, financiar bienes digitales públicos y exigir que la innovación responda a carencias sociales concretas.

3.2. La alianza entre proveedores de nube y desarrolladores de modelos

La inteligencia artificial contemporánea depende de una infraestructura costosa. Entrenar y operar modelos avanzados exige semiconductores especializados, enormes centros de datos, redes de alta velocidad y electricidad constante. Por ello, los desarrolladores de modelos suelen asociarse con proveedores de servicios de nube. La Comisión Federal de Comercio de Estados Unidos examinó las alianzas entre grandes proveedores de nube y desarrolladores de IA, entre ellos Microsoft, Alphabet, Amazon, OpenAI y Anthropic. Su informe describe participaciones de capital, derechos sobre ingresos, acceso a información, compromisos de uso de nube y algunas cláusulas de exclusividad o control (FTC, 2025).

Estas alianzas resuelven un problema real de financiamiento: una empresa joven difícilmente puede pagar por sí sola la infraestructura que necesita. Pero también crean dependencia. Quien

aporta el cómputo puede influir en la arquitectura del negocio, acceder a conocimiento estratégico y elevar los costos de cambiar de proveedor. La OCDE ha advertido que las relaciones entre capas –chips, nube, modelos y aplicaciones– pueden cerrar el mercado a competidores y reforzar posiciones dominantes (OCDE, 2025). La pregunta jurídica es evidente: si la justicia pública utiliza un modelo alojado en una nube privada, ¿quién conserva el control efectivo de la continuidad del servicio, el acceso a los registros, la conservación de la evidencia y la posibilidad de auditar el sistema?

Estas cláusulas no son contratos accesorios: pueden condicionar la trayectoria del desarrollador y reducir su libertad para migrar de proveedor. Cuando una administración pública contrata una aplicación construida sobre esa cadena de dependencias, hereda compromisos que rara vez aparecen en el contrato principal. La diligencia debida en el sector público exige identificar subcontratistas, conocer la localización de los datos, fijar condiciones de salida y anticipar los riesgos de interrupción del servicio (FTC, 2025).

La soberanía jurisdiccional se vuelve concreta en asuntos que parecen administrativos. ¿Puede el tribunal recuperar sus expedientes si termina la licencia? ¿Conserva registros suficientes para re-

construir una recomendación? ¿Puede auditar una actualización del modelo? ¿Existe una alternativa durante una caída del servicio? Si la respuesta depende de la voluntad del proveedor, el órgano judicial ha cedido más que una tarea tecnológica. Ha comprometido su capacidad de cumplir la función constitucional en sus propios términos.

3.3. El Estado como financiador, comprador y estratega

El segundo gran motor es el Estado. La historia de la informática demuestra que muchas tecnologías hoy comercializadas fueron posibles gracias a investigación pública, universidades, compras estatales y programas de defensa. En la actualidad, los gobiernos no se limitan a regular la IA: financian investigación, subsidian fábricas de semiconductores, construyen supercomputadoras, ofrecen incentivos fiscales, contratan plataformas y compran sistemas para seguridad, salud, educación y justicia.

La Unión Europea, por ejemplo, lanzó la iniciativa InvestAI con el propósito de movilizar 200.000 millones de euros, incluyendo una facilidad de 20.000 millones de euros destinada específicamente a las AI Gigafactories, que complementa la red de AI Factories desarrollada mediante

EuroHPC. China canaliza capital mediante fondos de orientación gubernamental; el AI Index 2026 estima que estos fondos desplegaron alrededor de 184.000 millones de dólares en empresas de IA entre 2000 y 2023. Estados Unidos, Europa, China, Japón, Corea del Sur y otros países también apoyan la industria de semiconductores y la capacidad de cómputo por considerarlas estratégicas (Comisión Europea, 2025; Stanford HAI, 2026; OCDE, 2025).

El financiamiento público puede ampliar capacidades nacionales y reducir dependencias. No obstante, plantea una exigencia democrática: si la sociedad asume riesgos, aporta infraestructura y financia investigación, debe participar también en la definición de los beneficios. No resulta aceptable socializar los costos y privatizar de manera absoluta el conocimiento, los datos o las rentas. El debate no es contrario a la empresa privada; es un debate sobre reciprocidad, condiciones de acceso, competencia, transparencia y orientación al interés general.

La compra pública puede orientar el mercado cuando incorpora cláusulas exigentes. Un poder judicial que reclama interoperabilidad, documentación, pruebas de sesgo, seguridad, portabilidad y acceso a registros envía una señal distinta de

aquel que solo compara precios. El costo inicial más bajo puede ocultar dependencia, pérdida de datos o imposibilidad de defensa. En tecnologías de alto impacto, la contratación debe valorar el costo de todo el ciclo de vida y no únicamente la licencia del primer año.

También debe evitarse que la palabra innovación debilite los controles presupuestarios. Los proyectos piloto merecen objetivos medibles, duración definida y criterios de suspensión. Cuando una prueba se prolonga sin evaluación, puede convertirse en política pública por simple inercia. La experimentación es legítima si existe consentimiento institucional informado, supervisión y posibilidad de retroceder. No lo es cuando las personas se transforman en sujetos de ensayo sin saber que una tecnología está influyendo en su expediente.

3.4. Los financiamientos invisibles: datos, trabajo, energía y territorio

Hay, además, formas de financiamiento que no aparecen en los balances como inversión en inteligencia artificial. La primera son los datos. Millones de personas generan textos, imágenes, preferencias, movimientos y relaciones que adquieren valor cuando pueden ser agregados y analizados.

En ocasiones existe consentimiento; en otras, el consentimiento es formal, extenso e incomprensible. El usuario recibe un servicio, pero también aporta la materia prima con la que se entrenan sistemas, se perfilan conductas y se venden predicciones.

La segunda forma es el trabajo humano oculto. Los sistemas llamados autónomos dependen de personas que etiquetan datos, corrigen respuestas, moderan contenido, traducen expresiones y revisan resultados. Ese trabajo suele estar fragmentado y externalizado. La literatura sobre el llamado trabajo fantasma ha mostrado que la apariencia de automatización puede descansar sobre una multitud de trabajadores invisibles, frecuentemente situados en países con menores salarios y menor protección laboral (Gray y Suri, 2019; Greenbaum y Gerstein, 2025). La IA no elimina al ser humano; muchas veces lo desplaza fuera del campo de visión.

La tercera forma es ecológica y territorial. Los centros de datos consumen electricidad, agua, suelo y equipos fabricados con minerales críticos. La Agencia Internacional de Energía proyecta que el consumo eléctrico mundial de los centros de datos podría superar los 945 teravatios hora en 2030, más del doble del nivel de 2024, siendo la IA uno

de los principales impulsores de ese crecimiento (AIE, 2025). No toda esa electricidad corresponde a inteligencia artificial, y la eficiencia mejora con rapidez; aun así, el costo material existe. La nube no está en el aire: está en territorios concretos, conectada a redes eléctricas, sistemas de agua, minas, puertos y comunidades.

Por eso, al preguntar quién financia esta revolución, la respuesta debe incluir a quienes aportan capital, pero también a quienes aportan datos, trabajo, energía y recursos naturales. La economía de la IA es una cadena global. En la parte superior se concentran propiedad intelectual y rentas; en la parte menos visible se distribuyen costos laborales, ambientales y sociales. Un enfoque de derechos humanos obliga a mirar la cadena completa.

La recomendación de la UNESCO sobre ética de la inteligencia artificial incorpora la sostenibilidad ambiental y la supervisión humana dentro de las obligaciones públicas. Este punto merece ser trasladado a la contratación judicial. Una institución no debería celebrar como “inteligente” un servicio que desconoce su consumo, su infraestructura o la forma en que fueron obtenidos los datos. La evaluación ética no puede empezar cuando el modelo entrega un resultado; debe

abarcó la cadena que hizo posible ese resultado (UNESCO, 2021).

La Agencia Internacional de Energía ha recordado una verdad material: no existe inteligencia artificial sin electricidad. Los centros de datos necesitan redes confiables, agua, equipos y suelo. En países con servicios energéticos frágiles, la expansión de infraestructura intensiva puede competir con otras necesidades. La política pública debe evitar una nueva forma de extractivismo digital en la que algunos territorios aporten energía, minerales y datos mientras el conocimiento y las rentas se concentran fuera de ellos (AIE, 2025).

4. ¿Cuáles son los intereses que impulsan esta transformación?

No existe un único interés. La revolución digital reúne objetivos legítimos y tensiones profundas. Las empresas buscan rentabilidad, crecimiento, control de mercado y protección de su propiedad intelectual. Los Estados buscan productividad, seguridad, influencia geopolítica, autonomía tecnológica y capacidad de vigilancia. Las instituciones públicas buscan reducir atrasos y mejorar servicios. Los usuarios buscan herramientas útiles, rápidas y accesibles. El problema aparece cuando los intereses con mayor capacidad financiera se presentan como si fueran el interés de toda la sociedad.

La lógica empresarial favorece sistemas escalables. Un modelo que puede utilizarse por millones de personas promete rentas extraordinarias. Esa escala incentiva la concentración porque los actores con más datos, cómputo y usuarios mejoran sus productos, atraen capital y adquieren

nuevos datos. Se forma un circuito acumulativo. La competencia puede estimular innovación, pero también puede empujar a lanzar sistemas antes de comprender sus riesgos, reducir la transparencia para proteger ventajas y convertir al usuario en objeto permanente de extracción de información.

La lógica estatal es distinta, aunque puede converger con la empresarial. La IA permite clasificar solicitudes, detectar fraude, priorizar inspecciones, identificar personas y anticipar riesgos. Esa capacidad seduce a administraciones que enfrentan escasez de recursos y presión por producir resultados. Sin embargo, un Estado que observa más no necesariamente comprende mejor. La acumulación de datos puede ampliar el poder de prevención, pero también normalizar la vigilancia y desplazar la presunción de inocencia hacia una cultura de sospecha permanente.

