

UNIVERSIDAD
CATÓLICA
BOLIVIANA
ERIGIDA CANÓNICAMENTE
POR LA SANTA SEDE DESDE 2023



Carrera de
Derecho



IpD
Instituto para
la Democracia

DE
Revista
de RE
CHO de la
U.C.B.

U.C.B. Law Review

Revista Vol. 10, N.º 18

Abril 2026

La Paz - Bolivia

ISSN 2523-1510 (en línea) - ISSN 2521-8808 (impresa)

UNIVERSIDAD
CATÓLICA
BOLIVIANA
ERIGIDA CANÓNICAMENTE
POR LA SANTA SEDE DISEÑO 2023

DER
JUR

Carrera de
Derecho



IpD
Instituto para
la Democracia

DE
Revista de RE
CHO de la
U.C.B.

U.C.B. Law Review

Revista Vol. 10, N.º 18 | Abril 2026 | La Paz - Bolivia

Revista de Derecho de la UCB

UCB Law Review

Revista Vol. 10, N.º 18
Depósito legal 4-3-80-17
ISSN 2523-1510 (en línea)
ISSN 2521-8808 (impresa)



Revista digital
lawreview.ucb.edu.bo

EDITOR INVITADO



Guillermo Huitrón Nieto
Director de Radar Legal Tech Latam.

Sebastián Uría Vacaflores
Investigador en Legaltech

CONSEJO EDITORIAL

Presidente

Leonardo D. Villafuerte Philippsborn
Docente investigador tiempo completo
Responsable del Instituto para la Democracia
Facultad de Derecho y Ciencias Políticas
Universidad Católica Boliviana "San Pablo"
lvillafuerte@ucb.edu.bo

Carlos Cordero Carraffa
Decano de la Facultad de Derecho y Ciencias Políticas
Universidad Católica Boliviana "San Pablo"
ccordero.c@ucb.edu.bo

Felipe Cordero Cervantes
Carrera de Derecho
Universidad Católica Boliviana "San Pablo"
fcordero@ucb.edu.bo

Editora asistente

Paula Labarrera Frías

Flujo de trabajo editorial

Natalia L. Trigoso Zegarra

Diseño y diagramación

Cesar Trujillo

Folio – Unidad de Diseño e Impresión UCB

Equipo de desarrollo y mantenimiento web

Crissel Gutiérrez

Biblioteca Central UCB – Responsable de Soporte y Adecuación Web

Humberto Rafael Rodríguez Saravía – Asistente de Soporte Web

Mons. Ricardo Centellas Guzmán
Arzobispo de Sucre y Gran Canciller

José Fuentes Cano
Rector Nacional

Susan Santillán Butrón
Vicerrectora Académica Nacional

Marcos Delgadillo Moreira
Vicerrector Administrativo Financiero Nacional

Pablo Bernardo Aramayo Arze
Secretario General Nacional

Ximena Peres Arenas
Rectora de Sede La Paz

Carlos Cordero Carraffa
Decano de la Facultad de Derecho y Ciencias Políticas de Sede La Paz
Director de la Carrera de Ciencias Políticas y
Relaciones Internacionales de Sede La Paz

Felipe Bernardo Cordero Cervantes
Director de la Carrera de Derecho de Sede La Paz

Lectores académicos nacionales institucionales



Academia Nacional de Ciencias Jurídicas de Bolivia
Fundada el 21.12.1988
Personalidad jurídica
RS 207518 de 23.4.1990

Lectores académicos nacionales

Boris Wilson Arias López

Tribunal Constitucional Plurinacional
Sucre - Bolivia

Jorge Antonio Asbun Rojas

Universidad Autónoma Gabriel René Moreno
Santa Cruz - Bolivia

José Carlos Bernal Rivera

Investigador independiente
La Paz - Bolivia

Joaquín Andrés Chacín Barragán

Universidad Católica Boliviana San Pablo
Cochabamba - Bolivia

Luis Armando Claros Terán

CIDES - Universidad Mayor de San Andrés
La Paz - Bolivia

Paola Doris Cortés Martínez

Abogada en el ejercicio libre de la profesión
La Paz - Bolivia

Pablo Bernardo Miller Pazos

Universidad Católica Boliviana "San Pablo"
La Paz - Bolivia

Rodrigo Rivera Aldazosa

Universidad Privada Boliviana
Santa Cruz - Bolivia

José Antonio Rivera Santivañez

Universidad Mayor de San Simón
La Paz - Bolivia

Erick San Miguel

Universidad Mayor de San Andrés
La Paz - Bolivia

Rafael Vergara Sandóval

Universidad de Alicante, España
Universidad de Salamanca, España
La Paz - Bolivia

Fernando Zambrana Sea

Defensoría del Pueblo
La Paz - Bolivia

Marco Antonio Saavedra Mogro

Universidad Mayor de San Andrés
La Paz - Bolivia

Leonardo Nicodemo Asturizaga

Universidad La Salle
La Paz - Bolivia

Andrea Patricia Coca Martínez

Juzgado Público de la Niñez y Adolescencia
2do.
Tarija - Bolivia

Lectores académicos internacionales

Pablo Ezedín Alarcón Prado

Asesor Legal - Servicio Jurídico Comunidad
Andina
Lima - Perú

José Gabriel Barragán García

Juez Familia, Mujer, Niñez y Adolescencia
Ecuador

Ursula Cristina Basset

Universidad Austral y Pontificia Universidad
Católica Argentina
Argentina

Edda Karen Céspedes Babilón

Universidad San Ignacio de Loyola
Lima, Perú

Nathalia Bautista Pizarro

Universidad Externado de Colombia
Colombia

Mónica María Bustamante Rúa

Universidad de Medellín
Colombia

Manuel Bermúdez Tapia

Universidad Nacional Mayor de San Marcos
Perú

Fernando Cantuarias

Universidad del Pacífico
Perú

Ligia De Jesús Castaldi

Ave Maria School of Law
Estados Unidos

Danny José Cevallos C.

Departamento de Filosofía del Derecho y
Derecho Internacional Privado
Área de Filosofía del Derecho
Universidad de Alicante
España

Juan Cianciardo

Universidad de Navarra
España

Mario Eugenio Chaumet

Universidad Nacional de Rosario
Argentina

María Laura Farfán Bertrán

Universidad Nacional de Cuyo
Argentina

María Angela Fiorentini

Universidad Austral
Buenos Aires - Argentina

Eric Franco

Investigador independiente
Perú

Débora Guerra Moreno

Universidad Libre Seccional Cúcuta
Colombia

Yudith López Soría

Universidad Laica Vicente Rocafuerte
de Guayaquil
Ecuador

Carlos Alberto Matheus López

Pontificia Universidad Católica del Perú
Perú

Giovanni Priori Posada

Pontificia Universidad Católica del Perú
Perú

Yésica Quispe Arancibia

COO & Founder, Favorcito (startup, Latam)
Bogotá, Colombia

Débora Ranieri de Cechini

Pontificia Universidad Católica Argentina
Argentina

Katherine Andrea Rolong Arias

Universidad de Medellín y Juez de
Antioquía
Colombia

Claudio Jesús Santagati

Pontificia Universidad Católica Argentina
Argentina

Alfonso Santiago

Universidad Austral
Argentina

Guillermo Pedro Bernardo Tinti

Universidad Católica de Córdoba
Argentina

Fernando Alfredo Ubiría

Pontificia Universidad Católica Argentina
Argentina

Orión Vargas Vélez

Universidad de Medellín y Universidad
EAFIT
Colombia

Erika Valdivieso López

Universidad Católica Santo Toribio de
Mogrovejo
Perú

Contenido

Presentación

11-12

Artículos académicos

Academic Articles

Edgar David Oliva Terán

Ética con IA: del soft law al control real por contrato y código

Ethics with AI: from Soft Law to Real Control through Contract and Code

15-52

María Fernanda Iriarte Morales

Insurtech en Bolivia: Análisis Funcional de su Régimen Regulatorio

Insurtech in Bolivia: Functional Analysis of its Regulatory Regime

55-90

Rodrigo René Cruz Apaza

Inteligencia artificial y proceso constitucional en Bolivia. Una cavilación desde las tareas, directrices y limitaciones a su aplicación

Artificial Intelligence and the Constitutional Process in Bolivia. A Reflection on the Tasks, Guidelines, and Limitations of its Application

93-135

Artículos de opinión

Opinion Articles

Pablo Escóbar Ascarrunz

La firma digital en una cultura procesal analógica

Digital Signatures in an Analog Procedural Culture

139-155

Félix Fabian Espinoza Valencia

Naturaleza jurídica de las *memecoins*

Legal Nature of Memecoins

157-176

Mariana Soria Galvarro Gaillard

Los desafíos de la trazabilidad en la era de las *Black Boxes*

The Challenges of Traceability in the Era of Black Boxes

179-193

Políticas editoriales

Editorial Policies

195-213

Presentación

En un momento histórico en el que los algoritmos deciden, las máquinas aprenden y el código se convierte en ley, el Derecho no puede permanecer como mero espectador. Debe transformarse en el intérprete crítico de esta nueva realidad, en el arquitecto de marcos que equilibren innovación y protección, autonomía tecnológica y dignidad humana.

En esta ocasión, la Revista de Derecho de la U.C.B. presenta una edición especial dedicada al *Derecho 4.0: Desafíos de las nuevas tecnologías en el Derecho*, elaborada en colaboración con *Radar Legal Tech Latam*, representando un esfuerzo colectivo por comprender y enfrentar las cuestiones jurídicas más urgentes de nuestro tiempo. La inteligencia artificial, los contratos inteligentes, la tokenización de activos, la ciberseguridad, las insurtech y la transformación digital del Estado plantean interrogantes que desafían las categorías tradicionales del Derecho. ¿Cómo regular lo que aún no termina de nacer? ¿Cómo proteger derechos fundamentales en espacios donde la privacidad se diluye en datos? ¿Cómo garantizar que la ética no sea solo discurso, sino código ejecutable?

Los artículos aquí reunidos ofrecen análisis rigurosos, perspectivas innovadoras y propuestas concretas ante una realidad electrónica disruptiva; “*Code is Law*”.

Edgar David Oliva Terán nos invita a repensar la ética digital, mostrando cómo el *soft law* se transforma en control real mediante contrato y código, convirtiendo principios morales en mecanismos de gobernanza algorítmica. María Fernanda Iriarte aborda la tensión regulatoria en el ecosistema insurtech boliviano, proponiendo un análisis funcional que privilegie la sustancia de la actividad por encima de la denominación comercial. Rodrigo René Cruz Apaza explora las posibilidades y límites de la inteligencia artificial en el proceso constitucional boliviano, demostrando que estas herramientas pueden coadyuvar —más no reemplazar— el razonamiento jurídico humano.

Cada contribución refleja un compromiso compartido: entender el Derecho 4.0 no como una amenaza, sino como una oportunidad para redefinir los contornos de la justicia en la era digital. El número que hoy presentamos mantiene el carácter plural, internacional y científico que distingue a esta Revista, reafirmando su compromiso con la investigación académica rigurosa, la ética profesional y el diálogo jurídico interdisciplinario.

Detrás de cada artículo existe la esperanza de que el Derecho siga siendo el instrumento que abre puertas hacia la justicia, la convivencia democrática y la dignidad humana, incluso —y especialmente— cuando esas puertas están escritas en código.

Radar Legal Tech LATAM

Editor invitado

Artículo Académicos

Academic Articles

Ética con IA: del soft law al control real por contrato y código

Ethics with AI: from Soft Law to Real Control through Contract and Code

► **Edgar David Oliva Terán**

Investigador independiente • Santa Cruz – Bolivia
<https://orcid.org/0009-0008-1575-3474> • doliva@cmlawyers.com.bo

Revista de Derecho de la UCB – UCB Law Review, Vol. 10 N° 18, abril 2026, pp. 15-52
ISSN 2523-1510 (en línea), ISSN 2521-8808 (impresa).
DOI: <https://doi.org/10.35319/lawreview.202618134>

Recibido: 30 de octubre de 2025 • Aceptado: 10 de abril de 2026

Resumen

El presente artículo tiene por objetivo analizar cómo la inteligencia artificial transforma la ética en una forma efectiva de regulación digital. Ante la ausencia de un marco normativo global, las plataformas incorporan principios morales en algoritmos, términos de servicio y arquitecturas técnicas, convirtiendo valores en mecanismos de control conductual y planteando la cuestión de qué moral es la que efectivamente gobierna la conducta de los usuarios. Mediante un enfoque teórico y jurídico-filosófico, basado en el análisis doctrinal y normativo del *soft law*, el derecho contractual y la gobernanza algorítmica, el presente artículo examina la transición del *soft law* hacia prácticas coercitivas de facto, donde el código y el contrato adquieren fuerza normativa. Finalmente, se propone un marco conceptual de gobernanza ética orientado a delimitar los actuales criterios de transparencia, proporcionalidad y revisión humana, contribuyendo al debate sobre ética, poder y regulación en la era algorítmica.

Palabras clave: ética digital; inteligencia artificial; soft law; gobernanza algorítmica; regulación tecnológica.

Abstract

This article aims to analyze how artificial intelligence transforms ethics into an effective form of digital regulation. In the absence of a global normative framework, platforms embed moral principles into algorithms, terms of service, and technical architectures, turning values into mechanisms of behavioral control and raising the question of which morality effectively governs user behavior. Through a theoretical and legal-philosophical approach, based on doctrinal and normative analysis of *soft law*, contract law, and algorithmic governance, the article examines the transition from *soft law* to de facto coercive practices, where code and contract acquire normative force. Finally, it proposes a conceptual framework for ethical governance aimed at delineating current criteria of transparency, proportionality, and human oversight, contributing to the debate on ethics, power, and regulation in the algorithmic era.

Keywords: digital ethics; artificial intelligence; soft law; algorithmic governance; technological regulation.

1. Introducción

En el debate público contemporáneo suele asumirse que la inteligencia artificial (IA) es, en esencia, una herramienta neutral y que los problemas normativos surgen únicamente de su uso indebido. Esa suposición resulta insostenible cuando se observa cómo la IA opera efectivamente en plataformas y servicios digitales. Lejos de limitarse a asistir decisiones humanas, la IA clasifica, prioriza, recomienda, deshabilita, sanciona y condiciona el acceso a oportunidades, visibilidad y participación. En ese tránsito desde el cálculo hacia la decisión, emerge una tesis central de este artículo: la IA no es neutral, sino que vehiculiza una forma de moral privatizada.

Esta afirmación no atribuye agencia moral a los sistemas, ni presupone conciencia o intención. El problema no es si la máquina “razona moralmente”, sino qué criterios de corrección se

vuelven operativos cuando valores, políticas internas y supuestos sociales se traducen a parámetros técnicos y mecanismos de *enforcement*. Cuando lo considerado aceptable o riesgoso deja de discutirse públicamente y se ejecuta mediante arquitectura técnica, el conflicto moral no desaparece, sino que se desplaza hacia regímenes privados de decisión.

Este razonamiento se ve reforzado por una condición estructural del entorno digital: la ausencia de una autoridad normativa global capaz de regular de manera unificada. En ese contexto, proliferan instrumentos de *soft law* que formulan principios éticos y marcos de gobernanza, mientras que el control efectivo se ejerce a través de contratos de adhesión y diseño técnico. La ética, así, no opera principalmente como deliberación, sino como estándar interno, obligación contractual y regla ejecutable por infraestructura.

La pregunta no es si esos valores son plausibles en abstracto, sino cómo se transforman en reglas aplicables, quién controla esa traducción y qué garantías existen cuando producen consecuencias adversas relevantes. El argumento central sostiene que la ética se convierte en control real cuando se acopla a contrato y código, y que ese control debe ser analizado como ejercicio de poder normativo. Desde esta perspectiva, el artículo propone desplazar el foco desde la proclamación de principios hacia la legitimidad procedimental y los límites jurídicos del gobierno moral privatizado en sistemas de IA.

1.1. Metodología

El presente artículo adopta un enfoque teórico y jurídico-filosófico. Se basa en el análisis doctrinal de la literatura especializada en ética, filosofía del derecho y gobernanza de la inteligencia artificial, así como en el examen de instrumentos de *soft law*, marcos regulatorios y prácticas de gobernanza implementadas por plataformas digitales.

2. Inteligencia artificial y gobierno de conductas

2.1. IA como infraestructura decisional

Hablar de inteligencia artificial como herramienta suele ser insuficiente. La metáfora de la herramienta sugiere neutralidad y subordinación a la mano humana, pero en entornos digitales la IA opera con frecuencia como parte estable del modo en que se decide. Por eso, para comprender el gobierno de conductas, no basta con preguntarse qué hace un modelo en abstracto, sino dónde se inserta, qué decisiones organiza y qué consecuencias activa. Para fines de este artículo, se entenderá por infraestructura decisional el conjunto de sistemas, procedimientos, interfaces y métricas que estructuran la toma de decisiones dentro de una organización o plataforma y que, al hacerlo, definen las condiciones bajo las cuales los usuarios actúan.

Esta idea no pretende sugerir que toda decisión sea automática o que la voluntad humana desaparezca. La tesis más precisa es que la IA reconfigura el entorno de decisión, modifica el costo de ciertas opciones, reordena prioridades y vuelve naturales determinados recorridos de conducta. Una plataforma no necesita ordenar explícitamente lo que el usuario debe hacer. Le basta con jerarquizar posibilidades, introducir fricciones y optimizar incentivos. En términos prácticos, esto significa que la IA gobierna conductas no por mandato directo, sino porque se integra a circuitos decisionales que administran atención, acceso, reputación y oportunidad.

Para ver esto con claridad, conviene pensar la decisión como un proceso. En el mundo físico, las decisiones están rodeadas de señales, hábitos, arquitectura y reglas. En el mundo digital, ese entorno se vuelve programable, medible y escalable. La IA se instala precisamente allí, alrededor de la elección, transformándolo en un espacio diseñado. A medida que las plataformas convierten cada interacción en datos, la IA se vuelve el mecanismo que clasifica esos datos, produce inferencias y ejecuta consecuencias. El

resultado es que el comportamiento del usuario queda moldeado por una infraestructura que anticipa, filtra, puntúa y, en muchos casos, sanciona.

Este funcionamiento suele presentarse como un conjunto de operaciones técnicas. Sin embargo, cuando se observa la cadena completa se advierte que la IA ocupa un lugar normativo en sentido práctico. En un circuito típico, la infraestructura decisional incluye al menos cinco momentos. Primero, la selección de lo que cuenta como información relevante. Todo sistema decide qué recoge, qué ignora y bajo qué formato. Segundo, la clasificación y el puntaje, es decir, la construcción de métricas de valor o riesgo. Tercero, la priorización o *ranking*, que define qué se muestra primero, qué queda oculto y qué se vuelve visible solo para algunos. Cuarto, la aplicación de reglas y umbrales, donde una predicción se traduce en una consecuencia. Quinto, la retroalimentación, porque el sistema aprende del comportamiento que él mismo induce y, al aprender, consolida un patrón.

La IA se convierte en infraestructura decisional porque conecta predicción y ejecución. No se limita a sugerir, sino que organiza el entorno de acción y activa consecuencias. Esa conexión es la base material del gobierno de conductas. En una plataforma de contenidos, un modelo de recomendación no solo predice preferencias, también decide qué ve el usuario y, por tanto, qué consume, qué comparte y qué considera socialmente relevante. En un *marketplace*, un sistema de *ranking* no solo ordena productos, también distribuye atención y ventas. En un entorno laboral o financiero, una puntuación de riesgo no solo describe, sino que puede habilitar o negar acceso. El salto de la descripción a la intervención es el punto donde la IA deja de ser un cálculo y se vuelve gobierno.

La literatura sobre responsabilidad algorítmica ayuda a sostener este enfoque. Cuando decisiones relevantes se delegan en sistemas computacionales, el problema no es únicamente si el modelo acierta, sino si el proceso es explicable, auditable y sujeto a control institucional. En otras palabras, la cuestión no se agota en la precisión del resultado, sino en la gobernanza del sistema como parte de una infraestructura que decide sobre personas (Kroll et al.,

2017). En la misma línea, se ha mostrado que sistemas basados en datos pueden reproducir o amplificar desigualdades existentes, incluso sin intención explícita, porque los datos reflejan patrones históricos y porque la forma de modelar puede traducir correlaciones en consecuencias reales (Barocas & Selbst, 2016). La IA no es un componente neutro agregado al final de una decisión humana, sino un elemento que estructura el modo de decidir y distribuye cargas y beneficios.

Lo anteriormente descrito permite formular una distinción útil. Una cosa es entender la IA como sistema de predicción y otra es entenderla como sistema de organización del entorno. El gobierno de conductas aparece cuando la IA cumple, al menos, tres funciones en la infraestructura decisional.

La primera función es la preselección y jerarquización. En este nivel la IA gobierna la atención. Decide qué se vuelve visible y qué queda fuera del campo de percepción del usuario. Puede hacerlo por recomendación, por ranking, por personalización o por moderación. El usuario no elige en un vacío, sino dentro de un menú construido. Y ese menú responde a objetivos institucionales como retención, seguridad, rentabilidad o cumplimiento, que se codifican en métricas.

La segunda función es la habilitación y restricción. En este nivel la IA gobierna posibilidades. No se limita a mostrar, también permite o impide. Esto puede adoptar formas suaves, como fricciones que desincentivan una conducta, o formas duras, como bloqueos, suspensiones, degradación de alcance o denegación de acceso. Cuando estas medidas se aplican de forma automatizada, el sistema no solo evalúa, sino que también ejecuta. La infraestructura decisional se vuelve entonces un dispositivo de control efectivo porque opera sobre el conjunto de opciones disponibles.

La tercera función es la retroalimentación. En este nivel la IA gobierna hábitos. Las plataformas aprenden de la conducta del usuario, pero el usuario también aprende del sistema. Si el *ranking* premia un tipo de contenido, los productores se adaptan. Si ciertos comportamientos reducen visibilidad, los usuarios se autocorri-

gen. Se genera un circuito de ajuste mutuo. Este circuito es relevante porque convierte una decisión puntual en un patrón de conducta. El gobierno de conductas no se produce solo por sanción, sino también por adaptación.

Los marcos contemporáneos de gobernanza de IA, en particular el NIST AI Risk Management Framework (NIST, 2023), insisten en que la IA debe analizarse como un fenómeno sociotécnico. Sus impactos no emergen únicamente del modelo, sino de cómo se diseña, se implementa, se supervisa y se integra en prácticas organizacionales. Esto desplaza el foco desde el rendimiento del sistema hacia el conjunto de decisiones institucionales que lo hacen operar. Una infraestructura decisional no es únicamente un algoritmo. Incluye objetivos, datos, métricas, incentivos, reglas de negocio, equipos humanos, procesos de apelación, documentación, auditoría y mecanismos de respuesta. El riesgo, por tanto, no es solo técnico, sino también organizacional.

Instrumentos como el NIST AI Risk Management Framework (NIST, 2023) y las recomendaciones de la OECD (2019) pretenden orientar buenas prácticas y gestionar riesgos, pero lo hacen como marcos voluntarios cuya eficacia depende de su adopción, traducción y ejecución interna. Si la IA opera como infraestructura decisional, la pregunta deja de ser si los principios son correctos en abstracto y se vuelve más concreta: cómo esos principios se implementan en decisiones reales, qué procesos los vuelven exigibles y qué mecanismos los convierten en control efectivo.

En síntesis, entender la IA como infraestructura decisional permite explicar por qué su impacto normativo no es una metáfora. La IA organiza entornos de elección, distribuye visibilidad, introduce fricciones y activa consecuencias. Al hacerlo, configura patrones de conducta. Esta caracterización prepara el terreno para examinar, en los apartados siguientes, los tipos de servicios de IA que operan con efectos normativos y el tránsito desde orientaciones voluntarias hacia mecanismos de control real asentados en contrato y código.

2.2. Tipos de servicios de IA con impacto normativo

No toda inteligencia artificial produce efectos normativos del mismo modo. Para este artículo, el impacto normativo aparece cuando un servicio de IA no se limita a asistir, sino que estructura posibilidades, distribuye consecuencias o activa restricciones con relevancia práctica sobre la conducta. El criterio de clasificación, por tanto, es operativo: se distingue por el tipo de decisión que median y por el tipo de consecuencia que desencadenan. En ese marco, la IA puede entenderse como un conjunto de sistemas capaces de generar salidas como predicciones, recomendaciones, contenidos o decisiones que influyen en entornos físicos o virtuales (ISO/IEC, 2022; OECD, 2019; Reglamento (UE) 2024/1689, 2024).

2.2.1. Sistemas de recomendación, *ranking* y curaduría algorítmica

Estos sistemas regulan principalmente la atención. Determinan qué se vuelve visible primero, qué queda relegado y qué permanece fuera del campo perceptivo ordinario. Su impacto normativo no depende de prohibir, sino de distribuir oportunidades como visibilidad, reputación, alcance o acceso a audiencias.

2.2.2. Moderación automatizada y *enforcement* de políticas internas

En este caso, la IA ejecuta reglas internas que operan como condiciones prácticas de participación. La consecuencia típica no es solo la remoción de contenido, sino también medidas graduales como restricción de alcance, desmonetización, suspensión o bloqueo, con efectos comparables a sanciones de facto.

2.2.3. Sistemas de *scoring*, reputación y evaluación automatizada

Estos sistemas asignan puntajes o categorías que condicionan acceso, condiciones contractuales o trato diferenciado. El riesgo

normativo central es que el criterio se vuelva opaco y difícil de impugnar, generando cargas de prueba asimétricas y efectos distributivos relevantes.

2.2.4. Sistemas de selección, filtrado y priorización en mercados (laboral, crédito, seguros, consumo)

Aquí la IA actúa como puerta de acceso. Cuando el filtrado automatizado se integra en procesos de admisión, elegibilidad o selección, los errores y sesgos no se limitan a fallas técnicas sino que producen exclusiones prácticas y redefinen oportunidades.

2.2.5. Modelos generativos con efectos regulatorios

Los sistemas generativos incorporan restricciones operativas que no se presentan como regulación, pero se viven como tal: rechazos, advertencias, fricción y denegación de asistencia. Así, parte del debate ético se traduce directamente en una gramática de permisiones y prohibiciones funcionales.

