

Cuando el derecho no alcanza a la máquina: inteligencia artificial, blockchain y la crisis de gobernanza jurídica en América Latina

When Law Cannot Keep Up with the Machine: Artificial Intelligence, Blockchain and the Legal Governance Crisis in Latin America

Daniel Horacio Cangelosi Sánchez

Doctor en Educación, Universidad Católica de Córdoba (2023)

Investigador Colaborador, Centro Nacional de Inteligencia Artificial de Chile (CENIA)

Presidente, Fundación Salud, Educación y Discapacidad (SalEduDis), Argentina

ORCID: 0000-0002-5291-5750 | cangelosisanchez@gmail.com

Resumen

La irrupción de la inteligencia artificial (IA) y las tecnologías blockchain en el sistema jurídico latinoamericano no es un fenómeno futuro: es una realidad presente que el derecho procesa con instrumentos diseñados para otra época. Este artículo examina la triple tensión que estas tecnologías producen sobre el ordenamiento jurídico de la región: primero, la IA como herramienta de decisión en contextos judiciales y administrativos genera problemas irresueltos de transparencia, sesgo algorítmico y responsabilidad civil; segundo, la blockchain como infraestructura de contratos inteligentes desafía los conceptos tradicionales de forma contractual, voluntad jurídica y jurisdicción; tercero, la adopción organizacional de IA sin diagnóstico previo del problema a resolver produce consecuencias jurídicas concretas que el marco contractual latinoamericano no está preparado para contener. A partir de evidencia empírica recogida en organizaciones de Argentina, México, Colombia, Chile y Perú, y de los datos del Índice Latinoamericano de Inteligencia Artificial 2025 (CENIA & CEPAL), el artículo propone que la respuesta del derecho a estas tecnologías no puede ser meramente reactiva: requiere una reconfiguración de las categorías jurídicas fundamentales de autoría, responsabilidad, forma y prueba, y el desarrollo de un estándar de diligencia debida tecnológica específico para operadores jurídicos latinoamericanos.

Palabras clave: inteligencia artificial, blockchain, contratos inteligentes, gobernanza algorítmica, responsabilidad civil, administración de justicia, América Latina, diligencia debida tecnológica.

Abstract

The emergence of artificial intelligence (AI) and blockchain technologies in the Latin American legal system is not a future phenomenon: it is a present reality that the law is processing with instruments designed for a different era. This article examines the triple tension that these technologies produce on the region's legal order: first, AI as a decision-making tool in judicial and administrative contexts generates unresolved problems of transparency, algorithmic bias, and

civil liability; second, blockchain as smart contract infrastructure challenges traditional legal concepts of contractual form, legal intent, and jurisdiction; third, the organizational adoption of AI without prior diagnosis of the problem to be solved produces concrete legal consequences that Latin American contract law is not equipped to contain. Drawing on empirical evidence gathered in organizations in Argentina, Mexico, Colombia, Chile, and Peru, and on data from the Latin American Artificial Intelligence Index 2025 (CENIA & CEPAL), the article argues that the law's response to these technologies cannot be merely reactive: it requires a reconfiguration of the fundamental legal categories of authorship, responsibility, form, and evidence, and the development of a technological due diligence standard specifically tailored to Latin American legal practitioners.

Keywords: artificial intelligence, blockchain, smart contracts, algorithmic governance, civil liability, administration of justice, Latin America, technological due diligence.



Artículo publicado bajo Licencia Creative Commons Atribución-No Comercial-Sin Derivar.

© Universidad Católica de Córdoba

DOI: [https://doi.org/10.22529/rbia.2026\(9\)02](https://doi.org/10.22529/rbia.2026(9)02)

Nota sobre el uso de inteligencia artificial

El presente artículo es una producción intelectual original del autor. La inteligencia artificial fue utilizada como herramienta de asistencia para la corrección gramatical y ortográfica del texto y para la verificación de la accesibilidad de las fuentes bibliográficas citadas. Las ideas, los argumentos, el marco teórico y las conclusiones son exclusivamente del autor.

1. Introducción: el derecho ante la máquina que decide

Un juez de primera instancia en una ciudad del norte de México recibe el informe de un sistema de análisis predictivo de riesgo de reincidencia. El sistema, entrenado con datos históricos del sistema penal, asigna al imputado un índice de riesgo alto. El juez, presionado por la carga procesal y la aparente objetividad del número, pondera ese índice en su decisión de prisión preventiva. Nadie en la sala puede explicar cómo el sistema calculó ese número. El imputado no sabe que un algoritmo participó en la decisión sobre su libertad. Y el abogado defensor carece de herramientas procesales para impugnarlo.