A ello se suma el interés geopolítico. Los semiconductores, los modelos fundacionales y la nube son considerados infraestructuras estratégicas. La competencia tecnológica entre potencias convierte la IA en una cuestión de seguridad nacional. Cuando el lenguaje de la carrera domina el debate, la prudencia puede ser interpretada como retraso y la regulación como obstáculo. Pero una sociedad democrática no debe aceptar que la ur-

gencia geopolítica suspenda los límites constitucionales. La historia enseña que las tecnologías desarrolladas bajo excepcionalidad terminan con frecuencia aplicándose en la vida ordinaria.

Desde la crítica social, autores como Shoshana Zuboff han descrito un capitalismo de vigilancia que convierte la experiencia humana en materia prima para predecir y modificar conductas. Nick Srnicek ha explicado la centralidad de las plataformas como infraestructuras que intermedian mercados y acumulan datos. Nick Couldry y Ulises Mejias han propuesto la idea de colonialismo de datos para mostrar cómo la vida cotidiana es apropiada como recurso económico (Couldry y Mejias, 2019). Estas teorías no deben tomarse como una descripción total de cada empresa o Estado. Sirven, más bien, para advertir una tendencia: cuando la extracción de datos se convierte en condición del negocio, la autonomía humana puede entrar en conflicto con la rentabilidad.

La pregunta sobre la hegemonía debe formularse con rigor. No se trata de afirmar que un pequeño grupo controla cada decisión del planeta. Se trata de reconocer que la capacidad de establecer infraestructuras, definir estándares y financiar investigación se encuentra desigualmente distribuida. Quien controla la arquitectura no necesita

ordenar cada conducta; puede diseñar el entorno dentro del cual las conductas se vuelven más probables, rentables o visibles. El poder digital opera muchas veces a través de opciones predefinidas, interfaces, puntuaciones y sistemas de recomendación.

El interés por predecir no es nuevo. Los Estados han clasificado poblaciones, elaborado registros y calculado riesgos desde hace siglos. La novedad reside en la escala, la velocidad y la capacidad de combinar fuentes antes separadas. Una base de datos tributaria, un sistema de salud, registros de movilidad y actividad en redes pueden construir un retrato que ninguna oficina poseía por sí sola. La interoperabilidad puede mejorar servicios, pero también crear una mirada estatal demasiado extensa. La pregunta jurídica no es si los datos existen, sino si deben ser reunidos y con qué límites.

En el sistema penal, la promesa de anticipación resulta especialmente seductora. Prevenir un delito parece preferible a investigarlo después. No obstante, cuanto más se adelanta la intervención, más débil puede ser el vínculo con un hecho concreto. La sospecha se desplaza hacia patrones, zonas, relaciones o conductas consideradas anómalas. El derecho penal corre entonces el riesgo

de abandonar el acto y aproximarse a un derecho de autor alimentado por correlaciones.

D'Aloia advierte que los sistemas informativos pueden influir en la libertad de pensamiento y en las estructuras democráticas. Si los algoritmos organizan aquello que una persona ve, jerarquizan temas y explotan vulnerabilidades, no solo predicen preferencias: participan en su formación. La autonomía política requiere espacios de información plural, posibilidad de comprender la mediación tecnológica y límites frente a técnicas de manipulación. El poder sobre la atención es también poder sobre la ciudadanía (D'Aloia, 2025).

Por ello, la regulación no debe reducirse a la protección del consumidor. Cuando una plataforma o un sistema público interviene en elecciones, libertades o acceso a derechos, el problema es constitucional. La persona no es únicamente usuaria de un servicio; es titular de derechos y miembro de una comunidad política. Esa condición impone obligaciones de transparencia, justificación y control que no pueden quedar sustituidas por términos de uso.

5. ¿Qué tipo de ser humano se está configurando?

La pregunta más profunda no es qué máquina estamos construyendo, sino qué imagen del ser humano queda incorporada en ella. Para que un sistema calcule, debe convertir la realidad en variables. La persona aparece entonces como un conjunto de datos: historial, ubicación, consumo, vínculos, expresiones, antecedentes, tiempos de respuesta y patrones de movimiento. Esa representación puede ser útil, pero nunca es la persona completa. El riesgo comienza cuando el perfil estadístico desplaza al sujeto concreto.

Surge así el ser humano puntuado. Una cifra estima su solvencia, su productividad, su propensión a abandonar un empleo, su riesgo de reincidencia o la probabilidad de que cometa fraude. La puntuación no impone necesariamente una decisión automática. Sin embargo, influye en quien decide y puede adquirir una apariencia de objetividad que oculta sus supuestos. Citron y Pasquale

advirtieron hace más de una década que una sociedad basada en puntuaciones opacas afecta oportunidades esenciales y exige una renovación del debido proceso (Citron y Pasquale, 2014).

También aparece el ser humano predecible. Las plataformas no se conforman con conocer lo que hicimos; intentan anticipar lo que haremos. Esa anticipación puede mejorar servicios, pero también permite orientar la atención, el consumo y la opinión. Cuando los sistemas aprenden qué estímulo retiene al usuario o qué mensaje provoca una reacción, la frontera entre persuasión y manipulación se vuelve difícil de identificar. La libertad no desaparece de manera visible; puede debilitarse por acumulación de pequeñas arquitecturas de elección.

En el trabajo se configura el ser humano optimizado. Sensores, programas de productividad y sistemas de gestión algorítmica registran tiempos, movimientos y resultados. La tecnología puede proteger al trabajador de tareas peligrosas y ampliar sus capacidades. También puede intensificar el ritmo laboral, fragmentar el empleo y reducir espacios de juicio profesional. La Organización Internacional del Trabajo estima que una de cada cuatro personas ocupadas trabaja en una actividad con algún grado de exposición a la IA

generativa, aunque la transformación de tareas es más probable que la sustitución completa en la mayoría de los casos (OIT, 2025). El resultado dependerá menos de la capacidad técnica que de las reglas laborales y de quién participe en las decisiones de adopción.

En la relación con el Estado aparece el ciudadano gestionado. Sus derechos, beneficios, riesgos o prioridades pueden ser evaluados mediante sistemas automatizados. La automatización bien diseñada puede reducir arbitrariedad y demoras. Pero también puede industrializar errores, convertir desigualdades históricas en reglas estadísticas y dificultar la identificación del responsable. La persona deja de enfrentarse a un funcionario y se enfrenta a un procedimiento cuya lógica no conoce.

¿Estamos diseñando una subordinación del ser humano a la máquina? La respuesta no debe ser fatalista. Las máquinas no poseen por sí mismas autoridad jurídica. La subordinación surge cuando las instituciones renuncian a comprender, supervisar y corregir; cuando el trabajador no puede cuestionar la métrica; cuando el ciudadano no sabe que fue perfilado; cuando el juez acepta una puntuación como si fuera una verdad; cuando el proveedor invoca secreto comercial para impe-

dir la defensa. La subordinación no es una propiedad inevitable de la IA. Es una decisión institucional, a veces explícita y a veces producida por la comodidad, la dependencia o la falta de capacidad pública.

5.1. El sujeto medido y la tentación de confundir dato con identidad

La persona contemporánea aparece ante las instituciones como una suma de registros: ingresos, historial, ubicación, contactos, compras, diagnósticos, sanciones y hábitos. Estos datos pueden ser útiles, pero nunca agotan una biografía. El problema comienza cuando la representación estadística ocupa el lugar del sujeto. Una puntuación de riesgo parece precisa porque ofrece un número; sin embargo, ese número depende de categorías previas y solo expresa una probabilidad bajo ciertas condiciones. La dignidad exige mantener abierta la diferencia entre lo que los datos sugieren y lo que una persona es.

La cuantificación también altera la conducta. Quien sabe que será puntuado aprende a actuar para el indicador. El trabajador adapta sus pausas, el estudiante escribe para el sistema de detección, el ciudadano evita ciertos espacios o expresiones. El control ya no necesita una orden directa: ope-

ra mediante la expectativa de evaluación. Esta forma de disciplina algorítmica merece atención porque puede reducir la espontaneidad, la creatividad y el derecho a experimentar sin que cada gesto se transforme en evidencia.

5.2. Automatización, dependencia cognitiva y pérdida de oficio

Las herramientas generativas pueden fortalecer el trabajo profesional cuando permiten comparar argumentos, ordenar información o superar tareas repetitivas. También pueden debilitar el oficio si sustituyen la lectura, la escritura y la deliberación. Un abogado que acepta resúmenes sin revisar pierde contacto con el expediente; un juez que adopta borradores automáticos puede terminar motivando con frases que no nacieron de su comprensión. La formación jurídica debe enseñar a utilizar la herramienta sin entregar a ella las capacidades que hacen posible juzgar.

La Organización Internacional del Trabajo ha señalado que la exposición a la inteligencia artificial generativa suele implicar transformación de tareas más que desaparición inmediata de ocupaciones. Esta diferencia es importante. El futuro no está escrito por la tecnología: dependerá de la organización del trabajo, la negociación y la dis-

tribución de ganancias. La productividad puede liberar tiempo para actividades de mayor valor o intensificar ritmos y vigilancia. La decisión es institucional, no automática (OIT, 2025).

Una quinta revolución industrial digna de ese nombre debería medir su avance por la capacidad de reducir trabajos degradantes, repartir beneficios, preservar autonomía profesional y permitir que el trabajador participe en el diseño del sistema. Si la máquina fija el ritmo, registra cada movimiento y convierte la evaluación en una presión permanente, la retórica humanista se vuelve una cubierta. La centralidad de la persona exige poder intervenir, comprender y disentir.

6. Inteligencia artificial y sistema de justicia

6.1. Tecnología instrumental y tecnología funcional

Para ordenar el debate conviene distinguir dos usos. La tecnología instrumental facilita tareas sin sustituir el juicio jurídico: expediente electrónico, búsqueda jurisprudencial, transcripción, traducción, agenda, anonimización, clasificación documental y detección de duplicados. En estos casos, el sistema mejora la gestión, aunque todavía debe proteger datos, seguridad y acceso. La tecnología funcional, en cambio, interviene en actividades que influyen directamente sobre la decisión: estima riesgo, recomienda medidas, prioriza sospechosos, valora patrones probatorios o propone el sentido de una resolución.