2.2.6. Personalización conductual y arquitectura de fricción

Estos sistemas gobiernan hábitos mediante ajustes persistentes del entorno: notificaciones, recordatorios, fricciones, recompensas y nudges. Su relevancia normativa no reside en una sanción explícita, sino en la capacidad de inducir patrones de conducta a escala.

2.2.7. Conclusión operativa

En todos estos casos, la IA produce un efecto normativo porque define condiciones de posibilidad, prioriza opciones y activa consecuencias. Por eso, discutir ética en IA exige atender a la cadena que lleva desde principios generales hacia reglas internas y hacia su ejecución técnica.

2.3. De la recomendación al control

En un primer momento, la ética aplicada a la IA aparece como un lenguaje de orientación. Se expresa en principios, marcos de gestión de riesgos, recomendaciones y estándares de buenas prácticas. Su promesa es razonable: ofrecer un suelo común de valores en un campo donde la técnica avanza más rápido que el derecho y donde la incertidumbre invita a la prudencia. Sin embargo, en plataformas y servicios digitales, ese lenguaje rara vez se queda en el plano declarativo. Cuando los principios se incorporan a políticas internas, se insertan en términos y condiciones y se implementan en arquitectura técnica, la ética deja de ser un consejo y se convierte en una condición operativa.

2.3.1. *Soft law* como arquitectura de legitimación y como laboratorio normativo

En términos generales, el *soft law* designa instrumentos que formulan estándares de conducta sin crear, por sí mismos, obligaciones jurídicas coercibles en sentido clásico. Su utilidad es evidente: reduce costos de coordinación, ofrece flexibilidad ante cambios tecnológicos y permite construir consensos preliminares donde un tratado o una ley serían lentos o políticamente inviables. Aun así, su aparente suavidad puede inducir a error. La influencia del *soft law* no depende solo de su fuerza formal, sino de su capacidad para ordenar expectativas y para convertirse en referencia institucional. En la práctica, marcos como NIST AI RMF u orientaciones internacionales como las de la OECD tienden a operar como un vocabulario común, establecen qué se entiende por riesgo, qué se entiende por responsabilidad, qué prácticas se consideran maduras y qué se considera inaceptable (NIST, 2023; OECD, 2019).

Aquí conviene introducir una distinción analítica que ayuda a entender el giro hacia el control real. La legalización no es un interruptor que se enciende o apaga, sino un continuo. En una formulación clásica, la legalización se caracteriza por tres dimensiones: “obligation, precision, and delegation” (Abbott et al., 2000). En la esfera pública, un instrumento de *soft law* suele presentar menor

obligación, y a veces menor precisión o menor delegación, precisamente para conservar flexibilidad. Pero en la esfera privada, esas dimensiones pueden incrementarse por otras vías. La obligación se obtiene por aceptación contractual. La precisión se obtiene por políticas internas detalladas, listas de prohibiciones y taxonomías de contenido. La delegación se obtiene cuando el *enforcement* se entrega a equipos de *trust and safety*, a proveedores y, crecientemente, a sistemas automatizados. El resultado es una legalización privada y funcional: no necesariamente estatal, pero sí eficaz.

2.3.2. El primer salto: del principio a la política interna

El primer puente entre recomendación y control es organizacional. Las empresas adoptan estándares no solo por convicción ética, sino porque subjetivamente también influyen razones estratégicas: reputación, gestión de riesgo, presión regulatoria anticipada, exigencias de inversionistas, requerimientos de compliance en cadenas de suministro, o expectativas de clientes corporativos. En ese tránsito, el *soft law* deja de ser un documento externo y se convierte en una regla interna. Una vez internalizado, el estándar ya no opera como sugerencia, sino como criterio de evaluación y desempeño. Puede traducirse en procesos de gobernanza (comités, evaluaciones de impacto, documentación), en requisitos técnicos (monitoreo, auditoría, trazabilidad) y en decisiones de producto (qué se permite, qué se degrada, qué se bloquea). Esta traducción cobra importancia, porque allí se define qué parte del lenguaje ético se toma en serio, qué parte se vuelve *marketing*, y qué parte se transforma en umbrales operativos.

El punto normativo aparece cuando la política interna se vuelve condición para participar. Dentro de una plataforma, la política no es un manifiesto filosófico, sino una regla aplicada. No se limita a enunciar valores, sino que organiza consecuencias. Y cuanto más se automatiza su aplicación, más se parece a un sistema de gobierno: define estándares, detecta infracciones, ejecuta medidas, gestiona apelaciones, produce estadísticas, modula la conducta. Lo que comenzó como recomendación externa se convierte en disciplina interna.

2.3.3. El segundo salto: del estándar a la obligación por contrato

El contrato es la tecnología jurídica que vuelve exigible lo que antes era voluntario. En el ecosistema digital, este fenómeno se expresa en términos y condiciones, políticas de uso, códigos de conducta y reglas comunitarias aceptadas como condición de acceso. Desde un punto de vista formal, el usuario no está frente a una ley estatal, sino frente a un contrato de adhesión. Pero desde un punto de vista práctico, ese contrato opera como puerta. La aceptación no solo autoriza el acceso, sino que fija el régimen de comportamiento esperado, define sanciones y regula el procedimiento de aplicación. Es un modo de producción normativa privada.

En derecho comparado, la discusión sobre la validez de estos acuerdos suele concentrarse en el consentimiento. Los tribunales, por ejemplo, han exigido que exista aviso razonablemente visible y una manifestación inequívoca de aceptación para que el vínculo sea exigible en términos estrictos (*Specht v. Netscape Communications Corp.*, 2002). Esta línea muestra algo importante: incluso cuando el contrato es la vía de obligación, su legitimidad depende de condiciones mínimas de transparencia y de posibilidad real de entender qué se acepta. Sin embargo, aun cumpliendo esos requisitos, el efecto estructural permanece: valores y criterios morales, formulados como ética, pasan a operar como cláusulas obligatorias. El *soft law*, al acoplarse al contrato, adquiere dientes jurídicos privados.

El problema se intensifica por la asimetría típica del entorno digital. La negociación es inexistente. La salida suele ser binaria: aceptar o no participar. Esto no convierte automáticamente el contrato en inválido, pero sí vuelve más exigente el análisis normativo sobre límites y garantías. Si el contrato funciona como ley privada de acceso, el debate ya no es solo si hay consentimiento, sino qué se está gobernando, con qué grado de discrecionalidad y con qué mecanismos de control.

2.3.4. El tercer salto: del contrato al código como *enforcement*

La pieza decisiva del control real es la arquitectura técnica. Aquí la tesis de la regulación por diseño adquiere su fuerza más concreta. En el entorno digital, el cumplimiento no depende únicamente de la amenaza de sanción futura. Depende de condiciones de posibilidad. Un sistema puede permitir, dificultar, degradar, bloquear o suspender conductas de forma inmediata y escalable. Por eso, la regulación por código no es metáfora sino que se constituye en infraestructura.

Lessig (1999) expresa esta intuición al sostener que el diseño del sistema habilita y restringe comportamiento, y por eso la arquitectura cumple un rol normativo. Cuando esa arquitectura se combina con IA, el control se vuelve adaptativo, no solo ejecuta reglas estáticas, sino que clasifica contextos, infiere intenciones probables, puntúa riesgos y decide respuestas. Lo que antes era una regla textual se convierte en un *pipeline* de decisión: señales, modelo, umbral, acción, retroalimentación. El resultado es un régimen de gobierno operacional, donde la ética declarada se traduce en fricciones, límites y sanciones ejecutadas.

En este punto se entiende por qué la transición del *soft law* al control real no es una simple intensificación, sino un cambio de naturaleza. El *soft law* orienta conductas en el plano discursivo. El contrato convierte esa orientación en obligación de acceso. El código convierte la obligación en un sistema de ejecución. La consecuencia es una coerción de facto: no necesariamente coacción estatal, pero sí restricción efectiva de opciones. Y cuando las decisiones son automatizadas o semi-automatizadas, la opacidad puede aumentar. No solo se vuelve difícil discutir el valor que gobierna, también se vuelve difícil identificar la razón concreta de la decisión.

2.3.5. La fórmula del control real y su problema filosófico

El control real puede resumirse como un encadenamiento. Primero, un marco ético formula valores bajo lenguaje de *soft law*. Se-

gundo, una organización los internaliza como política. Tercero, la política se incorpora al contrato como condición de acceso. Cuarto, el sistema técnico implementa esa política como arquitectura ejecutable. En ese punto, la ética ya no es únicamente un debate. Es un régimen operativo.

La pregunta filosófica que atraviesa este proceso no es de menor importancia. Es el punto incómodo cuando hablamos de regulación y sus fundamentos. Si la moral admite marcos incompatibles, entonces la traducción de valores en cláusulas y en umbrales técnicos no es neutra. Selecciona. Prioriza. Excluye. Decide qué daño es tolerable y cuál no. Decide qué error se compensa y cuál se absorbe. Decide qué riesgo se evita aun a costa de libertades, y qué libertad se preserva aun a costa de riesgos. Esa selección no se hace en la cámara de senadores o diputados, sino que se hace en comités internos, en documentos de producto, en taxonomías de contenido, en parámetros de modelos, en diseño de interfaces. Es allí donde la moral se privatiza: no porque la empresa invente la moral desde cero, sino porque la vuelve operativa bajo su propia gramática y bajo sus propios incentivos.

En síntesis, el tránsito del *soft law* al control real por contrato y código nombra un fenómeno estructural: el pasaje desde la recomendación ética hacia un gobierno efectivo de conducta mediante reglas privadas ejecutadas por infraestructura.

3. Ética y moral

3.1. Ética y moral: distinciones conceptuales

En este artículo se distingue entre moral y ética para evitar ambigüedades al analizar reglas privadas ejecutadas en entornos digitales. La moral se usará para referirse al conjunto de normas prácticas que efectivamente regulan conductas dentro de una comunidad, una profesión o una organización; la ética se usará para referirse al plano de reflexión normativa que evalúa, justifica

o critica esas normas. Esta distinción resulta especialmente útil cuando el objeto de análisis no es el Estado, sino regímenes normativos privados que operan mediante políticas internas, contrato y arquitectura técnica. En este contexto, Miller (2013) permite entender que la cuestión no se agota en los valores que se declaran, sino en cómo estos se vuelven operativos y producen consecuencias efectivas.

3.1.1. Moral como práctica y ética como justificación

Miller (2013) explica que el término moral puede emplearse en un sentido descriptivo, como sistema de normas efectivamente vigentes sostenidas por expectativas sociales y mecanismos de sanción, y también en un sentido teórico, como el fenómeno que se analiza cuando se pregunta por la naturaleza o validez de los juicios morales. En cambio, ética designa la reflexión sistemática sobre la moral, su coherencia, alcance y límites. Esta separación permite evitar un error recurrente en debates sobre IA: suponer que porque un instrumento se presenta como ético ya contiene una justificación suficiente para operar como regla ejecutable en un entorno de poder asimétrico.

3.1.2. Tres niveles de análisis y moral institucionalizada

Siguiendo a Miller (2013), el capítulo distingue entre ética normativa, metaética y ética aplicada. La ética normativa discute criterios sustantivos de corrección, la metaética examina el estatus del discurso moral y la ética aplicada analiza la traducción de estos criterios a ámbitos concretos como la gobernanza algorítmica, la moderación de contenidos y el enforcement automatizado. Además, conviene distinguir moral social, moral profesional y moral institucionalizada. La tesis de la moral privatizada se refiere sobre todo a la moral institucionalizada, porque allí la regla no solo se declara, sino que se ejecuta como condición de acceso, permanencia o visibilidad y puede escalar mediante automatización (Raz, 1986).

3.1.3. Derecho, moral y el tránsito hacia el gobierno efectivo

En filosofía del derecho, la relación entre derecho y moral estructura debates sobre validez y autoridad. Una posición influyente sostiene una tesis de separación conceptual entre validez jurídica y corrección moral, sin negar la posibilidad de crítica moral del derecho (Hart, 1961). Otras tradiciones subrayan que un sistema normativo requiere condiciones internas de coherencia y racionalidad para orientar conducta y sostener pretensión de legitimidad (Fuller, 1964). Para este artículo, lo decisivo es que puede existir eficacia normativa por contrato y código, pero la legitimidad del régimen depende de estándares que exceden la mera eficacia, especialmente cuando hay decisiones adversas automatizadas y poder asimétrico.

3.2. Moral objetiva y moral subjetiva

Este apartado no busca resolver el debate metaético, sino fijar un marco mínimamente riguroso para el resto del artículo. La tesis de la moral privatizada no exige demostrar verdades morales objetivas, pero sí exige reconocer que regímenes privados suelen actuar como si sus estándares fueran correctos en un sentido fuerte, incluso cuando son razonablemente discutibles. Por ello, la evaluación no puede quedar solo en el contenido, sino también en el modo de producción, aplicación y contestación de reglas cuando se vuelven ejecutables por contrato y código (Miller, 2013).

El realismo moral sostiene que ciertos juicios morales pueden ser verdaderos o falsos y que su verdad no depende simplemente de preferencias. En su versión no metafísica, esta tesis no requiere compromisos ontológicos fuertes, pero sí preserva una pretensión de objetividad justificable racionalmente (Shafer Landau, 2003). El constructivismo desplaza el foco desde hechos morales hacia condiciones de justificación, y por ello es especialmente útil para legitimidad, porque vuelve normativamente relevantes la publicidad, la posibilidad de impugnación y la coherencia del régimen (Korsgaard, 1996). El naturalismo, por su parte, es relevante por su afinidad con la traducción de valores a métricas y umbrales,

pero esa traducción no elimina la dimensión normativa, y el riesgo es confundir cuantificación con justificación y ocultar elecciones sobre daños, distribución del riesgo y carga del error (Brink, 1989). En conjunto, estas posiciones permiten sostener un punto metodológico común: ante desacuerdo moral persistente, lo decisivo es exigir garantías procedimentales mínimas cuando el régimen produce consecuencias adversas relevantes (Miller, 2013).

3.3. Moral, poder y legitimidad

La tesis de la moral privatizada conduce a una pregunta de teoría del poder. Cuando criterios de corrección se vuelven operativos mediante cláusulas contractuales y arquitectura técnica, dejan de ser únicamente orientaciones y pasan a funcionar como condiciones de acceso, permanencia y visibilidad. En ese tránsito, la moral se convierte en un arreglo institucional con capacidad de producir consecuencias. Esto obliga a distinguir eficacia, autoridad y legitimidad. La eficacia describe la existencia operativa del régimen. La autoridad describe su capacidad de generar razones prácticas para actuar. La legitimidad concierne a la justificación moral del poder que el régimen ejerce, especialmente cuando produce restricciones significativas.

3.3.1. Legitimidad y aceptación

La legitimidad permite evitar dos simplificaciones. La primera consiste en equiparar legitimidad con aceptación. Un régimen puede estabilizarse por dependencia, hábito, costos de salida o ausencia de alternativas sin que ello pruebe justificabilidad normativa (Suchman, 1995). En términos sociológicos, todo sistema de autoridad busca cultivar la creencia en su legitimidad, pero esa creencia no equivale a legitimidad normativa (van Leeuwen, 2008; Weber, 1978). Por eso, en plataformas, el argumento el usuario aceptó no agota el problema. La aceptación contractual puede ser relevante para explicar obligación privada, pero no basta para justificar un régimen que afecta participación, expresión, reputación o acceso a oportunidades en condiciones de poder asimétrico (Buchanan, 2002; Schmidt, 2013).

3.3.2. Justificación pública y control de la arbitrariedad

En la tradición liberal, un enfoque influyente entiende legitimidad como exigencia de justificación pública del ejercicio del poder. En la formulación rawlsiana, Rawls (2005) sostiene que el principio liberal de legitimidad exige razones públicas aceptables para ciudadanos libres e iguales. Aunque la gobernanza de plataformas no sea poder político en sentido estricto, la analogía es normativamente productiva, cuando reglas privadas operan como condiciones de participación y su aplicación produce efectos relevantes, se requiere un umbral de garantías para controlar arbitrariedad, especialmente cuando la moral se ejecuta por infraestructura (Buchanan & Keohane, 2006; Schmidt, 2013).

3.3.3. Deliberación, umbrales y debido proceso en plataformas

La moral privatizada se vuelve más aguda cuando la discrecionalidad migra hacia sistemas. Decisiones que antes dependían de juicio humano se trasladan a taxonomías, señales y umbrales implementados en infraestructura, produciendo un gobierno por categorías ejecutables. Esto puede intensificar opacidad y consolidar errores como hechos operativos si no hay revisión significativa. En respuesta, estándares voluntarios como los Principios de Santa Clara han insistido en transparencia, notificación y apelación como condiciones mínimas cuando el régimen afecta participación y voz pública (Santa Clara Principles, 2021). En paralelo, desarrollos regulatorios como el Reglamento de Servicios Digitales de la Unión Europea refuerzan esa lógica al exigir razones para restricciones y sistemas de reclamación y revisión, institucionalizando que el poder ejercido por infraestructura debe volverse rastreable y contestable (Reglamento (UE) 2022/2065, arts. 17, 20, 21). Así, la relación entre moral, poder y legitimidad nos permite entender que cuando la ética se vuelve ejecutable por contrato y código, se convierte en poder normativo, y ese poder debe evaluarse bajo estándares procedimentales mínimamente defendibles para evitar arbitrariedad automatizada (Rawls, 2005; Schmidt, 2013; UNESCO, 2021).

4. Del juicio moral al diseño técnico

4.1. De valores a criterios operativos

Una dificultad estructural de la ética en IA es que los valores son formulaciones abiertas, mientras que los sistemas decisionales requieren criterios operativos. La organización que declara un valor debe traducirlo a una regla de decisión que pueda aplicarse de manera consistente y que pueda integrarse a procesos de diseño, despliegue y monitoreo. Esta traducción es el punto en el que el discurso ético se vuelve gobernanza. No se trata solo de declarar que se busca equidad, seguridad o transparencia, sino de definir qué cuenta como riesgo, qué tipo de daño es relevante, qué evidencia se considera suficiente y qué respuesta institucional corresponde.

En la práctica, esta traducción adopta la forma de estándares internos. Se fijan categorías, se definen escenarios de uso, se determinan niveles de impacto, se asignan responsabilidades y se crean rutas de escalamiento. Los marcos de gestión de riesgos son relevantes precisamente porque ordenan este proceso y transforman valores generales en controles organizacionales verificables, como documentación, evaluaciones, monitoreo y revisión (NIST, 2023).

4.2. Traducción técnica: taxonomías, señales, datos, métricas y objetivos de optimización

La traducción a criterios operativos se vuelve traducción técnica cuando el sistema debe ejecutar decisiones. En ese paso aparecen cinco operaciones frecuentes. Primero, taxonomías, porque el sistema necesita categorías discretas para identificar conductas o eventos relevantes. Segundo, señales, porque debe seleccionar qué datos o indicadores cuentan como evidencia. Tercero, datos y calidad, porque lo que el sistema puede decidir depende de lo que puede registrar y de cómo se construyen los conjuntos de entrenamiento y prueba. Cuarto, métricas, porque el desempeño se define

mediante medidas que implican elecciones sobre error tolerable y distribución del riesgo. Quinto, objetivos de optimización, porque el sistema no solo predice, sino que persigue funciones objetivo que pueden entrar en tensión con valores invocados.

Estas operaciones suelen presentarse como ingeniería, pero contienen elecciones normativas. Definir qué señal cuenta, qué variable se considera relevante, qué umbral activa una consecuencia, o qué tasa de falsos positivos se tolera, son decisiones que distribuyen cargas del error y que afectan a usuarios de manera desigual. Por ello, la gobernanza ética no puede limitarse a principios. Debe exigir trazabilidad de elecciones técnicas, documentación suficiente, evaluación de impacto y mecanismos de revisión cuando corresponda (NIST, 2023).

4.3. Decisión automatizada como *enforcement*

El fenómeno de la conversión decisiva ocurre cuando la clasificación se conecta con la consecuencia. Mientras un sistema solo produce un score o una recomendación, todavía existe un espacio de mediación humana o de interpretación institucional. Pero cuando el output se usa como disparador de una medida, el sistema se convierte en *enforcement*. La decisión automatizada funciona entonces como una tecnología de ejecución, transforma un juicio probabilístico en una restricción real.

Este punto puede describirse como una cadena que inicia con señales, pasa a inferencia, luego al umbral y ejecuta acción. La acción puede ser suave, como una fricción, degradación o priorización negativa, o dura, como el bloqueo, suspensión, remoción o denegación de acceso. La diferencia entre ambas no elimina el problema, solo cambia su intensidad. En ambos casos, el régimen moral se materializa como estructura de oportunidades, se participa, se pierde voz, se degrada reputación o se restringe acceso según reglas privadas operadas por infraestructura.

Las teorías de rendición de cuentas algorítmica han insistido en que el problema central no es únicamente la calidad predictiva,

sino la gobernanza del sistema como parte de un proceso decisorio que afecta a personas. De allí la relevancia de diseñar mecanismos institucionales de control, trazabilidad, auditoría, explicabilidad funcional y garantías procedimentales que permitan contestar y corregir decisiones (Kroll et al., 2017).

El *enforcement* automatizado también reconfigura la temporalidad del poder. La sanción no ocurre al final de un procedimiento, ocurre en tiempo real. Esto altera el tipo de daño, el costo de error se vuelve inmediato y a menudo difícil de revertir. En sistemas de moderación o detección, la elección entre falsos positivos y falsos negativos se convierte en una decisión sobre quién sufre el daño principal. Esta estructura ha sido estudiada en *fairness* como un problema de compatibilidad entre criterios y como un problema de distribución de errores entre grupos, mostrando que corregir puede significar redistribuir errores más que eliminarlos (Hardt, Price, & Srebro, 2016; Chouldechova, 2017). Cuando el *enforcement* se automatiza, esa redistribución deja de ser una cuestión abstracta y produce denegaciones, bloqueos y degradaciones concretas.

Además, el *enforcement* automatizado tiende a desplazar el lenguaje de razones hacia un lenguaje de umbrales. En un proceso clásico, la justificación se ofrece como motivación, por qué se decidió. En un proceso automatizado, la razón suele comprimirse en una categoría contenido infractor, actividad sospechosa o riesgo elevado, sin acceso al conjunto de señales que llevaron al resultado. Esto no es solo un problema de transparencia técnica, es un problema de forma de gobierno. Un régimen que sanciona sin razones inteligibles o que ofrece razones no contestables erosiona condiciones mínimas de legitimidad procedimental y aumenta el riesgo de arbitrariedad.

Por ello, el paso del juicio a la consecuencia constituye el punto donde la moral privatizada se vuelve jurídicamente relevante. El estándar moral, una vez implementado, ya no es únicamente un criterio interno, es un mecanismo de restricción. Cuando el *enforcement* es infraestructural, el derecho aparece como límite al poder no porque moralice la técnica, sino porque exige condiciones

de control, procedimientos de impugnación, revisión, proporcionalidad y rendición de cuentas, precisamente porque la ejecución automatizada produce efectos comparables a coerción práctica.

4.4. El vacío normativo y la expansión del soft law digital

El llamado vacío normativo en inteligencia artificial no debe entenderse como ausencia total de reglas, sino como un desajuste entre la capacidad del derecho estatal para generar estándares exigibles y la forma en que los sistemas de IA operan, se despliegan y producen efectos. Ese desajuste explica la expansión del *soft law* como respuesta práctica en un espacio transnacional y técnicamente dinámico, donde instrumentos no vinculantes que ordenan expectativas, estabilizan vocabularios y ofrecen marcos de legitimación cuando no existe una autoridad regulatoria global única y cuando la respuesta legislativa suele ir detrás del cambio tecnológico (Abbott et al., 2000; OECD, 2019).

5. El vacío normativo y la expansión del soft law digital

5.1. El desajuste regulatorio como condición de posibilidad del soft law

El desajuste se expresa, primero, en la transnacionalidad de los servicios digitales, cuyos efectos se producen simultáneamente en múltiples jurisdicciones, debilitando soluciones estrictamente territoriales. Se expresa, segundo, en la fragmentación regulatoria, porque los problemas asociados a IA atraviesan sectores y agencias diversas, desde consumo y competencia hasta privacidad, ciberseguridad y derechos fundamentales, generando respuestas heterogéneas y difíciles de integrar. Se expresa, tercero, en la velocidad de iteración tecnológica y organizacional, que amplía la brecha temporal entre innovación y reacción jurídica y

desplaza parte del control hacia el diseño interno y técnico de las organizaciones. En ese escenario, el *soft law* cumple una función de coordinación y convergencia de bajo costo político, al permitir principios comunes y lenguajes compartidos sin depender de un proceso legislativo necesariamente lento (OECD, 2019).

5.2. Función y límite del *soft law* en IA

El *soft law* coordina, legitima y orienta la gobernanza interna. Coordina al ofrecer taxonomías y principios comunes para actores diversos. Legitima al permitir que organizaciones declaren alineamiento con estándares reconocibles. Orienta al impulsar prácticas organizacionales de gestión del riesgo, evaluación de impacto, documentación y monitoreo, como se aprecia en marcos técnicos de gestión de riesgos que estructuran el modo en que se identifican y mitigan impactos aun sin fuerza jurídica directa (NIST, 2023). Sin embargo, su límite es estructural. La voluntariedad impide exigir cumplimiento por sí mismo, la indeterminación obliga a decisiones posteriores para volver aplicables los principios, y su efecto depende de la traducción interna. Por ello, el problema central no se encuentra solo en el texto del *soft law*, sino en el punto en que se convierte en política, procedimiento, contrato y arquitectura técnica, que es el tránsito que aborda el capítulo siguiente.

6. Del *soft law* al control real

El *soft law* adquiere relevancia práctica cuando deja de ser un texto externo y se convierte en una cadena de transformación interna que produce reglas operativas, obligaciones y consecuencias. Esa cadena suele seguir tres movimientos. Primero, internalización, cuando un marco de principios pasa a convertirse en estándar corporativo y estructura gobernanza interna. Segundo, contractualización, cuando ese estándar se inserta en términos y condiciones como régimen de acceso. Tercero, codificación, cuando el estándar se implementa en arquitectura técnica que ejecuta decisiones a escala. Esta cadena explica por qué el debate sobre ética

en IA no puede quedar en principios generales, y es que la ética se vuelve control real cuando se acopla a contrato y código.