En otra ciudad, esta vez en el sur de Brasil, una empresa firma un contrato inteligente desplegado en una red blockchain para la entrega automática de pagos contra la verificación de hitos de una obra de construcción. Cuando una disputa surge sobre si un hito fue efectivamente alcanzado, ninguna de las partes puede modificar el contrato: el código se ejecutó de manera autónoma e irreversible. El sistema judicial no tiene jurisprudencia sobre cómo tratar ese

contrato. El notario que intervino en la negociación previa no tenía las herramientas conceptuales para advertir sobre las consecuencias de la inmutabilidad del código.

Estos dos escenarios, tomados de la realidad emergente del derecho latinoamericano, ilustran la tesis central de este artículo: la inteligencia artificial y la tecnología blockchain no son simplemente herramientas nuevas que el derecho debe regular, como reguló el telégrafo, el automóvil o el correo electrónico. Son tecnologías que cuestionan los fundamentos mismos de las categorías jurídicas con las que operamos: la autoría de una decisión, la forma y ejecutoriedad de un contrato, la atribución de responsabilidad ante un daño, y la producción y valoración de la prueba. El derecho latinoamericano, con marcos normativos que en muchos casos no han sido actualizados desde antes de la era digital, enfrenta un desafío de reconfiguración conceptual para el que el tiempo disponible es significativamente menor de lo que el ritmo legislativo regional sugeriría.

El artículo se articula en seis secciones. La primera —esta introducción— establece el problema. La segunda examina la IA como herramienta de decisión judicial y sus implicaciones para las garantías procesales. La tercera analiza la blockchain y los contratos inteligentes como desafío al derecho contractual tradicional. La cuarta examina el error estructural de adopción tecnológica sin diagnóstico jurídico previo y sus consecuencias contractuales. La quinta propone un estándar de diligencia debida tecnológica para operadores jurídicos latinoamericanos. La sexta cierra con conclusiones y agenda de investigación.

2. La inteligencia artificial en la administración de justicia: cuando el algoritmo decide

2.1 De la asistencia a la sustitución: el espectro de la automatización judicial

La inteligencia artificial está presente en los sistemas de justicia latinoamericanos con una profundidad que supera la percepción pública. Sus aplicaciones actuales van desde la asistencia documental —clasificación automatizada de expedientes, extracción de información de fallos, generación de borradores de resoluciones— hasta la predicción de resultados procesales, el análisis de riesgo de reincidencia y la detección de patrones de corrupción en la gestión judicial. El espectro que va de la asistencia a la sustitución no es tecnológico: es jurídico, y depende de qué tipo de decisión está siendo automatizada y en qué medida.

La distinción relevante para el derecho no es entre sistemas de IA 'simples' y 'complejos': es entre sistemas que asisten decisiones que permanecen bajo autoría humana y sistemas que producen resultados que, en la práctica, determinan decisiones aunque formalmente las firme un humano. En el primer caso, el juez, el fiscal o el administrador que usa la IA como herramienta mantiene la responsabilidad jurídica plena sobre su decisión. En el segundo caso, la responsabilidad se diluye: el operador jurídico que no puede explicar cómo funciona el sistema que utilizó, ni auditar sus resultados, ni demostrar que ejerció un juicio independiente, opera en una zona de opacidad que vulnera garantías procesales fundamentales.

El caso COMPAS en los Estados Unidos —sistema de análisis predictivo de riesgo de reincidencia que, según un estudio de ProPublica de 2016, clasificaba incorrectamente a acusados afroamericanos como de alto riesgo con el doble de frecuencia que a acusados blancos— es el ejemplo más citado de esta categoría de riesgo. Pero sería un error tratarlo como una anomalía del sistema norteamericano. El problema de fondo —sistemas entrenados con datos históricos que incorporan sesgos estructurales del sistema penal y los reproducen con apariencia de objetividad matemática— es inherente a la tecnología, no a su contexto de implementación.