La diferencia no siempre es absoluta. Una herramienta de clasificación aparentemente administrativa puede determinar qué expediente será atendido primero. Un buscador puede invisibilizar

precedentes. Una transcripción defectuosa puede cambiar el sentido de un testimonio. Por ello, incluso los usos instrumentales requieren control. Sin embargo, cuanto más cerca se encuentre la herramienta de una decisión que afecta derechos, mayor debe ser el nivel de transparencia, validación, contradicción y supervisión humana.

La frontera entre lo instrumental y lo funcional puede desplazarse sin que la institución lo advierta. Un sistema adquirido para ordenar expedientes puede empezar a sugerir cuáles merecen atención urgente; después, su puntuación puede utilizarse para asignar recursos; finalmente, esa prioridad puede influir en la posibilidad de investigar o defender. Por ello, cada cambio de finalidad debe ser evaluado. La ampliación silenciosa de funciones es una de las vías más comunes por las que una herramienta auxiliar adquiere poder decisorio.

Mendoza Andramuño subraya que la justicia digital requiere reformas normativas, organizativas y culturales. La tecnología no produce por sí sola un servicio judicial de calidad. Hace falta capacitación, trazabilidad, reglas de identidad, seguridad de comunicaciones y procedimientos alternativos. Una audiencia telemática puede garantizar acceso durante una emergencia y, a la vez,

comprometer la defensa si la persona no dispone de un espacio reservado para hablar con su abogado. El análisis debe descender siempre al funcionamiento concreto (Mendoza Andramuño, 2024).

6.2. Prevención y policía predictiva

En la etapa preventiva, los sistemas analizan datos históricos para identificar zonas, horarios o personas consideradas de mayor riesgo. La promesa es asignar recursos de manera eficiente. El problema es que los datos policiales no representan de manera neutral toda la criminalidad. Representan, en parte, dónde se patrulla, a quién se detiene, qué se denuncia y qué se registra. Lum e Isaac demostraron que un sistema entrenado con datos de detenciones por drogas podía reproducir y amplificar patrones policiales desiguales, generando un circuito de retroalimentación: se vigila más donde el modelo indica, se producen más registros y esos registros confirman la predicción (Lum e Isaac, 2016).

La policía predictiva territorial no acusa por sí sola a una persona, pero puede concentrar intervenciones sobre comunidades ya vigiladas. La predicción individual es todavía más delicada porque corre el riesgo de confundir probabilidad con culpabilidad. El derecho penal democrático res-

ponde a hechos y responsabilidades, no a la supuesta peligrosidad derivada de semejanzas estadísticas. Toda actuación preventiva debe respetar legalidad, necesidad, proporcionalidad y prohibición de discriminación.

Una política preventiva legítima debe publicar sus objetivos, medir impactos y permitir supervisión independiente. No basta con anunciar que la herramienta mejora la seguridad. Debe demostrarse si reduce daños, qué grupos soportan las intervenciones y cuántos falsos positivos genera. Cuando una predicción no puede ser impugnada porque se presenta como mera asignación de recursos, la afectación permanece oculta. El control debe alcanzar también decisiones administrativas que preparan o intensifican la coerción.

6.3. Investigación, reconocimiento facial y análisis masivo de datos

La investigación penal obtiene beneficios reales de la informática forense, el análisis de redes, la inteligencia de fuentes abiertas y la búsqueda de patrones en grandes volúmenes de información. Estas herramientas pueden descubrir vínculos que una revisión manual no encontraría y reducir el tiempo necesario para analizar miles de documentos. No obstante, la capacidad técnica de re-

copilar datos no equivale a autorización jurídica para hacerlo. La vigilancia masiva transforma una suma de datos dispersos en un retrato íntimo de la persona y puede afectar la expectativa razonable de privacidad incluso cuando parte de la información se encontraba públicamente accesible.

El reconocimiento facial ilustra la tensión. Puede ayudar a identificar a una persona buscada, pero un falso positivo puede conducir a una detención injusta. El Instituto Nacional de Estándares y Tecnología de Estados Unidos ha documentado diferencias demográficas en las tasas de error de numerosos algoritmos, aunque el desempeño varía entre proveedores y ha mejorado con el tiempo (NIST, 2019). Por ello, una coincidencia facial nunca debería tratarse como identificación concluyente. Debe funcionar como pista sometida a corroboración independiente, control judicial y reglas claras sobre bases de datos, conservación y eliminación.

La biometría posee una característica que agrava el daño: no puede reemplazarse con facilidad. Una contraseña comprometida puede cambiarse; un rostro, una huella o el patrón del iris acompañan a la persona. De ahí que la base jurídica, la seguridad y el plazo de conservación deban ser especialmente rigurosos. Las bases crea-

das para emitir documentos no deberían reutilizarse para vigilancia sin una norma específica, una finalidad delimitada y un examen de necesidad.

La investigación mediante fuentes abiertas plantea otra confusión. Que una publicación sea accesible no significa que el Estado pueda recopilarla de forma permanente, combinarla con otras bases y elaborar perfiles sin límites. La observación ocasional y el monitoreo sistemático tienen efectos diferentes. Cuando el poder público transforma fragmentos dispersos en una historia detallada, debe justificar la medida y someterla a controles equivalentes a su intensidad.

6.4. Prueba digital, IA generativa y cadena de custodia

La prueba digital plantea problemas de autenticidad, integridad y contexto. Un mensaje puede ser real, pero incompleto; una ubicación puede corresponder al dispositivo y no necesariamente a su propietario; una imagen puede haber sido editada; un audio puede ser sintético. La IA generativa aumenta la capacidad de producir contenidos verosímiles y obliga a fortalecer la pericia, la documentación del origen y la cadena de custodia.

La cadena de custodia digital no debe convertirse en un ritual vacío. Su función es permitir que

las partes y el tribunal reconstruyan qué se obtuvo, con qué herramienta, bajo qué versión del programa, quién tuvo acceso, qué transformaciones se realizaron y cómo se verificó la integridad. Si una herramienta de IA filtra, resume o clasifica evidencia, también debe conservarse un registro de sus parámetros y resultados. La defensa necesita acceder no solo al producto final, sino a la trayectoria que condujo a él.

La generación de contenido sintético obliga a abandonar la confianza ingenua en la imagen o la voz. La autenticación deberá apoyarse en metadatos, contexto, dispositivos de origen, testimonios y análisis pericial. Tampoco conviene caer en el extremo opuesto: la posibilidad de un montaje no convierte en falsa toda evidencia digital. El tribunal necesita un método que permita valorar la fuerza probatoria sin reemplazarla por certezas técnicas inexistentes.

Cuando una herramienta propietaria interviene en el análisis, el secreto comercial no puede impedir conocer su función. Tal vez no sea necesario revelar cada línea de código, pero sí los procedimientos, las tasas de error, los parámetros relevantes y las condiciones de uso. La igualdad de armas exige que la defensa pueda reproducir o someter a crítica la operación. Una prueba que

solo el proveedor comprende se aproxima peligrosamente a una afirmación de autoridad.

6.5. Riesgo de reincidencia, medidas cautelares y sentencia

Los sistemas de evaluación de riesgo se utilizan en algunas jurisdicciones para informar decisiones sobre libertad provisional, condena, clasificación o supervisión. Su atractivo reside en prometer consistencia. Sin embargo, la consistencia de un error no produce justicia. Dressel y Farid comprobaron que un conocido sistema comercial de predicción de reincidencia no superaba claramente la precisión de personas sin formación especializada y que variables simples podían alcanzar resultados semejantes (Dressel y Farid, 2018). El estudio no demuestra que todos los instrumentos sean inútiles, pero sí destruye la presunción de superioridad automática de la máquina.

Una puntuación de riesgo es una estimación poblacional, no una prueba de que una persona cometerá un delito. Si influye en una decisión sobre libertad, debe conocerse su propósito, margen de error, población de validación, variables utilizadas y desempeño en grupos relevantes. Además, el tribunal debe explicar de qué manera la consideró y por qué no sustituyó el análisis individual.

La persona no puede ser privada de libertad por ser estadísticamente parecida a otras.

La prisión preventiva exige valorar peligros procesales concretos y no anticipar la pena. Un modelo entrenado con reincidencia o detenciones anteriores puede introducir en la medida cautelar datos vinculados a desigualdades sociales, vigilancia selectiva o falta de defensa. El número parece individual, pero procede de experiencias de grupos. Si se utiliza, debe ser un elemento limitado, nunca una presunción de peligrosidad ni una razón para invertir la carga de la prueba.

En la sentencia, el problema se vuelve todavía más intenso. La culpabilidad requiere prueba de hechos y atribución personal. Ningún patrón puede suplir esa demostración. Incluso en la individualización de la pena, una recomendación algorítmica debe quedar subordinada a criterios legales, circunstancias acreditadas y motivación judicial. El juez no puede limitarse a declarar que “el sistema indicó” un resultado. Debe asumirlo, rechazarlo o apartarse de él mediante razones propias.

6.6. Justicia digital, audiencias telemáticas y acceso efectivo

La justicia digital no se reduce a inteligencia artificial. Incluye expediente electrónico, firma digital, notificaciones, gestión documental, interoperabilidad y audiencias telemáticas. Estas herramientas pueden disminuir desplazamientos, evitar pérdidas y acercar el servicio a comunidades alejadas. Su valor debe juzgarse por la tutela que ofrecen, no por la cantidad de trámites convertidos en formularios. Un procedimiento puede ser completamente electrónico y continuar siendo incomprensible o inaccesible.

La audiencia a distancia exige condiciones que reproduzcan las garantías esenciales de la presencia. La persona debe escuchar, ser escuchada, observar la prueba, comunicarse reservadamente con su defensa e intervenir sin obstáculos. La mala conexión, la ausencia de privacidad o la dificultad para apreciar reacciones pueden afectar la intermediación. No todas las actuaciones requieren el mismo régimen. La institución debe justificar cuándo la modalidad virtual es adecuada y ofrecer presencia física cuando la naturaleza del acto o las condiciones de la persona lo aconsejen.

