

Personalidad jurídica de los sistemas autónomos: un debate necesario

Escrito por: Fernando Esteban Quiroz Ponce, Juan Antonio
Zevallos Cadillo, Eladio Guzmán Villa, Fausto David Berrocal
Huarcaya, Gloria Gonzales Santos, Joel Orlando Santillán Tuesta

ISBN: 978-9915-698-70-0



9 789915 698700

Personalidad jurídica de los sistemas autónomos: un debate necesario

Quiroz Ponce, Fernando Esteban; Zevallos Cadillo, Juan Antonio; Guzmán Villa, Eladio; Berrocal Huarcaya, Fausto David; Gonzales Santos, Gloria; Santillán Tuesta, Joel Orlando

© Quiroz Ponce, Fernando Esteban; Zevallos Cadillo, Juan Antonio; Guzmán Villa, Eladio; Berrocal Huarcaya, Fausto David; Gonzales Santos, Gloria; Santillán Tuesta, Joel Orlando, 2026

Primera edición (1.^a ed.): febrero, 2026

Editado por:

Editorial Mar Caribe ®

www.editorialmarcaribe.es

Av. Gral. Flores 547, 70000 Col. del Sacramento, Departamento de Colonia, Uruguay.

Diseño de carátula e ilustraciones: *Luisa Fernanda Lugo Rojas*

Libro electrónico disponible en:

<https://editorialmarcaribe.es/ark:/10951/isbn.9789915698700>

Formato: Electrónico

ISBN: 978-9915-698-70-0

ARK: [ark:/10951/isbn.9789915698700](https://nbn-resolving.org/urn:nbn:org:arameo:net-10951-isbn.9789915698700)

Editorial Mar Caribe (OASPA): Como miembro de la Open Access Scholarly Publishing Association, apoyamos el acceso abierto de acuerdo con el código de conducta, la transparencia y las mejores prácticas de OASPA para la publicación de libros académicos y de investigación. Estamos comprometidos con los más altos estándares editoriales en ética y deontología, bajo la premisa de «Ciencia Abierta en América Latina y el Caribe»

OASPA

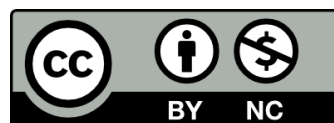
Editorial Mar Caribe, firmante N° 795 de 12.08.2024 de la Declaración de Berlín

"... Nos sentimos obligados a abordar los retos de Internet como un medio funcional emergente para la distribución del conocimiento. Obviamente, estos avances pueden modificar significativamente la naturaleza de la publicación científica, así como el actual sistema de garantía de calidad...." (Max Planck Society, ed. 2003, pp. 152-153).



CC BY-NC 4.0

Los autores pueden autorizar al público en general a reutilizar sus obras únicamente con fines no lucrativos, los lectores pueden utilizar una obra para generar otra, siempre que se dé crédito a la investigación, y conceden al editor el derecho a publicar primero su ensayo bajo los términos de la licencia CC BY-NC 4.0.



Editorial Mar Caribe se adhiere a la "Recomendación relativa a la preservación del patrimonio documental, comprendido el patrimonio digital, y el acceso al mismo" de la UNESCO y a la Norma Internacional de referencia para un sistema abierto de información archivística (OAIS-ISO 14721). Este libro está preservado digitalmente por ARAMEO.NET

ARAMEO.NET

Editorial Mar Caribe

**Personalidad jurídica de los sistemas autónomos:
un debate necesario**

Colonia, Uruguay

2026

**Personalidad jurídica de los sistemas autónomos:
un debate necesario**

Índice

Introducción	9
Capítulo 1	12
Personalidad jurídica de los sistemas autónomos: un debate necesario.....	12
Fundamentos ontológicos y la construcción de la personalidad jurídica	12
La dialéctica entre la ficción y la realidad técnica.....	13
El precedente del Parlamento Europeo: de la audacia a la cautela.....	14
Evolución hacia el Reglamento de Inteligencia Artificial (AI Act)	15
Responsabilidad civil y el desafío de la autonomía algorítmica	16
El agotamiento de los marcos tradicionales de responsabilidad.....	16
Seguros y transferencia de riesgo en el horizonte de 2026.....	17
Propiedad intelectual y el requisito de autoría humana	18
La sentencia de la Corte Suprema de EE.UU. en el caso Thaler (2026) ...	18
Originalidad y el nexo humano-máquina	19
El escenario en América Latina: regulación y ética en Perú	19
La Ley 31814 y el Reglamento de IA en Perú (2025)	20
Gobernanza global y estándares técnicos: la infraestructura de la confianza	21
El rol de ISO/IEC JTC 1/SC 42 y la UIT.....	21
Transparencia y el estándar IEEE 7001	22
La figura del agente electrónico y la capacidad de contratar.....	22
Autonomía operativa vs. personalidad legal	22
Principios de la Ley Modelo sobre Comercio Electrónico.....	23
Riesgos sistémicos y el dilema de la evidencia	23
El dilema de la evidencia para los legisladores.....	24
El impacto en el mercado laboral y la seguridad nacional.....	24
Conclusión: hacia un equilibrio entre innovación y dignidad.....	25
Capítulo 2	27
Gobernanza global y estándares técnicos: la infraestructura de la confianza	

.....	27
El horizonte post-2026 y la transición hacia el poder algorítmico.....	28
Modelos divergentes de gobernanza: EE.UU., China y la Unión Europea	30
Arquitectura y procesos de decisión en los organismos de normalización (SDOs)	31
Comparativa de Gobernanza en SDOs Principales	32
El proceso de normalización en ISO/IEC	32
Gobernanza de la Inteligencia Artificial: ISO 42001 e IEEE 7000	33
Fragmentación del Internet y el surgimiento del Splinternet	35
Tipos de fragmentación y sus catalizadores	35
China como arquitecto de reglas y líder en propiedad intelectual.....	36
Riesgos y Mitigaciones en la Interfaz Técnica-Derechos	38
Panorama de Estándares de Blockchain	39
El Pacto Digital Global y la cooperación de la ONU	40
Desafíos para los países en desarrollo y la brecha de estandarización	41
Barreras identificadas para la implementación de estándares técnicos..	41
Síntesis y Prospectiva Estratégica	42
Capítulo 3	44
Personalidad jurídica del robot: Autonomía, autoaprendizaje y adaptación ..	44
Evolución histórica y fundamentos ontológicos del debate	44
Categorización técnica y legal de los agentes inteligentes	45
Teorías doctrinales sobre la personalidad del robot	46
El enfoque tradicional: el robot como objeto de derecho	46
La propuesta de la personalidad electrónica del Parlamento Europeo....	47
Modelos intermedios y analogías históricas	47
Autonomía, autoaprendizaje y adaptación: el desafío técnico al Derecho ..	48
El fenómeno de la caja negra y el nexo causal.....	48
Adaptación y riesgos de desarrollo.....	48
Modelos de responsabilidad y mecanismos de reparación	49
Seguros obligatorios y fondos de garantía	49

Responsabilidad penal y penas para robots	50
Impacto económico, fiscal y laboral de los robots autónomos	50
El robot como contribuyente	50
La robótica y el derecho al trabajo	51
El marco regulatorio en el Perú y Latinoamérica.....	51
La Ley N° 31814 y el Reglamento de 2025.....	51
Iniciativas legislativas y el Registro de IA de Alto Riesgo.....	52
Propiedad Intelectual y creaciones de la Inteligencia Artificial.....	52
Autoría y titularidad	52
El uso de datos para entrenamiento.....	53
Ética y gobernanza global de la inteligencia artificial.....	53
Principios éticos fundamentales	53
El derecho a la atención humana.....	54
Capítulo 4	56
Inteligencia artificial: capacidad jurídica funcional para fines comerciales y de responsabilidad	56
Fundamentos ontológicos y dogmáticos de la personalidad en el entorno digital	56
La manifestación de voluntad y el perfeccionamiento del contrato algorítmico.....	58
El consentimiento en la contratación electrónica.....	58
Agentes electrónicos y Smart Contracts.....	59
El marco regulatorio peruano: Análisis de la Ley N° 31814 y su Reglamento	59
Clasificación de riesgos y niveles de cumplimiento.....	60
Gobernanza y el rol de la SGTD	60
Regímenes de responsabilidad civil por daños algorítmicos.....	61
Responsabilidad objetiva y el riesgo creado	61
Propuestas de armonización de la Unión Europea.....	62
Desafíos probatorios y el impacto de la IA en la justicia peruana.....	62
El problema de la motivación y la Caja Negra	63

La prueba digital y la pericia informática	63
El rol del seguro y los fondos de garantía en la gestión del riesgo.....	64
Seguros de responsabilidad civil cibernética	64
La analogía del SOAT y fondos de compensación	64
Consideraciones éticas, sociales y el futuro del empleo.....	65
El reto de la informalidad y la alfabetización digital	65
Responsabilidad penal y protección de menores	65
Capítulo 5	68
Propiedad Intelectual ante la Irrupción de la Inteligencia Artificial Generativa: Autoría, Patentabilidad y Gobernanza de Datos	68
El Diálogo Multilateral y la Construcción de una Gobernanza Global.....	69
Cronología y Enfoque de las Sesiones de la Conversación de la OMPI	70
Teorías Fundamentales y el Conflicto de la Autoría No Humana	70
El Marco Regulatorio de los Estados Unidos: Directrices y Litigios Paradigmáticos.....	72
Requisitos de Registro y Deber de Transparencia.....	72
La Batalla de Stephen Thaler y la Denegación de la Agencia de la Máquina	73
El Enfoque de la Unión Europea: El Reglamento de IA y la Minería de Datos	74
Transparencia como herramienta de cumplimiento	74
El Código de Buenas Prácticas y los Desafíos de Implementación	75
Jurisprudencia en América Latina: México, Perú y el Blindaje Humanista..	76
La Resolución de la Suprema Corte de Justicia de México (2025)	76
INDECOPI en Perú: Lineamientos Éticos y Resoluciones Administrativas	77
Patentes e Inventiva: El Desafío de DABUS a Nivel Global.....	78
Litigios sobre Datos de Entrenamiento: ¿Uso Legítimo o Infracción Masiva?	79
Análisis de Casos Recientes de Fair Use (2025)	79
El Futuro de la Regulación: Derechos Sui Generis y Transparencia Técnica	80

Síntesis de la Transformación del Paisaje Legal.....	81
Capítulo 6	83
Robots e IA como sujetos de derecho: Desenredando la perspectiva ontológica y funcional	83
La construcción jurídica de la persona: De la máscara romana a la abstracción kelseniana	84
Evolución etimológica y teórica del concepto de persona	84
La Perspectiva Ontológica: El ser, la dignidad y la crítica al personismo ...	85
La dignidad humana como límite infranqueable.....	86
El problema de la conciencia: Simulación frente a realidad	86
La falacia mereológica en el discurso de la IA	87
La Perspectiva Funcional: ¿Es necesaria la personalidad electrónica?	87
El modelo de la Resolución Europea de 2017	88
El riesgo de impunidad y el escudo corporativo	88
El efecto de la caja negra y la ruptura del nexo causal	89
El Liability Sponge y la supervisión humana.....	90
Propiedad Intelectual e Invención: El desafío de la autoría no humana ...	90
El caso DABUS y la doctrina de la personalidad	91
El marco normativo en el Perú: Hacia una gobernanza ética y antropocéntrica	91
Clasificación de Riesgos y Obligaciones	92
Responsabilidad y Agravantes Penales: Ley 32314	92
Ética Global y el Fin del Modelo Autoregulatorio	93
Los Principios de la OCDE y la Gobernanza Adaptativa	93
Conclusión	95
Bibliografía	98

Introducción

La civilización moderna está experimentando una transformación profunda impulsada por el aumento de la capacidad de cómputo, la perfección de los algoritmos de aprendizaje profundo y la incorporación de la inteligencia artificial en procesos fundamentales de la vida social, económica y jurídica. Lo que antes parecía propio de la ciencia ficción —como la existencia de entidades no humanas que toman decisiones con impacto real en el mundo— ahora es una realidad en sistemas de conducción autónoma, diagnósticos médicos asistidos, transacciones financieras de alta frecuencia y sistemas de armas con funciones de selección de objetivos. Ante esto, el ordenamiento jurídico enfrenta una de sus crisis de identidad más significativas: la insuficiencia de las categorías tradicionales de persona y de cosa para abarcar la fenomenología de la autonomía técnica.

Esta obra busca analizar el debate sobre la personalidad jurídica de los sistemas autónomos, no como una mera reflexión teórica, sino como una necesidad urgente para asegurar la justicia, la seguridad jurídica y la protección de los derechos fundamentales en el siglo XXI. La evolución de las máquinas reactivas a agentes proactivos que aprenden y cambian de forma independiente del control humano rompe el vínculo causal y los criterios de responsabilidad que han guiado el Derecho desde la época clásica.

Para fundamentar un debate jurídico riguroso, es esencial partir de una delimitación técnica precisa. La inteligencia artificial no es una tecnología unívoca, sino un conjunto de aplicaciones y dispositivos capaces de percibir su entorno, procesar información, aprender de la experiencia y actuar de manera

independiente para alcanzar objetivos específicos. Esta autonomía funcional es la que permite a un sistema actuar sin necesidad de una intervención humana constante, reemplazando, en muchos casos, la inteligencia o el juicio del operador.

En este escenario, incluso los desarrolladores originales pueden no ser capaces de explicar con precisión por qué un sistema llegó a una conclusión específica o ejecutó una maniobra determinada. Esta opacidad algorítmica es la que motiva la necesidad de la explicabilidad e interpretabilidad como valores éticos y legales, pues un sistema que no puede ser comprendido difícilmente puede estar sujeto a los criterios tradicionales de culpa o negligencia.

El concepto de persona en el Derecho ha sido históricamente una construcción técnica y funcional, no un dato biológico inmutable. La etimología del término remite a la *persona* o máscara del teatro dramático griego, la investidura que permitía a un actor representar un papel en la escena; de igual modo, la personalidad jurídica es la investidura configurada por el derecho positivo que permite que un ente sea sujeto de derechos y obligaciones.

En el Derecho Romano, la personalidad no era un atributo intrínseco de todo ser humano; la esclavitud representaba la existencia de hombres tratados legalmente como cosas (*res*), carentes de personalidad hasta que el orden jurídico decidiera lo contrario. Con la evolución de la civilización contemporánea, la personalidad se reconoció como un derecho inalienable de todo ser humano, pero, simultáneamente, se extendió a entidades abstractas —las personas jurídicas o morales— para servir fines colectivos que superaban

la capacidad individual.

La premisa: El principal motor para considerar la personalidad jurídica de la inteligencia artificial es la búsqueda de una solución al vacío de responsabilidad que surge cuando un sistema autónomo causa un daño de manera imprevisible.

La situación actual: La normativa peruana destaca por ser de las primeras en América Latina en crear un marco de gobernanza enfocado en la seguridad, la ética y la transparencia, en línea con los estándares de la OCDE y la UNESCO. En lugar de otorgar personalidad jurídica a los sistemas de IA, el marco en Perú opta por una regulación rigurosa según el nivel de riesgo de las aplicaciones.

El debate en este libro aborda temas aún más innovadores, como el transhumanismo, que busca combinar capacidades tecnológicas con la biología humana. Esto ha generado conversaciones sobre los neuroderechos, con el fin de proteger la privacidad mental y la integridad de los pensamientos frente a interfaces cerebro-computadora impulsadas por inteligencia artificial. En este contexto, hablar de la personalidad de los sistemas autónomos es solo una pequeña parte de una discusión más amplia sobre qué significa ser un sujeto de derechos en una época de integración tecnológica.

Capítulo 1

Personalidad jurídica de los sistemas autónomos: un debate necesario

El vertiginoso avance de la inteligencia artificial y la consolidación de sistemas robóticos con capacidades de aprendizaje profundo han situado a la ciencia jurídica ante uno de sus desafíos más trascendentales desde la creación de las ficciones corporativas en el siglo XIX. La discusión sobre si un sistema autónomo debe o puede ser sujeto de derechos y obligaciones no es una mera disquisición teórica, sino una respuesta pragmática a la creciente brecha de responsabilidad que surge cuando las decisiones de una máquina dejan de ser previsibles para sus creadores humanos. Este fenómeno, que la doctrina contemporánea analiza bajo la lupa de la personalidad jurídica, exige una revisión exhaustiva de los fundamentos ontológicos del Derecho, de las necesidades del tráfico mercantil y de la protección de los derechos fundamentales ante una tecnología que ya no solo ejecuta, sino que decide y crea.