2.2 Las garantías procesales ante el algoritmo opaco

El uso de sistemas de IA en decisiones judiciales o administrativas que afectan derechos de personas plantea al menos cuatro categorías de tensión con las garantías procesales reconocidas en los sistemas jurídicos latinoamericanos.

La primera es el derecho a conocer los fundamentos de la decisión. En todos los sistemas procesales de la región, las resoluciones judiciales deben ser motivadas: el juez debe expresar las razones de hecho y de derecho que sostienen su decisión. Si esas razones incluyen el resultado de un sistema de IA cuyo funcionamiento interno no puede ser explicado —lo que en la literatura técnica se denomina el problema de la caja negra—, la motivación de la resolución es incompleta. El afectado no puede conocer los criterios reales que determinaron la decisión sobre sus derechos.

La segunda tensión es el derecho de contradicción y el debido proceso. Si el imputado, el demandado o el administrado no sabe que un sistema de IA participó en la decisión que lo afecta, no puede impugnarlo. Y si lo sabe pero el sistema es opaco, tampoco puede hacerlo con efectividad. El derecho de contradicción requiere que la parte afectada tenga acceso a los elementos que determinaron la decisión en su contra. Un algoritmo no auditable es, desde esta perspectiva, un elemento de prueba irrecurrible.

La tercera tensión es la igualdad ante la ley. Si un sistema de IA produce resultados sistemáticamente diferentes para personas de distintos grupos raciales, socioeconómicos o de género —como documenta la literatura sobre sesgos algorítmicos—, su uso en decisiones judiciales o administrativas reproduce y amplifica desigualdades estructurales bajo la apariencia de neutralidad técnica. Esta forma de discriminación es especialmente perniciosa porque es invisible: no hay intención discriminatoria identificable, solo un patrón estadístico heredado de datos históricos que reflejan un pasado desigual.

La cuarta tensión es la atribución de responsabilidad ante el error. Cuando un sistema de IA contribuye a una decisión judicial errónea que causa daño a una persona, ¿quién responde? ¿El juez que utilizó el sistema sin auditarlo? ¿El proveedor de la tecnología? ¿El Estado que la contrató? La respuesta a esta pregunta es jurídicamente incierta en todos los sistemas latinoamericanos, y esa incertidumbre es en sí misma un problema: la posibilidad de atribución de responsabilidad es una de las principales palancas de los sistemas jurídicos para incentivar el comportamiento diligente. Sin atribución clara, no hay incentivo para la cautela.

2.3 El estándar de la explicabilidad como requisito jurídico

El Reglamento de Inteligencia Artificial de la Unión Europea (2024) establece que los sistemas de IA utilizados en la administración de justicia son sistemas de alto riesgo, sujetos a requisitos estrictos de transparencia, documentación y supervisión humana. Este estándar —la explicabilidad como requisito jurídico, no como opción técnica— anticipa la dirección hacia la que convergerá la regulación latinoamericana en los próximos años.

Para los operadores jurídicos de la región, la implicación práctica es clara: cualquier sistema de IA utilizado en contextos que afecten derechos de personas debe poder explicar sus resultados en términos comprensibles para el operador jurídico que los utiliza y para la parte afectada. Un sistema que no puede ser explicado no debe ser utilizado en esos contextos. Y un operador jurídico que utiliza un sistema que no puede explicar asume una responsabilidad que no puede trasladar al proveedor de la tecnología.

La pregunta correcta no es '¿qué modelo de IA es el más avanzado?' Es '¿qué modelo de IA es el más pertinente para mi problema específico con mis datos específicos en mi contexto específico?' La pertinencia siempre gana sobre la sofisticación. (Cangelosi Sánchez, 2025, p. 63)

Aplicado al contexto judicial, este principio significa que un sistema de análisis predictivo de riesgo entrenado con datos del sistema penal de los Estados Unidos no es pertinente para la realidad del sistema penal de Perú o Ecuador, aunque sea técnicamente más sofisticado que cualquier alternativa local. La pertinencia contextual —incluyendo la pertinencia jurídica, procesal y cultural— es un requisito de legitimidad, no solo de eficacia.

3. Blockchain y contratos inteligentes: el desafío al derecho contractual

3.1 Qué es la blockchain desde una perspectiva jurídica

La tecnología blockchain es, en su esencia más simple, un registro distribuido, inmutable y verificable de transacciones. Cada bloque de información está criptográficamente enlazado al anterior, lo que hace que la modificación retroactiva de cualquier registro sea computacionalmente inviable. Esta característica —la inmutabilidad— es simultáneamente su principal virtud tecnológica y su principal desafío jurídico.