La firma electrónica aporta autenticidad y trazabilidad si se apoya en una infraestructura con-

fiable. No obstante, una firma válida no corrige un acto producido sin competencia ni una decisión carente de motivación. La tecnología acredita una operación; el derecho determina su significado. Del mismo modo, una notificación electrónica solo cumple su función cuando existe constancia de entrega y la persona dispone de medios razonables para acceder. El formalismo digital puede ser tan excluyente como el papel.

La modernización debe conservar canales alternativos durante la transición. Obligar a utilizar una plataforma sin considerar conectividad, discapacidad, idioma o alfabetización puede transformar la eficiencia en una barrera. Mendoza Andramuño acierta al vincular justicia digital con cambio institucional y capacitación. El reto no consiste en imponer tecnología, sino en asegurar que nadie pierda su derecho por no dominarla (Mendoza Andramuño, 2024).

7. Derechos humanos en la sociedad algorítmica

7.1. Dignidad y autonomía

La dignidad exige que la persona sea tratada como sujeto y no como objeto de administración. Un sistema que clasifica sin informar, manipula sin consentimiento o decide sin permitir respuesta reduce a la persona a una entrada de datos. La autonomía requiere espacios reales para comprender y elegir. No basta con aceptar términos extensos o pulsar una casilla; el consentimiento debe ser específico y libre cuando constituya la base del tratamiento.

La dignidad también se expresa en el derecho a saber cuándo se interactúa con una máquina. La simulación de humanidad puede ser útil en un asistente, pero se vuelve problemática cuando induce confianza, obtiene información sensible o influye en una decisión. D'Aloia vincula esta transparencia con la libertad de decidir qué tareas se atribuyen a sistemas autónomos. En jus-

ticia, ninguna persona debería creer que conversa con un funcionario cuando recibe respuestas de un programa sin identificar (D'Aloia, 2025).

Tratar a la persona como fin implica reconocer circunstancias que el modelo no capta. Una historia de violencia, una discapacidad, una barrera lingüística o una relación de dependencia pueden cambiar el sentido de un dato. El control humano tiene valor cuando incorpora ese contexto y no cuando se limita a confirmar la puntuación. La dignidad no es una variable adicional; es el límite que impide reducir la decisión a variables.

7.2. Privacidad y protección de datos

La privacidad no protege únicamente secretos. Protege la posibilidad de desarrollar la personalidad sin observación constante. En la era algorítmica, el riesgo no reside solo en revelar un dato, sino en inferir características que la persona nunca comunicó: salud, orientación política, situación económica, relaciones o estado emocional. La acumulación de inferencias puede producir una vigilancia más profunda que la recolección de datos aislados. Los principios de finalidad, minimización, exactitud, seguridad y limitación temporal deben aplicarse durante todo el ciclo de vida del sistema.

La inferencia plantea un desafío adicional porque puede construirse a partir de datos aparentemente inocuos. Horarios de conexión, trayectos, vocabulario o contactos permiten deducir condiciones íntimas. La persona puede haber consentido el uso de cada dato aislado sin comprender el perfil resultante. Por ello, la protección debe alcanzar no solo los datos recopilados, sino las conclusiones elaboradas y sus efectos. Una inferencia incorrecta puede ser tan dañina como una filtración.

El Estado posee una responsabilidad reforzada porque muchas bases públicas se forman sin consentimiento libre. El ciudadano entrega información para recibir salud, educación, identidad o justicia. Esa dependencia impide convertir la aceptación en fundamento general para nuevos usos. La reutilización requiere competencia legal, compatibilidad de finalidades y garantías específicas. El simple hecho de que una institución tenga los datos no significa que pueda utilizarlos para cualquier propósito.

7.3. Igualdad y no discriminación

Un algoritmo puede discriminar sin utilizar expresamente una categoría protegida. El código postal, el historial laboral o determinados patro-

nes de consumo pueden funcionar como sustitutos de origen étnico, género o condición social. Barocas y Selbst explicaron cómo el análisis masivo de datos puede producir impactos desiguales incluso sin intención discriminatoria (Barocas y Selbst, 2016). La evaluación debe considerar resultados, no solo variables. También debe reconocer que existen varios criterios estadísticos de igualdad que pueden entrar en tensión; elegir entre ellos es una decisión normativa, no puramente matemática.

La igualdad ante la ley no se satisface aplicando la misma fórmula a todas las personas. Si los datos reflejan una sociedad desigual, la uniformidad puede reproducir esa historia. El análisis debe preguntar quién aparece en el conjunto de entrenamiento, quién queda fuera, qué errores recaen sobre cada grupo y qué consecuencias produce una clasificación equivocada. Una tasa global aceptable puede ocultar daños concentrados en una población pequeña.

Tampoco basta eliminar una variable sensible. El sistema puede reconstruirla mediante sustitutos. La auditoría debe examinar correlaciones y efectos, pero también el diseño institucional que utiliza el resultado. Una puntuación puede no mostrar diferencias graves y, aun así, producir

discriminación si activa revisiones más invasivas para ciertos grupos. El derecho debe observar la cadena completa: dato, modelo, decisión y consecuencia.

7.4. Libertad de expresión y pluralismo

Los sistemas de recomendación organizan gran parte de la información que vemos. Pueden ampliar voces, pero también premiar contenidos extremos, crear dependencias y concentrar el poder de moderación. La libertad de expresión no exige que toda plataforma distribuya todo contenido, pero sí demanda transparencia, procedimientos de reclamación y cuidado frente a decisiones automatizadas que silencian de forma desproporcionada. Cuando el Estado utiliza plataformas privadas para comunicar o vigilar, la relación entre poder público y arquitectura empresarial merece especial escrutinio.

La libertad de expresión posee una dimensión de recepción: para formar juicio, la ciudadanía necesita acceder a ideas diversas. Los sistemas de recomendación seleccionan aquello que se vuelve visible y aquello que queda enterrado. Esa selección no es censura estatal en todos los casos, pero adquiere importancia pública por su escala. Cuando una decisión automática reduce el alcance

de contenidos políticos, debe existir información suficiente y una vía de reclamación.

Los contenidos sintéticos agregan otra dificultad. Una imagen falsa puede dañar reputaciones, alterar procesos electorales o contaminar una investigación. La respuesta no debería conducir a una vigilancia general de toda comunicación. Se requieren mecanismos de autenticidad, educación mediática, responsabilidad proporcional y remedios rápidos. La lucha contra la manipulación no puede convertirse en una autorización para controlar el debate.

7.5. Trabajo, educación y acceso a los beneficios

La IA puede ampliar productividad y acceso al conocimiento, pero sus beneficios no se distribuyen automáticamente. El Fondo Monetario Internacional advierte que la IA puede elevar rendimientos del capital y aumentar desigualdades si complementa principalmente a trabajadores de altos ingresos o sustituye tareas sin mecanismos de protección y redistribución (FMI, 2024; 2026). Un enfoque de derechos exige educación, reconversión, protección social, participación de los trabajadores y políticas de competencia. La eficiencia no puede medirse únicamente por el número de puestos eliminados.

La formación no debe limitarse a aprender comandos o interfaces. Los profesionales necesitan comprender errores, límites, fuentes y responsabilidades. En las facultades de derecho, la alfabetización tecnológica debe convivir con teoría constitucional, argumentación y ética profesional. Un jurista capaz de operar una herramienta pero incapaz de cuestionarla será menos autónomo que quien conoce sus límites.

El acceso a los beneficios exige también infraestructura. Las regiones sin conectividad, capacidad de cómputo o datos de calidad pueden convertirse en consumidoras permanentes. UNCTAD propone concentrar políticas en infraestructura, datos y capacidades. Para América Latina, esto significa invertir en universidades, servicios públicos digitales, repositorios jurídicos abiertos y cooperación regional. La inclusión no se logra únicamente entregando cuentas de usuario (UNCTAD, 2025).

7.6. Democracia, libertad cognitiva y pluralismo

La democracia presupone ciudadanos capaces de formar opiniones sin manipulación oculta. Los modelos que personalizan mensajes, predicen vulnerabilidades o producen contenidos a gran es-

cala pueden alterar ese presupuesto. El problema no reside en toda persuasión, presente desde siempre en la política, sino en la combinación de opacidad, precisión individual y automatización. Quien recibe el mensaje puede ignorar por qué fue seleccionado y qué rasgo se intenta explotar.

La libertad cognitiva comienza a adquirir relevancia como una prolongación de la autonomía. No pretende aislar a la persona de toda influencia, algo imposible, sino impedir intervenciones diseñadas para sortear su capacidad de reflexión. Las prohibiciones de prácticas manipuladoras en el Reglamento europeo de inteligencia artificial expresan esa preocupación. El derecho debe cuidar que las excepciones por seguridad no conviertan la protección en una promesa vacía (Unión Europea, 2024).

Una democracia digital necesita transparencia sobre los sistemas que ordenan información pública, publicidad política y participación. También requiere investigación independiente y acceso a datos que permitan medir impactos sin exponer a los usuarios. La opacidad empresarial no puede impedir el estudio de infraestructuras que influyen en la conversación colectiva. El pluralismo depende hoy tanto de reglas jurídicas como de arquitecturas técnicas.

8. El debido proceso frente a decisiones algorítmicas

El debido proceso nació para contener el poder. Su sentido no desaparece cuando el poder se expresa mediante una interfaz o una puntuación. Al contrario, se vuelve más necesario porque la automatización puede ocultar al autor de la decisión, dispersar responsabilidades y producir una apariencia de inevitabilidad. La persona afectada debe poder saber, comprender, cuestionar y obtener una revisión efectiva.

8.1. Información previa y trazabilidad

El primer componente es la notificación. Nadie debería descubrir después de una decisión adversa que fue evaluado por un sistema automatizado. Debe informarse qué herramienta se utilizó, con qué finalidad y qué influencia tuvo. La mera mención de que se empleó inteligencia artificial no basta. Es necesario identificar la función concreta: búsqueda, clasificación, predicción, recomendación o decisión.