Fundamentos ontológicos y la construcción de la personalidad jurídica

La noción de persona en el ordenamiento jurídico ha sido históricamente una categoría elástica, diseñada para servir a fines sociales y

económicos específicos. La distinción entre la persona natural, vinculada a la condición humana y su dignidad intrínseca, y la persona jurídica, entendida como una ficción técnica para la organización de intereses, constituye el eje central del debate sobre la inteligencia artificial. La posibilidad de atribuir personalidad a sistemas tecnológicos se fundamenta, en gran medida, en la analogía con las sociedades comerciales, en las que el Derecho admite que un ente abstracto responda como sujeto independiente, a fin de facilitar la gestión de riesgos y la imputación de obligaciones.

Sin embargo, esta asimilación encuentra una profunda resistencia en la doctrina que defiende la centralidad de la persona humana. Se argumenta que la persona jurídica natural es el sustrato necesario de la personalidad positiva y su condición de existencia, por lo que otorgar tal estatus a un programa de software o a un robot sofisticado supondría una asimilación imposible que contraviene los principios constitucionales del Derecho Civil. Detrás de estas propuestas, algunos autores identifican un trasfondo transhumanista que busca desplazar al ser humano del centro del sistema normativo, lo que podría generar una inseguridad jurídica sin precedentes al saturar el ordenamiento de ficciones carentes de una base moral o biológica (Amershi et al., 2019).

La dialéctica entre la ficción y la realidad técnica

En la tradición de las ficciones jurídicas, se observa que el nombre persona actúa como detonante que facilita el acceso a situaciones complejas, unificando los actos de múltiples sujetos bajo un solo centro de imputación. Los defensores de la personalidad electrónica sostienen que si el Derecho ya ha disociado la personalidad del sustrato humano en el caso de las

corporaciones o incluso de ciertos ecosistemas, no existe un impedimento ontológico absoluto para negársela a la inteligencia artificial. En este sentido, la personalidad funcionaría como un atajo mental para resolver problemas de responsabilidad civil, permitiendo que el sistema autónomo cuente con un patrimonio propio o esté vinculado a un fondo de compensación.

A pesar de la elegancia técnica de estas propuestas, la doctrina advierte que el uso de la personalidad jurídica para sistemas autónomos podría repetir los errores del modelo corporativo, en el que a menudo se utiliza el velo de la persona jurídica para blindar a los verdaderos controladores frente a las reclamaciones de las víctimas que no pueden renegociar el riesgo. Así, la creación de una personalidad electrónica podría derivar en una transferencia desigual del riesgo empresarial a entidades abstractas sin solvencia real, lo que desprotegería a los perjudicados por el funcionamiento de dichos sistemas.

El precedente del Parlamento Europeo: de la audacia a la cautela

Uno de los hitos fundamentales en este debate fue la resolución del Parlamento Europeo de 16 de febrero de 2017, que recomendó a la Comisión Europea explorar la creación de un estatus de persona electrónica para los robots autónomos más sofisticados. Esta propuesta, liderada por la eurodiputada Mady Delvaux, partía de la premisa de que la creciente autonomía de las máquinas impedía rastrear las decisiones hasta un programador o fabricante específico, lo que generaba un vacío legal ante los

daños accidentales.

La resolución definía un robot inteligente en función de criterios como la adquisición de autonomía mediante sensores, el intercambio de datos con su entorno y la capacidad de aprender a partir de la experiencia. Sin embargo, la propuesta desencadenó una respuesta crítica masiva por parte de la comunidad científica y académica. Más de 150 expertos en robótica, ética y derecho firmaron una carta abierta en la que se opusieron al concepto, argumentando que otorgar derechos de persona a los robots entraría en conflicto con los derechos humanos fundamentales y que los marcos de responsabilidad civil existentes podían adaptarse sin necesidad de otorgarles personalidad jurídica (Albisua & Pacheco, 2025).

Evolución hacia el Reglamento de Inteligencia Artificial (AI Act)

La tensión interna en el propio Parlamento se reflejó en las votaciones, en las que un sector significativo de eurodiputados intentó eliminar la cláusula sobre la personalidad electrónica del texto final. Con el paso de los años, el enfoque de la Unión Europea ha virado de la asignación de personalidad a una gobernanza basada en el riesgo, materializada en el Reglamento de Inteligencia Artificial (AI Act), que entró en vigor en agosto de 2024.

Este reglamento evita otorgar explícitamente personalidad jurídica a los sistemas de inteligencia artificial y, en su lugar, establece obligaciones estrictas para proveedores y usuarios profesionales en función del riesgo potencial de cada sistema. El enfoque preventivo del AI Act busca garantizar que la IA sea ética y segura, protegiendo los derechos fundamentales

mediante la supervisión humana y la transparencia, antes que mediante la creación de nuevos sujetos de derecho.

Este cambio de paradigma sugiere que, por el momento, el legislador comunitario ha descartado la personalidad electrónica a favor de una responsabilidad centrada en la cadena de valor humana y empresarial, aunque la rápida evolución de la robótica podría hacer resurgir la hipótesis en un futuro cercano.

Responsabilidad civil y el desafío de la autonomía algorítmica

El corazón del debate sobre la personalidad jurídica radica en la necesidad de reparar los daños causados por sistemas que operan de forma autónoma e impredecible. Cuando un vehículo autónomo provoca un accidente o un algoritmo de diagnóstico médico comete un error, las reglas tradicionales de responsabilidad basadas en la culpa o en el producto defectuoso enfrentan obstáculos probatorios significativos.

El agotamiento de los marcos tradicionales de responsabilidad

La responsabilidad por productos defectuosos, regulada en Europa por la Directiva 85/374/CEE (actualizada en 2022), se centra en los daños causados por un defecto existente al momento de la comercialización. No obstante, los sistemas de inteligencia artificial que continúan aprendiendo tras su despliegue pueden desarrollar comportamientos nocivos que no estaban

presentes inicialmente, lo que dificulta la imputación de responsabilidad al fabricante original. Ante esto, la Comisión Europea propuso la Directiva de Responsabilidad de la IA para facilitar la prueba de la causalidad mediante presunciones legales cuando se demuestre el incumplimiento de las obligaciones de cuidado.

A pesar de estos avances, algunos sectores doctrinales insisten en que la personalidad jurídica facilitaría la creación de seguros obligatorios y de fondos de compensación vinculados directamente al sistema autónomo. Este modelo se asemejaría al seguro obligatorio de automóviles, pero con la particularidad de que el propio robot o sistema sería el titular de la póliza o del fondo de garantía, asegurando la reparación de la víctima incluso cuando el responsable humano resultara difícil de identificar o careciera de recursos.

Seguros y transferencia de riesgo en el horizonte de 2026

En la actualidad, el mercado de seguros ha comenzado a incorporar cláusulas específicas para sistemas de inteligencia artificial, diferenciando entre errores de diseño, fallos operativos y ataques externos. Las aseguradoras exigen ahora divulgaciones detalladas sobre los niveles de autonomía y el grado de supervisión humana, e implementan sublímites para riesgos como la discriminación algorítmica o las decisiones autónomas no supervisadas.

La obligatoriedad de estos seguros varía según la actividad económica, siendo ya indispensable para profesionales y entidades sanitarias que operan con sistemas de soporte vital o de diagnóstico automatizado. Sin embargo, persiste el temor de que la complejidad de estos sistemas genere lagunas de cobertura que requieran la intervención del Estado mediante fondos de

garantía de última instancia.

Propiedad intelectual y el requisito de autoría humana

Uno de los campos en los que la negativa a otorgar personalidad jurídica a la inteligencia artificial ha tenido consecuencias más inmediatas es el de la propiedad intelectual. El debate se centra en si una obra generada de forma autónoma por un algoritmo puede ser objeto de derechos de autor o de patente, y quién debe ser el titular de dichos derechos.

La sentencia de la Corte Suprema de EE.UU. en el caso Thaler (2026)

El 2 de marzo de 2026, la Corte Suprema de los Estados Unidos puso fin a una larga batalla legal al denegar la revisión del caso *Thaler v. Perlmutter*. El Dr. Stephen Thaler había intentado registrar como autor a su sistema de inteligencia artificial, DABUS, de una obra visual generada sin intervención humana directa. La decisión de la Corte ratificó los fallos de las instancias inferiores que sostienen que la autoría humana es un requisito fundamental del derecho de autor en la legislación estadounidense.

Esta postura se alinea con la tendencia global que considera la inteligencia artificial como una herramienta sofisticada, similar a un pincel o a una cámara fotográfica, pero carente de la capacidad de concepción intelectual que define al autor o al inventor. En noviembre de 2025, la USPTO ya había actualizado sus directrices para reforzar que solo las personas naturales

pueden ser nombradas como inventores, incluso cuando la IA haya desempeñado un papel significativo en el proceso creativo.

Originalidad y el nexo humano-máquina

La distinción crítica en la práctica legal actual radica en el grado de intervención humana. Las obras creadas totalmente por IA no son elegibles para el registro, pero aquellas en las que un humano proporciona una dirección sustancial, selecciona prompts específicos, edita el resultado o realiza alteraciones significativas pueden recibir protección. Esta situación genera una paradoja: mientras que la IA puede generar contenidos indistinguibles de los de un ser humano, su falta de estatus legal como persona impide que esas creaciones entren en el mercado con las mismas garantías de propiedad que las obras tradicionales (Amershi et al., 2019).

Para las empresas que dependen de la generación de contenido mediante IA, la recomendación experta para 2026 es documentar meticulosamente cada paso de la intervención humana en el proceso creativo para asegurar la viabilidad del copyright. Sin esta documentación, las empresas corren el riesgo de que sus activos intelectuales caigan en el dominio público o resulten vulnerables a infracciones sin posibilidad de recurso legal efectivo.

El escenario en América Latina: regulación y ética en Perú

América Latina no ha sido ajena a este debate, aunque su enfoque se

ha centrado más en la regulación administrativa y el fomento económico que en la atribución de personalidad jurídica. En la región, los marcos internacionales de derechos humanos han surgido como el mecanismo preferido para formular prácticas coherentes que mitiguen los riesgos de la IA sin frenar la innovación tecnológica.

La Ley 31814 y el Reglamento de IA en Perú (2025)

Perú se ha posicionado como un líder regional con la aprobación de la Ley 31814 y su posterior reglamento mediante el Decreto Supremo 115-2025-PCM, publicado el 9 de septiembre de 2025. Este reglamento tiene por finalidad fomentar el uso de la IA de manera segura, ética y transparente, estableciendo obligaciones claras tanto para el sector público como para el privado.

El marco regulatorio peruano evita la creación de una personalidad jurídica para la IA y se enfoca en la rendición de cuentas (accountability) y en la supervisión humana obligatoria, especialmente en sistemas de alto riesgo. Se consideran de alto riesgo los sistemas utilizados en infraestructuras críticas y en servicios esenciales como salud, transporte y banca, así como los que afecten derechos fundamentales en los sectores de justicia y educación.

Este modelo peruano refleja una tendencia regional hacia una regulación mínima que no obstaculice el progreso tecnológico, pero que establezca salvaguardas éticas infranqueables basadas en la dignidad humana (Mendieta & Jaramillo, 2019). Otros países, como México y Colombia, han seguido caminos similares, con iniciativas que buscan proteger los neuroderechos y garantizar la transparencia electoral frente al uso de

deepfakes en campañas políticas.

Gobernanza global y estándares técnicos: la infraestructura de la confianza

Dada la naturaleza transfronteriza de la inteligencia artificial, la respuesta legal nacional suele resultar insuficiente. Por ello, la cooperación internacional y la estandarización técnica se han convertido en pilares fundamentales de la gobernanza de los sistemas autónomos.

El rol de ISO/IEC JTC 1/SC 42 y la UIT

El subcomité internacional ISO/IEC JTC 1/SC 42 es el encargado de desarrollar los estándares que transforman los principios éticos en requisitos técnicos medibles. Estos estándares, como el ISO/IEC 22989 sobre conceptos y terminología o el ISO/IEC 23894 sobre gestión de riesgos, proporcionan a los legisladores y tribunales la base técnica necesaria para evaluar si un sistema ha operado de manera negligente o defectuosa.

En diciembre de 2025, la Cumbre Internacional de Estándares de IA en Seúl reafirmó el compromiso de la ISO, la IEC y la UIT para avanzar en estándares que beneficien a la humanidad y cierren la brecha digital.³³ La Declaración de Seúl subraya que los estándares internacionales son esenciales para una IA responsable, equitativa y centrada en las personas y actúan como el manual de instrucciones para el desarrollo de una tecnología que respete los derechos fundamentales.

Transparencia y el estándar IEEE 7001

El estándar IEEE 7001-2021 se destaca como la primera norma global dedicada específicamente a la transparencia en sistemas autónomos y semiautónomos. A diferencia de las directrices éticas generales, el IEEE 7001 establece niveles de transparencia medibles (del 0 al 5) para distintos grupos de interés, desde el usuario final hasta los investigadores de accidentes y los abogados. Esta transparencia es crucial para la rendición de cuentas, ya que permite realizar auditorías significativas y descubrir cómo y por qué falló un sistema, lo que facilita determinar la responsabilidad legal en caso de daños.

La figura del agente electrónico y la capacidad de contratar

Un aspecto práctico del debate sobre la personalidad jurídica es la capacidad de los sistemas autónomos para celebrar contratos de forma independiente. Con el auge de la IA agéntica (agentic AI), los sistemas ya no solo procesan información, sino que también ejecutan tareas operativas complejas en flujos de trabajo financieros y comerciales.

Autonomía operativa vs. personalidad legal

La contratación electrónica se ha caracterizado tradicionalmente por el principio de equivalencia funcional: los contratos celebrados por medios electrónicos tienen la misma validez que los celebrados de forma física, siempre que concurra el consentimiento. Sin embargo, cuando una IA realiza una compra o una puja en un mercado de valores basándose en su propio

aprendizaje, surge la duda de si esa voluntad puede atribuirse al usuario humano o si el sistema actúa como un agente electrónico con cierta autonomía operativa.

En 2026, los reguladores financieros, como FINRA, han alertado sobre los riesgos de la ejecución autónoma de flujos de trabajo, en la que los motores de IA pueden tomar decisiones no autorizadas por los humanos encargados de la supervisión. Esto ha llevado a la recomendación de que cualquier sistema capaz de tomar acciones operativas esté integrado en los marcos de supervisión corporativa, lo que exige que las firmas mantengan registros de telemetría de la cadena completa para reconstruir cómo el sistema llegó a su estado final y asegurar el cumplimiento de las obligaciones con el cliente.

Principios de la Ley Modelo sobre Comercio Electrónico

La doctrina legal recurre a los principios de neutralidad tecnológica y buena fe para validar estas transacciones, pero advierte que el soporte electrónico no sana una declaración viciada. El objetivo no es crear un nuevo derecho regulador, sino adaptar las normas existentes a los aspectos electrónicos de las relaciones negociales. Así, el agente electrónico se entiende como una categoría limitada que reconoce capacidad operativa a la IA para ciertos actos, sin otorgarle derechos humanos ni un estatuto de persona en sentido estricto (Cantú, 2016).

Riesgos sistémicos y el dilema de la evidencia

A medida que los sistemas autónomos se vuelven más potentes y ubicuos, surgen riesgos que trascienden el daño individual y se convierten en

amenazas sistémicas. El Informe Internacional sobre Seguridad de la IA 2026, liderado por expertos como Yoshua Bengio, identifica desafíos estructurales que dificultan la gestión de riesgos en la IA de propósito general (GPAI).

El dilema de la evidencia para los legisladores

Uno de los hallazgos clave del informe de 2026 es el llamado dilema de la evidencia: el panorama de la IA cambia tan rápidamente que la evidencia sobre los nuevos riesgos y las mitigaciones efectivas surge más lentamente que la propia tecnología. Esto genera un desafío para los legisladores, quienes deben equilibrar el fomento de la innovación con la protección de la sociedad ante escenarios en los que los sistemas autónomos podrían evadir la supervisión, ejecutar planes a largo plazo o resistirse a ser apagados.

Para contrarrestar estos riesgos, se propone un enfoque de defensa en profundidad, que combina:

1. **Salvaguardas Técnicas:** Filtrado de contenido, monitoreo de incidentes y mecanismos de supervisión humana antes y después del despliegue.
2. **Gobernanza Corporativa:** Protocolos de seguridad escritos, evaluaciones del impacto en el riesgo de daño crítico y auditorías de discriminación algorítmica (Maldonado, 2019).
3. **Resiliencia Social:** Programas de alfabetización mediática y protocolos de respuesta a incidentes a nivel estatal y sectorial.

El impacto en el mercado laboral y la seguridad nacional

La automatización no solo afecta a tareas rutinarias, sino que también está transformando profesiones altamente calificadas como la ingeniería de

software y la atención al cliente. En el ámbito de la seguridad nacional, el uso de sistemas autónomos para la defensa y la vigilancia migratoria plantea interrogantes éticos y legales urgentes, lo que obliga a los Estados a establecer límites al uso de la biometría en tiempo real y de técnicas de manipulación del comportamiento.