Desde una perspectiva jurídica, la blockchain ofrece tres capacidades que tienen relevancia directa para el derecho: primero, la certificación de existencia e integridad de documentos sin necesidad de un tercero de confianza centralizado; segundo, la trazabilidad inalterable de transacciones y cadenas de custodia; tercero, la ejecución automatizada de obligaciones contractuales a través de los denominados contratos inteligentes. Las tres capacidades tienen aplicaciones en el derecho contractual, notarial, registral y procesal que la práctica jurídica latinoamericana está comenzando a explorar, frecuentemente sin el marco conceptual adecuado.

3.2 El contrato inteligente y las categorías del derecho contractual

Un contrato inteligente (smart contract) es un programa informático desplegado en una red blockchain que ejecuta automáticamente las cláusulas de un acuerdo cuando se verifican las condiciones predefinidas en el código. Si la condición X ocurre, el sistema ejecuta la consecuencia Y sin intervención humana. Su atractivo es evidente: elimina la intermediación, reduce los costos de enforcement contractual y minimiza el riesgo de incumplimiento unilateral.

Pero desde la perspectiva del derecho contractual latinoamericano, el contrato inteligente plantea al menos cinco tensiones conceptuales que los operadores jurídicos deben comprender antes de asesorar sobre su uso.

La primera tensión es la de la forma contractual. Los sistemas jurídicos latinoamericanos, herederos de la tradición romano-germánica, reconocen en muchos supuestos requisitos formales para la validez o la eficacia de ciertos contratos: la escritura pública, la firma notarial, el registro. ¿Un contrato desplegado en código sobre una blockchain cumple esos requisitos formales? La respuesta varía por jurisdicción y por tipo de acto jurídico, y en la mayoría de los países de la región no existe todavía una respuesta legislativa o jurisprudencial definitiva.

La segunda tensión es la de la voluntad contractual y los vicios del consentimiento. El derecho contractual construye sobre la voluntad libre y consciente de las partes. Pero en un contrato inteligente, las consecuencias del acuerdo son ejecutadas automáticamente por el código, sin posibilidad de intervención posterior. Si una parte alega error, dolo, lesión o fuerza mayor, ¿puede invocar esos vicios del consentimiento para detener la ejecución de un código que ya se ejecutó o que está en proceso de hacerlo? La inmutabilidad de la blockchain colisiona frontalmente con los mecanismos de rescisión, nulidad y revisión judicial del contrato que el derecho contractual latinoamericano reconoce.

La tercera tensión es la de la jurisdicción y el derecho aplicable. Las redes blockchain son globales y descentralizadas: no tienen una sede jurídica identificable. Cuando surge una controversia en torno a un contrato inteligente entre partes ubicadas en distintos países, ¿qué tribunal es competente? ¿Qué derecho nacional se aplica? Las reglas de derecho internacional privado vigentes en la región fueron diseñadas para contratos entre partes con domicilios identificables, no para acuerdos ejecutados sobre infraestructuras distribuidas globalmente.

La cuarta tensión es la de la interpretación contractual. El derecho contractual latinoamericano reconoce que los contratos deben interpretarse de acuerdo con la intención real de las partes, la buena fe y la equidad. Pero el contrato inteligente no interpreta: ejecuta literalmente el código. Si el código no previó una situación —y ningún código puede prever todas las situaciones— el sistema ejecutará igualmente, aunque el resultado sea contrario a la intención real de las partes. La rigidez del código es la negación de la interpretación.

La quinta tensión es la de la reversibilidad y la reparación del daño. Cuando un contrato convencional produce un resultado injusto, el derecho ofrece mecanismos de reparación: la rescisión, la nulidad, la indemnización. Cuando un contrato inteligente produce un resultado injusto, la blockchain ya lo ejecutó y no puede deshacerse. La reparación, si es posible, debe buscarse fuera de la cadena, en el sistema judicial convencional. Pero ese sistema judicial convencional frecuentemente no sabe cómo tratar la evidencia blockchain ni cómo ejecutar una sentencia sobre un código distribuido globalmente.