La notificación debe realizarse antes de que la persona ejerza su defensa y no como una explicación tardía. También debe identificar la versión del sistema y el responsable institucional. Los modelos cambian mediante actualizaciones, ajustes o nuevos datos; por ello, conocer solo el nombre comercial no permite reconstruir la operación. La trazabilidad convierte una decisión técnica en un acto controlable y evita que la institución responda con generalidades.

8.2. Razones comprensibles y motivación

El segundo componente es el acceso a razones comprensibles. Esto no significa que toda persona deba recibir millones de parámetros o el código fuente completo. Significa que debe conocer los factores relevantes, los datos utilizados, la lógica general, las limitaciones y la manera en que el resultado influyó en la decisión. Wachter, Mittelstadt y Floridi advirtieron que el llamado derecho a explicación posee límites jurídicos y técnicos; por eso, la protección no debe descansar en una fórmula única, sino en un conjunto de obligaciones de transparencia y contestabilidad (Wachter, Mittelstadt y Floridi, 2017).

La explicación debe adaptarse al tipo de uso. En una clasificación sencilla puede bastar con

exponer reglas y datos. En un modelo complejo será necesario aportar documentación, pruebas, factores influyentes y márgenes de incertidumbre. El objetivo no es satisfacer curiosidad técnica, sino permitir que la persona comprenda por qué la decisión le afectó y qué puede discutir. La motivación judicial no se delega: el juez debe traducir la asistencia tecnológica en razones jurídicas propias.

8.3. Contradicción e igualdad de armas

El tercer componente es la posibilidad de contradicción. La defensa debe poder cuestionar la calidad de los datos, la validez del modelo, el margen de error, el contexto de aplicación y la interpretación del resultado. Si la acusación dispone de expertos, infraestructura y documentación técnica, la igualdad de armas puede exigir acceso a asistencia especializada para la defensa. Un proceso no es contradictorio cuando una parte presenta una puntuación amparada por secreto comercial y la otra solo puede aceptar su autoridad.

La contradicción debe ser material. Entregar cientos de páginas técnicas sin tiempo ni apoyo no coloca a la defensa en condiciones de responder. Cuando el resultado tenga peso relevante, el tribunal puede necesitar peritos independientes,

acceso controlado a información confidencial y recursos para la defensa pública. Proteger secretos legítimos es posible mediante reservas y órdenes de confidencialidad; lo que no es admisible es convertirlos en una barrera absoluta frente a la libertad personal.

8.4. Decisión humana y prohibición de la obediencia algorítmica

El cuarto componente es la decisión humana responsable. El control humano no consiste en que una persona pulse el botón final. Debe tener competencia, tiempo, información y autoridad para apartarse del sistema. La automatización puede generar sesgo de deferencia: el funcionario acepta la recomendación porque parece científica o porque teme asumir la responsabilidad de contradecirla. La supervisión es significativa solo si el decisor examina críticamente el resultado y motiva su propia conclusión.

La persona que decide debe saber que conservar la responsabilidad implica también poder detener el uso. Si la herramienta falla, carece de datos suficientes o fue aplicada fuera de su ámbito de validación, la respuesta correcta puede ser prescindir de ella. Un control humano sin facultad de suspensión es decorativo. Del mismo modo, la institución debe evitar incentivos que premien

la coincidencia con el sistema y castiguen al funcionario que se aparta con razones.

8.5. Revisión, reparación y aprendizaje institucional

El quinto componente es el recurso efectivo. La persona debe poder solicitar revisión ante una autoridad independiente y obtener corrección, reparación o exclusión de la evidencia cuando corresponda. Los sistemas deben conservar registros que permitan reconstruir la operación. Sin trazabilidad, el recurso se convierte en una formalidad. El Convenio Marco del Consejo de Europa sobre inteligencia artificial, abierto a firma en 2024, exige que las actividades de IA sean compatibles con derechos humanos, democracia y Estado de derecho. El Reglamento europeo de inteligencia artificial clasifica como de alto riesgo diversos usos en justicia y aplicación de la ley y establece obligaciones de gestión de riesgos, documentación, supervisión y calidad de datos (Consejo de Europa, 2024; Unión Europea, 2024).

El recurso debe permitir corregir datos, revisar el resultado y reparar consecuencias. Cuando la decisión se apoyó en una herramienta defectuosa, la respuesta no puede limitarse a resolver el caso individual. La institución debe identificar otros expedientes afectados, suspender el sistema

y comunicar el problema. Un error algorítmico puede repetirse miles de veces; por ello, el remedio necesita una dimensión colectiva y preventiva.

8.6. Opacidad, secreto empresarial y soberanía judicial

Finalmente, el debido proceso exige reconocer que la opacidad no es solo técnica. Puede ser comercial, institucional o deliberada. Un modelo interpretable puede permanecer oculto por contrato; un modelo complejo puede ser comprendido parcialmente mediante pruebas y documentación. Por eso, la respuesta jurídica no debe resignarse ante la expresión caja negra. Debe exigir el nivel de apertura necesario para que el poder sea controlable.

La protección del secreto empresarial tiene límites cuando entra en conflicto con el proceso. Un proveedor que ofrece tecnología para decidir sobre derechos acepta un nivel de escrutinio mayor que quien vende un servicio sin impacto público. La autoridad no debe contratar aquello que no puede someter a prueba. Si el diseño impide conocer datos, parámetros o fallos relevantes, la herramienta es incompatible con una decisión que deba ser motivada y recurrible.

9. Garantías no negociables para una justicia asistida por inteligencia artificial

Una justicia democrática puede recurrir a la inteligencia artificial para organizar expedientes, localizar información, analizar grandes volúmenes de documentos y apoyar determinadas tareas procesales. Sin embargo, su utilización solo resulta legítima cuando se encuentra rodeada de condiciones estrictas que protejan a la persona frente al poder tecnológico. Estas garantías no representan una resistencia al progreso ni una desconfianza irracional hacia la innovación. Constituyen, por el contrario, la frontera que permite distinguir entre una herramienta puesta al servicio de la justicia y una forma automatizada de arbitrariedad. Allí donde están comprometidas la libertad, la presunción de inocencia, la reputación o la posibilidad de ejercer la defensa, la rapidez nunca puede ocupar el lugar de las garantías.

La intensidad de los controles deberá guardar relación con el riesgo que produzca cada sistema, pero su cumplimiento no puede quedar librado a la voluntad de la institución que lo utiliza o de la empresa que lo suministra. Una aplicación destinada a ordenar documentos puede requerir medidas menos rigurosas que otra empleada para evaluar el riesgo de reincidencia, identificar personas, seleccionar sospechosos o recomendar una medida cautelar. El enfoque basado en riesgos adoptado por el Reglamento europeo de inteligencia artificial ofrece una referencia útil, aunque cada país deberá acomodarlo a su Constitución, a su legislación procesal y a la organización de sus tribunales. La calificación de una herramienta como de alto riesgo no significa que su uso quede autorizado de manera automática; indica, más bien, que solo podrá admitirse bajo obligaciones reforzadas de documentación, vigilancia, seguridad y control humano (Unión Europea, 2024).

El Convenio Marco del Consejo de Europa sobre inteligencia artificial añade una consideración de particular importancia: la evaluación no debe concentrarse únicamente en el resultado final del sistema. Es necesario examinar todo su ciclo de vida, desde el diseño y la selección de los datos hasta su adquisición, configuración, aplicación, supervisión y eventual retiro. Una herramienta

que ofrecía un desempeño aceptable al momento de su contratación puede perder precisión debido a cambios sociales, jurídicos o tecnológicos. También puede producir errores al ser utilizada en una población distinta de aquella con la que fue probada. Por esa razón, la vigilancia no termina cuando el programa comienza a funcionar; debe mantenerse durante todo el tiempo en que sus resultados tengan capacidad de influir sobre decisiones públicas (Consejo de Europa, 2024).

La primera garantía es la existencia de una base legal clara y de una finalidad definida. Ningún sistema capaz de afectar derechos puede operar únicamente por una decisión administrativa interna, una orden informal o una cláusula incluida en un contrato tecnológico. La ley debe precisar qué autoridad puede utilizarlo, para qué propósito, sobre qué personas, con qué datos y bajo cuáles límites. De igual manera, antes de su incorporación deberá realizarse una evaluación de impacto que examine sus posibles consecuencias sobre los derechos humanos, la privacidad, la igualdad, la presunción de inocencia y el debido proceso. Esa evaluación no debería quedar encerrada entre técnicos y funcionarios. La defensa pública, la academia, las organizaciones sociales y los grupos que puedan verse afectados tienen razones legítimas para participar en una discusión

que puede modificar la manera en que el Estado investiga, acusa y juzga.

La transparencia institucional exige, además, un registro público de los sistemas utilizados por los tribunales, las fiscalías, la policía y la administración penitenciaria. La ciudadanía debe poder conocer qué herramienta se emplea, quién la suministra, qué finalidad cumple, cuál es la versión instalada, qué validaciones generales ha superado y qué órgano asume la responsabilidad de su funcionamiento. Naturalmente, algunos detalles técnicos relacionados con la seguridad pueden requerir reserva, pero esa excepción debe ser concreta, motivada y limitada en el tiempo. El secreto no puede convertirse en una fórmula general para impedir el control de tecnologías que participen en el ejercicio del poder público.

En materia penal debe mantenerse una prohibición firme: ninguna decisión que restrinja la libertad, declare la culpabilidad, imponga una pena o determine una medida cautelar puede quedar exclusivamente en manos de un sistema automatizado. La inteligencia artificial podrá ofrecer información, advertir coincidencias o presentar escenarios, pero la decisión debe pertenecer a una autoridad humana identificable, competente y obligada a motivar su conclusión. El juez no pue-

de convertirse en un simple validador de la recomendación tecnológica. Su intervención debe ser sustantiva, lo que supone comprender las limitaciones del sistema, contrastar sus resultados con el resto de la prueba y tener la capacidad de apartarse de ellos cuando no sean convincentes o compatibles con el derecho.