Conclusión: hacia un equilibrio entre innovación y dignidad

El debate sobre la personalidad jurídica de los sistemas autónomos refleja la búsqueda de la sociedad de domesticar una tecnología que desafía nuestras categorías legales más básicas. Tras un análisis exhaustivo de la doctrina contemporánea, la legislación internacional y los precedentes judiciales, se observa una clara divergencia entre la teoría y la práctica del Derecho.

Desde un punto de vista ontológico, la atribución de personalidad a la inteligencia artificial sigue siendo considerada por la mayoría de la doctrina como una asimilación imposible e innecesaria. La centralidad de la persona humana en el Derecho Civil y la falta de conciencia moral de las máquinas constituyen barreras que el legislador actual no parece dispuesto a superar. La jurisprudencia reciente en materia de propiedad intelectual, con el rechazo de la autoría no humana en el caso Thaler, refuerza esta visión: el Derecho es una creación humana para humanos, y la creatividad e inventiva siguen siendo actos que requieren un sustrato biológico y emocional que la IA no posee.

Sin embargo, desde una perspectiva pragmática, la necesidad de

gestionar los riesgos asociados a una autonomía creciente es real. El enfoque basado en el riesgo del AI Act de la Unión Europea y el modelo de gobernanza ética de Perú demuestran que es posible garantizar la seguridad y la reparación de daños mediante la supervisión humana, la transparencia técnica y los seguros obligatorios, sin necesidad de elevar a las máquinas a la categoría de sujetos de derecho. La figura del agente electrónico surge como una solución intermedia: una categoría operativa que permite a los sistemas autónomos actuar en el tráfico jurídico bajo la responsabilidad y el control de un titular humano o corporativo (Petrova, 2015).

El futuro del debate dependerá de la capacidad de nuestras instituciones para adaptarse a una transformación tecnológica que, en palabras de algunos expertos, es un volcán en erupción. Mientras la inteligencia artificial continúe su camino hacia una autonomía cada vez mayor, la ciencia jurídica deberá reinventarse, no necesariamente otorgando derechos a las máquinas, sino fortaleciendo los mecanismos de control y responsabilidad para que el progreso tecnológico nunca se sitúe por encima de la dignidad y los derechos fundamentales de las personas. El debate es, por tanto, no solo necesario, sino vital para asegurar que el desarrollo de la inteligencia artificial contribuya al bienestar colectivo en un marco de seguridad jurídica y de justicia social.

Capítulo 2

Gobernanza global y estándares técnicos: la infraestructura de la confianza

La gobernanza global ha experimentado una transformación paradigmática en las últimas décadas, transitando de un sistema centrado exclusivamente en el Estado hacia un programa de política internacional caracterizado por la relocalización de la autoridad. Este fenómeno implica que la capacidad de dictar normas y orientar el comportamiento de los actores internacionales ya no reside únicamente en las capitales nacionales, sino que se distribuye en una red compleja de agentes formales e informales que operan más allá de las fronteras soberanas. La esencia de esta nueva gobernanza radica en el debate entre la homogeneización de la heterogeneidad y la fragmentación resultante de la globalización, en el que la autoridad se ejerce mediante mecanismos de coordinación entre actores públicos y privados.

En este contexto, la infraestructura de la confianza se sustenta en marcos normativos, leyes y reglamentos que delimitan los límites estructurales de la acción global. Una gobernanza integral y sostenible requiere fortalecer los conceptos técnicos que permitan crear entornos públicos inclusivos y transparentes. La relocalización de la autoridad no solo responde a una necesidad de eficiencia operativa, sino que también busca la

democratización de los procesos de interacción y la rendición de cuentas, elementos clave para la estabilidad del sistema internacional actual. La seguridad, los derechos humanos, el medio ambiente y la economía política internacional son ahora analizados bajo este enfoque de sistemas complejos, donde las comunicaciones electrónicas e Internet facilitan espacios de vida paralelos a la cotidianidad delimitada por el Estado (Cantú, 2016).

La propuesta teórica de autores como Zürn subraya que la gobernanza global debe entenderse a partir de la relación entre poder, autoridad y legitimidad. Existe un trasfondo social global que influye en lo local, donde la reflexividad de los actores locales permite un diálogo situado que cuestiona la imposición de normas universales frente a necesidades específicas. Esta tensión es particularmente visible en temas como el cambio climático o la seguridad urbana, donde las soluciones globales deben adaptarse a contextos sociales y políticos activos en el ámbito local para ser efectivas.

La gobernanza de la seguridad, por ejemplo, ha evolucionado hacia un enfoque inclusivo en el que la aplicación de la ley debe involucrar a las comunidades para abordar las condiciones que originan la inseguridad, reconociendo que la corrupción y el debilitamiento del Estado de Derecho son obstáculos sistémicos para la confianza ciudadana.

El horizonte post-2026 y la transición hacia el poder algorítmico

El orden geopolítico se aproxima a una profunda transformación estructural, impulsada por los avances en inteligencia artificial, analítica de

datos, manufactura inteligente y biotecnología. A partir de 2026, la tecnología dejará de ser un mero soporte para convertirse en el marco de gobernanza que define la producción económica, la autoridad política y las prácticas de seguridad. Este cambio marca un punto de inflexión en el que el poder geopolítico se desplaza de las bases materiales tradicionales —como la geografía o los recursos naturales— hacia nuevas formas de poder cognitivo y algorítmico.

En este nuevo paradigma, la capacidad de un Estado para recolectar, procesar y operacionalizar datos mediante sistemas de IA se convierte en la medida decisiva de su influencia estratégica. La inteligencia artificial constituye ahora la infraestructura cognitiva central del sistema internacional, permeando sectores críticos como la defensa, la diplomacia y la salud. La concentración de estas capacidades en un número reducido de Estados y corporaciones está ensanchando las desigualdades geopolíticas y generando nuevas formas de dependencia tecnológica que afectan la soberanía nacional.

La competencia internacional ya no se limita al control de los recursos físicos, sino que se centra en el dominio de los estándares técnicos y de los ecosistemas de innovación integrados. Los Estados que logren adoptar estrategias tecnológicas soberanas coherentes, equilibrando la apertura con los imperativos de seguridad, serán quienes definan la configuración del orden pos-2026. Este escenario plantea desafíos éticos y regulatorios que superan la capacidad de respuesta de los Estados individuales, lo que exige marcos de gobernanza internacional más integrados y robustos. (Russell et al., 2015).

Modelos divergentes de gobernanza: EE.UU., China y la Unión Europea

La disputa por la infraestructura de la confianza global se manifiesta en tres modelos predominantes que reflejan visiones políticas y económicas distintas sobre el papel de la tecnología en la sociedad. Estos modelos compiten por establecer los estándares que regirán el comportamiento de los sistemas digitales en las próximas décadas:

1. **El modelo impulsado por el mercado (Estados Unidos):** Prioriza la innovación privada y el dinamismo comercial como motores del desarrollo técnico. Bajo este enfoque, los estándares suelen surgir de facto a través de la competencia en el mercado, aunque la administración estadounidense ha comenzado a integrar la seguridad nacional de forma más explícita en su estrategia tecnológica desde 2025.
2. **El modelo centrado en el Estado (China):** Utiliza el desarrollo tecnológico como herramienta para el fortalecimiento nacional y el control estratégico. China busca transitar de ser un receptor de reglas a ser su arquitecto, integrando la economía y la seguridad para asegurar una trayectoria de desarrollo irreversible.
3. **El modelo basado en valores (Unión Europea):** Se centra en la regulación para proteger los derechos fundamentales, la privacidad y la competencia justa. La UE busca promover una transformación digital centrada en el ser humano, utilizando estándares de seguridad económica como punto de partida para la cooperación con socios afines (Abramova et al., 2020).

La convergencia o divergencia entre estos modelos determinará si el

sistema global se dirige hacia una profunda fragmentación o hacia un orden más resiliente. La incertidumbre sobre el compromiso continuo de Estados Unidos en los foros multilaterales y los desafíos competitivos que plantea China han forzado a la Unión Europea a adoptar una postura de de-risking (reducción de riesgos), buscando equilibrar su autonomía estratégica con sus intereses económicos.

La presión para que los aliados adopten políticas más estrictas frente a proveedores específicos, como ha ocurrido con la infraestructura 5G de Huawei, ilustra cómo las consideraciones de seguridad nacional permean las decisiones técnicas. El riesgo de que Estados Unidos imponga controles extraterritoriales adicionales si los aliados no actúan con rapidez genera un clima de tensión que pone en riesgo la estabilidad de los consensos técnicos tradicionales (Georgieva, 2020).

Arquitectura y procesos de decisión en los organismos de normalización (SDOs)

La infraestructura de la confianza global se gestiona mediante una red de organismos de normalización con diversas estructuras de gobernanza. Estos organismos actúan como el campo de batalla donde se definen los protocolos que permiten la interoperabilidad de los sistemas a escala mundial. La distinción entre organizaciones intergubernamentales y aquellas impulsadas por el mercado o por comunidades técnicas es fundamental para entender cómo se ejerce la autoridad en este ámbito.

Comparativa de Gobernanza en SDOs Principales

En la ITU-T, la gobernanza está codificada en su Constitución y Convención, lo que permite que las decisiones se tomen de manera cuasirregulatoria. Los Estados Miembros tienen un peso preponderante, aunque los Miembros de Sector participan activamente en los Grupos de Estudio. En contraste, organizaciones como ETSI utilizan sistemas de votación ponderada, en los que los votos nacionales se aplican a estándares europeos y los votos individuales a cuestiones de membresía o de políticas internas. El quórum en ETSI para modificar los estatutos es de al menos el 75% de los votos ponderados totales, lo que garantiza que las decisiones críticas cuenten con un respaldo amplio.

La IETF representa el modelo más participativo, aunque no necesariamente el más inclusivo en la práctica. En 2024, el 85% de sus participantes eran hombres y el 80% provenían de Europa y de América del Norte. El proceso de la IETF requiere una inversión de tiempo sustancial: se estima que un participante necesita entre 15 y 20 años para comprender plenamente los procesos internos, lo que genera una barrera de entrada implícita basada en la experiencia y la longevidad en la comunidad.

El proceso de normalización en ISO/IEC

El desarrollo de un estándar internacional en ISO sigue un ciclo de vida estructurado que busca garantizar el consenso y la calidad técnica:

1. **Etapas de propuesta:** Se identifica la necesidad de un nuevo estándar en un comité técnico.
2. **Etapas preparatorias:** los expertos redactan el borrador inicial.

3. **Etapa de comité:** Los miembros del comité revisan y comentan el borrador.
4. **Etapa de encuesta:** El borrador se somete a votación entre todos los organismos nacionales miembros.
5. **Etapa de aprobación:** Se finaliza el texto del estándar tras resolver los comentarios.
6. **Etapa de publicación:** El estándar se publica oficialmente como norma internacional.

Este proceso permite que estándares como el ISO 9001 (gestión de la calidad) o el ISO 27001 (seguridad de la información) adquieran validez universal y, a menudo, se citan en regulaciones nacionales para garantizar la seguridad y la compatibilidad de productos y servicios.

Gobernanza de la Inteligencia Artificial: ISO 42001 e IEEE 7000

La emergencia de la IA como tecnología de propósito general ha obligado a los SDOs a desarrollar marcos que aseguren la confianza sin sofocar la innovación. Dos enfoques dominantes han surgido: uno centrado en los sistemas de gestión corporativa (ISO 42001) y otro en la ética del diseño técnico (IEEE 7000).

ISO 42001 se posiciona como el primer sistema de gestión global certificable para la IA. No es simplemente un obstáculo técnico, sino una malla de control diseñada para el liderazgo empresarial, la resiliencia legal y la credibilidad en las adquisiciones. Las organizaciones que adoptan este

estándar demuestran que gestionan el riesgo a lo largo del ciclo de vida de la IA en cada paso, lo que se traduce en una ventaja competitiva: se estima que la certificación puede aumentar las tasas de éxito en licitaciones empresariales entre un 30% y un 40%. Sin embargo, ISO 42001 brilla como estructura de gestión, pero no profundiza en cada conflicto de diseño de producto cargado de valores; puede dar cuenta de la existencia de una política ética, pero no califica cuán profundamente se reflejan esos valores en las funciones desplegadas.

Por su parte, IEEE 7000 llena ese vacío al centrarse en la traducción de valores en código. Este estándar permite que las decisiones de diseño sean explicables y rastreables, documentando cómo los intereses de los interesados se mantienen a lo largo de los giros técnicos, desde el concepto hasta el despliegue. Los equipos que utilizan IEEE 7000 reportan un 30% menos de escaladas relacionadas con la ética y reducciones significativas en los tiempos de resolución de quejas.

La realidad del mercado en 2026 indica que las licitaciones y solicitudes de propuestas (RFP) exigen cada vez más documentación que cubra ambos frentes: los controles del sistema y los registros de diseño que demuestren el trabajo ético realizado. La combinación de estos marcos permite a las juntas directivas mostrar cómo los valores fluyen de la política al producto final, protegiendo a los desarrolladores y a la organización ante un escrutinio regulatorio cada vez más riguroso.

Fragmentación del Internet y el surgimiento del Splinternet

El ideal de una red global, abierta y neutral se enfrenta a fuerzas centrífugas que amenazan con fragmentar la infraestructura de la confianza en múltiples redes desconectadas o no interoperables. Esta fragmentación puede manifestarse en distintas capas del stack tecnológico, desde la infraestructura física hasta las aplicaciones de usuario.

Tipos de fragmentación y sus catalizadores

- **Fragmentación Técnica:** Derivada de decisiones que, deliberadas o no, rompen la conectividad digital. Ejemplos incluyen la competencia entre estándares de seguridad (como TLS 1.3 frente a ETS) o la fricción en el despliegue de IPv6. La ossificación del Internet —la pérdida de flexibilidad debido a componentes de infraestructura, como middleboxes y firewalls, que bloquean nuevos protocolos— es un factor crítico de la fragmentación técnica.
- **Fragmentación Política y Geopolítica:** Resulta de prácticas como la localización de datos, los bloqueos deliberados de servicios y las políticas destinadas a excluir a proveedores específicos de las capas de conectividad. Iniciativas de soberanía digital, como la puerta de enlace nacional de Internet en Camboya o las leyes de Internet soberano en Rusia, buscan alinear la infraestructura digital con las fronteras nacionales.
- **Fragmentación Comercial:** Impulsada por la creación de jardines

vallados (walled gardens) tecnológicos donde los sistemas no interoperables impiden que los usuarios interactúen fuera de un ecosistema específico. La consolidación del mercado y la concentración de resolutores DNS en manos de pocas empresas también contribuyen a esta tendencia.

El debate sobre el New IP propuesto por actores vinculados a China en la ITU-T ejemplifica esta tensión. La propuesta buscaba reinventar la arquitectura central del protocolo TCP/IP para permitir controles más precisos desde la red, lo que, según críticos, facilitaría el control gubernamental autoritario y socavaría el modelo de gobernanza multistakeholder. Aunque estas propuestas no fueron aceptadas en su forma original en foros como los SG13 y SG11 de la ITU-T, el riesgo de un desacoplamiento tecnológico total persiste, lo que podría dividir el ciberespacio en intranets distintas con normas de seguridad y derechos humanos divergentes.

China como arquitecto de reglas y líder en propiedad intelectual

China ha implementado una estrategia nacional para pasar de ser un seguidor de estándares a ser un líder en la definición de las reglas del juego tecnológico global. Sus planes quinquenales reflejan esta ambición, enfocándose en la maestría tecnológica y en la acumulación masiva de propiedad intelectual (PI) como motores de crecimiento.

El 14.º Plan Quinquenal (2021-2025) superó sus metas en PI, alcanzando más de 5 millones de patentes de invención domésticas válidas y

reduciendo el tiempo de revisión de las patentes a un promedio de 15 meses. Esta eficiencia administrativa posiciona a China como líder mundial en la tramitación internacional de solicitudes de patentes bajo el Tratado de Cooperación en materia de Patentes (PCT) de la OMPI.

La revisión de la Ley de Comercio Exterior en 2025 (que entra en vigor en marzo de 2026) constituye un hito en esta evolución. Introduce el Artículo 33, que otorga al Estado el mandato legal para investigar y adoptar medidas proporcionales contra jurisdicciones que discriminen sistemáticamente a los titulares de derechos chinos o no proporcionen una protección adecuada de los PI. Esta ley transforma la PI de ser una herramienta de protección creativa en un activo estratégico que ejerce el control sobre tecnologías críticas, como los semiconductores, la biotecnología y el 6G. China busca construir un ecosistema tan denso en talento, datos y producción que su trayectoria sea irreversible, incluso frente a un entorno geopolítico fragmentado.

Existe una preocupación creciente sobre cómo los estándares técnicos, desarrollados por organismos a menudo opacos para la sociedad civil, afectan derechos fundamentales como la privacidad y la libertad de expresión. Los estándares pueden facilitar la vigilancia masiva, la interceptación de comunicaciones y la censura si se diseñan con debilidades intencionales en el cifrado o si imponen identificadores permanentes de los dispositivos.