3.3 Las oportunidades: trazabilidad, registro y prueba

Sería un error, sin embargo, que el análisis de las tensiones obscureciera las oportunidades reales que la blockchain ofrece al sistema jurídico latinoamericano. Las más relevantes son tres.

La primera es la certificación notarial digital. La blockchain permite generar una constancia criptográfica de la existencia e integridad de un documento en un momento determinado, sin necesidad de un tercero centralizado. Para el notariado latinoamericano, esto no es una amenaza de desintermediación sino una herramienta de ampliación: la certificación blockchain puede complementar la función notarial extendiendo su alcance a contextos donde la presencia física del notario es inviable, preservando al mismo tiempo la función de asesoramiento jurídico que ningún algoritmo puede sustituir.

La segunda oportunidad es la trazabilidad en cadenas de custodia y registros públicos. La blockchain puede mejorar significativamente la integridad de los registros de propiedad, los libros societarios, las cadenas de custodia de evidencia criminal y los registros de contratos públicos. Varios países de la región —incluyendo Chile, Colombia y México— tienen proyectos piloto en esta dirección. La resistencia a la manipulación que ofrece la blockchain es especialmente valiosa en contextos de alta desconfianza institucional.

La tercera oportunidad es la producción y valoración de la prueba. Un registro blockchain puede constituir prueba de la existencia, integridad y autoría de un documento digital con un nivel de certeza criptográfica superior al de los medios probatorios digitales tradicionales. El desarrollo de estándares procesales para la admisión y valoración de evidencia blockchain en los sistemas judiciales latinoamericanos es una tarea urgente que el derecho procesal de la región todavía no ha abordado con la sistematicidad necesaria.

4. El error jurídico de la adopción tecnológica sin diagnóstico

4.1 La dimensión contractual del fracaso tecnológico

El Índice Latinoamericano de Inteligencia Artificial 2025 (CENIA & CEPAL, 2025) documenta que el 44% de la fuerza laboral de la región presenta alta exposición a la automatización. Esta cifra coexiste con un patrón documentado de adopción tecnológica defectuosa: las organizaciones latinoamericanas —incluyendo las organizaciones del sector justicia— tienden a adquirir tecnología antes de diagnosticar con precisión el problema que pretenden resolver. El resultado no es solo un fracaso estratégico: es un fracaso jurídico con consecuencias contractuales concretas.

En una provincia de la región de Cuyo, Argentina, el propietario de una empresa familiar de transporte de carga invirtió el equivalente a cuarenta mil dólares en un sistema de IA para la optimización de rutas. Dos años después, el sistema no era utilizado. El problema real no era la planificación de rutas sino la comunicación entre conductores y el área administrativa. Cuarenta mil dólares para resolver el problema equivocado (Cangelosi Sánchez, 2025). Este caso, replicado con variaciones en innumerables organizaciones latinoamericanas, tiene una dimensión jurídica que el debate sobre transformación digital raramente aborda: el contrato suscrito con el proveedor de tecnología fue un contrato que especificaba características de la tecnología, no resultados verificables. El comprador no tenía base legal para reclamar por resultados insatisfactorios porque nunca acordó, contractualmente, cuáles deberían ser esos resultados.

4.2 Cuatro consecuencias jurídicas del error metodológico

La adopción de IA sin diagnóstico previo produce al menos cuatro categorías de consecuencias jurídicas que los operadores del derecho deben conocer para asesorar adecuadamente a sus clientes.

La primera es la indeterminación del objeto contractual. En los contratos de tecnología tradicional, el objeto es relativamente determinado. En los contratos de IA, el objeto es probabilístico: un sistema que predice, clasifica o genera resultados con cierto nivel de precisión bajo ciertas condiciones. Si el contrato no especifica los indicadores de desempeño verificables, los plazos de medición y los criterios de aceptación, la organización carece de base legal para reclamar por resultados insatisfactorios. La vaguedad del objeto contractual —frecuente cuando el comprador no ha diagnosticado su problema— beneficia estructuralmente al proveedor.

La segunda consecuencia es la pérdida de control sobre datos propios. Las implementaciones de IA requieren que la organización provea datos para el entrenamiento y operación del sistema. Si el contrato no establece con precisión la propiedad de esos datos, su tratamiento durante la vigencia del contrato, las condiciones de su destrucción o devolución al término de la relación comercial y los formatos de exportación, la organización corre el riesgo de perder el control sobre un activo estratégico que ha tardado años en construir. En el contexto del sector justicia, este riesgo tiene dimensiones adicionales: los datos de expedientes judiciales, perfiles de imputados o historiales procesales son datos sensibles cuyo tratamiento está sujeto a restricciones específicas que un contrato mal especificado puede vulnerar.