La validación independiente y local constituye otra condición indispensable. Un programa probado en un país, una lengua o una población determinada no debe trasladarse mecánicamente a otro contexto. Las diferencias jurídicas, sociales, culturales y lingüísticas pueden alterar su comportamiento y producir errores que no estaban presentes en la experiencia inicial. Antes de ser utilizado, el sistema deberá demostrar su funcionamiento en las condiciones concretas en las que operará. Esto incluye revisar sus tasas de error, sus falsos positivos, su desempeño frente a distintos grupos y las consecuencias que puede generar cuando se equivoca. Una presentación comercial preparada por el proveedor no equivale a una validación científica ni sustituye una evaluación independiente.

La calidad, pertinencia y trazabilidad de los datos también deben ser objeto de examen. Los sistemas aprenden y producen inferencias a par-

tir de información que puede contener errores, omisiones o desigualdades históricas. Si los datos proceden de prácticas policiales concentradas durante años en ciertos territorios o grupos sociales, el modelo puede interpretar esa mayor vigilancia como una mayor propensión al delito. Asimismo, variables aparentemente neutrales, como el domicilio, el historial laboral o determinados patrones de movilidad, pueden funcionar como sustitutos de condiciones sociales protegidas. Por ello, la institución debe conocer la procedencia de los datos, verificar su exactitud, corregir información desactualizada y documentar las transformaciones realizadas durante su tratamiento.

Toda persona afectada tiene derecho a recibir una explicación suficiente y a contradecir el resultado. No es necesario entregarle millones de parámetros o exigirle conocimientos de programación, pero sí debe conocer qué elementos influyeron en la recomendación, cuáles fueron los datos considerados, qué límites posee la herramienta y de qué manera su resultado incidió en la decisión. La explicación debe permitir una defensa útil, no reducirse a una descripción general del producto. Junto con ello, la igualdad de armas exige que la defensa pueda acceder a la documentación, los registros y la asistencia especializada necesaria

cuando la acusación utiliza sistemas complejos. No existe contradicción efectiva cuando una parte presenta una puntuación revestida de autoridad científica mientras la otra carece de medios para examinarla.

Los sistemas deberán someterse a auditorías periódicas, pruebas de seguridad y vigilancia posterior a su puesta en funcionamiento. Su desempeño puede degradarse con el tiempo, cambiar después de una actualización o verse afectado por nuevas condiciones que no fueron previstas durante su desarrollo. Cada modificación relevante debe quedar registrada y, cuando corresponda, ser sometida a una nueva validación. La trazabilidad permitirá reconstruir qué versión fue utilizada en un caso, con qué configuración y bajo qué parámetros. Sin esta información, la revisión judicial se vuelve incompleta y la responsabilidad termina diluyéndose entre funcionarios, proveedores y programas.

La contratación pública debe proteger la soberanía institucional. Los contratos tienen que garantizar el acceso a los registros, la portabilidad de los datos, la continuidad del servicio, la posibilidad de auditoría y la recuperación de la información en caso de terminar la relación con el proveedor. El secreto empresarial no puede utilizar-

se para impedir que un tribunal conozca cómo se produjo una evidencia ni para negar a la defensa los elementos necesarios para cuestionarla. Cuando una empresa participa en funciones vinculadas con la justicia, sus intereses comerciales deben ceder ante las garantías procesales y el control jurisdiccional.

Del mismo modo, la responsabilidad debe permanecer claramente identificada. Es necesario saber quién responde por el diseño, la compra, la configuración, la validación, el uso y la supervisión de cada sistema. La expresión “lo decidió el algoritmo” no puede tener cabida en un Estado de derecho. La máquina carece de competencia jurídica y no puede asumir las consecuencias de sus errores. La institución que decide utilizarla conserva la obligación de prevenir daños, explicar sus actuaciones, corregir las decisiones equivocadas y reparar a las personas perjudicadas.

Algunas tecnologías merecen una protección especialmente rigurosa por su capacidad para extender la vigilancia sobre poblaciones enteras. El reconocimiento facial masivo, la policía predictiva individual, la inferencia biométrica y los sistemas que reconstruyen comportamientos a partir de múltiples bases de datos pueden alterar la relación entre ciudadanía y Estado. Estas herra-

mientas no deben normalizar una sospecha permanente ni convertir la vida cotidiana en una fuente inagotable de perfiles policiales. Su utilización requiere una justificación excepcional, una base legal precisa, límites temporales, control independiente y la demostración de que no existe una alternativa menos invasiva.

Cuando una prueba o decisión algorítmica haya vulnerado derechos, deben existir mecanismos efectivos de exclusión, corrección y reparación. No basta reconocer el error si sus consecuencias permanecen intactas. La persona afectada necesita una vía para solicitar revisión, corregir datos, cuestionar el procedimiento y obtener una respuesta de una autoridad independiente. En el proceso penal, ello puede exigir la exclusión de una evidencia obtenida o procesada sin las garantías debidas. En otros casos, corresponderá modificar la decisión, eliminar información, reconocer el daño y adoptar medidas para impedir su repetición.

Estas salvaguardas carecerían de fuerza si quienes administran justicia no cuentan con una formación crítica. Jueces, fiscales, defensores, policías y peritos necesitan comprender los conceptos esenciales de la inteligencia artificial, sus posibilidades y sus márgenes de error. La alfabeti-

zación tecnológica no consiste en aprender a obedecer la herramienta ni en aceptar sus resultados por su apariencia científica. Consiste en saber interrogarla: preguntar de dónde provienen los datos, qué mide, qué deja fuera, con qué población fue probada, cuántas veces se equivoca y quién responde por esas equivocaciones.

Por último, ninguna regulación será suficiente si el Estado carece de capacidad propia para aplicarla. Una institución que depende por completo de la explicación del proveedor no está en condiciones de ejercer un control adecuado. La soberanía digital no exige fabricar dentro del país cada componente tecnológico, pero sí comprender lo que se contrata, conservar los datos esenciales, poder cambiar de proveedor y evitar que los derechos procesales dependan de la buena voluntad de una empresa. Para ello se requieren equipos interdisciplinarios estables, integrados por juristas, ingenieros, especialistas en datos, defensores, fiscales y representantes de la sociedad. Las decisiones sobre el margen de error tolerable, las variables admisibles o los riesgos que pueden aceptarse no son puramente técnicas; expresan opciones jurídicas y políticas sobre quién soportará las consecuencias de la innovación.

También resulta conveniente crear registros públicos de incidentes, evaluaciones y medidas correctivas. Compartir esa información permite aprender de los errores y evita que distintas instituciones repitan las mismas fallas. La ciudadanía tiene derecho a conocer qué sistemas utiliza el Estado, cuánto cuestan, qué resultados han producido y qué acciones se adoptaron cuando ocasionaron daños. Una justicia asistida por inteligencia artificial solo podrá conservar su legitimidad si la tecnología permanece visible, discutible y subordinada al derecho. La promesa tecnológica merece atención, pero ninguna promesa, por atractiva que parezca, puede situarse por encima de la dignidad humana ni del debido proceso.

10. América Latina y el riesgo de una dependencia algorítmica

América Latina enfrenta una situación particular. La región necesita modernizar sistemas judiciales marcados por demoras, desigualdad de acceso y escasez de recursos. La IA puede contribuir a ordenar expedientes, mejorar búsqueda jurídica, traducir información, acercar servicios y detectar patrones de corrupción. Rechazar toda tecnología sería tan poco razonable como aceptarla sin condiciones.

El peligro es importar sistemas, categorías y datos contruidos en otros contextos. Un modelo entrenado con lenguaje, prácticas policiales o estructuras sociales extranjeras puede cometer errores sistemáticos al aplicarse localmente. Además, la dependencia de nubes, modelos y licencias externas puede trasladar datos sensibles y recursos públicos hacia proveedores que operan fuera del alcance efectivo de las autoridades nacionales.

La desigualdad digital también afecta el acceso a la justicia. Una audiencia virtual puede evitar desplazamientos y reducir costos, pero puede excluir a quien carece de conectividad, privacidad, equipo o alfabetización digital. La modernización no debe crear dos justicias: una rápida para quien está conectado y otra precaria para quien no lo está. Toda transformación debe conservar canales presenciales y apoyos adecuados.

La región necesita políticas propias: infraestructura pública o compartida, centros de investigación, estándares abiertos, compras transparentes, formación interdisciplinaria y cooperación entre poderes judiciales. También necesita participar en la gobernanza global de la IA. Si las normas se diseñan únicamente en los países que concentran capital y cómputo, las necesidades del Sur global aparecerán como problemas secundarios. La universalidad de los derechos humanos exige una conversación verdaderamente universal.

La dependencia algorítmica no se supera con discursos de soberanía vacíos. Se supera fortaleciendo instituciones, ciencia, educación y control democrático. Un país puede utilizar tecnología extranjera sin renunciar a sus garantías si establece condiciones, audita, protege sus datos y conserva la autoridad jurídica. Lo que no puede hacer

es delegar la definición de justicia a un producto que no comprende.

10.1. El desafío de importar modelos y exportar datos

América Latina corre el riesgo de ocupar una posición subordinada en la cadena digital: aportar datos, minerales, energía y trabajo de anotación, mientras importa modelos, licencias y criterios de decisión. Esa estructura puede reproducir una dependencia conocida bajo una forma nueva. No se trata de rechazar cooperación ni tecnología extranjera, sino de negociar condiciones que preserven conocimiento, datos y capacidad de adaptación.

Los sistemas jurídicos de la región poseen lenguajes, prácticas y problemas propios. Un modelo entrenado en jurisprudencia de otra tradición puede confundir instituciones o reproducir categorías ajenas. Incluso dentro del español existen diferencias terminológicas y culturales. La validación local debe examinar comprensión, errores y desempeño en poblaciones diversas. Traducir una interfaz no equivale a adaptar una tecnología.

10.2. Una agenda regional de garantías y capacidad

La región necesita cooperación para evitar que cada poder judicial negocie en soledad con proveedores de escala mundial. Podrían desarrollarse criterios comunes de contratación, repositorios de evaluaciones, laboratorios regionales y estándares de interoperabilidad. La coordinación reduciría costos y fortalecería la capacidad de exigir transparencia. También permitiría compartir herramientas abiertas para tareas de bajo riesgo, como búsqueda jurisprudencial o anonimización de resoluciones.