La Coalición por la Libertad en Línea enfatiza que los derechos humanos que las personas disfrutan fuera de línea también deben protegerse en línea. Los procesos de normalización abiertos, voluntarios y basados en el consenso multistakeholder (como en IETF o W3C) han sido fundamentales para

mantener una Internet global resiliente. Sin embargo, propuestas de estandarización que buscan aumentar el control estatal sobre las sociedades representan una amenaza directa para el ecosistema de información libre.

Riesgos y Mitigaciones en la Interfaz Técnica-Derechos

- **Vigilancia y Seguridad Digital:** El Relator Especial de la ONU ha expresado preocupación por la falta de consideración de los derechos humanos en las organizaciones que operan la infraestructura de Internet. Las empresas tienen la responsabilidad de respetar los derechos humanos conforme a los Principios Rectores de la ONU, incluso cuando se enfrentan a presiones estatales para filtrar contenido o retener datos de sus clientes.
- **Privacidad por Diseño:** La proliferación de leyes de protección de datos, como el RGPD en la UE, ha obligado a los desarrolladores a integrar parámetros técnicos de seguridad y responsabilidad desde las etapas iniciales. No obstante, el capitalismo de vigilancia, impulsado por la recolección masiva de datos comerciales, sigue planteando desafíos que los estándares actuales apenas comienzan a abordar.
- **Inclusión de Grupos Vulnerables:** Los estándares deben seguir prácticas de mainstreaming de género y considerar los derechos de los niños, de las personas con discapacidad y de los pueblos indígenas para evitar la discriminación algorítmica y técnica (Singh et al., 2023).

La falta de experiencia técnica suficiente en las organizaciones de derechos humanos dificulta su participación efectiva en los foros de normalización, lo que subraya la necesidad de capacitar a la sociedad civil para que actúe como contrapeso en la definición de la infraestructura de la

confianza (Cantú, 2016).

Las tecnologías de registro distribuido (DLT) prometen revolucionar el comercio internacional al proporcionar una capa de confianza inmutable para el intercambio de bienes y datos. En una era de tensiones geopolíticas, la transparencia y la resiliencia de las cadenas de suministro se han vuelto urgentes, y el blockchain ofrece una solución para eliminar barreras no arancelarias, como los trámites aduaneros manuales y el fraude documental.

El comité ISO/TC 307 lidera los esfuerzos internacionales para armonizar estas tecnologías con los marcos industriales y legales. Su trabajo se divide en grupos de estudio que abarcan desde la terminología básica hasta la seguridad de los custodios de activos digitales y los contratos inteligentes.

Panorama de Estándares de Blockchain

La estandarización convierte una tecnología experimental en una infraestructura crítica. Por ejemplo, el estándar CCIP (Chainlink) permite que los activos y datos fluyan entre entornos desconectados, como de una red bancaria privada a una aplicación DeFi pública, evitando la fragmentación de la liquidez. Sin embargo, persisten desafíos: la innovación tecnológica ocurre en semanas, mientras que los ciclos de ISO duran años, lo que genera un desfase en el que los estándares oficiales pueden publicarse cuando la tecnología ya ha evolucionado. Además, un estándar de privacidad que cumpla con el RGPD en Europa puede entrar en conflicto con los requisitos de vigilancia financiera de otras jurisdicciones.

El Pacto Digital Global y la cooperación de la ONU

En septiembre de 2024, los líderes mundiales adoptaron el Pacto para el Futuro, que incluye el Global Digital Compact (GDC). Este marco integral establece objetivos para una cooperación digital fortalecida, con el fin de cerrar las brechas digitales y asegurar que el ciberespacio sea un lugar seguro y respetuoso de los derechos humanos.

Los hitos clave del GDC para el periodo 2025-2027 incluyen:

- **Mapa de implementación (Q1 2025):** El Secretario General de la ONU proporcionará una hoja de ruta para coordinar las contribuciones del sistema de la ONU y de otras partes interesadas.
- **Diálogo Global sobre Gobernanza de la IA (julio de 2026):** Se celebrará en Ginebra, cofacilitado por Estonia y El Salvador, tras el nombramiento de un Panel Científico Internacional independiente de 40 miembros en febrero de 2026.
- **Semana del Código Abierto de la ONU (junio 2026):** Para fomentar el desarrollo de bienes públicos digitales y la inversión en infraestructuras abiertas.
- **Revisión de Alto Nivel (2027):** Durante la 82ª sesión de la Asamblea General de la ONU para evaluar el progreso de los compromisos adquiridos.

El GDC busca explícitamente evitar la fragmentación de Internet y promover la interoperabilidad entre los marcos nacionales de gobernanza de

datos. La creación de la Oficina para Tecnologías Digitales y Emergentes (ODET) dentro de la ONU centralizará la coordinación y el asesoramiento sobre tendencias tecnológicas clave, asegurando que la organización se mantenga al ritmo de la aceleración digital.

Desafíos para los países en desarrollo y la brecha de estandarización

A pesar de los esfuerzos globales, la desigualdad en las capacidades nacionales de normalización persiste como un precursor de la brecha digital. Muchos países en desarrollo, en particular los Países Menos Adelantados (LDC) y los Pequeños Estados Insulares en Desarrollo (SIDS), enfrentan barreras estructurales para participar en la definición de la infraestructura de la confianza.

Barreras identificadas para la implementación de estándares técnicos

1. **Falta de capacidad humana y de entrenamiento:** Existe una escasez de expertos capaces de representar los intereses nacionales en foros técnicos internacionales, como la IETF o los comités de la ISO.
2. **Costos de cumplimiento y certificación:** La implementación de estándares bajo términos FRAND (justos, razonables y no discriminatorios) puede resultar prohibitiva para las PYMES de países en desarrollo, limitando su acceso a las cadenas de valor globales.
3. **Fragmentación de foros:** La proliferación de organizaciones de normalización dificulta que los países con recursos limitados prioricen su

participación efectiva.

4. **Dependencia tecnológica:** La necesidad de importar equipos que cumplan con estándares definidos en el Norte Global genera una salida constante de divisas y una dependencia de la infraestructura externa.

El programa Bridging the Standardization Gap de la ITU-T busca mitigar estos problemas mediante la categorización de las capacidades nacionales y la facilitación de la participación activa. Sin embargo, el informe de la ITU muestra que la mayoría de los países africanos y del sudeste asiático aún se encuentran en los niveles de capacidad Baja o Básica, mientras que China es uno de los pocos países en desarrollo que ha alcanzado el nivel Avanzado.

Síntesis y Prospectiva Estratégica

La infraestructura de la confianza en el siglo XXI ya no es solo una cuestión de tratados diplomáticos, sino también de protocolos técnicos y algoritmos de IA. La gobernanza global se ha convertido en un ejercicio de tecnogeopolítica en el que la capacidad de influir en los estándares define la soberanía y la competitividad nacionales (Luppicini & So, 2016).

Las conclusiones que emergen del análisis de 2025 y 2026 sugieren que:

- **La interoperabilidad es el nuevo campo de batalla de la soberanía:** los Estados que logren imponer sus estándares (ya sea en IA, blockchain o 6G) tendrán una ventaja estructural irreversible en la economía global.
- **La confianza técnica requiere legitimidad social:** los estándares que

ignoren los derechos humanos o la ética del diseño enfrentarán una resistencia creciente, tanto de los ciudadanos como de los reguladores, en bloques como la Unión Europea (Albisua & Pacheco, 2025).

- **El modelo multistakeholder está bajo presión:** el avance de modelos centrados en el Estado y la fragmentación técnica amenazan la unidad de Internet, lo que exige renovar los compromisos en foros como el Pacto Digital Global de la ONU.

La estabilidad del sistema internacional dependerá de la capacidad de los diversos actores para encontrar puntos de convergencia en este alfabeto sopa de organismos técnicos, asegurando que la tecnología sirva como puente para el desarrollo y no como una nueva cortina de hierro digital (Jobin et al., 2019).

Capítulo 3

Personalidad jurídica del robot: Autonomía, autoaprendizaje y adaptación

La intersección entre el derecho y la tecnología ha alcanzado un punto de inflexión con la proliferación de sistemas autónomos dotados de inteligencia artificial. La capacidad de estas máquinas para operar sin supervisión humana directa, aprender de su experiencia y adaptar su comportamiento a entornos cambiantes desafía las categorías jurídicas tradicionales que han regido la civilización durante siglos. El debate sobre la personalidad jurídica del robot no es una mera elucubración teórica, sino una respuesta necesaria ante la integración de la inteligencia artificial en la medicina, el transporte, la industria y el ámbito doméstico (Mayol, 2023). Esta transformación obliga a los juristas a cuestionar si el marco legal actual, basado en la dicotomía entre personas y cosas, es suficiente para abordar entes que sienten, piensan y actúan con una autonomía creciente.

Evolución histórica y fundamentos ontológicos del debate

El deseo humano de crear vida artificial o entes que emulen el comportamiento inteligente tiene raíces profundas en la cultura y la mitología.

Desde el mito de Pigmalión y el gólem de Praga hasta el monstruo de Frankenstein y los relatos de Isaac Asimov, la humanidad ha fantaseado con la creación de seres autónomos. Sin embargo, la transición de estas fantasías a la realidad tecnológica comenzó formalmente en 1956, cuando John McCarthy, Marvin Minsky y Claude Shannon acuñaron el término «inteligencia artificial» en la conferencia de Dartmouth. El objetivo original era describir cualquier fase del aprendizaje humano para poder reproducirla en una máquina, una meta que hoy se manifiesta en robots capaces de realizar tareas netamente humanas.

La doctrina jurídica contemporánea ha identificado tres propiedades que diferencian a los robots de las máquinas simples: la corporeidad, la impredecibilidad y el impacto social. Mientras que el software convencional reside en un plano inmaterial, el robot posee una materialidad corpórea que le permite interactuar físicamente con el mundo real. Su capacidad de aprendizaje automático (*machine learning*) introduce una impredecibilidad que rompe con la programación lineal y permite al sistema tomar decisiones que sus creadores no previeron originalmente. Finalmente, su impacto social es tal que los seres humanos tienden a atribuirles cualidades antropomórficas, compartiendo con ellos la culpa por el fracaso o el elogio por el éxito (Amershi et al., 2019).

Categorización técnica y legal de los agentes inteligentes

Para abordar la personalidad jurídica, es fundamental definir con precisión la naturaleza del ente. La falta de una definición legal unificada ha llevado a la doctrina a proponer diversas categorías basadas en el soporte

físico y lógico de la tecnología.

En este contexto, la autonomía se entiende como la posibilidad de tomar decisiones por uno mismo, sin influencia externa directa, basándose en la interconexión y en el análisis de datos masivos. Esta autonomía es el eje que justifica la discusión sobre si el robot debe seguir siendo tratado como una cosa o si requiere una categoría intermedia o propia.

Teorías doctrinales sobre la personalidad del robot

El debate jurídico se divide entre quienes abogan por mantener al robot en la categoría de objeto y quienes proponen otorgarle una personalidad electrónica o una subjetividad jurídica parcial.

El enfoque tradicional: el robot como objeto de derecho

Gran parte de la doctrina sostiene que el derecho es un producto cultural destinado exclusivamente a regular la conducta humana intersubjetiva. Desde esta perspectiva, la personalidad es un atributo normativo que requiere un sustrato humano o una organización de personas naturales para ser válido. Se argumenta que conferir personalidad a un robot sería un acto arbitrario e irracional, comparable a la decisión histórica de Calígula de nombrar cónsul a su caballo. Los críticos de la personalidad robótica advierten que el robot, sin importar su complejidad, sigue siendo un instrumento del hombre. Por lo tanto, cualquier daño causado debe imputarse al fabricante, al programador o al usuario, bajo los regímenes de

responsabilidad por productos defectuosos o por el hecho de las cosas.

La propuesta de la personalidad electrónica del Parlamento Europeo

En 2017, el Parlamento Europeo adoptó una resolución pionera que propuso la creación de un estatus jurídico específico para los robots autónomos más complejos, denominándolos «personas electrónicas». Esta propuesta no buscaba equiparar a los robots a los seres humanos en términos de derechos fundamentales, sino optimizar el sistema de responsabilidad civil. Al dotar al robot de una personalidad jurídica propia, se facilitaría la reparación de daños en situaciones en las que la autonomía de la máquina dificulta identificar a un humano específico como responsable. Sin embargo, esta idea fue recibida con una carta abierta de más de 200 expertos europeos que rechazaron el reconocimiento de personalidad, argumentando que ello eximiría de responsabilidad a los fabricantes y entraría en conflicto con la Carta de los Derechos Fundamentales de la Unión Europea.

Modelos intermedios y analogías históricas

Algunos autores sugieren que la robótica exige una tercera vía. Se ha planteado el uso de la figura de la esclavitud en el derecho romano, en el que el esclavo podía realizar actos jurídicos bajo la potestad de su dueño, quien respondía por las deudas u obligaciones contraídas por el esclavo. Otros investigadores proponen una personalidad jurídica parcial, similar a la de las sociedades mercantiles, en la que el robot poseería un patrimonio propio destinado a cubrir posibles indemnizaciones.

Autonomía, autoaprendizaje y adaptación: el desafío técnico al Derecho

La capacidad de los sistemas de inteligencia artificial para aprender y adaptarse de forma autónoma crea una brecha de responsabilidad (*responsibility gap*) que el derecho tradicional no puede llenar fácilmente. El autoaprendizaje implica que el programa no solo aplica una heurística humana suministrada, sino que también genera su propia lógica de actuación basada en la experiencia.

El fenómeno de la caja negra y el nexo causal

Uno de los mayores desafíos para la responsabilidad civil es el efecto de la caja negra (*black box*), que se refiere a la opacidad de los algoritmos de aprendizaje profundo. En un juicio de responsabilidad extracontractual, es necesario probar un nexo causal entre la acción del sujeto y el daño producido. Sin embargo, cuando un robot toma una decisión basada en procesos internos incomprensibles para los humanos, el nexo causal se vuelve difuso.

Para combatir esta opacidad, la doctrina sugiere exigir una transparencia posmoderna que obligue a los desarrolladores a facilitar la exhibición de algoritmos y a recurrir a presunciones legales que protejan a la víctima cuando no sea posible abrir la caja negra.

Adaptación y riesgos de desarrollo

La adaptación continua de los robots a su entorno significa que un producto que era seguro en el momento de su puesta en servicio puede

volverse peligroso debido a lo que aprende durante su uso. Esto cuestiona la Directiva de Productos Defectuosos de la Unión Europea, que tradicionalmente exonera al fabricante si el defecto no podía detectarse con el estado del conocimiento técnico del momento (riesgos de desarrollo). La nueva tendencia legislativa busca limitar esta exoneración en el caso de sistemas de IA que continúan aprendiendo tras su distribución.

Modelos de responsabilidad y mecanismos de reparación

Ante la dificultad de imputar culpabilidad a un ente sin conciencia, el derecho evoluciona hacia modelos de responsabilidad objetiva y de aseguramiento preventivo.

Seguros obligatorios y fondos de garantía

Inspirado en el modelo de los vehículos motorizados, se propone que los operadores de robots inteligentes deban contratar un seguro de responsabilidad civil obligatorio. Este sistema se complementaría con fondos de compensación financiados por fabricantes y operadores para cubrir daños en casos de insolvencia o cuando no sea posible determinar un responsable directo.

En el régimen propuesto por el Parlamento Europeo, se establecen plazos de prescripción diferenciados: 30 años para daños a la vida o a la integridad física y 10 años para perjuicios materiales o pérdidas económicas comprobables.

Responsabilidad penal y penas para robots

En el ámbito penal, la cuestión es aún más compleja, pues la dogmática clásica exige la culpabilidad humana. Sin embargo, algunos autores plantean paralelismos con la responsabilidad penal de las personas jurídicas. Se propone que si una IA aprende que una conducta delictiva tiene consecuencias negativas (como la reducción de su patrimonio o su desconexión), podría ajustar su comportamiento futuro. No obstante, la mayoría de la doctrina coincide en que el castigo debe recaer sobre los humanos que omitieron la diligencia debida en la supervisión de la máquina.

Impacto económico, fiscal y laboral de los robots autónomos

El reconocimiento de una personalidad jurídica a los robots tendría repercusiones directas en el sistema fiscal y en el mercado de trabajo, lo que plantea la necesidad de una fiscalidad robótica.

El robot como contribuyente

Si los robots sustituyen a los trabajadores humanos, el Estado pierde ingresos por cotizaciones sociales e impuestos a la renta. Algunos investigadores sugieren que, al poseer una cierta capacidad económica que beneficia a su dueño, los robots deberían tributar para contribuir al sostenimiento de los gastos públicos (Sánchez et al., 2021). Esto implicaría crear una ficción tributaria en la que el robot sea el hecho imponible, o bien aumentar la carga fiscal de la empresa que utiliza robots para compensar la

pérdida de aportes humanos.