La tercera consecuencia es la exposición por sesgos algorítmicos no auditados. Cuando un sistema de IA produce resultados discriminatorios y la organización no puede demostrar que realizó una auditoría de sesgos razonable antes de su implementación, su exposición legal se amplía significativamente. En el sector privado, el caso de los sistemas de selección de personal que discriminan a candidatos por género o etnia es el más documentado. En el sector justicia, el riesgo es estructuralmente equivalente y jurídicamente más grave: los sesgos de un sistema de predicción de riesgo de reincidencia no solo producen un daño económico sino una vulneración de derechos fundamentales.

La cuarta consecuencia es la ausencia de mecanismos contractuales de responsabilidad. En la práctica contractual latinoamericana, los contratos de tecnología frecuentemente incluyen limitaciones de responsabilidad que exoneran al proveedor de daños derivados de resultados no

alcanzados. Un comprador que no ha establecido métricas verificables antes de la firma no tiene mecanismo para probar que los resultados prometidos no se alcanzaron. Y un comprador que no ha negociado cláusulas de ajuste o revisión ante incumplimiento asume todo el riesgo financiero y jurídico de la implementación.

5. Un estándar de diligencia debida tecnológica para operadores jurídicos

5.1 El principio rector: primero el diagnóstico jurídico

La diligencia debida tecnológica (technological due diligence) es la aplicación de los principios de investigación y análisis precontractual al proceso de adquisición de sistemas de inteligencia artificial y tecnología blockchain. Para los operadores jurídicos latinoamericanos —abogados, notarios, asesores de organizaciones del sector justicia—, el desarrollo de este estándar es una necesidad profesional urgente.

El principio rector de ese estándar debe ser el mismo que vertebra la práctica jurídica de calidad: primero el diagnóstico del problema, después la evaluación de la solución. Un operador jurídico que asesora a un cliente sobre la adquisición de un sistema de IA sin haber ayudado a definir con precisión el problema que el sistema debe resolver, los indicadores que medirán su éxito y los riesgos jurídicos asociados a su implementación, no está ejerciendo su función asesora con la diligencia que el mandato profesional le exige.

5.2 Las dimensiones del estándar

El estándar de diligencia debida tecnológica que se propone aquí opera en cinco dimensiones articuladas, aplicables tanto a la asesoría a organizaciones privadas como al asesoramiento en el sector justicia.

La primera dimensión es el diagnóstico jurídico del problema. Antes de evaluar cualquier solución tecnológica, el operador jurídico debe ayudar a su cliente a responder: ¿cuál es el problema jurídico u organizacional específico que la tecnología pretende resolver? ¿Qué evidencia existe de que ese es el problema real? ¿Qué indicadores jurídicamente verificables medirán la resolución exitosa del problema? ¿Qué datos propios son necesarios y en qué condición están? Esta dimensión del diagnóstico es una extensión directa de la función que los operadores jurídicos ya ejercen en otros contextos: la identificación rigurosa del problema antes de la prescripción de la solución.

La segunda dimensión es la evaluación jurídica del proveedor. La diligencia sobre el proveedor debe incluir: verificación del marco de gobernanza de datos; análisis de las cláusulas de propiedad intelectual y de portabilidad de datos; evaluación de los mecanismos de responsabilidad ante resultados fallidos; y revisión de las condiciones de salida del contrato. Un proveedor que no puede demostrar que sus sistemas han sido auditados para sesgos, que no acepta cláusulas de portabilidad de datos, o que incluye limitaciones de responsabilidad irrazonables, presenta señales de alerta que el operador jurídico debe identificar y comunicar a su cliente.

La tercera dimensión es la arquitectura contractual específica para IA y blockchain. Los contratos de tecnología en estos ámbitos deben especificar al menos los siguientes elementos: el problema que el sistema se compromete a resolver, expresado en términos verificables; los indicadores de desempeño y los plazos de medición; la propiedad, tratamiento, portabilidad y destrucción de los datos; las cláusulas de auditoría de sesgos y supervisión humana para decisiones de alto impacto; los mecanismos de responsabilidad ante resultados no alcanzados o daños a terceros; las

condiciones de salida del contrato y los costos de migración; y la ley aplicable y la jurisdicción competente para controversias.