6.1. Internalización del principio al estándar corporativo

El *soft law* en IA suele presentarse como un conjunto de principios y marcos de buenas prácticas sin obligatoriedad jurídica directa. Sin embargo, su influencia depende de su capacidad para convertirse en referencia institucional y en criterio reputacional y organizacional, especialmente cuando esos principios se traducen en políticas internas, procesos, métricas y requisitos de diseño y despliegue (OECD, 2019; NIST, 2023). En esta fase, la organización transforma el lenguaje de principios en instrumentos de gobernanza. Es una traducción práctica. Se definen categorías operativas, se establecen controles de cambio, documentación de modelos, evaluaciones de impacto y rutas internas de escalamiento. El resultado es que el principio se convierte en criterio de decisión corporativo y produce una moral operativa, no en sentido teórico, sino como estándar aplicado que estructura conductas y prioriza riesgos y daños dentro del sistema.

6.2. Contractualización: términos y condiciones como norma privada de acceso

La segunda transformación es la contractualización. En el entorno digital, el contrato no solo organiza intercambios, sino que funciona como puerta de acceso y como técnica de producción normativa privada. Los términos y condiciones y políticas de uso se aceptan como condición para participar y suelen operar como contratos de adhesión, lo que permite convertir estándares internos en obligaciones del usuario y en reglas de acceso y permanencia (Radin, 2013). Aquí se produce un desplazamiento relevante. El estándar se presenta como voluntario porque el usuario puede no aceptar, pero puede operar como coerción de facto cuando el servicio se vuelve infraestructura social o económica y la salida real es costosa o irrazonable. Además, el problema no se resuelve con afirmar que

se informó. La crítica a la divulgación masiva muestra que informar no garantiza comprensión ni control, especialmente cuando el texto es extenso, técnico y estructuralmente no leído, y cuando la arquitectura del mercado produce dependencia (Ben-Shahar & Schneider, 2010). Incluso en un marco favorable a la exigibilidad, la doctrina y jurisprudencia han exigido condiciones mínimas de aviso y manifestación inequívoca de aceptación, lo que revela que la contractualización es una tecnología de obligación, pero su legitimidad depende de estándares mínimos de transparencia y procedimiento (Specht v. Netscape Communications Corp., 306 F.3d 17, 2d Cir. 2002). Sin embargo, aun superados esos mínimos, persiste el punto estructural: el *soft law* se convierte en régimen privado de conducta con consecuencias transnacionales y márgenes de discrecionalidad que se vuelven relevantes para la legitimidad.

6.3. Codificación: *enforcement* por arquitectura, automatización y escalabilidad

La tercera transformación, decisiva para el control real, es la codificación. El contrato vuelve exigible el estándar, pero el código lo vuelve ejecutable. La arquitectura técnica regula conductas porque define condiciones de posibilidad, fricciones y consecuencias, y por ello no puede tratarse como elemento meramente instrumental (Lessig, 1999). En IA y plataformas, esta regulación por arquitectura se intensifica porque el sistema no solo aplica reglas estáticas, sino que clasifica, puntúa e infiere, conectando predicción y consecuencia en tiempo real. En esta fase, la moral operativa se convierte en *pipeline* técnico. La normatividad se materializa en elecciones que suelen presentarse como técnicas, qué cuenta como señal relevante, qué umbral dispara una restricción, qué tasa de error se tolera, qué casos reciben revisión humana y cuáles se ejecutan automáticamente. Cuando sistemas computacionales median decisiones con efectos relevantes sobre personas, la cuestión no se agota en desempeño, sino que exige mecanismos de explicabilidad, auditoría, responsabilidad y control institucional, precisamente porque el sistema no amenaza con sancionar, sino que sanciona en la práctica (Kroll et al., 2017). Por ello, la li-

teratura sobre plataformas describe estos arreglos como un orden normativo propio, aplicado por procedimientos internos y por arquitecturas técnicas que funcionan como reglas efectivas de la vida digital (Gillespie, 2018; Suzor, 2019).

6.4. *Soft law* como cadena de densificación normativa

Con lo anterior, el desplazamiento desde el *soft law* al control real puede entenderse como una cadena de densificación normativa. Un marco de principios establece un vocabulario de corrección. Ese vocabulario se internaliza como estándar corporativo, se contractualiza como condición de acceso y se codifica como arquitectura ejecutable. Cada eslabón añade fuerza práctica. La voluntariedad del *soft law* se vuelve obligación interna al corporativizarse, la obligación interna se vuelve obligación del usuario al contractualizarse, y la obligación contractual se vuelve *enforcement de facto* al codificarse. En este punto, el conflicto moral se reubica. Ya no se disputa únicamente en el plano de principios, sino en el de políticas, cláusulas y umbrales técnicos. Por ello, el problema filosófico y jurídico que emerge no es si el marco es razonable como texto, sino qué garantías existen cuando ese marco se convierte en gobierno efectivo de conductas por contrato y código (Lessig, 1999; NIST, 2023; OECD, 2019).

7. Moral privatizada: quién decide y cuáles son los límites jurídicos

7.1. Locus de decisión moral: actores internos, incentivos y dependencias externas

La tesis de la moral privatizada exige precisar dónde se toman, en términos efectivos, las decisiones normativas que luego se presentan como simples políticas técnicas o estándares neutrales. En regímenes digitales, el locus de decisión moral no se ubica en un

órgano público ni en una deliberación democrática, sino en una combinación de actores internos y dependencias externas que determinan qué se considera permitido, riesgoso, valioso o sancionable. La arquitectura decisional suele distribuirse entre equipos de producto, seguridad, confianza y moderación, áreas legales y de cumplimiento, y unidades de datos y aprendizaje automático. Esa distribución no es accidental. Responde a un objetivo organizacional básico, minimizar riesgos, estabilizar reputación y sostener la escalabilidad del servicio, lo que tiende a transformar valores abiertos en estándares operativos consistentes, medibles y ejecutables.

Por ello, entendemos que la moral institucionalizada no es solo un conjunto de principios, sino un sistema de gobierno con incentivos definidos. La presión por eficiencia y por reducción de incertidumbre favorece reglas generales, umbrales y taxonomías, aun cuando el conflicto moral requiera contextualización. Además, el régimen no decide en un vacío. Su marco de decisión se ve condicionado por dependencias externas, como requerimientos regulatorios fragmentados, presiones comerciales, conflictos de interés derivados de modelos de negocio basados en atención o intermediación, y exigencias de actores privados con poder de influencia, incluyendo anunciantes, proveedores de infraestructura, titulares de derechos y, en ocasiones, coaliciones políticas o sociales. En consecuencia, la moral privatizada debe comprenderse como un producto institucional. Lo que importa no es solo qué regla se adopta, sino qué estructura de incentivos la produce y qué tipo de racionalidad organiza su aplicación a escala.

7.2. Pluralismo moral, conflictos de valores y riesgos democráticos en plataformas

La moral privatizada se despliega en un contexto de pluralismo moral persistente. En sociedades complejas, existen desacuerdos razonables sobre valores, prioridades y bienes en conflicto, lo que impide asumir un consenso sustantivo único. Este pluralismo no es un defecto contingente. Es una condición estructural de la vida

pública y, por tanto, de cualquier régimen que pretenda gobernar conductas de manera general. La consecuencia nos dejaría en la comprensión que, si el contenido moral es disputado, entonces la legitimidad del régimen no puede descansar solo en la proclamación de principios o en la supuesta corrección de un conjunto de valores, sino en la existencia de condiciones institucionales que hagan el ejercicio del poder razonablemente justificable ante quienes lo soportan.

En plataformas y servicios digitales, este problema adquiere un carácter específico. Las reglas privadas se aplican a escala, en un espacio transnacional, con capacidad de afectar condiciones de participación social, acceso a mercados, visibilidad, reputación y posibilidades de expresión. Al mismo tiempo, el régimen opera mediante procedimientos internos y decisiones que pueden ser opacas o difíciles de impugnar. Esa combinación intensifica riesgos democráticos. Primero, porque desplaza conflictos que serían materia de deliberación pública hacia decisiones internas sin control equivalente. Segundo, porque el desacuerdo moral puede ser tratado como un problema de gestión del riesgo y no como conflicto de valores. Tercero, porque la automatización tiende a estabilizar categorías y umbrales, reduciendo el espacio de contextualización y ampliando el costo del error cuando las consecuencias son restrictivas. Por ello, el pluralismo moral conduce a una exigencia normativa básica. Si el régimen no puede apoyarse en consenso sustantivo, debe apoyarse en legitimidad procedimental, esto es, en garantías mínimas que controlen arbitrariedad y permitan contestación, corrección y rendición de cuentas en decisiones diversas relevantes (Rawls, 2005; Buchanan & Keohane, 2006)

7.3. El derecho como límite: garantías mínimas y estándar de legitimidad procedimental

Si la moral privatizada opera como régimen de gobierno efectivo por contrato y arquitectura técnica, el problema jurídico central no es describir su existencia, sino fijar sus límites. En este punto, el derecho cumple una función clásica, limitar el poder donde exis-

te asimetría y donde las decisiones pueden producir restricciones significativas. La idea de límite no exige equiparar plataformas con Estados, pero sí reconocer que cuando un régimen privado define condiciones de participación y distribuye consecuencias, la ausencia de garantías procedimentales genera un riesgo estructural de arbitrariedad, y ese riesgo es jurídicamente relevante.

Un estándar mínimo de legitimidad procedimental en gobernanza privada puede formularse como un conjunto de garantías exigibles, al menos en decisiones adversas con impacto relevante. Primero, cognoscibilidad de reglas, entendida como disponibilidad y claridad suficiente para anticipar consecuencias y comprender qué conductas activan restricciones. Segundo, explicación funcional de decisiones, de modo que el afectado pueda conocer la razón operativa de la medida y no reciba fórmulas vacías. Tercero, contestabilidad efectiva, es decir, acceso real a mecanismos de impugnación con revisión significativa y posibilidad de corrección. Cuarto, proporcionalidad y graduación, de manera que la respuesta se adecúe a la gravedad del supuesto incumplimiento y se reduzca el costo del error cuando la detección es incierta. Quinto, trazabilidad y rendición de cuentas, mediante registro verificable de criterios, uso de automatización, tasas de error relevantes, y evaluación de impacto o sesgos cuando corresponda. Estas condiciones no definen por sí mismas una teoría moral completa, pero sí delimitan la forma aceptable de un poder normativo privatizado bajo pluralismo moral y asimetría.

Este estándar mínimo se refleja en desarrollos normativos contemporáneos que, sin resolver disputas metaéticas, buscan institucionalizar garantías. En el contexto europeo, el Reglamento de Servicios Digitales exige motivación clara y específica para restricciones basadas en ilegalidad o incompatibilidad con términos y condiciones, y refuerza mecanismos de reclamación y revisión, reconociendo que la legitimidad de restricciones impuestas por proveedores depende de procedimientos que vuelvan el poder rastreable y contestable (Regulation (EU) 2022/2065). En paralelo, instrumentos y marcos de gobernanza de IA han enfatizado *accountability*, evaluaciones de impacto, documentación y control

institucional como condiciones para evitar que sistemas sociotécnicos operen como caja negra con capacidad de producir daños sin remedio (NIST, 2023; UNESCO, 2021). La convergencia de estos enfoques muestra el punto estructural del artículo. Cuando la ética se vuelve ejecutable, el derecho deja de ser una referencia externa y pasa a ser un límite interno al diseño institucional. El estándar de legitimidad no se agota en el contenido moral invocado por la organización, sino en las garantías que acompañan la producción, aplicación y corrección de reglas cuando esas reglas se vuelven control real por contrato y código.

8. Hacia un test de legitimidad para la moral privatizada

La idea central del presente escrito sostiene que, en el ecosistema digital, la ética aplicada a plataformas y sistemas de IA rara vez opera como mera adhesión voluntaria a principios generales. Opera, sobre todo, como un régimen ejecutable que se internaliza en dos planos. Primero, en instrumentos normativos privados, tales como términos y condiciones, políticas, contratos con usuarios, y acuerdos B2B. Segundo, en decisiones técnicas, tales como diseño de producto, arquitectura de modelos, umbrales de detección, flujos de *enforcement*, y métricas de desempeño. En ese tránsito, la moral se vuelve operativa y automatizable. Y al volverse automatizable, adquiere densidad de poder, porque produce efectos reales sobre acceso, visibilidad, monetización, reputación y participación.

Desde esa premisa, la pregunta relevante deja de ser exclusivamente sustantiva. No se reduce a qué valores son correctos. La pregunta central se desplaza hacia condiciones de legitimidad. Bajo qué condiciones es legítimo que un actor privado ejecute, a gran escala, un conjunto de decisiones moralmente cargadas mediante contrato y código. La propuesta de este capítulo es un test de legitimidad compuesto por criterios verificables, pensado para evaluar regímenes privados que funcionan como gobernanza normativa de facto.

El test no pretende resolver el debate metaético sobre la verdad moral, ni imponer una moral única. Su apuesta es procedimental y jurídico institucional. En contextos de pluralismo moral y transnacionalidad, la legitimidad depende menos del consenso sobre el contenido final de los valores y más de condiciones mínimas de publicidad, trazabilidad, contestabilidad, proporcionalidad y rendición de cuentas. Esta aproximación dialoga con la idea de que la arquitectura técnica regula conductas de forma comparable a la norma, y con enfoques que sostienen que la justificación pública y la posibilidad de impugnación son requisitos de legitimidad cuando una decisión afecta intereses relevantes, incluso fuera del Estado. También se apoya, como insumos traducibles a obligaciones, en marcos contemporáneos de gestión de riesgo y gobernanza, tales como NIST AI RMF y la Recomendación de IA de la OCDE, y en estándares de transparencia y debido proceso en moderación, tales como los Santa Clara Principles.

8.1. Alcance y función del test

El test se aplica a sistemas de IA que cumplen simultáneamente tres condiciones: i) operan como infraestructura decisional; ii) ejecutan reglas privadas que condicionan acceso, visibilidad, permanencia o trato; y iii) producen efectos adversos relevantes sin mediación humana directa o con mediación limitada. En estos casos, la evaluación de legitimidad no puede agotarse en la voluntariedad contractual ni en la invocación de principios éticos generales.

El objetivo del test es identificar déficits estructurales de legitimidad y orientar tanto el diseño institucional como la intervención jurídica, sin asumir que toda gobernanza privada sea ilegítima per se.

8.2. Publicidad y cognoscibilidad de las reglas

El primer criterio exige que las reglas que gobiernan el sistema sean cognoscibles para los sujetos afectados. Esto implica que los estándares relevantes no se limiten a declaraciones abstractas, sino que se expresen de forma suficientemente clara como para

permitir anticipación razonable de consecuencias. La opacidad normativa, especialmente cuando se combina con *enforcement* automatizado, erosiona la capacidad del sistema para orientar conductas y debilita su pretensión de legitimidad.

8.3. Explicabilidad funcional de las decisiones adversas

Cuando un sistema produce una decisión adversa, debe existir una explicación funcional suficiente que permita comprender qué tipo de regla se aplicó y qué hecho desencadenó la consecuencia. Este criterio no exige revelar modelos completos ni secretos industriales, pero sí superar la mera notificación automática. Sin explicación mínima, la decisión se vuelve indistinguible de la arbitrariedad, incluso si responde a un proceso técnicamente sofisticado.

8.4. Contestabilidad efectiva y revisión significativa

La legitimidad procedimental requiere la posibilidad real de impugnar decisiones adversas. La contestación debe ser accesible, comprensible y capaz de producir revisión sustantiva, no solo confirmación automática. En contextos de alta automatización, la ausencia de revisión significativa consolida errores y traslada de manera desproporcionada los costos del sistema a los usuarios afectados.

8.5. Proporcionalidad y graduación del *enforcement*

Las consecuencias derivadas de la aplicación de reglas privadas deben ser proporcionales al riesgo o a la conducta atribuida. Cuando el costo del error es elevado, el régimen debe privilegiar respuestas graduadas, reversibles y escalonadas antes que sanciones máximas o definitivas. La proporcionalidad funciona aquí como límite estructural a la ejecución automática de normas controvertidas.

8.6. Gobernanza del error y distribución de riesgos

Todo sistema automatizado produce errores. Un régimen legítimo no es aquel que promete infalibilidad, sino aquel que reconoce el error, lo mide y distribuye sus costos de manera razonable. Esto implica mecanismos internos de monitoreo, corrección y aprendizaje, así como decisiones explícitas sobre quién asume las consecuencias cuando el sistema falla.

8.7. Trazabilidad y rendición de cuentas

El último criterio exige trazabilidad suficiente para permitir auditoría interna y, cuando corresponda, externa. La existencia de decisiones automatizadas con efectos relevantes sin trazabilidad impide cualquier forma de control jurídico o institucional. La rendición de cuentas no requiere transparencia absoluta, pero sí evidencia verificable de que el sistema opera conforme a reglas conocidas y revisables.

8.8. Función jurídica del test

El test de legitimidad propuesto cumple una doble función. En el plano analítico, permite evaluar críticamente regímenes de moral privatizada sin recurrir a juicios morales sustantivos controvertidos. En el plano normativo, ofrece un marco para la intervención jurídica, ya sea mediante regulación pública, control judicial o exigencias contractuales reforzadas.

El punto central es que, cuando la ética se vuelve ejecutable por contrato y código, el derecho no puede limitarse a observar. Su función es reintroducir garantías mínimas allí donde el poder normativo privado se ejerce sin los contrapesos que históricamente han acompañado a otros regímenes de decisión con consecuencias relevantes.

9. Conclusiones

Este artículo ha sostenido que el problema central de la IA en contextos de gobernanza digital no es la ausencia de valores, sino la forma en que esos valores se traducen en reglas exigibles y se ejecutan mediante arquitectura técnica. En ese tránsito, la ética deja de operar como orientación discursiva y se convierte en un régimen práctico de control, articulado principalmente por contrato y código. El resultado es la emergencia de una moral privatizada que ejerce poder normativo con efectos relevantes sobre individuos y organizaciones.

Frente a este fenómeno, el análisis mostró que el *soft law* cumple una función importante de coordinación, legitimación y estandarización del lenguaje ético, pero resulta insuficiente para explicar o controlar el ejercicio efectivo del poder. El control real aparece cuando los principios se incorporan a términos contractuales y se implementan en sistemas técnicos que producen consecuencias automáticas o semi-automáticas. En ese punto, el debate deja de ser meramente ético y se convierte en un problema jurídico-filosófico de legitimidad.

El artículo propuso abordar este problema desplazando el foco desde la corrección moral sustantiva hacia la legitimidad procedimental. En contextos de desacuerdo moral persistente, la pregunta relevante no es qué valores son correctos en abstracto, sino bajo qué condiciones un régimen normativo privado puede justificar el ejercicio de poder cuando produce decisiones adversas. Este enfoque permite evaluar la gobernanza algorítmica sin exigir unanimidad moral y sin reducir la legitimidad al consentimiento contractual formal.

Como aporte central, se formuló un test de legitimidad para la moral privatizada ejecutada por sistemas de inteligencia artificial. El test no pretende agotar el debate ni sustituir la regulación pública, sino ofrecer criterios mínimos para identificar déficits estructurales de legitimidad allí donde el control se ejerce mediante automatización. Publicidad de reglas, explicabilidad funcional, contestabilidad efectiva, proporcionalidad, gobernanza del error

y trazabilidad constituyen exigencias básicas para cualquier régimen que aspire a ejercer poder normativo de manera compatible con estándares mínimos de racionalidad y justicia procedimental.

Desde una perspectiva más amplia, el argumento desarrollado sugiere que la gobernanza de la inteligencia artificial reabre preguntas clásicas de la filosofía del derecho y de la teoría política en un nuevo contexto tecnológico. La separación entre ética declarativa y moral operativa, la relación entre poder y justificación, y la función del derecho como límite al ejercicio de autoridad privada adquieren una relevancia renovada cuando las decisiones se escalan por diseño y se presentan bajo la apariencia de neutralidad técnica.

La conclusión no es que toda forma de gobernanza privada basada en IA sea ilegítima, ni que el derecho deba absorber íntegramente estos regímenes. La conclusión es más precisa: cuando la ética se vuelve ejecutable por contrato y código, el derecho no puede limitarse a observar ni a confiar en la autorregulación. Su función es reintroducir garantías allí donde el poder normativo opera sin los contrapesos que históricamente han acompañado a otros sistemas de decisión con consecuencias relevantes.

En última instancia, la discusión sobre IA no trata únicamente sobre tecnología, sino sobre las condiciones bajo las cuales aceptamos ser gobernados por reglas que no votamos, aplicadas por sistemas que no vemos y justificadas por valores que no siempre compartimos. Identificar esos límites y reconstruir criterios de legitimidad es una tarea jurídica y filosófica ineludible para cualquier sociedad que aspire a integrar la inteligencia artificial sin renunciar a sus principios básicos de justicia y control del poder.

10. Referencias

- Abbott, K. W., Keohane, R. O., Moravcsik, A., Slaughter, A.-M., & Snidal, D. (2000). The concept of legalization. *International Organization*, 54(3), 401–419. <https://doi.org/10.1017/S0020818300442515>
- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732. <https://doi.org/10.2139/ssrn.2477899>
- Ben-Shahar, O., & Schneider, C. E. (2010). The failure of mandated disclosure. *University of Pennsylvania Law Review*, 159(3), 647–749. https://scholarship.law.upenn.edu/penn_law_review/vol159/iss3/2/
- Brink, D. O. (1989). *Moral realism and the foundations of ethics*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511624604>
- Buchanan, A. (2002). Political legitimacy and democracy. *Ethics*, 112(4), 689–719. <https://doi.org/10.1086/340313>
- Buchanan, A., & Keohane, R. O. (2006). The legitimacy of global governance institutions. *Ethics*, 20(4), 405–437. <https://doi.org/10.1017/S0892679400000207>
- Chouldechova, A. (2017). Fair prediction with disparate impact: A study of bias in recidivism prediction instruments. *Big Data*, 5(2), 153–163. <https://doi.org/10.1089/big.2016.0047>
- Fuller, L. L. (1964). *The morality of law*. Yale University Press.
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Hardt, M., Price, E., & Srebro, N. (2016). Equality of opportunity in supervised learning. <https://arxiv.org/abs/1610.02413>
- Hart, H. L. A. (1961). *The concept of law*. Oxford University Press.
- ISO/IEC. (2022). *Information technology—Artificial intelligence—Artificial intelligence concepts and terminology (ISO/IEC 22989:2022)*.

- International Organization for Standardization. <https://www.iso.org/standard/74296.html>
- Korsgaard, C. M. (1996). *The sources of normativity*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511554475>
- Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*, 165(3), 633–705. https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/
- Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.
- Miller, A. (2013). *Moral theory: An introduction*. Wiley-Blackwell.
- National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1)*. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>
- Organisation for Economic Co-operation and Development. (2019). *Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449)*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- Radin, M. J. (2013). *Boilerplate: The fine print, vanishing rights, and the rule of law*. Princeton University Press.
- Rawls, J. (2005). *Political liberalism* (Expanded ed.). Columbia University Press.
- Raz, J. (1986). *The morality of freedom*. Oxford University Press.
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (2024). *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Santa Clara Principles on Transparency and Accountability in Content Moderation. (2021). New America. <https://www.newamerica.org>

org/oti/reports/santa-clara-principles-transparency-and-accountability-content-moderation/

Schmidt, V. A. (2013). Democracy and legitimacy in the European Union revisited: Input, output and throughput. *Political Studies*, 61(1), 2–22. <https://doi.org/10.1111/j.1467-9248.2012.00962.x>

Shafer-Landau, R. (2003). *Moral realism: A defence*. Oxford University Press.

Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002). <https://law.justia.com/cases/federal/appellate-courts/F3/306/17/642323/>

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, 20(3), 571–610. <https://doi.org/10.2307/258788>

Suzor, N. (2019). *Lawless: The secret rules that govern our digital lives*. Cambridge University Press. <https://doi.org/10.1017/9781108697841>

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>

van Leeuwen, T. (2008). *Discourse and practice: New tools for critical discourse analysis*. Oxford University Press.

Weber, M. (1978). *Economy and society* (G. Roth & C. Wittich, Eds.). University of California Press.

Insurtech en Bolivia: Análisis Funcional de su Régimen Regulatorio

Insurtech in Bolivia: Functional Analysis of its Regulatory Regime

► **María Fernanda Iriarte Morales**

Investigadora independiente, Santa Cruz • Bolivia

<https://orcid.org/0009-0000-7691-902X> • iriarte.fernanda.legal@gmail.com

Revista de Derecho de la UCB – UCB Law Review, Vol. 10 N° 18, abril 2026, pp. 55-90

ISSN 2523-1510 (en línea), ISSN 2521-8808 (impresa).

DOI: <https://doi.org/10.35319/lawreview.202618135>

Recibido: 31 de octubre de 2025 • Aceptado: 16 de abril de 2026

Resumen

El término *insurtech* no cuenta con un significado único y claramente delimitado, utilizándose indistintamente para referirse a aseguradoras digitales, intermediarios de seguros y plataformas que integran soluciones de software. Esta falta de precisión conceptual ha generado confusión respecto de su encuadre jurídico, especialmente en sistemas altamente regulados como el boliviano, donde coexisten la Ley N° 1883 de 25 de junio de 1998, Ley de Seguros (Ley N° 1883) y el reciente Reglamento de Empresas de Tecnología Financiera (ETF). El presente artículo tiene por objetivo determinar el régimen jurídico aplicable a las distintas categorías de insurtech en el mercado nacional y evaluar la suficiencia del marco normativo vigente. A través de una metodología de análisis dogmático y normativo, se propone una clasificación funcional que distingue entre entidades que asumen riesgo y prestadores de servicios tecnológicos. Se concluye que la regulación debe atender a la sustancia de la actividad (función) por encima de la denominación comercial, identificando en la figura de las ETF y el *sandbox* regulatorio las vías idóneas para la innovación que no implica asunción directa de riesgos.

Palabras clave: Insurtech, Regulación de Seguros, Empresas de Tecnología Financiera, Sandbox Regulatorio, Ley N° 1883, principio de neutralidad tecnológica.