Una agenda latinoamericana debe priorizar defensa pública, acceso rural, lenguas indígenas, discapacidad y protección de datos. Esos asuntos suelen quedar fuera de productos diseñados para mercados más rentables. La innovación pública puede comenzar por problemas modestos pero decisivos: localizar precedentes, mejorar notificaciones, traducir lenguaje judicial y facilitar información comprensible. El progreso no siempre se encuentra en el modelo más grande; a veces reside en una institución que escucha mejor.

La formación judicial regional requiere una base crítica. Los operadores deben conocer conceptos suficientes para preguntar por datos, va-

lidación, errores y seguridad, sin pretender sustituir a especialistas. A su vez, los equipos técnicos necesitan comprender debido proceso, prueba y motivación. La conversación interdisciplinaria no es un complemento; es la condición para que la tecnología no imponga sus categorías al derecho.

11. De la eficiencia a la legitimidad

En el discurso tecnológico, la eficiencia aparece como argumento definitivo. Menos tiempo, menos costo, más casos resueltos. Sin embargo, la justicia no es una fábrica de decisiones. Una sentencia rápida puede ser injusta; una predicción precisa en promedio puede destruir la vida de una persona concreta; un sistema uniforme puede reproducir de manera impecable una desigualdad histórica.

La eficiencia es valiosa cuando sirve a la tutela judicial efectiva. Deja de serlo cuando sustituye la deliberación, impide la defensa o reduce la dignidad a una variable. La legitimidad de una decisión no proviene únicamente de acertar. Proviene también del procedimiento: ser oído, conocer la acusación, discutir la prueba, comprender las razones y acudir ante una autoridad independiente. El debido proceso expresa el reconocimiento de que la persona merece algo más que un resultado estadísticamente plausible.

La inteligencia artificial puede ayudar a que el juez encuentre información, identifique inconsistencias y gestione una carga de trabajo excesiva. Pero no puede asumir la responsabilidad moral y constitucional de decidir sobre la libertad. Una máquina no comparece ante la sociedad, no explica su conciencia, no responde disciplinariamente y no experimenta la gravedad de condenar a un inocente. El juez puede utilizar herramientas; no puede esconderse detrás de ellas.

Tampoco debemos idealizar la decisión humana. Los seres humanos tienen prejuicios, se cansan y cometen errores. La alternativa no es humano perfecto contra máquina defectuosa. La cuestión es diseñar instituciones en las que capacidades diferentes se controlen mutuamente. Una herramienta puede alertar sobre inconsistencias; el juez puede aportar contexto y responsabilidad; la defensa puede cuestionar; la auditoría puede medir resultados; la ley puede fijar límites. La complementariedad solo es legítima cuando no diluye la autoría de la decisión.

La legitimidad exige, además, que la persona pueda reconocer al autor de la decisión. En la burocracia algorítmica, la responsabilidad tiende a fragmentarse: el proveedor culpa a los datos, el técnico al modelo, el funcionario al protocolo y la

institución al contrato. El derecho debe reconstruir esa cadena y asignar deberes. La complejidad no puede convertirse en una forma de impunidad.

La precisión estadística tampoco reemplaza la justicia del procedimiento. Un sistema podría acertar con frecuencia y seguir siendo inadmisibles si utiliza datos obtenidos sin base legal, impide contradicción o trata a la persona como representante de un grupo. La justicia no consiste solo en producir resultados correctos; consiste en alcanzarlos mediante un poder limitado y respetuoso.

La mejor relación entre persona y máquina no es la obediencia, sino la fricción productiva. La herramienta puede revelar patrones que el juez no vio; el juez debe cuestionar su alcance; la defensa pone a prueba la inferencia; la auditoría revisa los efectos. Cuando todas las partes aceptan el resultado porque “lo dice el sistema”, la tecnología ha dejado de asistir y ha comenzado a gobernar.

12. La abogacía ante la inteligencia artificial: competencia, independencia y responsabilidad

La discusión sobre inteligencia artificial y justicia no puede dejar a la abogacía en el papel de espectadora. El abogado participa en la construcción del expediente, selecciona hechos, formula hipótesis, ofrece prueba y controla el ejercicio del poder. Cuando utiliza sistemas generativos o recibe resultados producidos por algoritmos, su deber profesional no disminuye. Por el contrario, aumenta, porque debe comprender las limitaciones de una herramienta que puede producir una respuesta convincente sin que esa respuesta sea correcta. La rapidez no modifica la obligación de estudiar el caso, verificar las fuentes y asumir cada afirmación presentada ante el tribunal.

La herramienta puede ayudar a revisar documentos, comparar líneas jurisprudenciales, organizar evidencia o preparar una estructura inicial. Ninguna de esas funciones autoriza a sustituir el

juicio profesional. El abogado que presenta una cita inexistente, confunde los hechos o reproduce datos personales sin necesidad no puede atribuir el error al sistema. La relación con la tecnología debe conservar una regla sencilla: toda salida que ingresa al proceso se convierte en una afirmación humana y queda sometida a las responsabilidades ordinarias de diligencia, veracidad, lealtad y respeto al tribunal.

12.1. El deber de verificación y la prohibición de delegar el criterio profesional

La verificación no consiste en una lectura superficial. Implica regresar a la fuente primaria, comprobar vigencia, jurisdicción, contexto y alcance. Un modelo puede mezclar normas derogadas, decisiones de países distintos o fragmentos que sostienen una conclusión contraria a la sugerida. En asuntos penales, donde una palabra puede alterar la calificación jurídica o el sentido de una prueba, el deber es todavía más riguroso. La inteligencia artificial puede acelerar la búsqueda; no puede certificar la validez jurídica de lo encontrado. Esa tarea pertenece al profesional que conoce el expediente y responde por la estrategia.

Conviene documentar el uso de herramientas cuando intervienen en actividades sensibles. Registrar la versión, la fecha, la finalidad y las verificaciones efectuadas permite reconstruir el trabajo y explicar cómo se llegó a una conclusión. No toda asistencia requiere revelación pública, del mismo modo que no se informa cada búsqueda realizada en una base jurídica. Sin embargo, cuando el sistema produce una clasificación, modifica evidencia, elabora un análisis pericial o influye de manera relevante en la decisión, la transparencia puede ser necesaria para garantizar contradicción y confianza.

12.2. Secreto profesional, confidencialidad y gobierno de los datos

El deber de confidencialidad impide introducir expedientes, testimonios, diagnósticos, estrategias o datos de clientes en servicios cuyo tratamiento no ha sido evaluado. Antes de utilizar una plataforma, el profesional debe conocer dónde se alojan los datos, si se conservan, si se emplean para entrenamiento, quién puede acceder y cómo se eliminan. La facilidad de copiar un documento no reduce la sensibilidad de su contenido. En muchos casos será necesario anonimizar, trabajar en entornos institucionales o abstenerse de usar servicios abiertos. La protección del secreto no

es una preferencia tecnológica: forma parte del derecho de defensa.

Los despachos y las instituciones deben adoptar políticas internas que definan usos permitidos, información prohibida, procedimientos de revisión y respuesta ante incidentes. Una prohibición general puede llevar a usos clandestinos; una autorización sin límites expone a clientes y procesos. La política madura distingue riesgos, ofrece herramientas seguras y capacita al personal. También asigna responsabilidades: quién aprueba una aplicación, quién verifica contratos, cómo se reporta un error y qué medidas se adoptan cuando se ha compartido información de manera indebida.

12.3. Igualdad de armas en una justicia tecnológicamente desigual

La inteligencia artificial puede ampliar la distancia entre quienes disponen de infraestructura y quienes apenas cuentan con recursos básicos. Una fiscalía con laboratorios, analistas y acceso a bases masivas puede presentar resultados que una defensa pública no está en condiciones de examinar. La igualdad de armas exige algo más que entregar el informe final. Puede requerir acceso a registros, documentación, peritos y tiempo su-

ficiente. Cuando el Estado introduce una herramienta compleja, debe prever recursos para que la defensa pueda cuestionarla; de lo contrario, la innovación fortalece a una parte y debilita el carácter contradictorio del proceso.

La abogacía organizada tiene una tarea colectiva. Los colegios pueden elaborar guías, programas de formación, repositorios de incidentes y criterios de contratación. También pueden defender estándares abiertos y mecanismos de asistencia para profesionales pequeños o alejados de los centros urbanos. La competencia tecnológica no debe convertirse en un privilegio reservado a grandes firmas. Si la calidad de la defensa depende de pagar herramientas costosas, la transformación digital habrá creado una nueva barrera para el acceso a la justicia.

12.4. Independencia profesional y función constitucional de la abogacía

La independencia significa conservar la capacidad de decir no: no a una recomendación sin fundamento, no a una clasificación opaca, no a una prueba que no puede ser examinada y no a la presión por producir más trabajo a costa de la calidad. Los sistemas pueden sugerir la estrategia más frecuente o el argumento con mayor proba-

bilidad de éxito; el abogado debe considerar también la justicia del caso, la voluntad del cliente y las consecuencias humanas. La práctica jurídica no es una competencia de predicción. Su sentido reside en representar, argumentar, proteger y abrir espacios de escucha frente al poder.

En esta etapa, la abogacía debe asumir una doble función. Por una parte, utilizar con prudencia herramientas capaces de mejorar su trabajo. Por otra, convertirse en una instancia de control frente a los sistemas que adopten tribunales, fiscalías, policías y administraciones. El abogado debe preguntar qué datos se usaron, qué margen de error existe, quién configuró el modelo y cómo puede impugnarse el resultado. Su tarea no es defender el pasado frente a la técnica, sino impedir que la técnica se convierta en una autoridad sin razones.

El futuro profesional no pertenecerá a quien obedezca mejor a la máquina ni a quien pretenda ignorarla. Pertenecerá a quien pueda combinar conocimiento jurídico, comprensión tecnológica y responsabilidad humana. Esa combinación exige estudio continuo, pero también carácter. En un entorno que premia velocidad y volumen, la abogacía debe preservar el tiempo de leer, dudar y escuchar. Solo así la inteligencia artificial podrá incorporarse al ejercicio profesional sin des-

plazar aquello que le da legitimidad: la confianza del cliente, la lealtad procesal y la defensa de la persona concreta.