La cuarta dimensión es el asesoramiento sobre gobernanza interna. El operador jurídico debe ayudar a su cliente a construir una estructura de gobernanza interna que incluya: un inventario de los sistemas de IA en uso y su clasificación por nivel de riesgo; protocolos de supervisión humana para decisiones de alto impacto; mecanismos de transparencia hacia las personas afectadas por decisiones automatizadas; y revisiones periódicas de sesgos en los sistemas de mayor impacto. Esta dimensión de la gobernanza no es solo una recomendación de buenas prácticas: es una forma de construir la posición defensiva de la organización ante potenciales reclamos legales.

La quinta dimensión es la anticipación regulatoria. El operador jurídico que asesora sobre tecnología tiene la responsabilidad de informar a su cliente sobre el marco regulatorio emergente y sus implicaciones prácticas. El Reglamento de Inteligencia Artificial de la Unión Europea (2024), la normativa sectorial en desarrollo en Chile, Colombia, México y Argentina, y los marcos de protección de datos vigentes en la región, configuran un entorno regulatorio en rápida evolución que afecta directamente las decisiones de adopción tecnológica que las organizaciones toman hoy.

5.3 Las preguntas que el operador jurídico debe poder responder

Un operador jurídico que asesora sobre adquisiciones de IA o sobre el uso de contratos inteligentes blockchain debe ser capaz de responder, con información concreta, al menos las siguientes preguntas antes de emitir su consejo profesional:

- ¿El contrato especifica el problema que el sistema se compromete a resolver, o solo describe sus características técnicas?
- ¿El contrato garantiza la propiedad y portabilidad de los datos del cliente en formatos estándar al término de la relación?
- ¿Existen cláusulas de auditoría de sesgos y mecanismos de supervisión humana para decisiones de alto impacto?
- ¿El contrato establece métricas verificables de desempeño y consecuencias jurídicas ante su incumplimiento?
- ¿El sistema de IA puede explicar sus resultados en términos comprensibles para el operador jurídico y para la parte afectada?
- En el caso de contratos inteligentes blockchain: ¿cuál es la ley aplicable y la jurisdicción competente? ¿Qué mecanismos existen para la revisión judicial del contrato ante vicios del consentimiento o resultados injustos?
- ¿El proveedor tiene referencias verificables de implementaciones similares en el mismo contexto jurídico regional?
- ¿El cliente puede realizar un piloto acotado antes de comprometer el contrato completo?

La incapacidad de responder cualquiera de estas preguntas no es una deficiencia técnica: es una señal de alerta jurídica que el operador debe comunicar a su cliente antes de avanzar en la negociación.

6. Conclusiones y agenda de investigación

Este artículo ha argumentado que la inteligencia artificial y la tecnología blockchain plantean al derecho latinoamericano un desafío de reconfiguración conceptual que va más allá de la actualización normativa. Las categorías jurídicas fundamentales de autoría, responsabilidad, forma contractual, voluntad, jurisdicción y prueba requieren ser repensadas desde sus fundamentos para operar con coherencia en un entorno tecnológico que las cuestiona estructuralmente.

El análisis de la IA en la administración de justicia revela que la tensión entre los algoritmos opacos y las garantías procesales —motivación de la resolución, derecho de contradicción, igualdad ante la ley, atribución de responsabilidad— no puede ser resuelta con la sola adición de regulación técnica. Requiere que los operadores jurídicos comprendan lo suficiente sobre cómo funcionan estos sistemas para ejercer el control jurídico que les corresponde.

El análisis de la blockchain y los contratos inteligentes revela que la inmutabilidad del código colisiona frontalmente con los mecanismos de revisión, nulidad e interpretación que el derecho contractual latinoamericano reconoce, mientras que sus capacidades de trazabilidad y certificación abren oportunidades reales para el derecho notarial, registral y procesal que la práctica jurídica de la región está comenzando a explorar.

El análisis del error estructural de adopción tecnológica sin diagnóstico jurídico previo revela que las consecuencias de ese error no son solo operativas o financieras, sino jurídicas: contratos mal especificados que transfieren todo el riesgo al comprador, datos organizacionales sin protección adecuada, sesgos algorítmicos no auditados y ausencia de mecanismos contractuales de responsabilidad.