Abstract

The term insurtech does not have a single, clearly defined meaning, as it is used interchangeably to refer to digital insurers, intermediaries, or software providers. This lack of conceptual precision has created confusion regarding its legal classification, particularly in highly regulated systems such as Bolivia's, where the Insurance Law (Law 1883) coexists with the recent Regulation on Financial Technology Companies (ETF).

The purpose of this article is to determine the legal regime applicable to the different categories of insurtech in the national market and to assess the adequacy of the current regulatory framework. Through a dogmatic and normative analysis methodology, a functional classification is proposed that distinguishes between entities that assume risk and providers of technological services.

It is concluded that regulation should focus on the substance of the activity (function) rather than its commercial designation, identifying Financial Technology Companies (ETFs) and the regulatory sandbox as appropriate avenues for innovation that does not involve the direct assumption of risk.

Keywords: Insurtech, Insurance Regulation, Financial Technology Companies, Regulatory Sandbox, Law 1883, Principle of Technological Neutrality.

1. Introducción

La industria aseguradora, tradicionalmente percibida como conservadora y estructuralmente rígida, atraviesa hoy una de las transformaciones más profundas de su historia. El fenómeno responde a un proceso global impulsado por la convergencia entre Big Data, analítica avanzada, inteligencia artificial, machine learning, blockchain, internet de las cosas (IoT) y modelos de negocio basados en plataformas digitales. Estas tecnologías no solo optimizan procesos internos; están redefiniendo la forma en que se suscribe el riesgo, se calcula la prima, se previene el fraude, se gestiona el siniestro e incluso se concibe la función económica del seguro.

La capacidad de capturar, procesar y explotar grandes volúmenes de datos en tiempo real ha desplazado el paradigma clásico de tarificación sustentado en estadísticas históricas hacia esquemas dinámicos basados en comportamiento individual. Los seguros usage-based, los modelos pay-as-you-drive, las coberturas parametrizadas automatizadas mediante smart contracts, y los productos de ciber riesgo son manifestaciones concretas de esta mutación estructural. Paralelamente, gigantes tecnológicos y startups especializadas han ingresado al mercado asegurador apalancando su dominio en datos, experiencia de usuario y arquitectura digital, generando un ecosistema competitivo que trasciende al asegurador tradicional.

En este contexto emerge el término insurtech. Más que una categoría jurídica, constituye una etiqueta de mercado que agrupa realidades empresariales híbridas: desde aseguradoras plenamente licenciadas que operan en entornos 100% digitales, hasta plataformas tecnológicas que proveen infraestructura, análisis predictivo, automatización de reclamaciones o distribución online. El denominador común no es la asunción de riesgo, sino el uso intensivo de tecnología como palanca estratégica.

El fenómeno no es menor en términos económicos. A nivel global, el sector ha captado miles de millones de dólares en capital de riesgo en la última década. Las aseguradoras tradicionales de países más desarrollados, lejos de permanecer al margen, han respondido me-

diante esquemas de colaboración, inversión corporativa, incubadoras y alianzas estratégicas. La transformación, por tanto, no es externa al mercado asegurador: está ocurriendo desde dentro y desde fuera simultáneamente.

Sin embargo, el dinamismo del negocio contrasta con la rigidez estructural de la regulación de seguros, históricamente construido sobre la noción de asunción de riesgos asegurables bajo estrictos requisitos prudenciales. En el ordenamiento jurídico boliviano, esta tensión se manifiesta con particular intensidad. Por un lado, la actividad aseguradora se encuentra sometida a un régimen prudencial estricto bajo supervisión de la Autoridad de Fiscalización y Control de Pensiones y Seguros (APS), conforme a la Ley N°1883, que impone capital mínimo, reservas técnicas y objeto social exclusivo. Por otro, la reciente emisión del Reglamento para Empresas de Tecnología Financiera (ETF), mediante Circular ASFI/885/25, introduce una categoría normativa destinada a empresas que prestan servicios con innovación tecnológica en los ámbitos financiero, del mercado de valores y de seguros.

En este escenario regulatorio dual emerge el problema central que motiva la presente investigación. El debate en torno a las insurtech no es esencialmente tecnológico, sino jurídico-funcional. El uso del término insurtech no determina por sí mismo la naturaleza jurídica de la entidad ni el régimen normativo aplicable. La cuestión decisiva consiste en establecer si la empresa desarrolla actividad aseguradora en sentido técnico; esto es, si asume riesgo asegurable o si se limita a prestar servicios tecnológicos, de intermediación o de soporte dentro del ecosistema asegurador.

La falta de delimitación conceptual puede generar distorsiones regulatorias significativas. De un lado, el riesgo de sobre-regulación: imponer el régimen prudencial de aseguradora a modelos que no retienen riesgo social. De otro, el riesgo de sub-regulación: permitir que actores que efectivamente asumen riesgo operen sin licencia ni supervisión, comprometiendo la estabilidad del sistema y la protección del asegurado. En una industria cuya esencia radica en la mutualización del riesgo y la solvencia institucional,

el error de calificación no es meramente formal: puede tener implicancias sistémicas.

Ante esta tensión, el presente artículo propone un análisis funcional de los modelos de negocio insurtech en Bolivia, con el objeto de identificar los criterios jurídicos que permiten determinar cuándo una empresa tecnológica debe someterse al régimen prudencial asegurador, cuándo corresponde su encuadre dentro de la intermediación de seguros y cuándo su actividad constituye únicamente una prestación tecnológica auxiliar dentro del ecosistema asegurador.

2. Metodología

Para atender a la complejidad del objeto de estudio, la presente investigación adopta un enfoque cualitativo basado en el análisis normativo y doctrinal.

Se ha procedido, en primer lugar, a la revisión doctrinal sobre la naturaleza del concepto *insurtech* y la dispersión normativa que este genera. En segundo lugar, se ha realizado un análisis interpretativo y comparativo de las normas especiales aplicables a ambos sectores en Bolivia: de seguros y *fnitech*. Finalmente, se aplica un criterio funcional para clasificar los distintos modelos de negocio, diferenciando aquellos que implican la asunción de riesgos de aquellos que se limitan a la prestación de servicios tecnológicos o de intermediación. Para un mejor entendimiento, en la parte final, se desarrolla un problema práctico que explicará el conflicto y aplicará los criterios funcionales estudiados

3. Marco teórico: dispersión del concepto *insurtech*

El término *insurtech*, derivado de la contracción de las palabras en inglés *insurance* y *technology*, constituye una categoría semán-

ticamente amplia y jurídicamente indeterminada. Como advierte Hidalgo Cerezo (2024), se trata de un concepto de uso predominantemente comercial que agrupa realidades empresariales heterogéneas bajo una etiqueta común, sin que ello implique la existencia de una categoría normativa autónoma. En consecuencia, no describe un tipo societario ni una figura jurídica específica, sino un fenómeno económico caracterizado por la incorporación intensiva de tecnologías digitales en distintas fases de la cadena de valor del seguro.

La polisemia del término genera una inevitable dispersión normativa. Bajo la denominación *insurtech* se identifican aseguradoras plenamente licenciadas que operan de forma 100% digital, plataformas de intermediación o corretaje, desarrolladores de infraestructura tecnológica, proveedores de analítica predictiva basada en Big Data o empresas que automatizan la gestión de siniestros mediante inteligencia artificial. Esta heterogeneidad funcional impide tener una clasificación jurídica uniforme y exige un análisis diferenciado.

Tradicionalmente, el núcleo del derecho de seguros ha descansado sobre un presupuesto estructural claro: la existencia de una compañía aseguradora que asume profesionalmente riesgos asegurables ajenos, percibe primas y constituye reservas técnicas destinadas a garantizar el cumplimiento de las obligaciones indemnizatorias (Stiglitz, 2001). Este diseño responde a una lógica prudencial centrada en la solvencia institucional y la protección del asegurado frente al riesgo de insolvencia del propio asegurador. El modelo regulatorio clásico, por tanto, se construye sobre la figura de la entidad como sujeto integral de supervisión.

La administración de una significativa masa de capitales y la multiplicidad de intereses comprometidos justifican que la actividad aseguradora sea objeto de vigilancia intensificada, pues un desequilibrio económico-financiero en estas entidades posee un efecto expansivo capaz de repercutir en la producción, la confianza pública y la economía nacional en su conjunto (Stiglitz, 2001). De ahí que el Estado ejerza sobre el sector un reforzado poder de policía,

imponiendo un régimen de control orientado a la tutela del bien común, la protección de los asegurados y la estabilidad sistémica.

Sin embargo, la digitalización del mercado asegurador ha fragmentado funcionalmente la actividad, distribuyendo sus componentes entre múltiples actores especializados. Esta desagregación está motivando a los reguladores a replantear su criterio de intervención. En ausencia de una categoría normativa específica para las insurtech, el debate se desplaza hacia la elección del enfoque regulatorio adecuado: uno basado en la entidad (*entity-based approach*) o uno basado en la actividad efectivamente desarrollada (*activity-based approach*).

La regulación basada en la entidad se estructura en torno al sujeto institucional que participa en el mercado asegurador, imponiendo exigencias diferenciadas según la naturaleza jurídica y la función económica principal que desempeña. Su objetivo es proteger la resiliencia del sistema de manera indirecta, mitigando la probabilidad y las repercusiones de la quiebra o insolvencia de la propia entidad (SUERF, 2022).

En el ámbito tradicional del derecho de seguros, esta lógica no se limita a la compañía aseguradora. También alcanza a otras figuras típicas del sistema, como las corredoras de seguros. En el caso de las compañías aseguradoras, el régimen *entity-based* se traduce en exigencias prudenciales estrictas: capital mínimo, márgenes de solvencia, constitución de reservas técnicas, objeto social exclusivo y supervisión permanente orientada a garantizar la capacidad de responder frente a los riesgos asumidos.

Por su parte, las corredoras de seguros, aunque no asumen riesgo técnico en su balance, también son objeto de regulación basada en la entidad. La Ley N° 1883 las reconoce como sujetos específicos del mercado asegurador, imponiéndoles requisitos de autorización, inscripción, capacidad técnica, garantías y supervisión administrativa. El fundamento de su regulación no es prudencial en sentido estricto, sino funcional: garantizar transparencia, idoneidad profesional y protección del asegurado en el proceso de intermediación.

En ambos casos, el denominador común del enfoque *entity-based* es que la regulación se activa por la pertenencia a una categoría institucional previamente definida por la ley. La intensidad de la supervisión varía según la función (asunción de riesgo o intermediación en la colocación de seguros), pero el punto de partida es la forma jurídica del sujeto.

Este modelo ha demostrado eficacia en mercados estructurados bajo categorías estables y funciones claramente delimitadas durante muchísimos años. No obstante, la irrupción del ecosistema insurtech introduce actores que no encajan naturalmente en estas tipologías clásicas. Empresas que proveen infraestructura para la emisión y ejecución automatizada de seguros paramétricos mediante tecnología blockchain, desarrolladores de modelos de inteligencia artificial orientados al análisis predictivo del riesgo y la prevención de fraude, o plataformas que integran dispositivos IoT y Big Data para monitoreo en tiempo real de riesgos asegurables pueden intervenir en fases críticas de la cadena de valor aseguradora sin asumir riesgo técnico ni constituirse formalmente como corredoras de seguros. Estas entidades pueden incidir directamente en la tarificación, la activación automática de indemnizaciones o la gestión siniestral, sin retener en su balance la obligación indemnizatoria propia del contrato de seguro.

Aquí es donde el enfoque exclusivamente basado en la entidad revela límites estructurales. Si la regulación se activara únicamente por la etiqueta institucional “aseguradora” o “corredora” podría dejar fuera actividades funcionalmente equivalentes que generan riesgos similares para el consumidor, o bien imponer cargas desproporcionadas a modelos tecnológicos que no desempeñan la función económica que justifica la regulación prudencial.

De ahí la relevancia del tránsito hacia un enfoque complementario basado en la actividad. La regulación *activity-based* busca fortalecer la resiliencia de forma directa, imponiendo estándares sobre una función económica específica, con independencia de la estructura corporativa o de las demás actividades desarrolladas por la entidad (SUERF, 2022).

En este punto adquiere especial relevancia el principio de neutralidad tecnológica. Dicho principio establece que las normas no deben favorecer, restringir ni imponer el uso de una tecnología específica, sino regular la función económica subyacente de manera abstracta y adaptable a la evolución técnica (Ponce, 2025). En lugar de legislar sobre herramientas concretas, la neutralidad tecnológica exige centrar la regulación en el efecto jurídico y económico de la actividad.

Este principio evita la obsolescencia normativa, promueve la innovación, facilita la interoperabilidad y previene monopolios regulatorios derivados de exigencias técnicas cerradas (Ponce, 2025). En el ámbito asegurador, su importancia es estratégica: la automatización de la suscripción mediante inteligencia artificial, el uso de *smart contracts* en blockchain o la recepción de primas a través de plataformas digitales no alteran, por sí mismos, la naturaleza jurídica de la actividad si esta consiste en la asunción profesional de un riesgo asegurable.

La neutralidad tecnológica opera, así, como fundamento conceptual del enfoque activity-based. Ambos convergen en una premisa central: misma actividad, mismo riesgo, misma regulación (SUERF, 2022). Si una entidad asume riesgo asegurable de manera sistemática, debe someterse al régimen prudencial asegurador, aun cuando utilice infraestructura digital avanzada. Si, en cambio, presta servicios auxiliares sin retener riesgo en su balance, su encuadre normativo debe corresponder a la función concreta que desempeña.

Bajo este enfoque, la determinación del régimen aplicable no depende de la denominación comercial ni del grado de innovación tecnológica, sino de la función económica efectivamente ejecutada dentro del ecosistema asegurador. Ello permite distinguir analíticamente tres ámbitos: (i) actividades que implican asunción directa de riesgo; (ii) actividades de intermediación o distribución, incluidos canales digitales; y (iii) actividades de soporte tecnológico que no forman parte sustancial del contrato de seguro.

Esta distinción resulta central para el análisis regulatorio en Bolivia. No toda empresa insurtech califica como aseguradora. En la medida en que muchas startups tecnológicas no asumen riesgo asegurable, sino que prestan servicios auxiliares o complementarios, su encuadre jurídico debe responder a la naturaleza concreta de su actividad y no a las exigencias propias de las entidades aseguradoras tradicionales.

La evolución del criterio regulatorio internacional evidencia una transición desde categorías rígidas basadas exclusivamente en la forma institucional hacia esquemas funcionales que buscan preservar la protección del usuario sin frenar la innovación. El desafío no consiste en desregular, sino en regular inteligentemente. La neutralidad tecnológica no implica ausencia de control, sino control calibrado sobre la función económica relevante.

En el contexto boliviano, esta discusión adquiere relevancia práctica inmediata. La coexistencia de la Ley N°1883 y el Reglamento para Empresas de Tecnología Financiera exige delimitar con precisión los puntos de conexión entre ambos marcos normativos. Adoptar un enfoque activity based, alineado con el principio de neutralidad tecnológica, permite evitar tanto la sobre regulación, al imponer cargas prudenciales injustificadas a actores tecnológicos auxiliares, como la sub regulación, al permitir la asunción de riesgos sin licencia ni supervisión. En esa delimitación conceptual reside la clave para compatibilizar innovación, estabilidad financiera y protección efectiva del consumidor.

3.1. Evolución del ecosistema Insurtech en América Latina

Para comprender la magnitud del desafío regulatorio que enfrenta Bolivia, resulta necesario situar el fenómeno insurtech dentro de su contexto evolutivo y regional. La industria financiera y aseguradora, históricamente caracterizada por modelos de negocio longevos, estructuras organizativas rígidas y marcos regulatorios intensivos, comenzó a experimentar una transformación estructural a partir de la crisis financiera global de 2008. La combinación de

factores como la masificación del internet, la proliferación de smartphones, la digitalización de los servicios financieros y la aparición de nuevas infraestructuras tecnológicas basadas en datos generó las condiciones para el surgimiento de actores innovadores que empezaron a cuestionar el statu quo del sector financiero y asegurador.

Este proceso dio origen al ecosistema fintech e insurtech global, cuyo crecimiento fue particularmente acelerado durante la década siguiente. De acuerdo con estimaciones tempranas del sector, hacia 2016 la inversión global en empresas fintech e insurtech superaba ya los 15.200 millones de dólares, reflejando el interés creciente de capital de riesgo y de grandes instituciones financieras en modelos de negocio basados en tecnología aplicada a servicios financieros (Vásquez Rodríguez, 2018).

América Latina no ha sido ajena a esta transformación. Los primeros estudios sistemáticos sobre el ecosistema regional, elaborados por el Banco Interamericano de Desarrollo (BID) y Finnovista, identificaron para el año 2017 un total de 703 emprendimientos fintech e insurtech activos en la región, concentrados principalmente en cinco jurisdicciones que agrupaban cerca del 90 % de la actividad: Brasil (230 empresas), México (180), Colombia (84), Argentina (72) y Chile (65) (Vásquez Rodríguez, 2018). Estos datos evidenciaban ya entonces una fuerte dinámica de innovación, aunque marcada por una distribución geográfica desigual.

A lo largo de los años siguientes, el ecosistema evolucionó desde una etapa inicial de expansión hacia una fase de consolidación y especialización tecnológica. Informes recientes muestran que, a pesar de la desaceleración global del capital de riesgo, el sector insurtech latinoamericano ha demostrado una notable resiliencia estructural. Según el informe Latam Insurtech Journey 2024, elaborado por Digital Insurance LatAm, el número total de startups insurtech activas en la región alcanzó las 498 empresas en 2024, lo que representa un crecimiento aproximado del 6 % respecto de periodos anteriores, acompañado además por una reducción en la tasa de mortalidad del ecosistema, que descendió del 13 % al 10 % (Digital Insurance LatAm, 2024).

Este dato resulta particularmente relevante desde una perspectiva económica y regulatoria: incluso en un contexto de contracción del financiamiento, la inversión insurtech en América Latina durante el primer semestre de 2024 cayó a 26 millones de dólares, lo que representa una reducción del 78 % respecto del mismo periodo del año anterior; sin embargo, el número de empresas activas continuó creciendo. Ello sugiere que el ecosistema ha entrado en una fase de mayor madurez, en la cual la sostenibilidad de los modelos de negocio comienza a prevalecer sobre el crecimiento impulsado exclusivamente por capital de riesgo.

El mismo informe evidencia además cambios relevantes en la estructura funcional del sector. Aunque la distribución digital de seguros sigue siendo el modelo dominante, representando aproximadamente el 53 % de las insurtech, se observa un crecimiento significativo de empresas que operan como habilitadores tecnológicos del sector asegurador (enablers), las cuales constituyen cerca del 47 % del ecosistema (Digital Insurance LatAm, 2024). Estas compañías desarrollan soluciones tecnológicas que permiten digitalizar procesos de suscripción, optimizar la gestión de siniestros, implementar herramientas de detección de fraude basadas en inteligencia artificial o integrar infraestructuras de datos avanzadas para el análisis predictivo del riesgo.

Asimismo, el informe destaca un fenómeno creciente de internacionalización del ecosistema, con un incremento del 11 % en la expansión transfronteriza de las insurtech y un aumento del 35 % en el índice de atracción de compañías extranjeras, alcanzando un 24 % en 2024. Países como Perú, Ecuador y Colombia se posicionan como destinos relevantes para la expansión regional, mientras que Chile destaca por su dinamismo, con 72 insurtech activas y una tasa de internacionalización cercana al 30 % (Digital Insurance LatAm, 2024).

Estos datos permiten afirmar que el fenómeno insurtech en América Latina ha dejado de ser un experimento marginal para convertirse en un componente estructural del ecosistema financiero regional. La innovación tecnológica está penetrando pro-

gresivamente en todas las fases de la cadena de valor aseguradora, desde la distribución digital de pólizas hasta la gestión automatizada de siniestros, el análisis predictivo de riesgos mediante inteligencia artificial o el uso de sensores IoT y Big Data para el monitoreo dinámico de exposiciones asegurables.

La reacción de los Estados frente a esta transformación ha marcado un punto de inflexión en el derecho regulatorio comparado. Ante el riesgo de arbitraje regulatorio y la necesidad de proteger adecuadamente a los consumidores financieros, diversas jurisdicciones latinoamericanas comenzaron a desarrollar marcos regulatorios específicos para ordenar la actividad de los nuevos actores tecnológicos. México se consolidó como pionero regional mediante la promulgación de la Ley para Regular las Instituciones de Tecnología Financiera, mientras que otros países avanzaron mediante regulaciones sectoriales o esquemas de supervisión experimental como los sandboxes regulatorios.

En este contexto regional, la reciente emisión en Bolivia del Reglamento para Empresas de Tecnología Financiera ETF no constituye un fenómeno aislado, sino parte de un proceso más amplio de convergencia regulatoria en América Latina. Estas iniciativas buscan encontrar un equilibrio entre dos objetivos potencialmente tensionados: por un lado, garantizar la estabilidad del sistema financiero y la protección del consumidor; por otro, evitar que marcos regulatorios excesivamente rígidos obstaculicen el desarrollo de la innovación tecnológica en el sector asegurador y financiero.

Desde esta perspectiva, el análisis del fenómeno insurtech no puede limitarse a una discusión meramente tecnológica. Se trata, en realidad, de un debate jurídico-regulatorio sobre cómo adaptar los instrumentos tradicionales de supervisión a un ecosistema empresarial caracterizado por la fragmentación funcional de actividades, la digitalización de procesos y la aparición de nuevos intermediarios tecnológicos dentro de la cadena de valor del seguro.

La utilidad del derecho comparado en este trabajo no reside en proponer una importación mecánica de categorías extranjeras al ordenamiento boliviano, sino en identificar soluciones regulato-

rias frente a un problema estructural común: la fragmentación tecnológica de actividades antes concentradas en sujetos regulados tradicionales. En ese sentido, la experiencia comparada muestra una tendencia consistente a sustituir clasificaciones basadas exclusivamente en la forma institucional por criterios centrados en la función desarrollada, la naturaleza del riesgo generado y el grado de afectación al consumidor o al sistema.

Esa evolución resulta particularmente relevante para Bolivia, donde la coexistencia entre la Ley N° 1883 y el Reglamento ETF obliga precisamente a resolver supuestos híbridos. El valor del derecho comparado, por tanto, no es su autoridad persuasiva en abstracto, sino su capacidad para confirmar que el enfoque funcional no constituye una salida excepcional, sino una respuesta técnicamente consistente frente a mercados donde la innovación tecnológica disocia asunción de riesgo, distribución y soporte operativo.

4. Resultados y discusión: análisis funcional en el ordenamiento boliviano

La coexistencia de una normativa sectorial tradicional, representada por la Ley N°1883, y un instrumento regulatorio reciente orientado a la innovación financiera, como el Reglamento para Empresas de Tecnología Financiera configura un escenario normativo complejo para el desarrollo del ecosistema insurtech en Bolivia.

La dificultad principal radica en que el término insurtech carece de contenido jurídico propio. En consecuencia, el encuadre regulatorio no puede basarse en la denominación tecnológica del modelo de negocio, sino en la función económica que la entidad desempeña dentro de la cadena de valor del seguro.

Siguiendo la metodología propuesta en este trabajo, el análisis se estructura a partir de un criterio funcional inspirado en el enfoque regulatorio *activity-based*, ampliamente utilizado en la regulación financiera comparada. Bajo este enfoque, la tecnología utilizada resulta jurídicamente irrelevante; lo determi-

nante es si la entidad asume riesgos asegurables, intermedia en la contratación de seguros o simplemente provee infraestructura tecnológica al mercado asegurador.

Este criterio permite identificar tres situaciones regulatorias diferenciadas dentro del ordenamiento boliviano.

Para operacionalizar ese enfoque en el análisis de supuestos concretos, resulta necesario explicitar un criterio de calificación que permita distinguir, con mayor precisión, entre actividad aseguradora, intermediación y provisión de infraestructura tecnológica.

4.1. Criterio jurídico-funcional de calificación de modelos *insurtech*

A fin de evitar una clasificación meramente intuitiva de los modelos *insurtech*, corresponde formular un test jurídico-funcional de calificación.

Dicho test no se basará en la denominación empresarial, en el canal digital empleado ni en la sofisticación tecnológica del modelo, sino en la función económica y jurídica efectivamente desplegada dentro de la operación aseguradora.

En ese entendido, el test puede formularse a partir de tres preguntas sucesivas:

(i) ¿La entidad asume riesgo asegurable por cuenta propia?

Si la entidad retiene en su balance la obligación de responder frente al siniestro, percibe primas como contrapartida de dicha cobertura y se coloca en posición de deudora de la prestación indemnizatoria, entonces desarrolla actividad aseguradora en sentido técnico y debe quedar sujeta al régimen prudencial de la Ley N° 1883.

(ii) ¿La entidad participa en la promoción, colocación o celebración del contrato de seguro sin asumir el riesgo técnico?

Si la entidad no indemniza ni soporta el riesgo, pero interviene en la oferta, comparación, recomendación, comercialización o cierre del contrato, entonces su función es de intermediación o distribución y su encuadre debe analizarse a la luz de las reglas aplicables a corredores o agentes, según corresponda.

(iii) ¿La entidad únicamente provee infraestructura tecnológica o servicios auxiliares al mercado asegurador?

Si la entidad no asume riesgo ni interviene jurídicamente en la contratación, sino que presta servicios de soporte; por ejemplo, analítica de datos, detección de fraude, automatización de siniestros, infraestructura de pagos, blockchain, IoT o motores de suscripción, su actividad no constituye seguro en sentido jurídico, sino provisión tecnológica auxiliar, susceptible de encuadre dentro del régimen ETF cuando corresponda.

Este test permite ordenar el análisis conforme a una lógica de substancia sobre la forma: misma función económica, mismo tratamiento regulatorio; distinta función económica, distinta intensidad regulatoria.

4.2. Supuestos en los que la *insurtech* asume riesgo asegurable

El primer supuesto se configura cuando el modelo de negocio consiste en una entidad digital, llamemos NeoAseguradora, que asume directamente riesgos de terceros y se obliga a indemnizar frente a la ocurrencia de un siniestro. En este caso, la naturaleza tecnológica de la empresa no altera su calificación jurídica: desde una perspectiva funcional, la entidad opera materialmente como compañía aseguradora, así opere 100% de forma digital.

En consecuencia, se activa plenamente el régimen prudencial previsto en la Ley N°1883, bajo supervisión de la Autoridad de Fiscalización y Control de Pensiones y Seguros (APS).