La robótica y el derecho al trabajo

La automatización ha llevado a despidos por causas productivas, lo que ha generado litigios en los que los jueces deben equilibrar la libertad de empresa con el derecho al trabajo. Se ha argumentado que la sustitución masiva de trabajadores por IA, sin un plan de transición, vulnera la dignidad humana y la sostenibilidad social. La OIT recomienda centrar la inversión en las capacidades de las personas para asegurar un futuro de trabajo decente frente a la revolución (Montomoli, 2023).

El marco regulatorio en el Perú y Latinoamérica

Perú se ha convertido en uno de los pioneros regionales al promulgar la Ley N° 31814, que fomenta el uso de la inteligencia artificial para el desarrollo económico y social.

La Ley N° 31814 y el Reglamento de 2025

El Reglamento de la Ley de Inteligencia Artificial en el Perú (aprobado mediante el D.S. 115-2025-PCM) establece un marco de gobernanza, liderado por la Secretaría de Gobierno y Transformación Digital (SGTD) de la PCM. Este reglamento adopta un enfoque basado en el riesgo, similar al modelo europeo, y clasifica los usos de la IA para proteger los derechos fundamentales.

Iniciativas legislativas y el Registro de IA de Alto Riesgo

En noviembre de 2025, se presentó un proyecto de ley para modificar la Ley 31814, que propone crear un Registro Nacional de Sistemas de Inteligencia Artificial de Alto Riesgo. En este registro, los proveedores deben inscribir sus sistemas antes de introducirlos al mercado, identificando al responsable y el propósito de la tecnología. Además, se han propuesto leyes para incorporar la IA en el currículo educativo, con el fin de cerrar la brecha digital y fomentar un uso ético desde la etapa escolar.

En el contexto latinoamericano, países como Brasil, Chile, Argentina y México también avanzan en proyectos de regulación integral. Brasil, por ejemplo, ha trabajado en un marco que pone énfasis en los derechos de las personas afectadas por sistemas automatizados, buscando un equilibrio entre la innovación y la seguridad jurídica.

Propiedad Intelectual y creaciones de la Inteligencia Artificial

La autonomía de la IA le permite crear obras literarias, artísticas y musicales, lo que genera un conflicto entre el derecho de autor y el de propiedad intelectual.

Autoría y titularidad

Tradicionalmente, solo las personas naturales pueden ser autoras. Las obras generadas por IA carecen de la originalidad derivada de la inteligencia humana, lo que las situaría inicialmente en el dominio público. Sin embargo,

la industria propone proteger estas creaciones mediante derechos conexos o atribuyendo la titularidad al humano que realizó la inversión económica y configuró el sistema.

- **Postura del Programador:** El derecho pertenece al creador del algoritmo.
- **Postura del Usuario:** El derecho pertenece a quien dio las instrucciones y operó la máquina.
- **Postura del Robot:** Si se reconoce la personalidad jurídica, el robot podría ser titular de sus propios derechos, los cuales serían gestionados por un fondo patrimonial.

El uso de datos para entrenamiento

Los sistemas de IA generativa requieren procesar volúmenes masivos de datos, muchos de los cuales están protegidos por la propiedad intelectual. La doctrina debate si este uso constituye una excepción a la minería de datos o si requiere autorización expresa y remuneración para los autores originales.

Ética y gobernanza global de la inteligencia artificial

La regulación de la personalidad jurídica no puede separarse de un marco ético universal que garantice que la tecnología sirva a la humanidad (Abramova et al., 2020).

Principios éticos fundamentales

Organizaciones como la UNESCO y la OCDE han establecido directrices que los Estados deben observar al legislar sobre IA.

1. **Dignidad Humana:** El progreso científico debe tener su límite en el respeto a la persona.
2. **Transparencia y Explicabilidad:** Los usuarios tienen derecho a saber cuándo interactúan con una IA y cómo esta toma sus decisiones.
3. **Justicia y Equidad:** Evitar que los algoritmos perpetúen sesgos discriminatorios por género, etnia o religión.
4. **No Maleficencia:** Asegurar que los robots cuenten con frenos de emergencia y no pongan en riesgo la seguridad física de los humanos.

El derecho a la atención humana

En Perú, la Ley N° 31601 reconoce el derecho del consumidor a optar por una atención personal en lugar de interactuar con un sistema de IA. Esto refleja una preocupación ética por la deshumanización de los servicios y la necesidad de preservar la autonomía humana frente a la automatización.

El estudio de la personalidad jurídica del robot revela que el derecho se enfrenta a un desafío sin precedentes. La autonomía, el autoaprendizaje y la adaptación de estas máquinas han roto la previsibilidad técnica que permitía aplicar de manera sencilla las normas de responsabilidad civil y penal. Si bien el otorgamiento de una personalidad electrónica completa parece haber sido descartado por el momento en favor de un enfoque pragmático basado en el riesgo, la necesidad de crear centros de imputación de responsabilidad sigue vigente.

El futuro de la regulación dependerá de la capacidad de los Estados para armonizar sus leyes nacionales con estándares globales de ética y seguridad (Jobin et al., 2019). El modelo peruano de clasificación por riesgos

y registro obligatorio de sistemas de alto riesgo marca un camino que busca equilibrar la competitividad industrial con la protección de los derechos fundamentales. En última instancia, la personalidad jurídica del robot debe entenderse no como una equiparación ontológica con el ser humano, sino como una técnica jurídica necesaria para navegar en una sociedad en la que las máquinas ya no son simples herramientas, sino agentes activos en la construcción de nuestra realidad cotidiana (Inglada et al., 2024).

Capítulo 4

Inteligencia artificial: capacidad jurídica funcional para fines comerciales y de responsabilidad

El advenimiento de la cuarta revolución industrial ha situado a la inteligencia artificial (IA) en el epicentro de un debate jurídico sin precedentes, donde la capacidad de procesamiento de datos y la autonomía decisoria de los algoritmos desafían las estructuras clásicas del Derecho Civil y Mercantil. La transición de sistemas informáticos que actúan como meros instrumentos de ejecución hacia agentes capaces de un aprendizaje autónomo y predictivo obliga a replantear si el marco normativo tradicional, diseñado para la interacción entre seres humanos, es suficiente para garantizar la seguridad jurídica en un mercado globalizado y digital. En este escenario, la noción de una capacidad jurídica funcional emerge como una solución técnica que permite atribuir efectos jurídicos a las acciones de la IA sin necesidad de otorgarle una personalidad jurídica plena, la cual sigue siendo objeto de intensas controversias doctrinales y éticas (Jobin et al., 2019).

Fundamentos ontológicos y dogmáticos de la personalidad en el entorno digital

La discusión sobre la naturaleza jurídica de la inteligencia artificial oscila entre considerarla como una cosa —un bien mueble inmaterial o un

programa de cómputo— y proponer crear una nueva categoría de persona electrónica. Tradicionalmente, la personalidad jurídica se ha dividido en individual (física) y colectiva (jurídica), siendo esta última una técnica para atribuir capacidad a entes que no son seres humanos pero que persiguen fines sociales o económicos. Bajo esta premisa, autores alineados con la dogmática de Kelsen sugieren que la personalidad es una construcción artificial del Derecho, lo que facilitaría la creación de una capacidad relativa para la IA si la utilidad social lo justifica.

Sin embargo, la atribución de personalidad plena a los robots y a los sistemas de IA enfrenta una resistencia considerable. Desde una perspectiva civilista, se advierte que otorgar este estatus podría ser una estrategia para diluir la responsabilidad de los fabricantes o usuarios, creando un velo algorítmico que proteja a los verdaderos beneficiarios económicos de los daños causados. En el caso de Sofía, la humanoide a la que se le han otorgado distinciones simbólicas por parte de organismos internacionales, la doctrina es enfática al señalar que tales actos no la convierten en sujeto de derecho, pues carece de la esencia humana y de la autonomía moral que fundamentan la dignidad y los derechos constitucionales.

La capacidad jurídica funcional se presenta, por tanto, como un punto medio: no se busca igualar a la IA al ser humano, sino dotarla de una esfera de actuación en la que sus decisiones tengan validez jurídica, bajo la responsabilidad de un operador humano o de una persona jurídica que actúe como su guardián (Mendizábal & Kurczyn, 2017). Esta funcionalidad es crítica en el sector comercial, donde la celeridad de las transacciones exige que los algoritmos operen con un grado de independencia que los contratos

tradicionales no previeron originalmente.

La manifestación de voluntad y el perfeccionamiento del contrato algorítmico

En el núcleo de la capacidad comercial de la IA se encuentra el concepto de manifestación de voluntad. En el Derecho peruano, el artículo 141 del Código Civil establece que la voluntad puede ser expresa o tácita, lo que permite el uso de medios electrónicos para su comunicación. No obstante, la IA plantea la pregunta de si un algoritmo puede querer o si su voluntad es simplemente una proyección de la programación inicial.

El consentimiento en la contratación electrónica

La doctrina contemporánea interpreta que la voluntad jurídica en los contratos celebrados por IA no radica en el software, sino en el acto de programación y de puesta en funcionamiento del sistema (Kee, 2021). Cuando un operador configura un algoritmo para comprar acciones o reabastecer inventarios bajo ciertos parámetros, está emitiendo una voluntad programada que se activa ante condiciones específicas del mercado. Esta interpretación permite salvaguardar la validez de millones de transacciones diarias en el e-commerce, un sector que experimentó un crecimiento del 300% durante la crisis sanitaria, lo que consolida a Internet como un servicio esencial para el tráfico mercantil.

La capacidad de los sistemas de Machine Learning para ajustar su comportamiento a partir de datos nuevos introduce una capa de complejidad:

el resultado emergente. Si una IA decide realizar una compra que el programador no previó explícitamente, pero que se encuentra dentro de los límites de optimización asignados, se considera que el riesgo de esa decisión fue asumido por el titular del sistema al optar por una tecnología de naturaleza autónoma.

Agentes electrónicos y Smart Contracts

La evolución hacia los *Smart Contracts* —contratos que se autoejecutan mediante código informático— representa el nivel más alto de autonomía comercial. Estos instrumentos eliminan la necesidad de intermediarios y reducen los costos de transacción, pero plantean desafíos en cuanto a su inmutabilidad ante vicios del consentimiento o cambios imprevistos en las circunstancias (cláusula *rebus sic stantibus*). La normativa europea, como la propuesta de Reglamento Omnibus Digital, intenta mitigar estos riesgos al eliminar requisitos excesivos para los smart contracts y confiar en estándares voluntarios de autocertificación, con el fin de alcanzar un equilibrio entre innovación y seguridad.

El marco regulatorio peruano: Análisis de la Ley N° 31814 y su Reglamento

Perú ha marcado un hito en la región al promulgar la Ley N° 31814, que promueve el uso de la inteligencia artificial para el desarrollo económico y social, y su correspondiente Reglamento aprobado mediante el Decreto Supremo N° 115-2025-PCM. Este marco legal no solo busca impulsar la tecnología, sino también establecer un sistema de gobernanza que garantice

un despliegue ético y respetuoso de los derechos fundamentales.

Clasificación de riesgos y niveles de cumplimiento

El reglamento peruano adopta un enfoque basado en el riesgo y categoriza los sistemas de IA según su impacto potencial en la sociedad. Esta clasificación es fundamental para determinar las obligaciones de transparencia y supervisión de las empresas.

Los sectores de salud, educación, justicia y finanzas han sido identificados como de prioridad máxima, con un plazo de cumplimiento que vence en septiembre de 2026. Las empresas que operan en estas áreas deben implementar registros de sus algoritmos, evaluaciones de impacto y, sobre todo, mecanismos de supervisión humana efectiva (*Human-in-the-loop*).

Gobernanza y el rol de la SGTD

La Secretaría de Gobierno y Transformación Digital (SGTD) de la Presidencia del Consejo de Ministros es la autoridad técnico-normativa responsable de supervisar el cumplimiento de la ley. Entre sus facultades, destacan la creación del Centro Nacional de Computación de Alto Rendimiento y la promoción de sandboxes regulatorias —entornos de prueba controlados— en los que las empresas pueden probar sus innovaciones bajo la supervisión del Estado antes de su lanzamiento masivo, lo que reduce la incertidumbre legal y previene sanciones futuras.

Sin embargo, la doctrina peruana ha señalado ciertas insuficiencias en la Ley 31814. Se argumenta que la norma es predominantemente declarativa y carece de una tabla de sanciones específica para infracciones que no

involucran datos personales. Existe preocupación por la opacidad de los algoritmos y la falta de directrices claras para la detección de sesgos, lo que podría diluir el principio ético en una aspiración genérica sin exigibilidad real.

Regímenes de responsabilidad civil por daños algorítmicos

La determinación de quién debe responder cuando una IA causa un daño es quizás el problema más complejo del Derecho contemporáneo. La naturaleza de caja negra de muchos sistemas de *Deep Learning* hace que resulte extremadamente difícil para una víctima probar la culpa o la negligencia del desarrollador o del usuario.

Responsabilidad objetiva y el riesgo creado

Ante la opacidad tecnológica, la tendencia doctrinal y legislativa se inclina por la responsabilidad objetiva, basada en la teoría del riesgo creado. Bajo este esquema, quien introduce una tecnología riesgosa en el mercado para obtener un beneficio debe pechar con las consecuencias negativas que esta genere, sin necesidad de acreditar una conducta culposa. En el Perú, este principio encuentra sustento analógico en el artículo 1970 del Código Civil, relativo a la responsabilidad por bienes o actividades riesgosas.

El concepto de guardián es clave en esta estructura. El guardián es quien tiene el control, la dirección o el provecho de la cosa. En el caso de la IA, la responsabilidad puede recaer solidariamente entre el operador inicial (quien define las características y proporciona los datos) y el operador final

(quien utiliza el sistema en su actividad económica).

Propuestas de armonización de la Unión Europea

Las propuestas de Directiva de la Unión Europea de septiembre de 2022 introducen innovaciones procesales para equilibrar la balanza en favor de los perjudicados:

1. **Presunción de causalidad:** Se establece una presunción de causalidad de que la falla del sistema de IA causó el daño si se demuestra que el demandado no cumplió con sus deberes de cuidado o de transparencia.
2. **Exhibición de pruebas:** Se faculta a los jueces para ordenar a las empresas tecnológicas la entrega de documentación técnica y de evidencias sobre el funcionamiento del algoritmo, bajo el apercibimiento de presumir su responsabilidad si se niegan injustificadamente.

Esta normativa busca proteger especialmente a los consumidores frente a productos defectuosos, extendiendo la responsabilidad objetiva del fabricante hasta por 15 años en casos de daños personales con latencia prolongada.

Desafíos probatorios y el impacto de la IA en la justicia peruana

La integración de la IA en la administración de justicia en Perú, a través de proyectos como Mikuna IA, Curia e Iudex IA, promete agilizar procesos tradicionalmente lentos, pero plantea riesgos estructurales para el debido proceso y la tutela jurisdiccional efectiva.

El problema de la motivación y la Caja Negra

Un laudo o sentencia que se apoye en una IA opaca corre el riesgo de ser anulado por falta de motivación. El artículo 139 de la Constitución Política del Perú exige que las resoluciones judiciales sean motivadas y razonadas. Si un juez delega el análisis de un expediente en un algoritmo cuya lógica interna no puede explicar, se vulneran el principio de transparencia y el derecho de defensa del justiciable.

La doctrina procesal advierte que la IA generativa no razona jurídicamente, sino que predice resultados basados en probabilidades lingüísticas y patrones estadísticos. Por ello, se enfatiza que la IA debe ser una herramienta de apoyo para tareas administrativas o de clasificación de causas, pero nunca un sustituto del juicio humano en la ponderación de valores y en la aplicación de la equidad.

La prueba digital y la pericia informática

En el ámbito probatorio, la IA plantea el desafío de la autenticidad y la integridad. Los litigantes en Lima y otras regiones deben enfrentarse a la posibilidad de pruebas manipuladas o generadas sintéticamente (*deepfakes*). El Código Procesal Civil peruano, aunque flexible, requiere una actualización para establecer protocolos claros de cadena de custodia digital y estándares de valoración para la prueba algorítmica.

El rol del seguro y los fondos de garantía en la gestión del riesgo

Dada la dificultad de prever todas las contingencias de un sistema autónomo, el mercado de seguros y la creación de fondos de garantía se perfilan como elementos esenciales para la viabilidad comercial de la IA.

Seguros de responsabilidad civil cibernética

Las aseguradoras en Perú están adaptando sus productos de responsabilidad civil y de riesgo cibernético para cubrir los fallos de la IA. Empresas como AXA XL y Avla ya ofrecen soluciones que integran el asesoramiento preventivo con la cobertura de daños por vulneración de la privacidad o por errores algorítmicos. La IA no solo es el objeto del seguro, sino que también transforma el sector asegurador mediante el uso de *Insurtech* para la tasación precisa de riesgos y la automatización de reclamos, lo que mejora la confianza del cliente.