El estándar de diligencia debida tecnológica propuesto para operadores jurídicos latinoamericanos opera en cinco dimensiones: diagnóstico jurídico del problema, evaluación jurídica del proveedor, arquitectura contractual específica para IA y blockchain, asesoramiento sobre gobernanza interna, y anticipación regulatoria. Su implementación no requiere que el abogado o el notario se convierta en ingeniero de sistemas: requiere que comprenda los riesgos jurídicos específicos de estas tecnologías y que incorpore esa comprensión a su práctica asesora.

La agenda de investigación que emerge de este análisis incluye al menos tres líneas prioritarias: primero, el desarrollo de marcos comparados de responsabilidad civil ante decisiones automatizadas en los distintos sistemas jurídicos latinoamericanos; segundo, el análisis de la jurisprudencia emergente sobre contratos inteligentes y evidencia blockchain en los países con mayor desarrollo en la materia; tercero, el diseño de estándares formativos para la incorporación de la diligencia debida tecnológica en los programas de formación jurídica de la región. El derecho latinoamericano tiene la tradición conceptual para responder a estos desafíos. La pregunta es si lo hará a tiempo.

Referencias

- Cangelosi Sánchez, D. H. (2025). Primero el problema, después la tecnología: guía práctica de inteligencia artificial para empresarios latinoamericanos. Fundación SalEduDis / Edición del autor.
- CENIA & CEPAL (2025). Índice Latinoamericano de Inteligencia Artificial (ILIA) 2025. Comisión Económica para América Latina y el Caribe, Santiago. <https://www.cepal.org/es/publicaciones/82514-indice-latinoamericano-inteligencia-artificial-ilia-2025>

- CEPAL (2024). Inteligencia artificial y transformación digital en América Latina y el Caribe. Comisión Económica para América Latina y el Caribe, Santiago. https://conferenciaelac.cepal.org/9/sites/elac9/files/s2401013_es.pdf
- Comisión Europea (2024). Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial). Diario Oficial de la Unión Europea. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689>
- Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine Bias. ProPublica. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
- Acemoglu, D., & Johnson, S. (2023). Power and Progress: Our Thousand-Year Struggle Over Technology and Prosperity. PublicAffairs. ISBN: 978-1-541-70253-0
- Kissinger, H. A., Mundie, C., & Schmidt, E. (2024). Genesis: Artificial Intelligence, Hope, and the Human Spirit. Little, Brown and Company.
- Lee, K.-F. (2018). AI Superpowers: China, Silicon Valley, and the New World Order. Houghton Mifflin Harcourt. ISBN: 978-1-328-54639-5
- Ng, A. (2019). AI for Everyone [Curso en línea]. DeepLearning.AI / Coursera. <https://www.coursera.org/learn/ai-for-everyone>
- Superintendencia Financiera de Colombia (2023). Principios para el uso de Inteligencia Artificial en el sector financiero colombiano. Superintendencia Financiera de Colombia, Bogotá.
- Szabo, N. (1994). Smart Contracts. Recuperado de <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>
- UNCITRAL (2016). Notas de la CNUDMI sobre la organización del proceso arbitral. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Viena. https://uncitral.un.org/es/texts/arbitration/explanatorytexts/organizing_arbitral_proceedings

Nota sobre el autor

Daniel Horacio Cangelosi Sánchez es Doctor en Educación por la Universidad Católica de Córdoba (Argentina, 2023) y cuenta con más de treinta y seis años de experiencia en educación, inclusión, salud y políticas públicas en más de catorce países de América Latina y Europa. Es Presidente de la Fundación Salud, Educación y Discapacidad (SalEduDis), Investigador Colaborador del Centro Nacional de Inteligencia Artificial de Chile (CENIA) Director de tesis de posgrado en la Universidad de Cartagena, Colombia y Profesor Asociado de la Universidad de la Marina Mercante. Su investigación se focaliza en la intersección entre inteligencia artificial, gobernanza organizacional e inclusión desde una perspectiva empírica y comparada.

ORCID: 0000-0002-5291-5750 | cangelosisanchez@gmail.com

Declaración de conflicto de intereses: el autor declara que el libro citado como fuente principal (Cangelosi Sánchez, 2025) es de su autoría. No existe financiamiento externo ni conflicto de intereses adicional.