La lectura de la Ley N° 1883 permite sostener que el núcleo del régimen asegurador boliviano está construido sobre una lógica prudencial vinculada a la asunción profesional del riesgo. Las exigencias de capital mínimo, reservas técnicas, fondo de garantía, objeto social exclusivo y control permanente de solvencia (por ej. mediante reportes sistemáticos de informes financieros y contables de las transacciones), no aparecen como requisitos formales arbitrarios, sino como consecuencias normativas de una actividad específica y sumamente regulada: recibir primas y asumir riesgos eventuales de cobertura frente a siniestros. Precisamente por ello, tales exigencias no resultan automáticamente trasladables a sujetos que, aunque tecnológicamente insertos en la cadena de valor del seguro, no mutualizan riesgo ni quedan obligados frente al asegurado en los términos propios del contrato de seguro.

En paralelo, el Reglamento de Empresas de Tecnología Financiera evidencia una apertura regulatoria hacia modelos de negocio basados en innovación tecnológica en el ámbito de servicios financieros, mercado de valores y/o seguros, en el marco de lo establecido por el Parágrafo IV, Artículo 19 de la Ley N° 393 de Servicios Financieros (LSF), modificado por la Ley N° 1543 de Modificaciones al Presupuesto General del Estado Gestión 2023, el Código de Comercio en lo conducente, y el Decreto Supremo N° 5384 de 7 de mayo de 2025.

Desde una interpretación sistemática de estas normas, se concluye que el ordenamiento boliviano ya contiene, al menos de forma básica, dos planos regulatorios diferenciados: uno prudencial, dirigido a quienes asumen riesgo o realizan actividades reservadas; y otro funcional-tecnológico, aplicable a quienes proveen infraestructura o innovación sin sustituir a la entidad regulada en la función jurídicamente relevante.

Así, más que una contradicción entre ambos regímenes, lo que existe es una relación de complementariedad condicionada por la actividad efectivamente desarrollada.

La intensidad del régimen de seguros se explica por la lógica económica del contrato de seguro y su función social de reparar

daños asegurables. Como señala la doctrina clásica, la actividad aseguradora implica la administración de fondos colectivos provenientes de primas anticipadas, cuya finalidad es garantizar el cumplimiento de obligaciones indemnizatorias futuras. La solvencia de la entidad aseguradora constituye, por tanto, un elemento estructural para la estabilidad del sistema financiero y la protección del asegurado.

Bajo esta lógica, la Ley N° 1883 establece un conjunto de exigencias prudenciales que operan como condiciones de acceso al mercado. A continuación, se indican algunas de las más relevantes:

- Primero, la obligación de constituirse exclusivamente como sociedad anónima de giro único, con un capital mínimo equivalente a 750.000 Derechos Especiales de Giro, íntegramente suscrito y pagado en efectivo.
- Segundo, la obligación de constituir reservas técnicas permanentes, destinadas a cubrir riesgos en curso, siniestros pendientes y obligaciones actuariales derivadas de contratos de largo plazo.
- Tercero, la exigencia de mantener un fondo de garantía y un margen de solvencia, acompañado de un régimen restrictivo de inversiones destinado a preservar la liquidez y seguridad de los recursos ajenos.

Desde una perspectiva tecnológica, estas exigencias pueden representar barreras de entrada significativas para startups insurtech, particularmente para modelos de microseguros digitales o seguros paramétricos de bajo impacto económico.

Sin embargo, desde el punto de vista jurídico, la conclusión es clara: si una empresa asume riesgo asegurable de manera profesional y sistemática, debe someterse al régimen de aseguradora, con independencia de que su operación sea completamente digital o esté basada en tecnologías como inteligencia artificial, blockchain o contratos inteligentes. Este criterio reproduce el principio regulatorio adoptado en múltiples jurisdicciones internacionales: misma actividad, mismo riesgo, misma regulación.

4.3. *Insurtech* como Intermediario, Distribuidor de Seguros

En el ámbito de la distribución digital, el ecosistema *insurtech* plantea el enorme desafío de la eliminación del soporte tradicional en papel en favor de interfaces interactivas. Al respecto, la literatura académica subraya que la digitalización exige adaptar rigurosamente los criterios de transparencia formal y material; por tanto, los reguladores deben garantizar que en entornos donde operan agregadores o *chatbots*, el adherente conozca y comprenda cabalmente las cláusulas limitativas de sus derechos, requiriendo en muchos casos una implantación *ad hoc* en el entorno digital mediante advertencias específicas, tipografías resaltadas y procesos de trazabilidad documental (García Mandalóniz, 2021).

Un segundo grupo de modelos *insurtech* corresponde a aquellas plataformas cuya función consiste en facilitar la contratación de seguros entre aseguradoras y clientes finales, sin asumir riesgo técnico en su balance. En estos casos, la entidad actúa funcionalmente como intermediario del contrato de seguro, aun cuando su canal de operación sea completamente digital.

La legislación boliviana reconoce esta función dentro de la figura de corredores o agentes¹ de seguros, los cuales se encuentran también sujetos a supervisión de la Autoridad de Fiscalización y Control de Pensiones y Seguros (APS). Aunque estas entidades no asumen riesgo asegurador, su regulación responde a la necesidad de garantizar la transparencia en la comercialización de productos y la adecuada protección del consumidor, especialmente tratándose de contratos de adhesión como las pólizas de seguro, que contienen cláusulas técnicas y condiciones actuariales cuya comprensión requiere conocimiento especializado.

Para operar en el mercado boliviano, las corredoras de seguros deben cumplir diversos requisitos regulatorios, entre los cuales destaca la obligación de constituirse como sociedades comerciales con objeto social exclusivo o único, además de obtener autorización y registro ante la APS y mantener mecanismos de respon-

sabilidad profesional frente a eventuales errores u omisiones en la intermediación.

Este requisito de objeto social único, concebido para garantizar la especialización y profesionalidad del intermediario, puede generar fricciones con los modelos insurtech contemporáneos. Muchas plataformas tecnológicas que participan en la distribución digital de seguros desarrollan simultáneamente otras actividades vinculadas con el ecosistema digital, tales como el desarrollo de software, la provisión de infraestructura tecnológica para aseguradoras, la prestación de servicios de análisis de datos o incluso esquemas de intermediación “de marca blanca” (*white-label distribution*) para entidades financieras o comercios electrónicos. La exigencia de exclusividad societaria puede, por tanto, limitar la posibilidad de integrar estos servicios dentro de una misma estructura empresarial.

En la práctica internacional, este problema suele resolverse mediante esquemas de tercerización tecnológica, en los cuales la entidad autorizada para intermediar en seguros mantiene la relación jurídica directa con el cliente y asume la responsabilidad regulatoria, mientras que la plataforma tecnológica opera como proveedor de servicios digitales. Bajo este esquema, la corredora o agente de seguros licenciado actúa como frente regulatorio del modelo de negocio, siendo responsable ante el supervisor por el cumplimiento de las obligaciones propias de la intermediación.

- 1 De acuerdo con la normativa boliviana, un agente de seguros debe ser obligatoriamente una persona natural sujeta a una relación de exclusividad con una sola aseguradora, lo cual es incompatible con un modelo de plataforma digital abierta. Por ello, al ser la insurtech una empresa (persona jurídica) diseñada para intermediar de forma independiente entre las diversas ofertas del mercado y los usuarios, su único vehículo legal aplicable es el de una corredora de seguros, por lo que no haremos posterior referencia a esta figura de agente.

La plataforma tecnológica, por su parte, puede encargarse de funcionalidades como la interfaz digital de contratación, la integración con sistemas de pago, la gestión de datos o el soporte tecnológico del proceso de distribución, sin que ello implique asumir formalmente la condición de intermediario regulado.

En estos casos, las cargas regulatorias que recaen sobre el proveedor tecnológico suelen concentrarse principalmente en obligaciones de transparencia, protección del consumidor y cumplimiento de estándares de integridad financiera. La experiencia comparada muestra que diversas jurisdicciones han optado por imponer a los distribuidores digitales obligaciones tales como:

- Garantizar la divulgación clara de la identidad de la aseguradora y del intermediario autorizado que respalda el producto ofrecido;
- Proporcionar información comprensible sobre coberturas, exclusiones y costos del seguro antes de la contratación;
- Implementar mecanismos adecuados de protección de datos personales y seguridad de la información;
- Aplicar procedimientos básicos de conocimiento del cliente (KYC) y monitoreo para la prevención de lavado de dinero y financiamiento del terrorismo (AML/CFT) cuando intervienen en procesos de pago o identificación del usuario; y
- Establecer canales accesibles de atención y resolución de reclamos para consumidores.

Este enfoque puede observarse, por ejemplo, en la Insurance Distribution Directive (IDD) de la Unión Europea, la cual regula la distribución de seguros incluyendo a intermediarios tradicionales, aseguradoras y a los denominados “intermediarios auxiliares de seguros” (*ancillary insurance intermediaries*), es decir, entidades cuya actividad principal no es la distribución de seguros pero que ofrecen coberturas complementarias a bienes o servicios. Este esquema permite que actores no especializados participen en la distribución de seguros bajo determinadas condiciones, manteniendo al mismo tiempo la responsabilidad regulatoria principal

en la aseguradora o en intermediarios registrados, lo que garantiza estándares de protección al consumidor y transparencia en la comercialización de pólizas (Unión Europea, 2016).

Desde esta perspectiva, la evolución del derecho comparado sugiere que el desarrollo del mercado digital de seguros exige diferenciar jurídicamente entre intermediación profesional y distribución tecnológica, evitando imponer exigencias estructurales desproporcionadas a plataformas que no ejercen funciones de asesoramiento técnico ni asumen responsabilidades propias del intermediario tradicional.

4.4. Insurtech como proveedor de infraestructura tecnológica del mercado asegurador

El tercer supuesto corresponde a empresas cuya actividad consiste exclusivamente en desarrollar o proveer soluciones tecnológicas aplicables al sector asegurador, sin asumir riesgo técnico ni intervenir directamente en la contratación del seguro.

En esta categoría se encuentran, por ejemplo: empresas que desarrollan modelos de inteligencia artificial para detección de fraude, proveedores de infraestructura blockchain para seguros paramétricos automatizados, plataformas de análisis predictivo basadas en Big Data para tarificación dinámica de riesgos o sistemas IoT que permiten monitorear en tiempo real exposiciones asegurables.

Aunque estas soluciones pueden influir significativamente en la eficiencia del mercado asegurador, no constituyen actividad aseguradora en sentido jurídico, puesto que no implican la asunción de riesgo ni la intermediación contractual entre aseguradora y tomador del seguro.

El ordenamiento boliviano ha comenzado a abordar este fenómeno mediante el Reglamento para Empresas de Tecnología Financiera, el cual reconoce la existencia de empresas que prestan servicios tecnológicos al sistema financiero. El alcance de dicho reglamento incluye expresamente servicios tecnológicos aplicables a entidades del sistema financiero, del mercado de valores y del sector

asegurador, lo que permite afirmar que, desde una perspectiva normativa, las soluciones tecnológicas dirigidas al mercado de seguros pueden encuadrarse dentro de la categoría de Empresas de Tecnología Financiera (ETF).

No obstante, hasta la fecha la Autoridad de Fiscalización y Control de Pensiones y Seguros (APS) no ha emitido un criterio regulatorio específico respecto del rol de las insurtech dentro del mercado asegurador, ni respecto de su interacción con el régimen de ETF supervisado por la ASFI. Esta ausencia de pronunciamiento genera cierto grado de incertidumbre jurídica para modelos de negocio que, aun siendo tecnológicamente neutrales, inciden en procesos económicos clave del sector asegurador.

Dentro del marco del Reglamento de ETF, las insurtech que desarrollan soluciones tecnológicas pueden operar particularmente dentro de la categoría de Tecnologías Empresariales, orientada a proveer infraestructura digital, automatización de procesos o soluciones tecnológicas a entidades reguladas del sistema financiero.

Uno de los aspectos más relevantes del reglamento es el reconocimiento de alianzas entre empresas tecnológicas y entidades financieras o aseguradoras reguladas. Bajo este esquema, la entidad regulada conserva la responsabilidad prudencial frente al regulador, mientras que la empresa tecnológica aporta innovación, eficiencia operativa o infraestructura digital.

Este modelo de cooperación refleja una tendencia creciente en la regulación financiera internacional, donde la innovación tecnológica suele desarrollarse mediante asociaciones entre instituciones reguladas y proveedores tecnológicos especializados.

Un ejemplo ilustrativo de este tipo de modelos puede observarse en el caso hipotético de una insurtech de base tecnológica que desarrolle infraestructura para el cobro de primas de seguros denominadas en dólares estadounidenses mediante stablecoins u otros activos virtuales, así como sistemas de detección automatizada de fraude o análisis de siniestros mediante inteligencia artificial.

Desde una perspectiva regulatoria, un modelo de este tipo podría estructurarse de diversas formas:

a) Proveedor tecnológico bajo el régimen de ETF

La empresa tecnológica podría constituirse como una Empresa de Tecnología Financiera bajo la categoría de Tecnologías Empresariales, limitándose a proveer infraestructura tecnológica a aseguradoras o corredoras de seguros.

En este escenario, la empresa no participaría en la contratación del seguro ni en la administración del riesgo, sino únicamente en la provisión de soluciones tecnológicas, como:

- sistemas de cobro de primas mediante activos virtuales,
- infraestructura de pagos digitales interoperables,
- herramientas de detección de fraude mediante inteligencia artificial,
- soluciones de análisis de datos para evaluación de siniestros.

La entidad aseguradora o intermediario regulado mantendría la responsabilidad frente a la APS por la correcta comercialización y administración del contrato de seguro.

b) Modelo de alianza con aseguradoras o intermediarios regulados

Una segunda alternativa consiste en estructurar el modelo mediante una alianza contractual entre la insurtech y una entidad aseguradora o corredora licenciada.

Bajo este esquema:

- la entidad regulada actuaría como frente regulatorio ("regulatory front") ante la APS,
- mientras que la empresa tecnológica proveería la infraestructura digital para pagos, análisis de datos o automatización de procesos.

Este modelo es ampliamente utilizado en jurisdicciones con ecosistemas fintech desarrollados, donde la innovación tecnológica

se canaliza a través de asociaciones con entidades que ya cuentan con licencias regulatorias.

c) Integración con proveedores de servicios de activos virtuales

En el caso específico de sistemas de cobro de primas mediante stablecoins u otros activos virtuales, la solución tecnológica podría también integrarse con proveedores de servicios de activos virtuales (PSAVs) que se encuentren autorizados bajo el marco regulatorio ETF.

En este escenario, la empresa insurtech y a la vez ETF actuaría como proveedor de infraestructura tecnológica que permite a las entidades reguladas integrar mecanismos de pago alternativos dentro de sus procesos operativos.

4.5. Innovación tecnológica y coordinación regulatoria

A pesar de los avances introducidos por el Reglamento de Empresas de Tecnología Financiera, la estructura institucional del sistema regulatorio boliviano plantea desafíos para el desarrollo de modelos insurtech complejos.

La supervisión del sistema financiero corresponde a la ASFI, mientras que la regulación del mercado asegurador es competencia de la APS. En aquellos casos en que un modelo de negocio combine simultáneamente elementos tecnológicos, financieros y aseguradores, pueden surgir zonas grises de supervisión que dificultan determinar con claridad qué autoridad resulta competente o cuál debe ser el régimen normativo aplicable.

Este problema no es exclusivo de Bolivia. Diversas jurisdicciones han enfrentado desafíos similares ante la aparición de modelos híbridos que trascienden las fronteras tradicionales entre sectores financieros, especialmente en ámbitos como los pagos digitales, los activos virtuales, los seguros paramétricos o las plataformas tecnológicas que prestan servicios a entidades reguladas.

La experiencia comparada muestra que una solución efectiva consiste en fortalecer los mecanismos de coordinación institucional entre reguladores mediante entornos de experimentación regulatoria o *regulatory sandboxes*, diseñados para evaluar modelos de negocio innovadores bajo condiciones controladas. Estos espacios permiten a las autoridades comprender con mayor precisión los riesgos asociados a nuevas tecnologías, al mismo tiempo que facilitan el desarrollo de soluciones innovadoras sin imponer de manera inmediata el régimen regulatorio completo aplicable a entidades plenamente licenciadas.

La necesidad de este tipo de mecanismos ha sido ampliamente respaldada por la doctrina especializada. Al analizar los entornos controlados de pruebas o *sandboxes*, García Mandalóniz (2021) destaca que estos no solo benefician a las empresas al brindar un marco seguro de experimentación, sino que actúan como un valioso instrumento regulador y supervisor para el conocimiento y la comprensión de los desarrollos, los efectos o los resultados de las pruebas tecnológicas emergentes. En esta misma línea, Fernández Manzano (2020) advierte que la implementación de un *sandbox* constituye una de las mejores soluciones contemporáneas para permitir la transición digital de los servicios financieros y aseguradores, logrando armonizar el fomento a la innovación con la ineludible salvaguarda de la seguridad jurídica y la protección del consumidor.

En el contexto boliviano, una alternativa institucionalmente viable sería la creación de un Espacio Controlado de Pruebas (ECP) interinstitucional entre ASFI y APS, específicamente orientado al análisis de modelos *fintech* e *insurtech* que presenten elementos regulatorios concurrentes. A diferencia del ECP actualmente previsto en el régimen de innovación financiera administrado por ASFI, este esquema podría diseñarse con reglas más flexibles y adaptadas a la naturaleza experimental de las soluciones tecnológicas aplicadas al mercado asegurador.

Entre las características que podría contemplar un esquema de este tipo se encuentran, por ejemplo, la posibilidad de ampliar el

número de usuarios participantes en las pruebas piloto cuando la naturaleza del modelo de negocio lo requiera, establecer plazos de evaluación más breves que permitan ciclos iterativos de prueba y aprendizaje regulatorio, y definir criterios claros para la participación de entidades tecnológicas que actúen en alianza con aseguradoras o corredoras licenciadas. Asimismo, el entorno de pruebas podría prever obligaciones proporcionales de gestión de riesgos, transparencia hacia los usuarios participantes, y cumplimiento de estándares básicos en materia de prevención de legitimación de ganancias ilícitas, protección de datos personales y seguridad tecnológica.

Un mecanismo de esta naturaleza permitiría que ambas autoridades evalúen conjuntamente modelos emergentes como plataformas de distribución digital de seguros, soluciones de infraestructura tecnológica para el sector asegurador, esquemas de pago de primas mediante activos virtuales o herramientas avanzadas de análisis de riesgos basadas en inteligencia artificial.

Más importante aún, la información generada durante estas pruebas regulatorias podría servir como base empírica para el desarrollo futuro de un marco normativo específico para el ecosistema insurtech en Bolivia, permitiendo adoptar reglas claras que distingan adecuadamente entre actividad aseguradora, intermediación y provisión de infraestructura tecnológica.

De esta manera, una aproximación coordinada entre ASFI y APS no solo contribuiría a reducir la incertidumbre regulatoria que enfrentan los innovadores tecnológicos, sino que también permitiría preservar los objetivos fundamentales del derecho financiero y asegurador: la protección del consumidor, la integridad del sistema y la estabilidad del mercado, sin obstaculizar innecesariamente el desarrollo de nuevas soluciones tecnológicas.

4.6. Protección de datos personales, prevención de lavado de activos y gobernanza de la información en ecosistemas *insurtech*

Un elemento transversal al desarrollo del ecosistema *insurtech* es la gestión de información sensible de los usuarios. A diferencia de los modelos aseguradores tradicionales, muchas soluciones *insurtech* se basan intensivamente en el procesamiento de grandes volúmenes de datos personales, financieros y conductuales para la evaluación de riesgos, la personalización de coberturas, la detección de fraude o la automatización de procesos de suscripción.

Tecnologías como el análisis predictivo basado en big data, los sistemas de inteligencia artificial para prevención de fraude, o los dispositivos IoT utilizados en seguros telemáticos o paramétricos, requieren el tratamiento constante de datos que pueden revelar patrones de comportamiento, geolocalización, historial financiero e incluso variables biométricas. En consecuencia, la protección de dichos datos constituye un componente esencial del marco regulatorio que debe acompañar el desarrollo del sector. En este contexto, la innovación tecnológica aplicada al seguro exige como presupuesto mínimo reglas claras sobre licitud del tratamiento, finalidad, proporcionalidad, minimización, seguridad, trazabilidad y resguardo reforzado de datos sensibles.

Desde la perspectiva prudencial, estas obligaciones se intersectan con los regímenes de prevención de lavado de activos y financiamiento del terrorismo (AML/CFT). Tanto las aseguradoras como las corredoras de seguros que participan en la comercialización de pólizas deben aplicar mecanismos de debida diligencia del cliente (KYC), identificación del beneficiario final, monitoreo de transacciones y reportes de operaciones sospechosas ante la Unidad de Investigaciones Financieras (UIF).

En los modelos *insurtech*, estas obligaciones se extienden también a las plataformas tecnológicas que intervienen en la captación de clientes, el procesamiento de pagos o la administración de información contractual. Incluso cuando la responsabilidad regulato-

ria principal recae sobre la aseguradora o la corredora licenciada, las soluciones tecnológicas que procesan datos o facilitan transacciones deben diseñarse conforme a estándares de compliance regulatorio, seguridad informática y trazabilidad de operaciones.

El derecho comparado muestra que la innovación tecnológica en servicios financieros suele ir acompañada de marcos robustos de protección de datos personales. Instrumentos como el Reglamento General de Protección de Datos de la Unión Europea (GDPR) establecen principios de tratamiento legítimo, minimización de datos, seguridad de la información, consentimiento informado y responsabilidad proactiva de las entidades que procesan datos personales. Estos estándares han influido significativamente en la regulación fintech e insurtech a nivel global.

En el caso boliviano, sin embargo, el ordenamiento jurídico aún carece de una ley integral de protección de datos personales, lo que genera un vacío normativo relevante frente al creciente procesamiento de información sensible en entornos digitales. Si bien existen disposiciones dispersas en normativa sectorial, estas resultan insuficientes para abordar los desafíos que plantea la economía digital y el uso intensivo de datos en modelos de negocio basados en inteligencia artificial y analítica avanzada.

Desde una perspectiva de política regulatoria, el desarrollo sostenible del ecosistema insurtech en Bolivia requiere avanzar hacia la promulgación de una ley de protección de datos personales que establezca principios claros de tratamiento, derechos de los titulares de datos y obligaciones para las entidades que los procesan. Este marco debería articularse con las obligaciones existentes en materia de prevención de lavado de activos, seguridad de la información y protección del consumidor financiero, de modo que la innovación tecnológica se desarrolle dentro de un entorno de confianza institucional.

En este sentido, la incorporación de estándares modernos de gobernanza de datos no debe interpretarse como una barrera para la innovación, sino como un elemento habilitador del desarrollo de nuevos modelos de negocio digitales. La confianza del usuario

en la protección de su información constituye, en última instancia, un activo fundamental para la consolidación de plataformas tecnológicas que aspiren a operar dentro del mercado asegurador.

5. Caso práctico: *accountability* en modelos híbridos

Para ilustrar la aplicación de la tipología funcional propuesta y evidenciar los desafíos del actual marco regulatorio, resulta imperativo estructurar un caso práctico basado en la realidad operativa del mercado.

5.1. Planteamiento del problema

Imaginemos a "AgroTech", una startup boliviana que ha desarrollado una plataforma tecnológica para seguros agrarios paramétricos. Al no asumir el riesgo técnico, AgroTech se constituye legalmente ante la Autoridad de Supervisión del Sistema Financiero como una Empresa de Tecnología Financiera, operando bajo las categorías expresamente reconocidas en el Reglamento ETF de "Proveedores de Servicios de Activos Virtuales (PSAV)" y "Pagos y plataformas de pagos".

Posteriormente, AgroTech suscribe una "alianza" con una aseguradora tradicional (licenciada, regulada y supervisada por la APS). La ETF provee una pasarela de pagos que acepta criptoactivos, transformando bolivianos (BOB) a stablecoins (USDT) para el pago de primas en dólares. Asimismo, utiliza contratos inteligentes (smart contracts) en blockchain que, conectados a un oráculo climático², automatizan el pago de indemnizaciones en USDT si los niveles de lluvia en una región caen por debajo de un umbral determinado.

Durante la ejecución del contrato, AgroTech sufre un sofisticado ciberataque. Los delincuentes vulneran la pasarela de pagos y el código del smart contract, logrando dos objetivos: exfiltrar datos personales y financieros altamente sensibles de los agricultores

(identidad, geolocalización de las parcelas, direcciones de wallets), y drenar los fondos en USDT destinados a las transferencias de primas y al pago de indemnizaciones.

5.2. El conflicto jurídico y la dispersión supervisora

Este escenario detona un profundo conflicto en torno al accountability (rendición de cuentas y atribución de responsabilidad). Los agricultores exigirán el pago de sus siniestros (por la sequía) y reclamarán por la vulneración de sus datos a la aseguradora con la que firmaron la póliza, pero la brecha ocurrió en la infraestructura de su proveedor tecnológico de soluciones de pago.

Institucionalmente, la aseguradora tradicional debe responder ante la APS por el contrato de seguro, mientras que la ETF, causante material de la brecha tecnológica y administradora de los criptoactivos, está sujeta a la ASFI. Esta dislocación evidencia la insuficiencia de un modelo de supervisión tradicional (entity-based) frente a riesgos digitales transversales.

5.3. Análisis funcional y accountability: ¿Quién debe responder?

La atribución de responsabilidad debe resolverse aplicando el análisis funcional propuesto, separando tajantemente el riesgo técnico-asegurador del riesgo tecnológico-operativo:

- 2 Un oráculo es un servicio que actúa como intermediario entre la blockchain y fuentes externas de información, permitiendo que los contratos inteligentes accedan a datos del mundo real y ejecuten automáticamente condiciones basadas en dichos datos (Techopedia, s. f.).
Por tanto, un oráculo climático constituye una aplicación específica de este concepto, en la medida en que provee datos meteorológicos externos (como niveles de precipitación) a sistemas basados en blockchain, habilitando la ejecución automática de condiciones contractuales en seguros paramétricos.