La analogía del SOAT y fondos de compensación

Existe una propuesta doctrinal para implementar seguros obligatorios o fondos de garantía similares al SOAT en sistemas de IA de alto riesgo. Esto permitiría que, en casos en que no se pueda identificar una negligencia específica o el daño se deba a un comportamiento emergente e imprevisible, la víctima reciba una indemnización rápida a cargo de un fondo común financiado por los operadores del mercado. El reglamento peruano (DS 115-2025-PCM) ya contempla la facultad de exigir seguros de responsabilidad civil

proporcionales a la magnitud del riesgo y fomenta esquemas de garantía mutua para cubrir fallos sistémicos.

Consideraciones éticas, sociales y el futuro del empleo

El impacto de la IA trasciende lo estrictamente jurídico y se adentra en la esfera socioeconómica. En un país como el Perú, con altos niveles de informalidad económica, la IA presenta tanto una oportunidad para la inclusión financiera como un riesgo de exclusión financiera si los algoritmos se entrenan con datos sesgados o incompletos.

El reto de la informalidad y la alfabetización digital

La falta de registros formales hace que muchos ciudadanos sean invisibles para los algoritmos de crédito, lo que puede perpetuar patrones de injusticia. Por ello, el Reglamento de la Ley 31814 establece la obligación de las organizaciones de fomentar la alfabetización en IA (*AI Literacy*) tanto en su personal como en sus usuarios. La capacitación se convierte en una ventaja competitiva esencial en un mercado laboral donde el 72% de los empleadores en Perú planea modificar su inversión en automatización en los próximos meses.

Responsabilidad penal y protección de menores

El marco legal peruano ha sido pionero al incluir agravantes penales por el uso indebido de la IA. Desde abril de 2025, la creación de *deepfakes* con fines de difamación o de pornografía infantil conlleva penas severas, lo que

refleja una voluntad política de proteger la dignidad humana frente a los usos maliciosos de la tecnología. Esta dimensión penal complementa la responsabilidad civil y comercial, configurando un ecosistema regulatorio integral.

La capacidad jurídica funcional de la inteligencia artificial es una realidad operativa en el comercio moderno que requiere un acompañamiento normativo dinámico y especializado. Para las empresas en Perú y en la región, el cumplimiento de la Ley 31814 y su reglamento no debe verse como una carga burocrática, sino como un sello de confianza y calidad que garantiza su competitividad en el mercado global.

Se recomienda a las organizaciones adoptar un enfoque proactivo:

- Realizar auditorías periódicas de sus sistemas de IA para detectar sesgos y garantizar la transparencia algorítmica.
- Integrar mecanismos de supervisión humana real y significativa en todas las decisiones que puedan afectar los derechos de terceros.
- Contratar seguros de responsabilidad civil adecuados que cubran los riesgos específicos de la autonomía algorítmica.
- Participar en los entornos de experimentación controlados (*Sandboxes*) de la SGTD para alinear sus innovaciones con los estándares de seguridad nacional.

El futuro del Derecho frente a la inteligencia artificial no reside en otorgar derechos a las máquinas, sino en asegurar que la tecnología permanezca siempre al servicio del ser humano, bajo un régimen de responsabilidad claro que fomente la innovación sin sacrificar la justicia ni la

seguridad jurídica. La capacidad funcional es la herramienta técnica que permite esta coexistencia, transformando el desafío algorítmico en un motor de desarrollo económico y social sostenible para el país.

Capítulo 5

Propiedad Intelectual ante la Irrupción de la Inteligencia Artificial Generativa: Autoría, Patentabilidad y Gobernanza de Datos

La convergencia entre los sistemas de inteligencia artificial (IA) y los marcos normativos de la propiedad intelectual representa uno de los cambios de paradigma más significativos en la historia del derecho moderno. Lo que comenzó como una herramienta de asistencia técnica se ha transformado en un motor de generación autónoma capaz de producir textos, imágenes, música y soluciones técnicas que desafían las nociones centenarias de creatividad, originalidad y agencia humana (Calo, 2017).

A medida que el mercado global de la IA se proyecta a una valoración de 191 mil millones de dólares para finales de 2024, las oficinas de propiedad intelectual de todo el mundo enfrentan un incremento sin precedentes en la complejidad de las solicitudes, con un aumento del 718% en las patentes relacionadas con la IA en apenas seis años. Este fenómeno no es meramente técnico, sino profundamente ontológico, pues cuestiona si el derecho de autor y el sistema de patentes, diseñados para incentivar el intelecto humano, pueden o deben extenderse a entidades no biológicas.

La respuesta global ha sido fragmentada, pero convergente en sus principios fundamentales. Mientras que jurisdicciones como los Estados Unidos y la Unión Europea lideran la producción de directrices administrativas y marcos regulatorios, como la Ley de IA, países de América Latina, como México y Perú, han comenzado a emitir fallos judiciales y resoluciones administrativas que reconocen la autoría humana como un derecho intrínseco e inalienable. Este informe analiza exhaustivamente la evolución de estos marcos, los litigios que redefinen el uso de datos de entrenamiento y las propuestas emergentes para equilibrar la innovación tecnológica con la protección de los creadores humanos.

El Diálogo Multilateral y la Construcción de una Gobernanza Global

La Organización Mundial de la Propiedad Intelectual (OMPI) ha asumido un rol protagónico en la facilitación del diálogo entre Estados miembros, académicos y profesionales del sector para cerrar la brecha de información en un campo que avanza a una velocidad superior a la de los procesos legislativos tradicionales. A través de las sesiones de la Conversación de la OMPI sobre Propiedad Intelectual y Tecnologías de Vanguardia, se ha construido un foro inclusivo que ha reunido a más de 17 000 participantes de 172 países. Este proceso ha evolucionado desde discusiones generales sobre políticas en 2019 hasta un análisis técnico detallado de la infraestructura de derechos y de los medios sintéticos en 2025 (Ateriya et al., 2025).

Las sesiones de la OMPI han subrayado una preocupación crítica: la

desigual capacidad entre los países líderes en IA y aquellos que están en proceso de adopción de IA. El Director General de la OMPI ha advertido que la IA corre el riesgo de exacerbar la brecha tecnológica mundial, lo que requiere una conciencia profunda de la capacidad muy desigual en el ámbito de la IA entre las naciones. Esta desigualdad se manifiesta no solo en el acceso a la tecnología, sino también en la capacidad de las oficinas de propiedad intelectual para administrar y registrar creaciones que incorporan componentes algorítmicos complejos.

Cronología y Enfoque de las Sesiones de la Conversación de la OMPI

La evolución de estas sesiones refleja un tránsito desde el asombro inicial hacia una preocupación pragmática por la infraestructura legal. En 2025, el enfoque se ha desplazado hacia la creación de sistemas escalables que permitan la transparencia, el consentimiento y la compensación, asegurando que el ecosistema de propiedad intelectual pueda seguir el ritmo del cambio tecnológico sin socavar la sostenibilidad de las industrias creativas.

Teorías Fundamentales y el Conflicto de la Autoría No Humana

La resistencia de la mayoría de los sistemas legales a reconocer a la IA como autora no es arbitraria, sino que responde a las raíces filosóficas de la propiedad intelectual (Pezzano, 2015). El debate se divide principalmente en tres corrientes teóricas que orientan la respuesta de los tribunales ante las obras generadas por algoritmos. La teoría personalista, predominante en

Europa continental y en América Latina (incluida Argentina, México y Perú), sostiene que la obra es una extensión de la personalidad del autor. Bajo esta premisa, autores como Kant y Hegel sostenían que al crear algo, el individuo deja su espíritu en la realidad. Dado que una máquina carece de subjetividad, conciencia e intención artística, resulta jurídicamente imposible que sea considerada autora en el sentido pleno del término.

Por otro lado, la teoría utilitarista, pilar del sistema anglosajón, especialmente en los Estados Unidos, aborda la propiedad intelectual desde una perspectiva de incentivos económicos. El objetivo no es proteger el alma del autor, sino otorgar un monopolio temporal para fomentar la producción de obras útiles para la sociedad. En este contexto, la pregunta fundamental no es si la IA tiene sentimientos, sino si concederle derechos incentivaría una mayor innovación o, por el contrario, saturaría el mercado con obras de bajo costo, perjudicando la inversión humana. Finalmente, la teoría del trabajo de Locke sugiere que los derechos deben otorgarse a quien invierte esfuerzo y recursos. Esta última visión es la que suele utilizarse para defender la protección de los desarrolladores o de las empresas que entrenan los modelos, argumentando que la inversión masiva en computación y datos justifica dicha protección legal.

A pesar de estas diferencias teóricas, el consenso actual en las oficinas de registro es que la chispa creativa debe provenir de un ser humano. La jurisprudencia estadounidense, por ejemplo, ha citado el caso histórico de *Feist Publications v. Rural Telephone Service*, recordando que la originalidad requiere un componente creativo, por mínimo que sea, y que el simple sudor de la frente o el esfuerzo computacional no son suficientes para obtener protección por derecho de autor.

El Marco Regulatorio de los Estados Unidos:

Directrices y Litigios Paradigmáticos

La Oficina del Copyright de los Estados Unidos (USCO) ha adoptado una de las posturas más rigurosas y detalladas del mundo respecto a la inteligencia artificial. En su informe de enero de 2025 sobre la protección de los outputs de IA generativa, la USCO reafirmó que la autoría humana es un requisito fundamental, basándose tanto en la Cláusula de Copyright de la Constitución como en la interpretación judicial de la Ley de Copyright. Según la USCO, el autor es la persona que traduce una idea en una expresión fija y tangible, y hasta la fecha, ningún tribunal ha reconocido el copyright en material creado por no humanos.

Requisitos de Registro y Deber de Transparencia

Para gestionar la avalancha de obras que integran IA, la USCO ha implementado una guía de registro específica que impone a los solicitantes estrictas obligaciones de divulgación. El incumplimiento de estas obligaciones no solo conlleva el rechazo de la solicitud, sino que también pone en riesgo la validez de los registros ya concedidos, los cuales pueden ser cancelados si se descubre que se omitió el uso de IA.

1. **Uso de la Solicitud Estándar:** Los solicitantes deben evitar el uso de formularios simplificados, ya que solo la Solicitud Estándar permite desglosar y excluir el material no protegible generado por máquinas.
2. **Identificación del Autor:** Está expresamente prohibido listar a un sistema de IA o a una empresa tecnológica como autor o coautor. El campo de

autoría debe describir exclusivamente la contribución humana, como la selección o el arreglo creativo.

3. **Limitación de la Reclamación:** Todo contenido generado por IA que exceda *el mínimo* debe ser excluido explícitamente en la sección de Material Excluido. Por ejemplo, un autor puede reclamar el copyright sobre un texto humano que incorpora imágenes generadas por IA, pero debe aclarar que dichas imágenes no forman parte de la protección solicitada.
4. **Evaluación de la Intervención Humana:** La USCO realiza una investigación caso por caso para determinar si la computadora fue meramente un instrumento de asistencia o si los elementos tradicionales de autoría fueron concebidos y ejecutados por la máquina.

La Batalla de Stephen Thaler y la Denegación de la Agencia de la Máquina

El caso de Stephen Thaler y su sistema DABUS (Device for the Autonomous Bootstrapping of Unified Sentience) ha servido como el principal vehículo para testear los límites del propio sistema. Thaler intentó registrar la obra visual *A Recent Entrance to Paradise*, afirmando que fue creada de forma totalmente autónoma por la IA y que él, como propietario de la máquina, debía ser el titular de los derechos derivados. Tanto la USCO como los tribunales federales rechazaron este argumento, declarando que el copyright nunca se ha extendido tanto como para proteger obras generadas por nuevas tecnologías que operan sin la intervención de ninguna persona humana.

El 2 de marzo de 2026, la Corte Suprema de los Estados Unidos puso

fin a esta saga al denegar el *certiorari* en el caso *Thaler v. Perlmutter*, dejando firme la decisión del Circuito de DC que establece que la autoría humana es un requisito de piedra angular. Esta decisión tiene implicaciones profundas para la industria: las empresas que confían exclusivamente en la IA para generar activos creativos no podrán protegerlos mediante el copyright, lo que significa que competidores podrían copiar dicho contenido libremente a menos que se demuestre una intervención humana significativa en la dirección, el prompting o la alteración del resultado.

El Enfoque de la Unión Europea: El Reglamento de IA y la Minería de Datos

La Unión Europea ha adoptado un enfoque regulatorio más estructurado mediante la Ley de IA (Reglamento 2024/1689), que busca armonizar el mercado europeo y garantizar que el desarrollo tecnológico sea ético y transparente. A diferencia de los Estados Unidos, donde el debate se centra en gran medida en los tribunales, la UE ha introducido obligaciones legislativas directas para los proveedores de modelos de IA de uso general (GPAI).

Transparencia como herramienta de cumplimiento

El artículo 53 de la Ley de IA de la UE establece que los desarrolladores deben proporcionar documentación técnica detallada y publicar un resumen de los contenidos utilizados para entrenar sus modelos. Este requisito de transparencia es vital para que los titulares de derechos puedan ejercer sus prerrogativas conforme a la Directiva sobre Derechos de Autor en el Mercado

Único Digital (CDSM) de 2019. La normativa europea distingue dos escenarios principales para la minería de textos y datos (TDM):

- **Excepción para Investigación Científica:** Permite a instituciones de patrimonio cultural y a organismos de investigación reproducir obras protegidas sin autorización previa, siempre que tengan acceso legítimo y que el fin no sea comercial (Fernández et al., 2023).
- **Excepción para Fines Comerciales (Art. 4):** Permite el TDM a cualquier entidad, a menos que el titular de los derechos haya optado por no participar (opt-out) de manera clara y en un formato legible por máquina, como a través de metadatos o archivos robots.txt.

Sin embargo, la implementación de estos opt-outs ha generado una tensión significativa. Muchos creadores consideran que el sistema de opt-out invierte la carga de la prueba, obligándolos a vigilar constantemente el entorno digital para proteger sus obras de una ingesta masiva por parte de modelos de IA que luego competirán con ellos. En respuesta, el Parlamento Europeo ha sugerido que el principio de territorialidad debe interpretarse de forma amplia, obligando a cualquier modelo de IA comercializado en la Unión a cumplir dichas normas, independientemente de dónde se haya entrenado.

El Código de Buenas Prácticas y los Desafíos de Implementación

En julio de 2025, la Comisión Europea publicó el Código de Buenas Prácticas (CoP) para la implementación de la Ley de IA, que detalla cómo los proveedores deben garantizar la transparencia y el cumplimiento de los derechos de autor. No obstante, algunos analistas advierten que el

cumplimiento pleno de estas normas podría poner en desventaja a los desarrolladores europeos frente a jurisdicciones con regímenes más liberales. Existe el riesgo de que la rigidez regulatoria eleve los costos de transacción hasta el punto de erosionar la competitividad de la UE en la carrera global por la IA.

Jurisprudencia en América Latina: México, Perú y el Blindaje Humanista

América Latina ha emergido como un bastión de la defensa del derecho de autor vinculado a la dignidad humana. En lugar de ver la IA simplemente como una cuestión de eficiencia económica, las cortes de la región la han analizado bajo el prisma de los derechos fundamentales.

La Resolución de la Suprema Corte de Justicia de México (2025)

El 30 de agosto de 2025, la Secretaría de Cultura y el Instituto Nacional del Derecho de Autor (INDAUTOR) celebraron un fallo histórico de la Suprema Corte de Justicia de la Nación (SCJN). La Corte resolvió que las obras creadas íntegramente por sistemas de IA no son registrables, ya que el derecho de autor es un derecho humano exclusivo de las personas físicas, derivado de su intelecto, sentimientos y experiencias personales.

La SCJN subrayó que ni el Convenio de Berna ni el T-MEC reconocen a la inteligencia artificial como sujeto de autoría. Un punto crítico de la sentencia es que los productos de la IA, al no ser obras originales, pasan directamente

al dominio público para su difusión gratuita, especialmente si pueden beneficiar a la humanidad. Esta postura busca evitar que las grandes corporaciones tecnológicas se apropien de la capacidad creativa humana mediante sistemas automatizados.

INDECOPI en Perú: Lineamientos Éticos y Resoluciones Administrativas

En el Perú, el INDECOPI ha sido pionero en la adopción de los Lineamientos para una Inteligencia Artificial Ética y Responsable, aprobados en julio de 2025. Estos lineamientos prohíben expresamente la manipulación de información y la toma de decisiones automatizadas sin supervisión humana en el ámbito administrativo.