13. A manera de conclusión: poner la inteligencia al servicio de la humanidad

La revolución industrial digital no es una fuerza natural que avance al margen de la voluntad humana. Es una construcción económica, política y jurídica. La financian corporaciones, inversionistas, Estados y ciudadanos; la sostienen trabajadores, datos, energía y territorios. Sus beneficios pueden ser inmensos, pero también puede concentrar riqueza, ampliar vigilancia y convertir decisiones públicas en productos privados.

Preguntar quién la financia permite comprender quién puede orientar sus objetivos. Las grandes empresas tecnológicas poseen una capacidad excepcional para invertir y desplegar sistemas. Los fondos de capital buscan retornos. Los Estados persiguen competitividad y seguridad. Los proveedores de nube y chips controlan insumos esenciales. Esa estructura no prueba una conspiración; prueba una asimetría. Y toda asimetría de

poder exige derecho, control público y participación democrática.

La cuarta revolución industrial ha hecho posible una sociedad en la que casi toda actividad deja una huella. La propuesta de una quinta revolución intenta colocar al ser humano en el centro, pero ese propósito no se cumplirá mediante una etiqueta. Será humano un sistema en el que la persona conserve autonomía, pueda comprender y cuestionar, participe en las decisiones que afectan su trabajo y su vida, y reciba una parte justa de los beneficios de la innovación.

En el ámbito de la justicia, el límite debe ser todavía más firme. Ninguna puntuación debe sustituir la presunción de inocencia. Ningún secreto comercial debe vencer al derecho de defensa. Ningún sistema debe privar de libertad sin una decisión humana motivada. Ninguna promesa de rapidez debe justificar una vigilancia desproporcionada. La tecnología puede asistir; la responsabilidad no puede automatizarse.

La pregunta final no es si la inteligencia artificial llegará a los tribunales, porque ya ha llegado. La pregunta es bajo qué Constitución entrará. Puede ingresar como una herramienta sometida a la ley, auditada, discutible y orientada a ampliar derechos. También puede ingresar como

una autoridad silenciosa, protegida por contratos y presentada como neutral. Entre esas dos posibilidades se juega una parte del futuro del debido proceso.

Tal vez el desafío no consista en construir máquinas que se parezcan cada vez más al ser humano. Tal vez consista en impedir que el ser humano sea tratado cada vez más como una máquina: medible, predecible, reemplazable y administrado sin razones. Una justicia digna de ese nombre debe recordar que detrás de cada dato hay una historia, detrás de cada expediente hay una vida y detrás de cada decisión existe una responsabilidad que ninguna tecnología puede asumir por nosotros.

La promesa tecnológica merece ser examinada, no adorada ni temida. Sus beneficios pueden ampliar derechos cuando corrigen demoras, acercan información y apoyan tareas complejas. Sus riesgos aparecen cuando la velocidad ocupa el lugar de la motivación, la puntuación sustituye a la prueba y el contrato privado limita el control público. La respuesta no está en una confianza abstracta, sino en instituciones capaces de preguntar, probar, documentar, corregir y detener.

La última palabra debe seguir perteneciendo a una persona jurídicamente responsable. No porque el juicio humano sea infalible, sino porque el

Estado de derecho exige un autor que dé razones, escuche contradicción y responda por la decisión. Allí se encuentra la frontera que la revolución industrial digital no debe cruzar: la tecnología puede ampliar la inteligencia de la justicia, pero no puede reemplazar su conciencia constitucional.

Referencias

- Agencia Internacional de Energía. (2025). *Energy and AI*. París: IEA.
- Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. *California Law Review*, 104, 671-732.
- Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, 82(5), 977-1008.
- Canales Cortés, L. (Comp.). (2024). *La virtualidad en la justicia y la inteligencia artificial en el derecho procesal moderno*. Edinexo.
- Citron, D. K., & Pasquale, F. (2014). The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, 89, 1-34.
- Comisión Europea. (2021). *Industry 5.0: Towards a Sustainable, Human-Centric and Resilient European Industry*. Bruselas.
- Comisión Europea. (2025). *AI Continent Action Plan e iniciativa InvestAI*. Bruselas.
- Consejo de Europa. (2024). *Convenio Marco sobre Inteligencia Artificial, Derechos Huma-*

- nos, Democracia y Estado de Derecho, CETS núm. 225.
- Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.
- Cuarezma Terán, S. J., y Coronel de Trinidad, J. (2024). La revolución industrial digital en el sistema de justicia penal: inteligencia artificial, derechos humanos y debido proceso. En L. Canales Cortés (comp.), *La virtualidad en la justicia y la inteligencia artificial en el derecho procesal moderno*. San José: Edinexo.
- D'Aloia, A. (2025). Inteligencia artificial, derechos fundamentales y democracia constitucional. *Teoría y Realidad Constitucional*, 55, 101-114.
- Dressel, J., & Farid, H. (2018). The Accuracy, Fairness, and Limits of Predicting Recidivism. *Science Advances*, 4(1), eaao5580.
- Federal Trade Commission. (2025). *Partnerships Between Cloud Service Providers and AI Developers*. FTC Staff Report on AI Partnerships & Investments 6(b) Study. Washington, D. C.
- Fondo Monetario Internacional. (2024). *Gen-AI: Artificial Intelligence and the Future of Work*. Washington, D. C.

- Fondo Monetario Internacional. (2026). Global Economic and Financial Implications of Artificial Intelligence: Lessons from a Scenario-Planning Exercise. Washington, D. C.
- Gray, M. L., & Suri, S. (2019). Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass. Houghton Mifflin Harcourt.
- Greenbaum, D., & Gerstein, M. (2025). Hidden Human Costs of AI. *Science*, 387(6729), 32.
- Lum, K., e Isaac, W. (2016). To Predict and Serve? *Significance*, 13(5), 14-19.
- Mendoza Andramuño, G. (2024). Justicia digital: nueva visión del derecho y su incidencia jurídica en la administración de justicia moderna. Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM.
- National Institute of Standards and Technology. (2019). Face Recognition Vendor Test, Part 3: Demographic Effects. NISTIR 8280.
- Organización Internacional del Trabajo. (2025). Generative AI and Jobs: A Refined Global Index of Occupational Exposure. Ginebra.
- Organización para la Cooperación y el Desarrollo Económicos. (2025). Competition in Artificial Intelligence Infrastructure. París: OECD Publishing.
- Organización para la Cooperación y el Desarrollo Económicos. (2026). Venture Capital In-

- vestments in Artificial Intelligence through 2025. París: OECD Publishing.
- Rojas Rodriguez, Luis & Alvarado, Walter. (2025). Introducción a la inteligencia artificial en el contexto del derecho penal.
- Rojas Rodríguez, L. A., y Durán Alvarado, W. H. (2025). Introducción a la inteligencia artificial en el contexto del derecho penal. Manuscrito académico.
- Srnicek, N. (2017). Platform Capitalism. Polity Press.
- Stanford Institute for Human-Centered Artificial Intelligence. (2026). AI Index Report 2026. Stanford University.
- UNCTAD. (2025). Technology and Innovation Report 2025: Inclusive Artificial Intelligence for Development. Ginebra: Naciones Unidas.
- UNESCO. (2021). Recomendación sobre la ética de la inteligencia artificial. París.
- Unión Europea. (2024). Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial.
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76-99.
- Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.



Sergio J. Cuarezma Terán. Prof. Dr. Dr. h. c. mult. Exmagistrado de la Corte Suprema de Justicia de Nicaragua. Rector, Profesor e Investigador de Derecho penal del Instituto de Estudio e Investigación Jurídica (INEJ), Nicaragua; Investigador *senior* del Instituto de Estudios Penales “Alimena”, Instituto de Investigación Interdepartamental de la Universidad de Calabria, Italia; Miembro del Comité Permanente de América Latina para la Prevención del Delito (COPLAD), Experto del Instituto Latinoamericano de Naciones Unidas para la Prevención del Delito y Tratamiento del Delincuente (ILANUD); y Miembro de la Comisión Redactora del Código Penal Tipo de Latinoamérica.



José Coronel De Trinidad. Magíster en Ciencias de Datos por la Pontificia Universidad Católica de Chile, graduado con Distinción Máxima; Magíster en Ciencias Forenses y Criminalística, por la Universidad Autónoma de Chiriquí, Panamá, y el Instituto de Estudio e Investigación Jurídica (INEJ), Nicaragua; Máster en Educación Superior e Investigación por el Instituto de Estudio e Investigación Jurídica (INEJ), Nicaragua; Especialista en Ciencias Forenses y Criminalística sobre la prueba científica por la Universidad Autónoma de Chiriquí, Panamá, y el Instituto de Estudio e Investigación Jurídica (INEJ), Nicaragua; Ingeniero en Sistemas de Comunicación por la Universidad Americana (UAM), Nicaragua, graduado *cum laude*. Director de Tecnología Educativa del Instituto de Estudio e Investigación Jurídica (INEJ), Nicaragua, y del Instituto Internacional de Estudio e Investigación Jurídica (INEJ), Afiliado a la Ciudad del Saber, Panamá.

El presente trabajo tiene como finalidad analizar críticamente los efectos de la revolución industrial digital y, en particular, de la inteligencia artificial sobre los derechos humanos y las garantías del debido proceso. Bajo la pregunta «¿Qué hay detrás de la promesa tecnológica?», el trabajo busca examinar tanto las oportunidades como los riesgos que acompañan la incorporación de sistemas automatizados en la justicia y en el ejercicio profesional de la abogacía, proponiendo una reflexión jurídica orientada a asegurar que la innovación permanezca subordinada a la dignidad humana, la transparencia, la igualdad y el Estado democrático y social de derecho.



UNIVERSIDAD JUÁREZ
AUTÓNOMA DE TABASCO
“ESTUDIO EN LA DUDA. ACCIÓN EN LA FE”

ISBN 978-99924-21-65-9