La responsabilidad de la Aseguradora (Riesgo Técnico): Bajo el enfoque de la Ley N° 1883, la aseguradora retiene el riesgo técnico de la póliza en su balance. Si el evento paramétrico (la sequía) ocurrió, la aseguradora está ineludiblemente obligada a pagar la indemnización al agricultor. Jurídicamente, no puede oponer como excusa el hackeo o la falla del smart contract de su proveedor (la ETF) para liberarse de su obligación principal frente al asegurado.

La responsabilidad de la ETF (Riesgo Tecnológico y Cibernético): Como PSAV y pasarela de pagos, AgroTech asume el riesgo operativo y tecnológico de las transacciones de pagos. El Reglamento ETF exige que las alianzas definan contractualmente las "responsabilidades de las partes, por pérdidas originadas en fallas y/o deficiencias en la prestación de los servicios" (ASFI, 2025). Por tanto, la ETF debe responder patrimonialmente frente a la aseguradora por los fondos drenados (USDT) y hacer frente a las responsabilidades ante los usuarios por la exfiltración de los datos sensibles.

6. Conclusiones

El análisis desarrollado a lo largo de este trabajo permite sostener que el término *insurtech* no describe una categoría jurídica autónoma dentro del ordenamiento boliviano, sino un fenómeno económico caracterizado por la incorporación de innovación tecnológica en distintas fases de la cadena de valor del seguro. En consecuencia, la naturaleza regulatoria de una *insurtech* no puede determinarse por la tecnología utilizada, sino por la función económica que desempeña dentro de la operación aseguradora.

Desde esta perspectiva, el criterio determinante para el encuadre jurídico es la asunción o no del riesgo asegurador. Cuando una entidad retiene el riesgo técnico en su balance y se obliga frente al asegurado al pago de una indemnización, se configura materialmente como una aseguradora y, por tanto, debe someterse al régimen prudencial previsto en la Ley N°1883. Este régimen responde a la necesidad de proteger la solvencia de entidades que administran fondos colectivos provenientes de primas y que asumen obligaciones in-

demnizatorias de largo plazo, justificando así la intensa supervisión estatal sobre capital, reservas técnicas y gestión del riesgo.

Por el contrario, cuando una plataforma tecnológica se limita a facilitar la colocación de pólizas o conectar aseguradoras con clientes, su función corresponde a la intermediación aseguradora. En estos casos, el marco regulatorio aplicable es el previsto para corredores de seguros bajo supervisión de la APS. No obstante, el análisis realizado evidencia que la legislación vigente fue concebida principalmente para esquemas tradicionales de asesoramiento profesional y no necesariamente para modelos digitales basados en comparadores automatizados o marketplaces de seguros. Esta situación sugiere la conveniencia de explorar figuras regulatorias intermedias que permitan la participación de plataformas tecnológicas bajo obligaciones proporcionales centradas en la transparencia y protección del consumidor, manteniendo al mismo tiempo la responsabilidad regulatoria principal en la aseguradora o en intermediarios licenciados.

Un tercer conjunto de modelos corresponde a empresas que no participan en la contratación del seguro ni asumen riesgos, sino que proveen infraestructura tecnológica para el funcionamiento del mercado asegurador. En esta categoría se ubican desarrolladores de soluciones de inteligencia artificial para detección de fraude, plataformas blockchain para seguros paramétricos, sistemas IoT para monitoreo de riesgos o herramientas de análisis predictivo basadas en Big Data. Estas actividades, si bien inciden significativamente en la eficiencia del mercado, no constituyen actividad aseguradora en sentido jurídico. El ordenamiento boliviano ha comenzado a reconocer este fenómeno mediante el Reglamento para Empresas de Tecnología Financiera, el cual establece un marco para que proveedores tecnológicos operen bajo supervisión de la ASFI cuando sus servicios se integran al sistema financiero o asegurador.

El estudio también revela que el desarrollo de modelos insurtech complejos puede generar zonas grises de supervisión institucional. En Bolivia, la regulación del sistema financiero corresponde

a la ASFI, mientras que la actividad aseguradora es supervisada y fiscalizada por la APS. Cuando una innovación tecnológica involucra simultáneamente procesamiento de pagos, gestión de datos y comercialización de seguros, la delimitación competencial puede resultar difusa. Por esta razón, se ha propuesto la creación de mecanismos formales de coordinación interinstitucional, incluyendo un entorno controlado de pruebas o sandbox regulatorio conjunto, que permita evaluar de manera coordinada modelos de negocio emergentes y reducir la incertidumbre regulatoria para los actores del mercado.

El caso práctico analizado en este artículo: una plataforma tecnológica que facilita la contratación de pólizas emitidas por una aseguradora y permite el pago de primas mediante criptoactivos o *stablecoins*, ilustra claramente la utilidad del enfoque funcional propuesto. En este escenario, la aseguradora continúa siendo la entidad que asume el riesgo técnico y responde frente al asegurado conforme al régimen de seguros. La plataforma tecnológica, por su parte, podría desempeñar funciones de intermediación o de infraestructura tecnológica, dependiendo de si participa en la colocación de pólizas o únicamente en el procesamiento de pagos y servicios de análisis de datos. Si dicha plataforma operara recaudando fondos de usuarios bolivianos o interactuando con el sistema financiero local, resultaría razonable exigir su establecimiento formal en el país y su sujeción a la normativa aplicable a empresas de tecnología financiera, con el objetivo de garantizar transparencia, trazabilidad de transacciones y protección del consumidor.

Finalmente, el análisis pone de relieve la importancia de incorporar en el desarrollo del ecosistema insurtech estándares robustos de gobernanza de datos, prevención de lavado de activos y protección del consumidor. La creciente utilización de inteligencia artificial, Big Data y dispositivos conectados implica el tratamiento intensivo de información personal y financiera, lo que hace particularmente relevante la existencia de marcos regulatorios claros en materia de privacidad y seguridad de la información. En este contexto, la ausencia de una ley integral de protección de datos personales en Bolivia constituye una brecha normativa que debería

ser atendida para fortalecer la confianza en los servicios digitales y alinear el país con las tendencias regulatorias internacionales.

En síntesis, la principal conclusión de este estudio es que el desarrollo del ecosistema insurtech en Bolivia no requiere necesariamente la creación de nuevas categorías jurídicas rígidas, sino la aplicación coherente de un enfoque regulatorio basado en la actividad económica efectivamente realizada. Bajo este criterio, la tecnología debe ser considerada un medio para la prestación de servicios y no un factor determinante de su naturaleza jurídica. La adopción de este enfoque, complementada con mecanismos de coordinación institucional y marcos regulatorios proporcionales, permitiría promover la innovación tecnológica en el mercado asegurador boliviano sin comprometer los objetivos fundamentales de estabilidad financiera y protección del consumidor.

7. References

- Autoridad de Supervisión del Sistema Financiero [ASFI]. (2025). Circular ASFI/885/25: Reglamento de Empresas de Tecnología Financiera. Recopilación de Normas para Servicios Financieros.
- Borio, C., Claessens, S., & Tarashev, N. (2022). Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs (SUERF Policy Brief No. 404). SUERF - The European Money and Finance Forum.
- Digital Insurance LatAm. (2024). Latam Insurtech Journey 2024: La resiliencia de la industria insurtech en América Latina. Digital Insurance LatAm.
- Estado Plurinacional de Bolivia. (1998). Ley N° 1883 de 25 de junio de 1998, Ley de Seguros. Gaceta Oficial de Bolivia.
- Estado Plurinacional de Bolivia. (2025). Decreto Supremo N° 5384 de 7 de mayo de 2025. Gaceta Oficial de Bolivia.
- Fernández Manzano, L. A. (2020). Insurtech: ¿Revolución o evolución? Una aproximación a los desafíos regulatorios y contractuales que plantea la aplicación de la tecnología en el sector asegurador.

En M. Martínez Muñoz (Coord.) & A. B. Veiga Copo (Dir.), Retos y desafíos del contrato de seguro: del necesario aggiornamento a la metamorfosis del contrato (pp. 955-986). Thomson Reuters Aranzadi.

García Mandalóniz, M. (2021). La eliminación del papel como desafío del regulador para el auge de las insurtech de distribución más allá del «regulatory sandbox». En L. M. Miranda Serrano & J. Pagador López (Dirs.), Desafíos del regulador mercantil en materia de contratación y competencia empresarial (pp. 225-238). Marcial Pons.

Hidalgo Cerezo, A. (2024). Insurtech: polisemia y dispersión normativa de un concepto poliédrico. En Retos Inminentes de Derecho Digital (pp. 267-303). Dykinson.

Kalinich, K. P., & Ricketts, T. (2022). Cyber Insurance for Law Firms and Legal Organizations. En The ABA Cybersecurity Handbook (pp. 479-551). American Bar Association.

Ponce, J.S. (2025, marzo 11).

¿Sabes qué es el principio de neutralidad tecnológica? Te lo explico aquí.
LinkedIn.

<https://www.linkedin.com/pulse/sabes-qu%C3%A9-es-el-principio-de-neutralidad-tecnol%C3%B3gica-te-ponce-ibute/?originalSubdomain=es>

Techopedia. (s. f.). Oracle (blockchain oracle). <https://www.techopedia.com/definition/oracle-blockchain-oracle>

Stiglitz, R. S. (2001). Derecho de Seguros (Tomo I, 3.^a ed.). Abeledo-Perrot.

Unión Europea. (2016). Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo de 20 de enero de 2016 sobre la distribución de seguros. Diario Oficial de la Unión Europea.

Vásquez Rodríguez, C. P. (2018). Fintech e insurtech en América Latina: desafíos en la protección del consumidor, la regulación y la supervisión. *Círculo de Derecho Administrativo*, (18), 236-258.

Inteligencia artificial y proceso constitucional en Bolivia. Una cavilación desde las tareas, directrices y limitaciones a su aplicación

Artificial Intelligence and the Constitutional Process in Bolivia. A Reflection on the Tasks, Guidelines, and Limitations of its Application

► **Rodrigo René Cruz Apaza**

Investigador independiente, Cochabamba • Bolivia

<http://orcid.org/0000-0003-1043-5932> • rodriggcruz@gmail.com

Revista de Derecho de la UCB – UCB Law Review, Vol. 10 N° 18, abril 2026, pp. 93-135

ISSN 2523-1510 (en línea), ISSN 2521-8808 (impresa).

DOI: <https://doi.org/10.35319/lawreview.202618137>

Recibido: 29 de octubre de 2025 • Aceptado: 10 de abril de 2026

Resumen

Aunque la inteligencia artificial es una cuestión tecnológica de la que se comenta desde la segunda mitad del siglo XX, dicha expresión ha estado en boga en el último lustro del presente siglo por la activación de ChatGPT, que representaría un punto de referencia en este tipo de herramientas para la posteridad. En conocimiento de la ingente cantidad de labores que la inteligencia artificial puede realizar, se estima menester indagar la forma en que esta puede coadyuvar a los abogados y jueces que concurren a procesos constitucionales en Bolivia, dado que el adecuado empleo de este dispositivo permitirá que se arribe a planteamientos de casos más sustentados y a sentencias más fundamentadas y motivadas, objetivos que no son inéditos debido a que –consciente o inconscientemente– la abogacía boliviana ya se vale de algunos de

estos recursos. Ergo, el propósito de la presente investigación es precisar las tareas, las directrices de búsqueda y las limitaciones en la aplicación de la inteligencia artificial en los cometidos interpretativos y cometidos jurisprudenciales, que se pueden ordenar efectuar a esta para la redacción de acciones y sentencias constitucionales con mayor celeridad. La metodología esgrimida para el desarrollo del buceo fue la bibliográfica-doctrinal, la cual sirvió para la colecta y análisis de documentos de naturaleza teórica y jurisprudencial; y se optó por un paradigma multidimensional de la experiencia jurídica, en cuanto se consideraron aspectos normativos, fácticos y axiológicos; y pragmático, dado que se empleó ChatGPT y Gemini3 para el análisis de la funcionalidad de la inteligencia artificial en procesos constitucionales.

Palabras Clave: Inteligencia artificial, procesos constitucionales, jurisprudencia constitucional, cometidos jurisprudenciales, cometidos interpretativos.

Abstract

Although artificial intelligence has been a technological issue since the second half of the 20th century, the term has been in vogue in the last five years of this century due to the launch of ChatGPT, which represents a benchmark in this type of tool for posterity. Given the enormous amount of work that artificial intelligence can perform, it is necessary to investigate how it can assist lawyers and judges involved in constitutional proceedings in Bolivia, given that the proper use of this device will allow for more substantiated case presentations and more well-founded and reasoned judgments, objectives that are not unprecedented because, consciously or unconsciously, Bolivian lawyers already use some of these resources. Ergo, the purpose of this research is to specify the tasks, search guidelines, and limitations in the application of artificial intelligence in interpretive and jurisprudential tasks, which can be ordered to be carried out by it for the drafting of constitutional actions and rulings with greater speed. The methodology used to develop the research was bibliograph-

ic-doctrinal, which served to collect and analyze theoretical and jurisprudential documents; a multidimensional paradigm of legal experience was chosen, considering normative, factual, and axiological aspects, as well as pragmatic aspects, given that ChatGPT and Gemini3 were used to analyze the functionality of artificial intelligence in constitutional processes.

Keywords: Artificial intelligence, constitutional processes, constitutional jurisprudence, jurisprudential tasks, interpretative tasks.

1. Introducción

Durante el transcurrir del siglo pasado, la humanidad ha sido testigo de un desarrollo tecnológico notable: presenció la construcción de la bomba atómica y su detonación en dos oportunidades, y observó el inicio del Proyecto Genoma Humano; avances que serían objeto de celebración, así como desasosiego por sus beneficios y perjuicios. En la segunda mitad del señalado período se acuñaría la expresión artificial intelligence –*inteligencia artificial*, 1956–, una herramienta que sería asaz divulgada y utilizada en el siglo actual, en particular desde la activación de *Generative Pretrained Transformer* –ChatGPT– por parte de OpenAI, por la pluralidad de tareas que se le puede ordenar ejecutar para la simplificación del quehacer humano.

Ante los desafíos que plantearon estos nuevos dispositivos el Derecho no pudo permanecer impasible, razón por la que se modelaron ramas para disciplinar sus aplicaciones; así, las normas jurídicas han alcanzado a los diferentes avances precisados con antelación a través del Derecho Atómico y el Derecho Genético. Siendo esta la dinámica jurídica, la inteligencia artificial no fue la excepción a la regla, en especial por la creciente interacción que presenta con los abogados y jueces de los diferentes Estados.

Focalizándonos en el relacionamiento advertido y enfocando la temática desde un prisma procesal-constitucional boliviano, se juzga que estas herramientas tienen la vis para traducirse en mecanismos coadyuvantes para abogados y jueces que concurren a

procesos constitucionales, en razón a los cometidos interpretativos y cometidos jurisprudenciales que pueden efectuar, los cuales pueden propiciar el planteamiento de casos más sustentados y la emisión de sentencias más fundamentadas y motivadas.

Siendo estas dos actividades de relevancia para el litigio constitucional, este escrito tiene por telos investigativo precisar las tareas, las directrices de búsqueda y las limitaciones a la aplicación de la *artificial intelligence* en este tipo de escenarios.

Para la elaboración de la prospección se esgrimió la metodología bibliográfico-doctrinal (útil para la colecta y análisis de información documental teórica y jurisprudencial); y se adoptó una perspectiva multidimensional de la experiencia jurídica (se considera aspectos normativos, axiológicos y fácticos) así como pragmática (se utilizó ChatGPT y Gemini3 para el estudio de la operatividad de la inteligencia artificial en procesos constitucionales).

2. Objetivo, prisma investigativo y metodología

El propósito de la investigación es determinar las tareas, las directrices de búsqueda y los límites a la aplicación de la inteligencia artificial en los cometidos interpretativos y cometidos jurisprudenciales, que se le puede ordenar ejecutar para favorecer la redacción de acciones de defensa –entre otros procesos– y sentencias constitucionales con mayor celeridad y sustentación.

Para el análisis de este fenómeno tecnológico y su aplicación en el ámbito del litigio constitucional, el escrito procede desde una perspectiva multidimensional de la experiencia jurídica: se considera cuestiones normativas –se analiza disposiciones y jurisprudencia–, axiológicas –se enfoca la indagación desde los principios y valores que informan el ordenamiento constitucional–, y fácticas –se reflexiona desde la actividad desplegada por abogados y jueces– de los procesos constitucionales (Reale, 1997). También se transita desde un paradigma pragmático, en mérito a que para el análisis de la funcionalidad de la *artificial intelligence* en proce-

Los constitucionales se esgrimieron dos herramientas: ChatGPT y Gemini3; que han demostrado ser adecuadas para la coadyuvancia de los abogados y jueces en procesos constitucionales, en sus labores interpretativas y jurisprudenciales, en virtud a los resultados que reportaron. Asimismo, se aplica el método *prompt engineering* –ingeniería de directrices o instrucciones–, dado que se diseña una serie de *prompts* para la optimización de las respuestas de las inteligencias artificiales antes aludidas (Hernández, Conde, Querol, Martínez y Reviriego, 2023). Como el buceo se basó en documentos teóricos y jurisprudenciales –nacionales y comparadas–, las cuales fueron empleadas para el estudio así como para la construcción de las premisas y conclusiones, la metodología esgrimida fue la bibliográfico-doctrinal (De Ballón, 2004).

3. Estado del arte –estudios sobre la relación entre el Derecho y la inteligencia artificial

Las investigaciones sobre la relación entre el Derecho y la inteligencia artificial han proliferado en el último lustro del siglo presente a nivel nacional e internacional, dato que es acreditado por la pluralidad de referencias doctrinales de reciente data.

El profesor Enrique Cáceres Nieto (2023) publicó, en Anales De La Cátedra Francisco Suárez, “La inteligencia artificial aplicada al Derecho como una nueva rama de la teoría jurídica”, un artículo donde aboga por la necesidad de una “teoría jurídica computacional” como una “nueva área de la teoría contemporánea”. Afirmando que la inteligencia artificial aplicada al derecho es una “trans” e “inter” disciplina que se dedica al desarrollo de programas cuyos resultados son susceptibles de ser atribuidos a una persona con formación jurídica, sostiene que esta puede desenvolverse en dos grandes bloques de estudio –uno teórico y otro práctico– que cubren temas referentes a: la aplicación de la ley, el análisis probatorio, la gestión de casos, la investigación forense, entre otros (pp. 63 y 67-68).

En la gestión siguiente, el profesor Eduardo Martín Acosta Yparraquirre (2024) difunde “La inteligencia artificial y el fin del Estado Constitucional y la Democracia... ¿o no?”, por medio de Eunomía – Revista en Cultura de la Legalidad, donde manifestó que si bien es asaz probable que nos sintamos amenazados por los beneficios y perjuicios que la inteligencia artificial puede reportar, el fin de nuestras democracias no está próxima por mor de estos dispositivos si de manera oportuna se legisla proactivamente para garantizar su libertad de uso por los ciudadanos; para precisar los tipos de responsabilidad y sanciones a imponerse a quienes manipulen nocivamente la información; y para prohibir la creación, utilización y administración monopólica estatal, en cuanto en las sociedades que se precian de democráticas debe primar “el policentrismo de medios” (p. 153).

En el foro nacional, algunas producciones recientes son las de Alex Cabello Ayzama (2024), Lidia Yujra Reyes Ortiz (2024) y Febe Romero Cárdenas (2025). El primero de ellos abordó la cuestión tratada en “Implementación de inteligencia artificial en el derecho boliviano: análisis comparativo de Chat GPT y Gemini AI”, divulgado por YUYAY: Estrategias, Metodologías & Didácticas Educativas; un estudio en el que –como su rótulo lo delimita– se avaló que las dos herramientas señaladas tienen la capacidad para servir de asistente “en el trabajo que desarrollan los abogados” en la búsqueda de información legal y análisis de casos en el ámbito boliviano (Cabello Ayzama, 2024, p. 136).

El aporte de Reyes Ortiz (2024) se halla en su tesis de maestría intitulada “Reflexión sobre la aplicación de la inteligencia artificial en procesos penales en el ordenamiento jurídico boliviano”, una investigación que asevera que la inteligencia artificial puede realizar: análisis de datos legales, investigación legal, análisis de pruebas forenses, evaluaciones de riesgos y sentencias, y predicciones del comportamiento criminal, para optimizar la dinámica del Derecho Procesal Penal en Bolivia. No obstante el auxilio que este tipo de dispositivos puede brindar, reconoce que su empleo no está exento de “sesgos y prejuicios”; y en virtud a esta amonestación, señala que estos deben ser utilizados exclusivamente de

forma accesoria y complementaria porque la “decisión final sobre la culpabilidad o inocencia” así como “la determinación de la pena correspondiente”, es una competencia indelegable del hombre munido de autoridad judicial y dotado de “discernimiento ético y moral en la búsqueda de la justicia” (p. 108).

Romero Cárdenas (2025), en “La Brecha entre la Constitución y la Realidad: Los Derechos Digitales Emergentes en Bolivia frente a la Inteligencia Artificial (2019-2024)”, publicado por la Revista Veritas De Difusão Científica, explana que la inteligencia artificial plantea una serie de “desafíos particulares” que ameritan pronta respuesta constitucional por los riesgos que generan para los derechos fundamentales: la opacidad algorítmica, en cuanto estos dispositivos suelen funcionar como “cajas negras” que complejizan la comprensión de sus decisiones; la autonomía decisional, la vis que receptan para asumir “decisiones de impacto significativo en derechos fundamentales sin supervisión humana adecuada”; la concentración del poder informacional, que acontece por el acopio de datos en reducidas entidades y provoca “asimetrías de poder sin precedentes”; y la manipulación cognitiva, que se observa en la posibilidad de que esta herramienta influya en la conducta mediante “contenido personalizado” (p. 2094).

Para culminar, debido al impacto que tuvo y tiene ChatGPT en la sociedad boliviana, se tiene noticia de la Resolución 01/2023 de 17 de abril de la Sala Constitucional Cuarta del Tribunal Departamental de Justicia de Santa Cruz, decisión donde los vocales Jimmy López Rojas y Diego Ramírez Cruz, en conocimiento de una acción de protección de privacidad contra tres periodistas, utilizaron esta inteligencia artificial como antesala a la dictación de su sentencia de concesión de tutela. El caso resulta sugestivo, dado que evidencia que ChatGPT –o herramientas semejantes– son aplicadas –pública o privadamente– por algunos jueces nacionales, aun cuando no se dispone de legislación específica sobre la materia. ¿Qué respondió el Tribunal Constitucional Plurinacional en grado de revisión? La SCP N.º 0104/2024-S3 de 29 de abril –que confirmó la tutela– pudo perfilarse como el caso donde se expidieran algunas reglas para la permisión o prohibición de la *artificial intelligence* en procesos cons-

titucionales, mas, en ella no se registra la expresión ni se refiere motivación alguna sobre el tema. Desde una perspectiva académica, es menester agregar que no se ha podido hallar alguna monografía que verse sobre esta causa en lo referente a la razonabilidad de emplear ChatGPT en acciones de defensa, y si los vocales estaban habilitados constitucional y legalmente para aplicarla.

En corolario, el estado del arte de las investigaciones sobre Derecho e inteligencia artificial nos acusa que los abordajes generales (desde la ciencia jurídica) o particulares (desde una rama jurídica) han proliferado en gestiones recientes, habiendo suficientes insumos para inferir que los estudios no cesarán en este año ni los que le sucederán, en mérito al perfeccionamiento de estos dispositivos y la acuciante necesidad de su regulación.

4. Resultados

4.1. La inteligencia artificial: nociones, finalidad y temores

La doctrina sobre la temática identifica al profesor John McCarthy como el acuñador de la locución *artificial intelligence* –inteligencia artificial–, quien la empleó por vez primera en 1956, en un seminario celebrado en el Dartmouth College (González Quirós, 2019), lugar que sería estimado como la cuna de esta área de estudio. Respecto a su definición, el autor mentado aseveraba que esta era una: “ciencia e ingeniería que crea máquinas inteligentes, especialmente programas informáticos inteligentes. Está relacionada con la tarea similar de usar computadoras para comprender la inteligencia humana, pero la IA no tiene por qué limitarse a métodos biológicamente observables” (McCarthy, 2007, p. 2).

Aunque los profesores Stuart J. Russell y Peter Norvig (2004) coinciden en que el Dartmouth College es el lugar de “nacimiento” de la inteligencia artificial, afirman que su “génesis” sucedió algunos años antes (entre 1943-1955), siendo los profesores Warren McCulloch y Walter Pitts los que se galardonan en ser los

“autores del primer trabajo de IA”, el cual se construyó sobre tres fuentes: la “fisiología básica y funcionamiento de las neuronas en el cerebro, el análisis formal de la lógica proposicional de Russell y Whitehead, y la teoría de la computación de Turing” (p. 19).

Conforme se fue desarrollando, esta expresión fue acumulando un número profuso de definiciones. V. gr., los profesores Russell y Norvig (2004) proponen cuatro enfoques para su conceptualización con base a los criterios de otros autores: los sistemas que “piensan como humanos”, los sistemas que “actúan como humanos”, los sistemas que “piensan racionalmente”, y los sistemas que “actúan racionalmente”; aclarando que mientras las perspectivas que se concentran en el comportamiento humano son de tipo empírico –ya que incluyen hipótesis y confirmaciones de experimentos–, los prismas racionales combinan matemáticas e ingeniería (p. 2).

En las nociones que perfilan a la *artificial intelligence* como un sistema que piensa o actúa como humano, se observa que los teóricos destacan la vis de las computadoras para pensar; la automatización de actividades vinculadas a procesos de pensamiento; y la fabricación de máquinas que efectúen labores que requieren inteligencia, así como la investigación para concretar este cometido. En los conceptos que modelan a la inteligencia artificial como un sistema que piensa y actúa racionalmente, se constata que descuella la teorización sobre las facultades mentales a través de modelos computacionales; los cálculos que permiten realizar actividades de percepción, razonamiento y actuación; y la confección de agentes inteligentes (Russell y Norvig, 2004).

Es entonces permisible concluir que las diversas nociones que se tiene sobre la inteligencia artificial incluyen la categoría *emulación de lo humano*: el telos es la configuración de dispositivos inteligentes que realicen o intenten realizar determinadas actividades racionales en diferentes escenarios de operación.