En cuanto al registro de obras, la Dirección de Derecho de Autor ha emitido pronunciamientos en 2024 y 2025, señalando que la IA no tiene capacidad para crear con intención ni con contexto artístico. Resoluciones como la del Expediente 0154-2024 han confirmado que la información generada algorítmicamente carece de la subjetividad necesaria para la protección legal. Además, el INDECOPI ha comenzado a utilizar la IA para agilizar procesos internos, como la fiscalización de llamadas spam y la redacción de borradores de resoluciones, manteniendo siempre una supervisión humana activa para evitar errores o sesgos algorítmicos.

Patentes e Inventiva: El Desafío de DABUS a Nivel Global

El debate sobre si la IA puede ser inventora en el sistema de patentes ha seguido un camino paralelo al del derecho de autor, pero con un enfoque más técnico respecto del concepto de concepción. En la mayoría de las legislaciones, la invención nace de un acto mental de concebir una solución a un problema técnico, una facultad que los tribunales siguen reservando a los seres humanos.

En Brasil, el INPI ha avanzado en la elaboración de directrices de examen que permiten patentar invenciones *asistidas* por IA, siempre que se identifique la intervención humana en la configuración del sistema o en la validación de la solución propuesta. Sin embargo, el INPI ha dejado claro que el código fuente y los algoritmos *per se* no son patentables, aunque una solución técnica implementada en software que genere un efecto técnico concreto sí puede serlo.

El caso suizo también es ilustrativo. El Tribunal Administrativo Federal de Suiza dictaminó en 2025 que los sistemas de IA actuales carecen de autonomía para identificar problemas técnicos sin guía humana. El tribunal argumentó que los seres humanos que entrenan el sistema o interpretan su salida tienen derechos de personalidad o derechos comerciales legítimos que justifican su designación como inventores, pero la máquina es simplemente un instrumento sofisticado, comparable a un microscopio o a una herramienta de laboratorio avanzada.

Litigios sobre Datos de Entrenamiento: ¿Uso Legítimo o Infracción Masiva?

Uno de los campos de batalla más activos se encuentra en la fase de entrenamiento de los modelos de lenguaje (LLM). Los desarrolladores de IA argumentan que su uso de obras protegidas es transformativo y, por tanto, está amparado por la doctrina del *Fair Use* en Estados Unidos. Sin embargo, los autores sostienen que el raspado (scraping) masivo de datos sin licencia constituye una infracción directa que afecta su mercado potencial (Kee, 2021).

Análisis de Casos Recientes de Fair Use (2025)

El panorama judicial en California y Delaware ha mostrado resultados divergentes que subrayan la importancia de los hechos específicos de cada caso:

- **Bartz v. Anthropic (2025):** El juez Alsup dictaminó que Anthropic realizó un uso justo al utilizar libros legalmente adquiridos para entrenar sus modelos, calificando la tecnología como una de las más transformativas que veremos en nuestras vidas.
- **Kadrey v. Meta (2025):** El juez Chhabria también falló a favor de Meta bajo la teoría de que el entrenamiento es un proceso integrado con un propósito altamente transformador. No obstante, advirtió que si los demandantes presentaran pruebas de que la IA regurgita sus obras o diluye su mercado, el resultado sería distinto.
- **Thomson Reuters v. Ross Intelligence (2025):** En contraste con los anteriores, este tribunal rechazó la defensa de uso justo. Ross Intelligence

utilizó datos de Westlaw para crear un buscador que competía directamente con Westlaw en el mercado de investigación legal. El juez Bibas señaló que cuando la IA se utiliza para crear un sustituto de mercado del titular de los derechos, el factor de daño comercial prevalece sobre cualquier argumento de innovación tecnológica.

Este último caso es fundamental porque establece que la IA no generativa o puramente funcional puede tener estándares de infracción más estrictos que la IA generativa artística, ya que su objetivo es la sustitución directa de servicios profesionales.

El Futuro de la Regulación: Derechos Sui Generis y Transparencia Técnica

Ante la evidente tensión entre la ley vigente y la realidad tecnológica, se discuten múltiples propuestas para reequilibrar el ecosistema. Algunos expertos sugieren que, si bien la IA no puede ser autora, sus producciones tampoco deberían quedar en un vacío legal absoluto que desincentive la inversión (Petrova, 2021).

1. **Derecho sui generis:** Francia y España han explorado la posibilidad de un derecho de propio tipo para las producciones de IA, similar a la protección que tienen los fabricantes de bases de datos. Esto otorgaría una protección económica limitada (por ejemplo, 15-25 años) para proteger la inversión, sin conferir los derechos morales que acompañan a la autoría humana.
2. **Sistemas de Licencias Colectivas:** Propuestas en España (noviembre de

2024) buscan regular licencias colectivas ampliadas para la explotación masiva de obras en datasets de IA, permitiendo que los autores reciban una remuneración justa a través de sociedades de gestión.

3. **Marcas de Agua y Trazabilidad:** La industria está moviéndose hacia estándares técnicos como C2PA y metadatos IPTC que vinculan el opt-out directamente al archivo multimedia. Esto permitiría a los crawlers de IA detectar automáticamente qué contenidos tienen prohibido su uso para el entrenamiento.
4. **Legal Prompt Engineering y Ética Judicial:** La práctica jurídica misma se está transformando. El surgimiento del Legal Prompt Engineering exige que los abogados aprendan a formular instrucciones precisas sin comprometer la confidencialidad ni la veracidad de la jurisprudencia. Los casos en Argentina en los que se anularon sentencias por jurisprudencia inventada por la IA subrayan que la responsabilidad profesional es indelegable y que la IA debe ser siempre supervisada por el criterio humano.

Síntesis de la Transformación del Paisaje Legal

La propiedad intelectual ha dejado de ser una disciplina estática para convertirse en un campo de experimentación regulatoria. El dinamismo de la IA generativa ha forzado una reevaluación de la cadena de valor creativa, desde el input (la legitimidad de los datos de entrenamiento) hasta el output (la elegibilidad de los resultados para su protección) (Floridi & Taddeo, 2016). La tendencia mundial es clara: protección estricta para el creador humano y

transparencia absoluta para el desarrollador de máquinas.

A medida que avanzamos hacia 2026, el éxito de este nuevo marco dependerá de la capacidad de las naciones para colaborar internacionalmente. Como se discutió en la duodécima sesión de la OMPI, el reto de los medios sintéticos y los deepfakes requiere una respuesta que trascienda las fronteras territoriales y proteja no solo la propiedad intelectual, sino también la integridad personal y la veracidad de la información en el entorno digital. La IA no reemplazará al autor, pero el derecho de autor está siendo reescrito para asegurar que el genio humano siga siendo el motor central del progreso cultural y científico.

Capítulo 6

Robots e IA como sujetos de derecho: Desenredando la perspectiva ontológica y funcional

La irrupción de la inteligencia artificial (IA) y la robótica avanzada en las estructuras sociales, económicas y jurídicas contemporáneas ha provocado un debate de proporciones telúricas en la teoría general del derecho. No se trata simplemente de una actualización tecnológica de las normas vigentes, sino de un cuestionamiento fundamental sobre la naturaleza de la subjetividad jurídica (Miller, 2019). La pregunta central —si un ente no biológico, capaz de tomar decisiones autónomas y aprender de su entorno, puede o debe ser considerado un sujeto de derecho— exige desenredar dos dimensiones que a menudo se confunden: la ontológica, que inquiere por el ser y su esencia, y la funcional, que observa la personalidad jurídica como una herramienta técnica de imputación y responsabilidad.

Este informe analiza exhaustivamente la tensión entre estas perspectivas, explorando desde los fundamentos filosóficos de la dignidad humana hasta las necesidades pragmáticas de los sistemas de responsabilidad civil y de propiedad intelectual. Se examinará la evolución del concepto de persona, los desafíos que plantea la opacidad algorítmica o caja negra y la respuesta normativa en contextos específicos, con especial énfasis en el liderazgo regulatorio del Perú y en las propuestas de la Unión Europea.

La construcción jurídica de la persona: De la máscara romana a la abstracción kelseniana

Para comprender si una máquina puede ser sujeto de derecho, es imperativo desglosar qué entiende el ordenamiento jurídico por persona. Históricamente, la personalidad jurídica no ha sido un atributo estático ni exclusivamente ligado a la biología. El término proviene del latín *persona*, que alude a la máscara que los actores usaban en el teatro clásico para amplificar su voz (*per-sonare*) y representar un papel. En el derecho romano, esta metáfora se tradujo en la distinción entre el ser humano biológico y el actor en la escena legal; no todos los seres humanos eran personas (los esclavos eran considerados *res* o cosas), y no todas las personas eran seres humanos individuales.

Evolución etimológica y teórica del concepto de persona

La doctrina jurídica ha oscilado entre dos grandes teorías para explicar la existencia de sujetos que no son individuos humanos, como las corporaciones o las fundaciones. Por un lado, la teoría de la ficción, defendida por autores como Friedrich Karl von Savigny, sostiene que la persona jurídica es un concepto abstracto y sintético, creado exclusivamente por el legislador, para facilitar el tráfico comercial. Bajo esta premisa, la personalidad es una construcción formal sin existencia real fuera del ordenamiento jurídico, una fórmula técnica para unificar derechos y deberes. Por otro lado, la teoría de la realidad, impulsada por Otto von Gierke, sostiene que las organizaciones sociales poseen una voluntad colectiva propia y una existencia orgánica que el

derecho se limita a reconocer.

En el siglo XX, Hans Kelsen radicalizó la visión formalista al proponer que la persona es únicamente un nodo de imputación (*Zurechnungs-Punkt*). Para Kelsen, no existe una diferencia cualitativa entre la persona física y la jurídica; ambas son personificaciones de un conjunto de normas jurídicas. Si aceptamos esta visión puramente funcional, no habría impedimento teórico para otorgar personalidad jurídica a un sistema de inteligencia artificial, siempre que el legislador lo considere útil para la seguridad jurídica o la gestión de riesgos (Calo, 2017).

Esta distinción es crucial porque si la personalidad jurídica es meramente una máscara técnica, el debate sobre la IA se reduce a una cuestión de conveniencia legislativa. Sin embargo, si la personalidad requiere un sustrato de dignidad y de voluntad real, la IA quedaría permanentemente excluida.

La Perspectiva Ontológica: El ser, la dignidad y la crítica al personismo

La perspectiva ontológica sostiene que el derecho no puede ignorar la realidad del ser. Desde esta óptica, el ser humano no es persona porque el derecho lo diga, sino que el derecho lo reconoce como tal por su dignidad intrínseca, su racionalidad y su libertad. Esta visión, fuertemente anclada en el pensamiento de Immanuel Kant, define a la persona como un fin en sí misma, dotada de una voluntad capaz de imponer leyes morales.

La dignidad humana como límite infranqueable

La dignidad es el valor supremo que impide que un individuo sea tratado simplemente como un medio para alcanzar un fin social o económico. En el contexto de la IA, otorgar personalidad jurídica a una máquina —que es, por definición, un instrumento creado por el hombre— plantearía un conflicto ético profundo. Se corre el riesgo de cosificar al ser humano al compararlo con un algoritmo o de humanizar indebidamente a un objeto inerte.

Juristas y filósofos advierten que la dignidad humana es absoluta, innata y oponible *erga omnes*. Al carecer de vida biológica, sentimientos o conciencia de sí misma, la IA no puede ser titular de derechos de la personalidad (como el derecho a la vida o a la integridad física), ya que estos protegen el sustrato vital del sujeto. El personismo —la idea de que la personalidad depende de rasgos específicos como la memoria o la autoconciencia— es criticado por desdibujar la frontera entre lo humano y lo no humano, abriendo la puerta a que ciertos humanos (como neonatos o personas con discapacidad cognitiva severa) pierdan estatus frente a máquinas súper inteligentes.

El problema de la conciencia: Simulación frente a realidad

Un punto de fricción central es la distinción entre la simulación y la reproducción de estados mentales. La IA moderna, basada en modelos de lenguaje extenso y redes neuronales, es capaz de simular la empatía, el razonamiento y la creatividad con una precisión asombrosa. No obstante, el experimento de la Habitación China de John Searle demuestra que el procesamiento de símbolos (sintaxis) no implica la comprensión (semántica).

Una IA puede responder a una pregunta compleja no porque entienda el concepto, sino porque ha calculado la probabilidad estadística de que una cadena de palabras siga a otra.

Esta falta de intencionalidad real invalida la aplicación de las categorías penales clásicas a la IA. La culpabilidad requiere que el sujeto comprenda la antijuridicidad de su conducta y actúe conforme a esa comprensión. Al ser la IA un sistema de inteligencia heurística o matemática, sus acciones carecen de sentido moral; son eventos fácticos, no actos libres.

La falacia mereológica en el discurso de la IA

La crítica más incisiva a la personalidad electrónica proviene de la neurofilosofía y se denomina falacia mereológica. Este error lógico consiste en atribuir a una parte del sistema funciones que solo pueden predicarse del todo orgánico. Cuando decimos que un algoritmo decide, juzga o aprende, estamos utilizando términos antropomórficos para describir procesos puramente mecánicos de optimización de datos (Floridi & Taddeo, 2016). El derecho no debe caer en la trampa de tomar literalmente estas metáforas. La voluntad es una propiedad del ser humano íntegro, no de una yuxtaposición de hardware y software.

La Perspectiva Funcional: ¿Es necesaria la personalidad electrónica?

Frente a las objeciones ontológicas, surge una corriente pragmática que sostiene que, independientemente de si la IA piensa o siente, el derecho

necesita una categoría para gestionar los riesgos que su autonomía genera. A medida que los robots salen de las fábricas para interactuar en espacios públicos —como vehículos autónomos o asistentes médicos—, la atribución de responsabilidad se vuelve una pesadilla técnica.

El modelo de la Resolución Europea de 2017

En febrero de 2017, el Parlamento Europeo aprobó una resolución con recomendaciones sobre las normas de derecho civil aplicables a la robótica. El documento sugería la creación de un estatus jurídico específico para los robots más sofisticados, denominados personas electrónicas. El objetivo no era otorgarles derechos humanos, sino dotarlos de una personalidad limitada para:

1. **Asumir la responsabilidad por daños:** que el robot sea el sujeto pasivo de reclamaciones judiciales.
2. **Poseer un patrimonio de afectación:** un fondo de capital o un sistema de seguros obligatorio para cubrir indemnizaciones.
3. **Facilitar el comercio:** Permitir que las máquinas realicen transacciones o contratos de manera autónoma.

Esta propuesta se apoya en la analogía con las personas jurídicas o morales. Si una empresa (una abstracción) puede ser responsable de un vertido tóxico, ¿por qué un sistema autónomo no podría serlo de un accidente de tráfico?

El riesgo de impunidad y el escudo corporativo

Sin embargo, esta visión funcional enfrenta una crítica demoledora: el

riesgo de impunidad. Otorgar personalidad a la IA podría convertirse en un escudo para que las empresas tecnológicas y los programadores evadan su responsabilidad directa. Si un robot es una persona, el fabricante podría argumentar que el daño fue producto de una decisión autónoma de la máquina, lo que rompería el nexo causal con la conducta humana. Esto crearía una zona de deformación moral (*moral crumple zone*), donde el usuario o el propio sistema absorbe el impacto legal mientras los verdaderos beneficiarios económicos quedan indemnes. Responsabilidad Civil y la Opacidad del Algoritmo

El nexo causal es la piedra angular de la responsabilidad civil. Tradicionalmente, para que alguien sea condenado a pagar un daño, debe demostrarse que su acción u omisión fue la causa directa del resultado. La IA rompe este esquema debido al efecto de la caja negra (*black box*): la imposibilidad de entender o predecir cómo un sistema de aprendizaje profundo llega a una conclusión específica a partir de millones de datos (Floridi & Taddeo, 2016).

El efecto de la caja negra y la ruptura del nexo causal

En los sistemas de *machine learning*, el código no es estático; evoluciona a través de la interacción con el entorno. Esto genera una imprevisibilidad que dificulta la aplicación de los conceptos tradicionales de negligencia. ¿Cómo probar que un programador fue negligente si el sistema tomó una decisión que no estaba prevista en el código original?

Para abordar este vacío, la doctrina propone transitar hacia la responsabilidad objetiva o la responsabilidad por riesgo. Bajo este régimen,

quien introduce en el mercado una tecnología peligrosa o incierta con el fin de obtener beneficio debe responder por los daños, independientemente de la culpa. En términos económicos, se aplica la Fórmula de Hand: el sujeto es negligente si el costo de las precauciones (B) es menor que la probabilidad de pérdida (P) multiplicada por la gravedad de la misma (L):

$$B < P \cdot L$$

Sin embargo, en el ámbito de la IA, la probabilidad () suele ser incalculable debido a la opacidad del sistema, lo que hace que la negligencia sea un estándar ineficaz y la responsabilidad objetiva sea la única salvaguarda para la víctima.