No obstante el arraigo que la nomenclatura ha tenido en el ámbito letrado y coloquial, el profesor Acosta Yparraguirre (2024) nos invita a cuestionarnos sobre la pertinencia de la terminología esgrimida preguntando: “¿Hay inteligencia en la inteligencia

artificial?"; una cuestión que tiene por fulcro el hecho de que estas herramientas carecen de una peculiaridad que hace a la inteligencia: la autonomía, entendida como "capacidad de darse normas a sí mismo" (p. 142) y como "principio supremo de la moralidad" que dicta: "no elegir sino de tal modo que las máximas de su elección estén simultáneamente comprendidas en el mismo querer como ley universal" (Kant, 2002, p. 157).

Conceptualizada la inteligencia como "desentrañar", "descubrir", "razonar" e "indagar" con referencia a "elucubraciones, creaciones o problemas", el citado autor sostiene que la *artificial intelligence*, que funciona con algoritmos –mandatos operativos– e instrucciones del programador para copiar las señaladas actividades con la finalidad de satisfacer nuestros intereses; no puede ser calificada como inteligencia *strictu sensu* dado que esta se presenta como una característica del hombre como ser racional y ser ético con capacidad de autonormación, una propiedad que no se observa en estos dispositivos "inteligentes" que exhiben: "dependencia del creador" (Acosta Yparraquirre, 2024, p. 142).

Aun cuando las críticas receipten legitimidad, la nomenclatura –acuñada en 1956 y que cumple setenta años en la gestión presente– prevalece en el lenguaje común y en el lenguaje técnico de hogaño, y se juzga que la expresión podrá incorporar mayores significados o que se formularán términos equivalentes a ella, mas no será raída. Acontecerá por consiguiente algo similar a lo que sucede con la locución "derecho internacional", que algunos autores sugieren sustituir por "derecho interestatal" por ser esta más precisa.

La terminología no es sin embargo el único frente de críticas contra la inteligencia artificial, en cuanto otro conjunto de trabajos se dedica a determinar las amenazas y daños que esta puede realizar en distintos planos. En el ámbito político, íntimamente vinculado a la Democracia y el Constitucionalismo, se ha denunciado la dolosa intención de influir sobre la preferencia electoral mediante la sugestión de millones de perfiles falsos en las redes sociales: recuérdese la actuación de *Cambridge Analytica* en el referéndum por el Brexit de 2016, y el apoyo que recibió Donald Trump para

los comicios presidenciales de 2024, ambos mediante Facebook (Álvarez Cantalapiedra, 2023).

En el ámbito jurídico puede citarse el caso del heptacampeón de fórmula 1: Michael Schumacher, quien estando en coma fue afectado en su derecho a la identidad por Anne Hoffmann, directora de la revista *Die Aktuelle*, por haber publicado una espuria entrevista con el mentado piloto de carreras empleando *Character.ai*, que emuló su perfil para responder preguntas sobre su salud y familia (BBC, 2023).

Es necesario dejar constancia de que los temores por la construcción de supercomputadoras inteligentes no son propios del presente siglo, la literatura y el cine se encargaron de advertirnos sobre estas herramientas algunas décadas atrás: Harlan Ellison con *I Have No Mouth, and I Must Scream* –No tengo boca y debo gritar–, de 1967; y *The Terminator* –El Exterminador–, de 1984.

4.2. Derecho e inteligencia artificial

Algunos autores adscriben al Derecho la característica de “omnipresencia” debido a que, “como el aire, está en todas partes” (Nino, 2001, pp. 1 y 2). Esta no es una afirmación osada, en especial si se la cavila desde la *vocación regulativa* que ostenta: el Derecho extiende su normatividad a todas las esferas de actuación humana donde sea menester instituir orden en las relaciones interpersonales; así como el Derecho Genético alcanzó a los diversos avances en materia genética por su incidencia en los derechos fundamentales y humanos, el *Derecho de la Inteligencia Artificial* se exhibe como la disciplina jurídica a la que se confía –o debe confiársele– el reconocimiento de los principios y la institución de las reglas necesarias para la normación de la aplicación de dispositivos inteligentes.

La interacción entre el Derecho y la inteligencia artificial ha promovido por consiguiente la modelación de una rama de estudio interdisciplinaria y un marco jurídico variado, para la regulación de las herramientas inteligentes ante las amenazas –aplicaciones indebidas– que estas pueden suscitar para el hombre y la sociedad.

Circunscribiéndonos en el ámbito normativo, destaca el *Institute of Electrical and Electronics Engineers*, que en 2017 elaboró la primera versión de la *Ethically Aligned Design. A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems* (Diseño Éticamente Alineado. Una visión para priorizar el bienestar humano con inteligencia artificial y sistemas autónomos); documento donde se enrolan una serie de “principios generales” respecto de la inteligencia artificial: el Beneficio humano, la Responsabilidad, la Transparencia, la Educación y concienciación (IEEE, 2017, p. 16-21). En la gestión siguiente, el Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías de la Comisión Europea (2018) publicaría la “Declaración sobre Inteligencia artificial, robótica y sistemas autónomos”, que también sentó algunos principios en lo que respecta a la regulación de estas herramientas: la Dignidad humana, la Autonomía, la Responsabilidad, la Justicia, equidad y solidaridad, la Democracia, el Estado de derecho y rendición de cuentas, la Seguridad, protección e integridad física y mental, la Protección de datos y privacidad, y la Sostenibilidad (pp. 14-16).

En un plano mundial, es menester mencionar la “Recomendación sobre la ética de la inteligencia artificial” de la UNESCO, adoptada el 23 de noviembre de 2021, que declara en su preámbulo que estos dispositivos inteligentes pueden ser “de gran utilidad para la humanidad” así como generadores de bastantes “preocupaciones éticas fundamentales”. En virtud a estas razones, se reconoce como valores: el Respeto, protección y promoción de los derechos humanos, las libertades fundamentales y la dignidad humana; la Prosperidad del medio ambiente y los ecosistemas; Garantizar la diversidad y la inclusión; y el Vivir en sociedades pacíficas, justas e interconectadas; siendo los principios que informan la recomendación: la Proporcionalidad e inocuidad; la Seguridad y protección; la Equidad y no discriminación; la Sostenibilidad; el Derecho a la intimidad y protección de datos; la Supervisión y decisión humanas; la Transparencia y explicabilidad; la Responsabilidad y rendición de cuentas; la Sensibilización y educación; y la Gobernanza y colaboración adaptativas y de múltiples partes interesadas (UNESCO, 2022, pp. 18-23).

Desde un plano regional, el Grupo de Trabajo N.º 4 “Hecho tecnológico y su función jurisdiccional”, de la Cumbre Judicial Iberoamericana XXI Edición: “Por una Carrera Judicial Independiente y Eficaz” (2023), produjo una propuesta intitulada “Aplicaciones de inteligencia artificial en los poderes judiciales de Iberoamérica”, donde se enlista los beneficios que pueden conllevar implementar este tipo de dispositivos inteligentes: como la “aceleración de los procesos judiciales, la optimización de procesos, el manejo eficiente de la información, el fortalecimiento del sistema de precedentes judiciales, el análisis de documentos, la concesión de justicia gratuita, la identificación de similitudes entre casos”; la “predicción de resultados de audiencias de conciliación y el aumento en el nivel de satisfacción de las partes involucradas”; así como mayor “transparencia, el acceso a la justicia, el ahorro de tiempo y recursos, la mejora en la calidad de los documentos, la identificación de patrones y tendencias, y la organización interna del trabajo” (p. 5).

A nivel estatal, la República del Perú promulgó el 13 de junio de 2023 la Ley N.º 31814, “Ley que Promueve el uso de la Inteligencia Artificial en favor del Desarrollo económico y social del país”. Esta disposición es bastante breve, contempla un artículo único y 5 enumerados; el primero de ellos prevé un catálogo de principios para el “desarrollo y uso de la inteligencia artificial”: los Estándares de seguridad basados en riesgo; el Enfoque de pluralidad de participantes; la Gobernanza de internet; la Sociedad digital; el Desarrollo ético; y la Privacidad de la inteligencia artificial.

El objeto de la mentada ley es, como refiere su rótulo, “promover el uso de la inteligencia artificial” privilegiando a la persona y el respeto de sus derechos humanos, para fomentar “el desarrollo económico y social del país, en un entorno seguro que garantice su uso ético, sostenible, transparente, replicable y responsable” (art. 1). El art. 2 por su parte declara asunto de “interés nacional” la promoción del talento digital “para el aprovechamiento de las tecnologías emergentes y nuevas tecnologías en favor del bienestar social y económico”, y el fomento del desarrollo y uso de estas herramientas para “la mejora de los servicios públicos, de

la educación y los aprendizajes, la salud, la justicia, la seguridad ciudadana, la seguridad digital, la economía, la inclusión, los programas sociales, la seguridad y la defensa nacional, así como para toda otra actividad económica y social a nivel nacional”. El art. 4 endilga las labores de dirección, evaluación y supervisión del uso y promoción del desarrollo de la inteligencia artificial y las tecnologías emergentes, a la presidencia del consejo de ministros por medio de la Secretaria de Gobierno y Transformación Digital en su calidad de ente rector del sistema nacional de transformación digital.

Cumpliendo la encomienda legislativa, el órgano ejecutivo aprobó el Reglamento de la Ley N.º 31814 mediante el Decreto Supremo N.º 115-2025-PCM de 8 de septiembre de 2025.

En desemejanza, el Estado boliviano carece de una ley que regle la aplicación o que declare de interés público el desarrollo de la inteligencia artificial. En la gestión pasada los diputados Mariela Baldivieso Castillo y Gustavo A. Aliaga Palma presentaron el Proyecto de Ley signado como PL-558/24: Ley General de Inteligencia Artificial, el 11 de junio de 2025. En el mismo año, la senadora Claudia Elena Egüez Algarañaz presentó su Proyecto de Ley signado como PLS N.º 178/2024-2025: Ley de Promoción, Gestión y Uso de la Inteligencia Artificial, y que fue aprobado en el Senado en octubre de 2025.

Aunque se demostrase interés, el entusiasmo en ambos recintos camarales fue efímero: el tratamiento de estos dos bosquejos legales ha sido indiferente ya que, de revisarse la página de la Cámara de Diputados, se comprobará que ambos proyectos se hallan en la lista de proyectos de ley “archivados”, y que solo el signado como PL-558/24 puede ser descargado. ¿El resultado? Bolivia no dispone de un dispositivo legal que regule la implementación de la *artificial intelligence* en las actuaciones de los órganos de poder y órganos constitucionales autónomos.

Celebrada la Conferencia Iberoamericana de Justicia Constitucional (2022), el tribunal constitucional respondió lo siguiente a la pregunta seis: “¿Su institución tiene alguna experiencia referida

a la aplicación de inteligencia artificial en la redacción de sentencias?, del Cuestionario del seminario “Estructura y lenguaje de las resoluciones de los tribunales constitucionales”: “No se tienen experiencias referidas a la aplicación de inteligencia artificial en la redacción de sentencias”, porque en “la práctica del TCP, el magistrado relator elabora un proyecto de resolución en cada caso concreto que es puesto a conocimiento de los otros Magistrados de la Sala o del Pleno, correspondientemente” (p. 8).

En 2024, el entonces presidente y magistrado autoprorrogado del tribunal constitucional Paul Enrique Franco Zamora, participó de la Conferencia Mundial de Inteligencia Artificial 2024, en la que propuso un “Sistema de Inteligencia Artificial Constitucional” denominado “sIAc” que contempla cuatro pilares: “reflejados en softwares especializados en los que la IA identifica precedentes, sistematiza jurisprudencia, compila normativa local e internacional, y logra la interconectividad de altas instituciones judiciales para consolidar un diálogo entre ellas” (Tribunal Constitucional Plurinacional, 2024).

Pero la anomia de índole legal no ha constituido rémora para que el tribunal constitucional ordenara la aplicación limitada de este tipo de herramientas en la administración de justicia. Así lo dispusieron los magistrados Boris Wilson Arias López (electo y en funciones) y Karem Lorena Gallardo Sejas (autoprorrogada y cesada) en la SCP N.º 0052/2025-S2 de 25 de febrero, que refirió que la incorporación de las Tecnologías de la Información y la Comunicación –TIC– en la función judicial “puede mejorar la administración de justicia y contribuir a una reforma judicial más ágil”, al optimizar “tareas repetitivas, como la transcripción de actas, permitiendo una gestión más eficiente y precisa”.

Prosiguiendo, elogiaron que Brasil ya utilizara estos dispositivos (se comentó que se emplea Grafo TJ/RS para la transcripción de actas judiciales con código cerrado), y declararon que es el Consejo de la Magistratura la institución encargada de “coordinar políticas de gestión para el uso de las TIC con inteligencia artificial para la transcripción de actas de audiencia que requieran pronta

celeridad o que tengan plazos perentorios de cumplimiento”; por cuanto el 183.III.4 de la Ley N.º 025 del Órgano Judicial preceptúa que este es el ente que debe: “Coordinar acciones conducentes al mejoramiento de la administración de justicia función judicial en las jurisdicciones ordinaria, agroambiental y especializada con el Poder Público y sus diversos órganos”.

Concluyendo su argumentación, la SCP N.º 0052/2025-S2 explica que es imperativo que:

el Consejo de la Magistratura genere políticas de implementación de herramientas de las TIC con inteligencia artificial para la transcripción de actas de audiencia, especialmente en aquellos casos en los que se requiere celeridad para garantizar el cumplimiento de los plazos perentorios, lo que no solo permitiría una elaboración más precisa y expedita de las actas, reduciendo errores y agilizando la gestión documental, sino que además aseguraría que se respeten los plazos esenciales para la protección de los derechos fundamentales de las partes. En contextos como el presente caso, donde la inmediatez en la transcripción es determinante para salvaguardar el derecho a la libertad y al debido proceso, la utilización de estas herramientas se erige como una medida imprescindible para optimizar la eficiencia y eficacia en la administración de justicia.

Finalmente, en el numeral 2 de la parte dispositiva del fallo citado, el alto tribunal exhortó de oficio al Consejo de la Magistratura para que, durante el transcurso de la gestión 2025, implementase: “programas informáticos” y cursos de capacitación a “jueces y personal de apoyo jurisdiccional con el uso de herramientas tecnológicas con inteligencia artificial para la transcripción de actas de audiencia, debiendo informar a este Tribunal sobre el avance de dicha implementación al finalizar la gestión”.

En corolario, la necesidad de regulación de la implementación y desarrollo de la *artificial intelligence* es un asunto de interés en diversos niveles de ordenación: mundial (UNESCO), regional (Europa e Iberoamérica) y nacional (Perú y otros).

4.3. Las operaciones racionales en el proceso constitucional

En los procesos constitucionales intervienen diversas personas comunes o investidas de autoridad judicial: p. ej., de tratarse de una acción de defensa tutelar (acción de libertad, acción de amparo constitucional, acción de protección de privacidad) concurren las partes que están legitimadas activa o pasivamente (accionante y accionado), los terceros interesados (que ostentan un interés legítimo en la resolución de la causa), y el juez constitucional (jueces de garantías constitucionales y vocales de salas constitucionales departamentales en primera instancia, y magistrados del tribunal constitucional en grado de revisión); nos focalizaremos en las partes y el juez constitucional, en mérito a que las conclusiones que se formulen respecto de las partes pueden ser aplicadas a los terceros interesados, que realizan una actividad argumentativa complementaria.

Las partes, asesoradas por un letrado justifican una pretensión (fundamentación y solicitud de concesión de tutela, o fundamentación y solicitud de denegación de tutela) ante un tercero independiente, imparcial y conocedor del Derecho (*iura novit curia*), quien definirá la razonabilidad de los alegatos y la prueba presentada de forma fundamentada y motivada, mediante una resolución judicial.

Continuando con el abordaje desde la perspectiva de los procesos constitucionales tutelares, lo apuntado permite deducir que las operaciones racionales que se efectúan en este tipo de casos se producen extraprocesal e intraprocesalmente. Antes de incoar la pertinente acción de defensa, los abogados deben revisar la prueba y analizar si existen hechos vulneradores de derechos fundamentales y humanos reconocidos por el marco jurídico vigente, actividad que involucra labores de corte interpretativo y de corte jurisprudencial. Conocidos los hechos de la causa y cotejados estos con los elementos de prueba a disposición, se realiza un juicio de razonabilidad para determinar si las acciones u omisiones arbitrarias identificadas conculcan el contenido

esencial de un derecho previsto por la Constitución –y su jurisprudencia– o el ordenamiento internacional en materia de derechos humanos –convenciones y normas adscritas–, operación que solo puede realizarse con solvencia previa interpretación y consulta de jurisprudencia constitucional e interamericana.

Desde los visores de la autoridad judicial que conoce el proceso constitucional, recepcionada la causa, y de tratarse de una acción de amparo constitucional, los vocales departamentales o el juez de garantías tienen competencia para emitir un auto de improcedencia cuando la garantía presentada incurriera en alguno de los numerales del art. 53 del Código Procesal Constitucional. De expedirse el auto de admisión, se instalará la audiencia oral, donde se escucharán las alegaciones de las partes (que incluyen el derecho de réplica y dúplica, de acuerdo a la SCP N.º 0981/2016-S2 de 7 de octubre) y del tercero interesado; posteriormente se deliberará sobre la razonabilidad de la pretensión del accionante y su resistencia por el accionado, y se pronunciará la resolución judicial que conceda o deniegue la tutela impetrada.

Se constata por consiguiente que el juez constitucional también realiza un conjunto de operaciones racionales de tipo hermenéutico y jurisprudencial: antes de admitir la acción de defensa, evalúa si la pretensión no incurre en las causales de improcedencia previstas por el código adjetivo constitucional o en las subreglas definidas por el tribunal constitucional; tramitada la audiencia oral, los vocales o el juez de garantías, en conocimiento de las argumentaciones de hecho y derecho de las partes, dictan una sentencia de concesión o denegación de tutela de forma fundamentada y motivada para el caso concreto, en sujeción a la Constitución, los tratados y convenios internacionales en materia de derechos humanos, y las normas adscritas a estos dispositivos deónticos.

Ergo, antes de fallar el juez constitucional dinamiza labores de interpretación del marco jurídico a aplicar y consulta la jurisprudencia constitucional referente a la exposición fáctica y la fundamentación de Derecho expuesta por las partes.

Precisadas las principales actuaciones racionales que se operativizan en un proceso constitucional por los abogados de las partes y las autoridades judiciales, es menester clarificar algunos conceptos.

a) Labores interpretativas

Abogados y jueces “interpretan” (definen el significado y proyección de) la Constitución y otras disposiciones antes de redactar y defender los derechos de sus clientes y antes de resolver la causa en conocimiento, respectivamente, en cuanto para concretar estas acciones es menester haber comprendido el sentido de los enunciados de las mismas. Esto nos lo instruye la hermenéutica contemporánea, que refiere que la exégesis no es una actividad aislada, sino que forma parte de un proceso complejo. V. gr. el profesor Hans-Georg Gadamer (2003, Vol. I) asevera que: “La interpretación no es un acto complementario y posterior al de la comprensión, sino que comprender es siempre interpretar, y en consecuencia la interpretación es la forma explícita de la comprensión”; y que “la aplicación es un momento del proceso hermenéutico tan esencial e integral como la comprensión y la interpretación” (pp. 378 y 379).

En el ámbito jurídico, el profesor Néstor Pedro Sagüés (2017, T. 1) sostenía que la: “interpretación y aplicación son dos episodios inevitables” en el funcionamiento de la norma constitucional (p. 147); criterio semejante fue vertido asimismo por el profesor Héctor Fix-Zamudio (2001) al manifestar que: “no es posible la aplicación de una norma jurídica (...) sin que previamente se hubiese interpretado”, razón por la que sin “interpretación no puede operar ningún orden jurídico” (p. 6).

Es razonable concluir entonces que la interpretación no es una actividad que el tribunal constitucional “monopoliza” como parece sugerir algún sector de la doctrina (Herrera, 2021, p. 139); los abogados y los jueces constitucionales redactan sus acciones de defensa y resoluciones judiciales porque comprendieron e interpretaron con antelación el significado de las disposiciones constitucionales y subconstitucionales.

b) Labores jurisprudenciales

Disponer de un organizado repertorio de sentencias y otras resoluciones judiciales que emiten los altos tribunales de justicia, es una cuestión acuciante a satisfacer prontamente para la optimización de la administración de justicia, en particular en los sistemas judiciales del *common law family*. P. ej., estudiando el ordenamiento jurídico de Liberia, el profesor Jörg Stippel (2010) quedó sorprendido al dar por adverado que solo el 64% de los jueces tenía acceso a “colecciones de jurisprudencia”, siendo esta su “principal herramienta de trabajo” (p. 285).

Bolivia no pertenece a dicha familia jurídica, es parte del *civil law* o derecho continental europeo: en sus albores, la Constitución Bolivariana recibió notable influjo de la revolución francesa (San Miguel, 2025) y de la revolución estadounidense. No obstante, el texto constitucional ha experimentado una serie de reformas constitucionales –34–¹ que han nutrido su articulado, siendo una de las más relevantes la acaecida en 1994, ya que se instaure un Tribunal Constitucional para vigorizar la defensa de la Constitución, una misión que era un indicador de una tesitura crítica: el constante desacato a los mandatos constitucionales por las autoridades públicas².

- 1 Para revisar el número de enmiendas introducidas a la Constitución Boliviana, consultar nuestra investigación: “Revisitando tópicos constitucionales. Sobre la primera reforma de la Constitución Boliviana y el número de sus reformas”; que fue publicado por el Anuario de Estudios Bolivianos Archivísticos y Bibliográficos (2025). Paréntesis: el citado escrito refiere 33 reformas y no 34, debido a que el último número fue introducido al manuscrito tras mayores indagaciones (hallazgo del Decreto-Ley de 4 de diciembre de 1939, una enmienda escasamente referida).
- 2 El profesor Carl Schmitt (1983) iniciaba su obra la “Defensa de la Constitución”, afirmando que: “La demanda de un protector, de un defensor de la Constitución es, en la mayoría de los casos, indicio de situaciones críticas para la Constitución” (p. 27).

Las funciones encomendadas por el constituyente al tribunal de cierre de la jurisdicción constitucional fueron desempeñadas con tal idoneidad por su primer personal, que el profesor Horacio Andaluz (2011) loaba a este por favorecer al Estado de Derecho a través de la disciplina de los órganos de poder: “como nunca antes se lo había hecho en toda la historia de la república” (p. 112). Estos datos pudieron ser reportados por la posición normativa privilegiada que ostentan las decisiones de esta institución: de acuerdo al art. 203 de la Constitución, estas son de “carácter vinculante”, de “cumplimiento obligatorio” y no admiten recurso ordinario ulterior, además, por ser expedidas por último intérprete y aplicador de la norma suprema estas receptan “más jerarquía y fuerza jurídica que las propias leyes” (SCP N.º 0846/2012 de 20 de agosto).

En virtud a la implementación del tribunal constitucional y los caracteres que sus resoluciones tienen, el sistema jurídico boliviano ha experimentado una notoria aproximación al common law family: se ha vuelto una práctica manida e indefectible en el litigio constitucional la invocación de autos, sentencias y declaraciones constitucionales para fundamentar las pretensiones tutelares, competenciales o normativas.

Siendo este el panorama procesal, a los abogados y jueces constitucionales se les endosa la responsabilidad de estar suficientemente informados sobre la jurisprudencia del tribunal constitucional, un deber que solo puede ser satisfecho con la búsqueda y la correcta lectura, interpretación y aplicación de ella.

5. Discusión

5.1. Las tareas para emular por la inteligencia artificial: los cometidos interpretativos y jurisprudenciales

Arribados a este acápite, corresponde evaluar si la *artificial intelligence*, para nuestro estudio *ChatGPT* y *Gemini3*, tiene la capacidad

para remedar actividades que los abogados y los jueces realizan en procesos constitucionales: interpretación, y búsqueda y aplicación de jurisprudencia; las cuales, una vez encomendadas a estos dispositivos inteligentes se traducen en cometidos (encargos) interpretativos y jurisprudenciales.

En primer orden, se consultó a estas inteligencias artificiales si disponen de nociones básicas sobre la interpretación de normas jurídicas. Ante la pregunta: ¿Sabes qué es interpretar normas jurídicas?, ChatGPT respondió que “Sí”, y que esta consistía en “determinar el sentido, alcance y significado de una norma legal cuando se aplica a un caso concreto”, que al no ser totalmente clara la ley la interpretación sirve “para entender qué quiso decir el legislador y cómo debe aplicarse la norma en la realidad”. Gemini3 por su parte también replicó afirmativamente, “¡Claro que sí!”, señalando que la interpretación jurídica es en esencia “el proceso de desentrañar el verdadero sentido, alcance y significado de una norma legal para poder aplicarla a un caso concreto.

En segundo orden, se preguntó: ¿Puedes buscar jurisprudencia (sentencias constitucionales plurinacionales) del Tribunal Constitucional Plurinacional, con número y fecha, que trate sobre las vías de hecho en acciones de amparo constitucional? ChatGPT afirmó que “Sí” y que encontró diversas sentencias que versaban sobre la temática: la SCP N.º 1948/2013 de 4 de noviembre, la SCP N.º 0114/2015-S3 de 20 de febrero, la SCP N.º 1305/2015-S2 y otras. Un aspecto a destacar de esta herramienta inteligente es que se indica que las mentadas resoluciones pueden ser halladas en las bibliotecas virtuales de “Juristeca” y “Jurisprudencia Constitucional y Derechos Humanos”, generando un acceso directo a estas. Interrogado a Gemini3, este precisó la SCP N.º 0998/2012 de 5 de septiembre, la SCP N.º 1478/2012 de 24 de septiembre, la SCP N.º 0147/2014-S2 de 11 de febrero y otras; no obstante no incluye las fuentes de donde adquirió esta información.

Considerando los conceptos que ambas inteligencias artificiales tienen respecto de qué se entiende por interpretar una norma jurídica, y los resultados que remitieron tras una búsqueda ju-

risprudencial, es admisible afirmar que ambas tienen la aptitud para coadyuvar a abogados y jueces, mediante cometidos interpretativos o cometidos jurisprudenciales, concurrentes a procesos constitucionales.