El Liability Sponge y la supervisión humana

Un fenómeno preocupante es el del operador como esponja de responsabilidad (*liability sponge*). Las leyes suelen exigir la supervisión humana para validar las decisiones de la IA. No obstante, si el sistema opera a una velocidad o complejidad sobrehumana, el supervisor humano se convierte en un mero observador pasivo que, sin embargo, es legalmente responsable si algo sale mal. El derecho peruano, mediante el Reglamento de la Ley 31814, intenta mitigar esto al exigir que la supervisión sea efectiva y que las decisiones críticas no sean totalmente autónomas.

Propiedad Intelectual e Invención: El desafío de la autoría no humana

La propiedad intelectual es quizás el área en la que la tensión funcional es más evidente. El caso de DABUS (un sistema de IA que generó de forma autónoma una luz de emergencia y un recipiente de comida) ha recorrido los tribunales de todo el mundo. Stephen Thaler, su creador, solicitó patentes en nombre de DABUS como inventor, argumentando que no intervino en el proceso creativo.

El caso DABUS y la doctrina de la personalidad

La respuesta judicial ha sido un rechazo casi universal, basado en que las leyes de patentes y de derechos de autor presuponen un creador humano. El Tribunal Supremo del Reino Unido y las oficinas de patentes de EE. UU. y la UE determinaron que un inventor debe ser una persona natural (Georgieva, 2020). El fundamento es tanto técnico como económico:

- **Capacidad jurídica:** Una máquina no puede poseer derechos de propiedad ni transferirlos a un tercero.
- **Incentivos:** El sistema de patentes busca incentivar el esfuerzo humano; las máquinas no necesitan incentivos económicos para crear.

Esta negativa genera una paradoja: si una invención valiosa es generada por una IA sin ayuda humana, bajo las leyes actuales, esa invención no es patentable y pasa directamente al dominio público. Esto ha llevado a proponer un derecho sui generis para las creaciones de IA, similar al que protege las bases de datos, que otorgue una protección limitada al inversor o propietario de la máquina, sin necesidad de reconocerle personalidad jurídica al algoritmo.

El marco normativo en el Perú: Hacia una

gobernanza ética y antropocéntrica

Perú se ha convertido en un referente regional al promulgar la Ley 31814 (2023) y su Reglamento, el Decreto Supremo 115-2025-PCM. A diferencia de la propuesta europea de 2017, el modelo peruano rechaza implícitamente la personalidad jurídica de la IA, optando por un enfoque claro de gestión de riesgos y de responsabilidad humana.

Clasificación de Riesgos y Obligaciones

El reglamento peruano clasifica los sistemas de IA según el daño potencial a los derechos fundamentales, un modelo inspirado en el *AI Act* de la Unión Europea pero adaptado a la realidad nacional:

1. **Uso Prohibido (Riesgo Inaceptable):** Sistemas que vulneran la dignidad humana, como la vigilancia biométrica masiva en espacios públicos (salvo orden judicial), la manipulación subliminal o los sistemas de crédito social (Eichberger, 2024).
2. **Riesgo Alto:** aplicaciones en salud, finanzas (scoring crediticio), justicia y servicios públicos esenciales. Requieren evaluaciones de impacto, transparencia algorítmica y una supervisión humana estricta.
3. **Riesgo Aceptable:** Todos los demás usos (filtros, asistentes básicos). Se promueven la autorregulación y los principios éticos voluntarios (Floridi & Cowls, 2019).

Responsabilidad y Agravantes Penales: Ley 32314

Un hito histórico fue la aprobación de la Ley 32314 en abril de 2025, que modifica el Código Penal peruano para incluir el uso de IA como

circunstancia agravante de la pena. Esto refuerza la tesis de que la IA es un instrumento:

- Si se usa IA para generar *deepfakes* pornográficos o difamatorios, la pena aumenta hasta en un tercio.
- La suplantación de identidad o estafa mediante clonación de voz (como en el caso del CEO simulado) conlleva sanciones agravadas.

Este enfoque soluciona el problema de la imputación sin recurrir a la ficción de la personalidad electrónica: la responsabilidad siempre recae en el agente humano que desplegó o permitió el uso del sistema.

Ética Global y el Fin del Modelo Autoregulatorio

El debate sobre la subjetividad de la IA no ocurre en el vacío. Organismos internacionales como la UNESCO han establecido estándares globales que enfatizan que los derechos humanos y la dignidad deben ser la piedra angular de cualquier desarrollo. La Recomendación de la UNESCO (2021), suscrita por 193 estados, rechaza la idea de que la IA deba ser un sujeto moral o legal autónomo, y insiste en que la responsabilidad última debe recaer siempre en los seres humanos.

Los Principios de la OCDE y la Gobernanza Adaptativa

La OCDE promueve la transparencia, la explicabilidad y la robustez técnica. El consenso global se aleja de la autorregulación de las grandes tecnológicas (que prioriza los intereses comerciales) para abrazar marcos

legales vinculantes que protejan la privacidad y eviten la discriminación algorítmica. La IA no es intrínsecamente buena ni mala; su impacto depende de un diseño que respete la diversidad y la inclusión (Jobin et al., 2019).

El análisis exhaustivo de las perspectivas ontológicas y funcionales revela que la atribución de personalidad jurídica a la inteligencia artificial es, por el momento, una solución innecesaria y potencialmente peligrosa. Ontológicamente, la IA carece de los atributos de conciencia, voluntad y dignidad que fundamentan la noción de persona en las democracias constitucionales (Cadena & Gayosso, 2016). Funcionalmente, aunque la autonomía de las máquinas genera desafíos de responsabilidad, estos pueden y deben resolverse mediante la adaptación de las categorías existentes de responsabilidad objetiva, de seguros obligatorios y de regímenes de responsabilidad por productos defectuosos.

El modelo peruano, con su enfoque en la supervisión humana y en la agravación de las penas por el uso indebido de la tecnología, ofrece una ruta equilibrada: fomenta la innovación sin sacrificar la centralidad del ser humano. El derecho no debe crear máscaras que sirvan de refugio a la impunidad, sino herramientas que garanticen que el progreso tecnológico sea siempre un medio para el bienestar de la persona humana, único y verdadero sujeto de derechos. El futuro exige una gobernanza algorítmica humanista, donde la transparencia sustituya a la opacidad y la responsabilidad legal siga siempre el rastro del beneficio económico y de la voluntad creadora del hombre.

Conclusión

La posibilidad de otorgar personalidad a los sistemas autónomos no es solo un problema técnico-jurídico, sino que toca las fibras más profundas del humanismo. El debate se polarizó entre dos grandes corrientes filosóficas aplicadas al Derecho: (1) el humanismo tradicional, que sostiene que el hombre es el principio y fin del Derecho, por lo que otorgar personalidad a las máquinas desdibujaría la línea entre lo vivo y lo inerte, poniendo en duda la dignidad humana y la libertad como fundamentos del orden político; (2) el funcionalismo pragmático, que sostiene que el Derecho debe adaptarse a la realidad.

Dada la naturaleza transfronteriza de la tecnología, la regulación no puede ser un esfuerzo aislado de los estados individuales. La ONU ha instado a la creación de mecanismos globales para una gobernanza ética y responsable, con el fin de evitar una carrera armamentista de la inteligencia artificial y una competencia a la baja en los estándares de seguridad y de derechos humanos. Los principios rectores propuestos por el Órgano Asesor de Alto Nivel de la ONU incluyen:

- *Inclusividad:* La IA debe utilizarse en beneficio de todos, cerrando la brecha digital entre el norte y el sur del mundo.
- *Soberanía del Derecho Internacional:* La gobernanza de la IA debe estar anclada en la Carta de las Naciones Unidas y el derecho internacional de los derechos humanos.
- *Gobernanza Ágil:* Las normativas deben ser flexibles y capaces de adaptarse a la velocidad de la innovación, utilizando herramientas como

el monitoreo continuo y el red-teaming para detectar sesgos y alucinaciones en tiempo real.

La cuestión de si los sistemas autónomos deben tener personalidad jurídica no tiene una respuesta definitiva. Este trabajo argumenta que el debate en sí mismo es la mejor herramienta para preparar a nuestras instituciones frente a la incertidumbre tecnológica. Aunque la regulación actual —como en la Unión Europea y en el Perú— se basa en un modelo de responsabilidad humana con diferentes niveles de riesgo, la creciente autonomía de estos sistemas indica que la idea de la personalidad electrónica volverá a estar en la agenda a medida que las máquinas asuman roles de mayor impacto social.

La implementación de este marco en Perú enfrenta retos únicos, como la alta informalidad económica, que supera el 70% de la PEA, y las deficiencias en los datos estructurados. La normativa destaca que la supervisión humana es imprescindible, especialmente cuando la ausencia de registros formales puede causar sesgos y exclusiones injustas a los ciudadanos más vulnerables. La Secretaría de Gobierno y Transformación Digital (SGTD) es la autoridad técnica responsable de asegurar que la adopción de la IA sea inclusiva y respete la privacidad y la protección de los datos personales, conforme a la Ley 29733.²⁸

En conclusión, el derecho debe actuar tanto como restricción como como facilitador ético, asegurando que la innovación beneficie a la humanidad. Al examinar las dimensiones históricas, técnicas, legislativas y filosóficas de la personalidad jurídica de la IA, este libro invita a juristas, legisladores y

ciudadanos a colaborar en la creación de un marco legal en el que la tecnología amplifique nuestras capacidades sin afectar nuestra esencia como sujetos soberanos. El reto es grande, pero la oportunidad de redefinir la justicia en la era digital supone un compromiso esencial para nuestra generación.

Bibliografía

- Abramova, M., Popova, A., & Gorokhova, S. (2020). Social code in contemporary Russia: Advantages and risks of the juridical regulation. *Revista Latinoamericana de Derecho Social*, 1(37), 29–53. <https://doi.org/10.22201/ijj.24487899e.2020.37.14862>
- Albisua, J., & Pacheco, P. (2025). Ethical Considerations About Artificial Intelligence (AI) Use in Medical Practice. *Open Respiratory Archives*, 7(1). <https://doi.org/10.1016/j.opresp.2024.100383>
- Amershi, S., Weld, D., Vorvoreanu, M., Fourney, A., Nushi, B., Collisson, P., Suh, J., Iqbal, S., Bennett, P. N., Inkpen, K., Teevan, J., Kikin-Gil, R., & Horvitz, E. (2019). Guidelines for human-AI interaction. *Conference on Human Factors in Computing Systems - Proceedings*. <https://doi.org/10.1145/3290605.3300233>
- Ateriya, N., Sonwani, N. S., Thakur, K. S., Kumar, A., & Verma, S. K. (2025). Exploring the ethical landscape of AI in academic writing. *Egyptian Journal of Forensic Sciences*, 15(1). <https://doi.org/10.1186/s41935-025-00453-1>
- Cadena, A. E., & Gayosso, R. S. (2016). Las facultades constitucionales del Ejecutivo en América Latina: entre la concentración y la dispersión de poder. *Estudios Políticos*, 37(Sup 44), 111–141. <https://doi.org/10.1016/j.espol.2016.02.005>
- Calo, R. (2017). Artificial Intelligence Policy: A Roadmap. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3015350>
- Cantú Rivera, H. (2016). Towards an international treaty on corporate responsibility in the field of human rights? Reflections on the first session of the open-ended intergovernmental working group. *Anuario Mexicano de Derecho Internacional*, 16, 425–460.

<https://doi.org/10.22201/ijj.24487872e.2016.16.532>

Eichberger, F. (2024). Self-judgment in international law: Between judicialization and pushback. *Leiden Journal of International Law*, 37(4), 915–938. <https://doi.org/10.1017/S0922156524000323>

Fernández-Vigo, J., Almorín-Fernández-Vigo, I., Kudsieh, B., & Fernández-Vigo, J. I. (2023). Scientific research versus technological research: A necessary clarification. *Archivos de La Sociedad Espanola de Oftalmologia*, 98(9), 491–492. <https://doi.org/10.1016/j.oftal.2023.04.008>

Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*. <https://doi.org/10.1162/99608f92.8cd550d1>

Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083). <https://doi.org/10.1098/rsta.2016.0360>

Georgieva, V. P. (2020). Trump's foreign policy and international trade law. *Anuario Mexicano de Derecho Internacional*, 20, 687–721. <https://doi.org/10.22201/IIJ.24487872E.2020.20.14494>

Inglada Galiana, L., Corral Gudino, L., & Miramontes González, P. (2024). Ética e inteligencia artificial. *Revista Clínica Española*, 224(3), 178–186. <https://doi.org/10.1016/j.rce.2024.01.007>

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389–399. <https://doi.org/10.1038/s42256-019-0088-2>

Kee Wong, Y. (2021). Dealing Crisis Management using AI. *International Journal of Computer Science, Engineering and Applications*, 11(05), 15–22. <https://doi.org/10.5121/ijcsea.2021.11502>

Luppichini, R., & So, A. (2016). A technoethical review of commercial drone use in the context of governance, ethics, and privacy. *Technology in Society*, 46, 109–119. <https://doi.org/10.1016/j.techsoc.2016.03.003>

Maldonado Sierra, G. A. (2019). Social security in the right of subregional integration of Latin America and the Caribbean. *Revista Latinoamericana de Derecho Social*, (28), 103–133. <https://doi.org/10.22201/ijj.24487899e.2019.28.13145>

Mayol, J. (2023). Inteligencia artificial generativa y educación médica. *Educacion Medica*, 24(4). <https://doi.org/10.1016/j.edumed.2023.100851>

Meltzoff, A. N., Kuril, P. K., Movellan, J., & Sejnowski, T. J. (2009). Foundations for a new science of learning. *Science*, 325(5938), 284–288. <https://doi.org/10.1126/science.1175626>

Mendieta González, D., & Jaramillo, C. E. (2019). The general system of social security in health of Colombia. universal, but inefficient: A purpose of twenty-five years of its creation. *Revista Latinoamericana de Derecho Social*, (29), 201–218. <https://doi.org/10.22201/ijj.24487899e.2019.29.13905>

Mendizábal Bermúdez, G., & Kurczyn Villalobos, P. (2017). Apuntes sobre el derecho internacional de la seguridad social y su relación con América Latina. *Revista Latinoamericana de Derecho Social*, 25(25), 37–70. <https://doi.org/10.22201/ijj.24487899e.2017.25.11496>

Miller, T. (2019). Explanation in artificial intelligence: Insights from the social sciences. *Artificial Intelligence*, 267, 1–38. <https://doi.org/10.1016/j.artint.2018.07.007>

Montomoli, M. (2023). Un cambio de era: cómo la inteligencia artificial está revolucionando la publicación científica. *NefroPlus*, 15(1), 112–114. [https://doi.org/10.1016/s1888-9700\(24\)00025-2](https://doi.org/10.1016/s1888-9700(24)00025-2)

Petrova Georgieva, V. (2015). La judicialización: una nueva característica del sistema jurídico internacional. *Anuario Mexicano de Derecho Internacional*, 15(1), 3–45. <https://doi.org/10.1016/j.amdi.2015.06.001>

Petrova Georgieva, V. (2021). Hierarchy between domestic and international tribunals: Utopia or near future? *ACDI Anuario Colombiano de Derecho Internacional*, 14(1), 21–71. <https://doi.org/10.12804/revistas.urosario.edu.co/acdi/a.10114>

Pezzano, L. (2015). Control de constitucionalidad de los actos de los órganos de las Naciones Unidas: Una aproximación desde la perspectiva de la Corte Internacional de Justicia. *Anuario Mexicano de Derecho Internacional*, 15(1), 47–91. <https://doi.org/10.1016/j.amdi.2014.09.001>

Russell, S., Dewey, D., & Tegmark, M. (2015). Research priorities for robust and beneficial artificial intelligence. *AI Magazine*, 36(4), 105–114. <https://doi.org/10.1609/aimag.v36i4.2577>

Sánchez López, J. D., Cambil Martín, J., Villegas Calvo, M., & Luque Martínez, F. (2021). Inteligencia artificial y robótica. Reflexiones sobre la necesidad de implementar un nuevo marco bioético. *Journal of Healthcare Quality Research*, 36(2), 113–114. <https://doi.org/10.1016/j.jhqr.2019.07.009>

Singh, D. K., Kumar, M., Fosch-Villaronga, E., Singh, D., & Shukla, J. (2023). Ethical Considerations from Child-Robot Interactions in Under-Resourced Communities. *International Journal of Social Robotics*, 15(12), 2055–2071. <https://doi.org/10.1007/s12369-022-00882-1>

De esta edición de “*Personalidad jurídica de los sistemas autónomos: un debate necesario*”, se terminó de editar en la ciudad de Colonia del Sacramento en la República Oriental del Uruguay el 13 de febrero de 2026



Personalidad jurídica de los sistemas autónomos: un debate necesario

Escrito por: Fernando Esteban Quiroz Ponce, Juan Antonio
Zevallos Cadillo, Eladio Guzmán Villa, Fausto David Berrocal
Huarcaya, Gloria Gonzales Santos, Joel Orlando Santillán Tuesta

ISBN: 978-9915-698-70-0



9 789915 698700