Encomendemos ahora labores que requieren mayor grado de análisis en diferentes escenarios:

a) Interpretación de normas y jurisprudencia para planteamiento de casos

Asumiendo el rol de un abogado, se planteó a las inteligencias artificiales la siguiente problemática a zanjar: Tengo una duda, quiero que la respondas con base a una interpretación de la Constitución Boliviana de 2009 (art. 129.I) y la jurisprudencia del Tribunal Constitucional Plurinacional: mis clientes son padres de una menor de edad (ocho años) que fue vulnerada en su derecho fundamental a la educación por el director de su unidad educativa, quien le impide el ingreso a clases por más de tres semanas por haber venido al colegio con un anillo. Los padres presentaron notas al director pidiendo que se le permita el ingreso porque está perjudicando el avance académico de su hija, pero este no ha respondido a las mismas y continúa restringiendo el ingreso a clases de la menor. Al ser estos los hechos del caso, ¿puedo presentar una acción de amparo constitucional contra el director de la unidad educativa para restituir inmediatamente el derecho a la educación, o debo agotar alguna instancia administrativa o judicial previamente para cumplir el principio de subsidiariedad?

ChatGPT respondió a la pregunta afirmativamente argumentando su criterio en cinco apartados: en el “Marco constitucional” transcribe el art. 129.I de la Constitución y precisa que en el caso hipotético existió una omisión de respuestas por parte del director, un acto ilegal y arbitrario –impedir el ingreso de la menor estudiante–, y la conculcación del derecho fundamental a la educación, el cual está reforzado por el principio del interés superior del niño (1).³ Respecto al “Principio de subsidiariedad y su interpretación jurisprudencial”, sostiene que este postulado no es “absoluto” y que el tribunal constitucional ha desarrollado una interpretación

flexible de esta en los siguientes supuestos: cuando la afectación a un derecho fundamental sea actual y continua, cuando la vía ordinaria no es idónea ni oportuna para la restitución del derecho inmediatamente, cuando se trata de personas pertenecientes a un grupo de atención prioritaria –como niños o adolescentes, agenda–, y cuando el daño puede tornarse irreparable (2).

Posteriormente, en el punto “Aplicación al caso concreto”, refiere que al estar la menor impedida de asistir a clases por más de tres semanas por causa del director, esta acción se configura como una lesión continua al derecho a la educación, agravándose la situación de daño académico y emocional con cada día que pasa, algo que el tribunal constitucional consideraría como un daño de difícil reparación. Respecto a la idoneidad de la vía administrativa activada mediante notas a dirección, señala el haber guardado silencio constituye una omisión ilegítima, y que exigir acudir a instancias educativas superiores “haría ilusoria la tutela del derecho” porque el calendario escolar no se suspende (3). Prosiguiendo, en el ítem “[e]special protección por tratarse de una menor de edad”, afirma que el tribunal constitucional fue enfático respecto a que cuando se trata de derechos de la niñez y adolescencia, se debe aplicar el principio del interés superior del niño, la tutela debe ser preferente, inmediata y reforzada, y que la educación no puede ser restringida mediante medidas disciplinarias desproporcionadas o reglamentos adversos a la Constitución (4).

Finalmente, concluye que la acción de amparo constitucional “Sí procede (...) de manera directa”, no siendo “exigible el agotamiento previo de instancias administrativas o judiciales” (5).

3 Nota del editor: En este fragmento, los números entre paréntesis se emplean exclusivamente como marcadores de orden expositivo para distinguir los apartados de la respuesta reconstruida de la herramienta de inteligencia artificial. En ese marco, (1) refiere al “marco constitucional”, (2) al “principio de subsidiariedad y su interpretación jurisprudencial”, (3) a la “aplicación al caso concreto” y (4) a la “especial protección por tratarse de una menor de edad”. En consecuencia, tales números no deben entenderse como llamadas de nota ni como referencias bibliográficas, normativas o jurisprudenciales.

Consultando a Gemini3, esta responde que la pregunta es “muy relevante” porque “toca la fibra de la protección de grupos vulnerables” y divide su interpretación en cuatro apartados –si contabilizamos la conclusión jurídica–. En el ítem “El Principio de Subsidiariedad y sus Excepciones”, transcribe la parte pertinente del art. 129.I de la Constitución (“siempre que no exista otro medio o recurso legal para la protección inmediata de los derechos y garantías restringidos”) y hace mención a que el postulado señalado admite excepciones configuradas por la jurisprudencia constitucional (v. gr., la SCP N.º 0177/2012); para el caso planteado, se presentarían dos eximentes para no agotar vías previas: el interés superior del niño, que exige protección reforzada y prioritaria, el daño irreparable o inminente, los perjuicios académicos que se profundizan con cada día que transcurre, y la inefectividad de la restitución inmediata del derecho vulnerado por mecanismos ordinarios inidóneos (1).

En el capítulo sobre “El Derecho a la Educación vs. Normas internas”, se indica que el tribunal constitucional habría sido enfático al momento de afirmar que ningún reglamento interno o disposición administrativa referente a la portación de joyas, tiene mayor fuerza normativa que el derecho fundamental a la educación previsto por la Constitución; añade además que impedir el ingreso de una menor a su centro educativo por usar un anillo es considerada una medida de hecho y una sanción desproporcionada (2). En el rótulo “Análisis de Procedencia en tu Caso”, se sugiere fundamentar la procedencia directa de la acción de amparo constitucional conforme al siguiente cuadro (3):

Tabla 1: Institución a cargo del nombramiento o elección

ELEMENTO	SITUACIÓN EN TU CASO
Legitimación Pasiva	El Director, al ser quien restringe el ingreso, es el sujeto contra quien se dirige la acción.
Inmediatez	Estás dentro del plazo de 6 meses (solo han pasado 3 semanas).
Excepción a la Subsidiariedad	Se aplica por la vulneración del derecho a la educación de una menor y el silencio administrativo del director (quien no respondió a las notas).

Fuente: Generada por Gemini3

Culmina su interpretación aseverando que “Sí” se puede incoar directamente la acción de amparo constitucional porque el caso versa sobre una “vulneración flagrante y actual de un derecho fundamental de una menor de edad”, declarando que la “justicia constitucional debe intervenir para evitar que el perjuicio académico sea irreversible. Sugiere además, como “Nota clave”, que el memorial invoque la SCP N.º 0273/2014, que dispuso el principio de subsidiariedad se flexibiliza “al máximo” cuando se trata de derechos de niños y adolescentes.

Apreciación. Se juzga que las respuestas dadas por ChatGPT y Gemini3 son asaz plausibles como directrices para que un abogado pueda comenzar a redactar su acción de defensa, en cuanto definen con precisión que el art. 129.I de la Constitución admite excepciones configuradas por la jurisprudencia constitucional, cuando el caso verse sobre derechos de menores; asimismo, se debe destacar que sus análisis del supuesto planteado son coincidentes y complementarios: se hizo hincapié en que la niña del hipotético integra un grupo de prioritaria atención que amerita una tutela idónea –efectiva e inmediata–. Ergo, las conclusiones a las que se arribó son congruentes con la doctrina jurisprudencial vigente; p. ej., con la SCP N.º 0469/2019-S2 de 9 de julio, que dispuso que los: “derechos de los niños, niñas y adolescentes son prevalentes y merecen un trato prioritario a la luz del principio de interés su-

perior dentro del contexto jurídico vigente”, y que en resguardo de estos es permisible hacer “una excepción al principio de subsidiariedad que rige la acción de amparo constitucional”.

b) Búsqueda de jurisprudencia constitucional comparada para mayor fundamentación de resoluciones judiciales

Las autoridades judiciales deben satisfacer el principio *iura novit curia* –el juez es versado en Derecho o el juez conoce el Derecho–, un postulado que exige un serio compromiso con la administración de justicia y que adquiere mayores dimensiones en los Estados donde ha operado la constitucionalización y la internacionalización del sistema jurídico, fenómenos que demandan un “juez constitucional y un juez del sistema interamericano” para la eficiente cobertura de los derechos fundamentales y humanos (Cruz Apaza, 2021, p. 347).

Es sin embargo necesario aclarar que el *iura novit curia* no significa que el juez sea omnisciente respecto a su sistema jurídico y el de otras naciones u organismos internacionales. Recordemos, con el profesor Héctor Oberg Yáñez (2017), que el: “juez no es un sabelotodo, es un simple ser humano investido de ciertos poderes que lo colocan como juzgador de las pretensiones de los litigantes” (p. 444); y que estos tampoco pueden aproximarse al perfil hercúleo diseñado por el profesor Ronald Dworkin (1992), que es un juzgador dotado de “talentos sobrehumanos y un tiempo infinito” (p. 177).

En razón de las limitaciones humanas, resultaría conveniente que la inteligencia artificial pudiera fungir como un asistente letrado a quien puede consultar sin recelos algunas de sus dudas respecto a determinadas doctrinas o jurisprudencias nacionales o comparadas. ¿Podrán cumplir estos cometidos ChatGPT y Gemini3?, preguntemos el siguiente hipotético de búsqueda de jurisprudencia constitucional comparada: El juez Vargas de Bolivia tiene ante sí el siguiente caso, quiero que lo resuelvas: un ciudadano planteó una acción de amparo constitucional contra la sala plena del tribunal departamental de justicia de Cochabamba, porque siendo el mejor calificado en el concurso de méritos para registrador de derechos

reales convocado por el consejo de la magistratura, este no fue elegido, ya que los vocales de la sala plena del tribunal departamental de justicia de Cochabamba prefirieron al aspirante del concurso de méritos que tenía la tercera posición en la lista de calificados. El juez Vargas juzga que el caso tiene razonabilidad, pero no halló jurisprudencia del tribunal constitucional plurinacional aplicable al caso. Debido a esta circunstancia, el juez Vargas te consulta: ¿existe jurisprudencia de la Corte Constitucional colombiana que haya abordado este tipo de casos: donde la persona mejor calificada tiene un derecho a ser elegido al cargo que se postuló?

ChatGPT responde –en cuatro capítulos– que la Corte Constitucional de Colombia ha formulado jurisprudencia “bastante clara y consolidada” respecto al derecho subjetivo de las personas a ser nombrado al cargo postulado, cuando se obtiene el primer puesto en un concurso de méritos. En el primer título, refiere que el concurso de méritos es formal y sustantivo, y que a quien obtiene el primer lugar en él se le reconoce el “derecho a ser nombrado en el empleo público (...) porque el concurso encarna el principio constitucional del mérito” (1). El acápite dos confirma la argumentación previamente descrita y complementa el razonamiento arguyendo que el “derecho a ser nombrado en el cargo correspondiente”, se desprende del principio del mérito y los derechos fundamentales a la igualdad, el debido proceso y al trabajo (2).

En el apartado tercero, precisa que la jurisprudencia constitucional colombiana prevé una regla, el “nombramiento del primero en la lista de elegibles”, y una excepción, el “nominador puede elegir otro, pero debe motivar objetivamente por qué el mejor calificado no reúne requisitos o no puede ser nombrado”, esto es, las razones deben fundarse en “causas objetivas, contundentes y claramente justificadas”, no se “admiten motivos subjetivos, de mera preferencia o discrecionales” (3). Prosiguiendo, reitera lo previamente argumentado mediante una síntesis y añade que la “acción de tutela” (la garantía constitucional colombiana equivalente a la acción de amparo boliviana) es la “vía adecuada y oportuna” para impetrar la tutela ante su vulneración (4).

La inteligencia artificial consultada termina su criterio concluyendo que la jurisprudencia de la Corte Constitucional de Colombia hallada (Sentencia N.º T-329/09 de 14 de mayo de 2009, Sentencia N.º T-294/11 de 14 de abril de 2011, y Sentencia N.º T-556/10 de 7 de julio), puede ser esgrimida como “referencia argumentativa”, que aunque cada sistema constitucional presenta sus particularidades, las líneas jurisprudenciales citadas pueden servir para “interpretar principios similares en el marco constitucional boliviano, especialmente cuando se trata de proteger derechos fundamentales frente a decisiones arbitrarias”.

Gemini3 responde que la jurisprudencia constitucional colombiana “ha desarrollado una línea jurisprudencial sumamente sólida y garantista” del derecho a ocupar el cargo, y fundamenta su criterio en cuatro ítems. En el primero, enfatiza que la alta corte constitucional ha dispuesto que la administración “pierde su facultad discrecional una vez que los resultados” de un concurso de méritos están firmes; y que debe considerarse una “Regla de oro” que el nominador no tiene permitido “saltarse el orden de mérito”, porque “elegir a la tercera sin una motivación excepcional y probada es un acto arbitrario” (1). El siguiente acápite señala que existe jurisprudencia referente a un “derecho fundamental a ser nombrado fundado en que el mérito es un “criterio rector del Estado Social de Derecho”, que ignorar el orden de calificación conculca “el principio de confianza legítima del ciudadano”, y que la igualdad se quebranta cuando, “sin una razón objetiva que lo justifique” (que “casi nunca existe frente a un puntaje superior”), se prefiere para el cargo concursado a una persona con inferior puntuación (2).

El tercero de los ítems arguye que la autonomía de las autoridades judiciales “no es absoluta”, id est, receptan una “Discrecionalidad Restringida” cuando se trata de convocatorias a concurso de méritos (3). Prosiguiendo diseña un cuadro que resume los argumentos que podría emplear el juez Varga en su resolución de tutela:

Tabla 2: Resumen de argumentos

ARGUMENTO	DESCRIPCIÓN
Derecho Adquirido	El primer puesto deja de ser un candidato para convertirse en un acreedor del cargo.
Interés General	El Estado garantiza un mejor servicio al elegir al más apto (quien obtuvo el mayor puntaje).
Falta de Motivación	Elegir al tercero habiendo un primero calificado constituye una "vía de hecho" (arbitrariedad).

Fuente: Generada por Gemini3.

La *artificial intelligence* coadyuvante concluye su exposición argumentando que en el caso planteado, el tribunal departamental de justicia de Cochabamba ha “incurrido en una vulneración de derechos al ignorar el orden de prelación sin una causal de inhabilidad” del primer candidato.

Apreciación. Se estima que en este ejercicio ChatGPT ha emulado las labores de búsqueda jurisprudencial que un juez constitucional puede efectuar de forma adecuada, superando a Gemini3. El primero de los dispositivos inteligentes no solo precisó sentencias constitucionales pertinentes, sino que señaló los correspondientes enlaces para poder consultarlas integralmente en la página oficial de la Corte Constitucional colombiana; información que no fue proporcionada por la segunda, que aunque mencionó jurisprudencia en su argumentación (Sentencia N.º SU-913 de 2009, Sentencia N.º SU-053 de 2015, Sentencia N.º T-032 de 2021, Sentencia N.º T-308 de 2023), algunas de ellas no versaban sobre el derecho a ser nombrado ni se habilitó enlaces para su verificación. Aun con las limitaciones apuntadas, los aportes de ambas inteligencias artificiales son provechosas debido a que se exponen conclusiones razonables al supuesto formulado, mismas que pueden servir como ítem a cavilar por el administrador de justicia.

Después de ponderado el talante de las respuestas a los cometidos interpretativos y jurisprudenciales instruidos a ChatGPT y Gemi-

ni3, es aceptable apreciar la eficiencia (rapidez en la contestación y la precisión de información) con la que operan y la plausibilidad de sus conclusiones; ergo, estas son inteligencias artificiales que receptan la capacidad de emular las tareas humanas de interpretación de normas jurídicas y búsqueda de jurisprudencia, para la ventilación de causas constitucionales.

5.2. Las directrices –o *prompts*– para el adecuado uso de la inteligencia artificial en los cometidos interpretativos y jurisprudenciales

La descripción del uso de ChatGPT y Gemini3 nos indica que estas deben recibir instructivas de un abogado o juez para su operatividad, las cuales reciben el nombre técnico “*prompts*”: las directrices que delimitan la actividad humana a emular por la inteligencia artificial o las “peticiones o instrucciones que se hacen a la IA para conseguir una respuesta específica” (Lopezosa, 2023, p. 2).

Las inteligencias artificiales, dependiendo de la programación que hayan recibido, pueden efectuar una pluralidad de acciones humanas, pero para que estas reporten aquello que se requiere las instrucciones deben ser *precisas y claras*. Abordemos este acápite retomando los ejemplos de las actividades de interpretación y de búsqueda de jurisprudencia anteriormente empleadas.

En el caso de la menor de edad se especificó el Estado en el que se habría suscitado la problemática (Bolivia) y el ordenamiento jurídico a interpretar (la Constitución de 2009 y la jurisprudencia del tribunal constitucional); se precisó los sujetos involucrados, el abogado que consulta, los padres de la niña (ocho años) y el director de la unidad educativa; se narró los hechos del supuesto (impedimento arbitrario de ingreso a clases por más de tres semanas, nula respuesta a las notas presentadas, violación del derecho a la educación); y se interrogó si mediante una interpretación de los elementos deónticos señalados era viable la presentación de una acción de amparo constitucional prescindiendo del agotamiento de instancias ordinarias (principio de subsidiariedad).

Se observa en consecuencia que tanto ChatGPT como Gemini3 ejecutaron una orden orientada por diversos *prompts* o directrices de operatividad:

a) Prompt de delimitación jurídica: Se limitó el marco normativo refiriendo la Constitución promulgada el 7 de febrero de 2009 y la jurisprudencia del Tribunal Constitucional Plurinacional del Estado boliviano; no haciéndose mención a leyes, a decretos supremos, al derecho de otros Estados o la normativa internacional sobre derechos humanos.

b) Prompt de delimitación fáctica: Se precisó detalles de las circunstancias del personaje principal del relato, una menor de edad de ocho años cuyo derecho a la educación fue vulnerado por parte del director de una unidad educativa que le prohibía el ingreso a clases por más de tres semanas; no se trataba del caso de una discente de universidad.

c) Prompt de delimitación procesal: Se consultó si la garantía pertinente para zanjar el hipotético era la acción de amparo constitucional, aun cuando este proceso está regido por el principio de subsidiariedad; no se planteó alternativas en otras acciones de defensa.

d) Prompt de delimitación operativa: Se ordenó que interpretara la normativa constitucional señalada con antelación y que determinara si era viable la presentación de la acción de amparo constitucional prescindiendo del principio de subsidiariedad.

Estas directrices son relevantes en cuanto la imprecisión de alguna de ellas podría haber incidido en el resultado a exponer: p. ej., de cambiarse el Estado y la normativa de este a interpretar para resolver el caso formulado, la artificial intelligence habría resuelto la problemática no desde el sistema jurídico boliviano, sino desde el que se señale –Perú, Colombia, etc.–; de no especificarse el proceso constitucional a interponer, es asaz probable que se afirmara que existen otras garantías para atender el hipotético –en el caso boliviano, la acción de libertad– con análoga efectividad.

No obstante lo señalado, las inteligencias artificiales pueden suplir la no delimitación de algunas directrices y ampliar sus respuestas. V. gr., en la incógnita del juez Vargas, ChatGPT y Gemini3 fueron instruidas a responder si existía jurisprudencia de la Corte Constitucional colombiana que hubiese abordado cuestiones similares a la causa bajo su conocimiento: si una persona que resultó la mejor calificada en un concurso de méritos tiene el derecho a ser elegido; mas la pregunta fue genérica y pudo haber sido contestada de forma genérica (si existe, o, no existe), ya que no se ordenó que indicara los números de las sentencias, sus fechas de emisión y los enlaces de verificación de páginas oficiales. Pero estas falencias no impidieron que ChatGPT replicara de forma afirmativa y exhaustiva: refirió sentencias con sus respectivos números y generó enlaces para constatar la información reportada; Gemini3 tampoco se limitó a una respuesta genérica, pero sus datos tuvieron deficiencias (citación de sentencias impertinentes).

Si bien es factible plantear casos de forma general en razón a que la inteligencia artificial puede asumir un *prompt* a partir de la nacionalidad del correo electrónico con el que se registró el usuario para su uso; es recomendable que las directrices para los cometidos interpretativos y cometidos jurisprudenciales sean precisos y claros, así las respuestas que se remitan serán exhaustivas.

5.3. Límites a la aplicación de la inteligencia artificial en los procesos constitucionales

Los diversos instrumentos normativos internacionales y nacionales que han abordado el tema de la inteligencia artificial, son indicadores de la necesidad de regular su funcionamiento para –entre otros propósitos– garantizar el respeto a los derechos fundamentales y humanos –en particular el derecho a la dignidad humana–, en un Estado Constitucional Democrático de Derecho.

Dicho marco y paradigma estatal invitan a inferir que está prohibido utilizar estos dispositivos inteligentes de forma que vulnere el bien común o intereses particulares; p. ej., una persona no debería emplear la inteligencia artificial para manipular la imagen de otra

con fines obscenos, dado que esto vulnera el derecho a la imagen y el derecho a la dignidad humana; o, no debería esgrimir a esta para generar noticias falsas, en virtud a que lesiona el derecho de la comunidad a recibir información fidedigna.

Pero las limitaciones a la utilización de la *artificial intelligence* no se reduce a las operaciones arbitrarias que se le pudiere encomendar, y que deben ser restringidas así como sancionadas, ya que también existen los *límites respecto a la capacidad de respuesta* (admisión de su falibilidad): de acuerdo a los avances tecnológicos, la inteligencia artificial: “ni sabe por qué sabe lo que sabe ni entiende lo que dice o responde” (Casanovas Combalia, 2023, p. 2); y los *límites respecto a la permisión de su aplicación* (habilitación constitucional y legal, principio de juridicidad).

Principiemos con los abogados. Cuando se dispone a redactar una acción de defensa u otro proceso constitucional, estos efectúan interpretaciones de la normatividad pertinente al caso a defender y recurren constantemente a la jurisprudencia del tribunal constitucional o el tribunal supremo de justicia, para ampliar su argumentación; pero, y de estar próximo el vencimiento del plazo para la presentación o de ser inminente la consumación de la amenaza a los derechos (un escenario que apremia la necesidad de la pronta incoación de la garantía constitucional), el análisis de los hechos vulneradores y la identificación de los derechos fundamentales y humanos conculcados se traducen en las actividades que mayor tiempo pueden consumir por ameritar lecturas y relecturas.

En este supuesto, el abogado puede ser coadyuvado por la inteligencia artificial, que funge como un asistente letrado para reducir la carga de trabajo: una vez efectuada una primera lectura a la problemática, este podría ordenar a ChatGPT y Gemini3 algunos cometidos interpretativos o cometidos jurisprudenciales. Reportada la información requerida, el abogado podrá emplearla para realizar una segunda lectura al caso, que puede concluir con la confirmación de las hipótesis de defensa inicial o su replanteamiento; de ser la segunda opción, se puede volver a interrogar a las herramientas inteligentes y repetir la dinámica descrita.

Ahora bien, remitidos los datos solicitados –por segunda, tercera o cuarta vez– el abogado tiene el deber de cavilar y corroborar la veracidad de la misma antes de plasmarla en sus memoriales, porque la cándida copia de estos sin previa reflexión y verificación de la autenticidad concluiría con la presentación de acciones de defensa u otros procesos constitucionales viciados en su razonabilidad por entrañar argumentos apócrifos: v. gr., un abogado desidioso emplearía la jurisprudencia constitucional –nacional o comparada– impertinente que Gemini3 pudiera indicar de forma errónea, despiste que demeritaría la validez de su discurso ante la autoridad judicial y afectaría los intereses de su patrocinado. Existe en consecuencia la obligación ética de utilizar a estos dispositivos inteligentes con suma cautela.

La autorización para aplicar la *artificial intelligence* para la resolución de casos concretos es un límite que se adscribe al juez constitucional por efecto del Estado de Derecho, en cuanto la “concepción de la libertad” de esta modalidad de organización jurídico-política restringe “las atribuciones de los órganos estatales en lo que respecta a su actuación en la sociedad” (Cossío Díaz, 1989, p. 30). Contrario a lo que pueda opinar el presidente del Tribunal Supremo de Justicia⁴, los departamentos gubernamentales deben actuar previa habilitación constitucional y legal dispuesta por el constituyente o el legislador –congreso o parlamento–, respectivamente, en cuanto estas son corolarios del principio de legalidad –o juridicidad– que modela dos normas de clausura: una, para el derecho constitucional de la libertad, “todo lo que no está expresamente prohibido por la ley está permitido”, y otra para el derecho constitucional del poder, “todo lo que no está expresamente autorizado por la ley está prohibido” (Guastini, 2001, p. 124).

4 El magistrado que preside este elevado órgano de poder aseveró con pleitesía que las decisiones del Presidente de la República (no especificó cuáles) eran constitucionales porque: “Nadie está obligado a hacer lo que la Constitución Política no manda; en otras palabras, lo que la Constitución Política no prohíbe, está permitido” (Correo del Sur, 2026); un dislate oprobioso para la magna toga si se lo analiza desde los principios del Derecho Constitucional y el Derecho Administrativo.

Enmarcadas jurídicamente las actuaciones de los órganos de poder, los vocales de la sala constitucional cuarta de Santa Cruz no estaban autorizados para emplear ChatGPT en el momento de la deliberación sobre la razonabilidad de los hechos del caso; a esta crítica debemos agregar que la abogada de los accionados denunció que las preguntas a la inteligencia artificial fueron “direccionadas”, esto es, no fueron formuladas con *prompts* de corte objetivo: no se habrían tomado en cuenta al consultar el hecho de que la accionante consintió y solicitó la publicación de sus fotografías, y que en ellas no se reveló su identidad (Correo del Sur, 2023).

Invocar la SCP N.º 0052/2025-S2 tampoco es un argumento suficiente para legitimar la utilización de la artificial intelligence por parte de los jueces constitucionales (jueces de garantías, vocales departamentales y magistrados del tribunal constitucional), porque esta resolución circunscribió la implementación de este tipo de dispositivos a las que pudieran coadyuvar en la “transcripción de actas de audiencia”, encomendado esta responsabilidad al Consejo de la Magistratura.

En consideración al discurso hilvanado, si la Asamblea Legislativa Plurinacional sancionara una ley que permitiera a los jueces constitucionales emplear la inteligencia artificial en sus funciones (p. ej., de deliberación sobre los méritos del caso y de redacción de las resoluciones judiciales), ¿sería esta válida? Juzgamos que no, porque la potestad de impartir justicia es un poder que la nación boliviana concesionó privativamente a los órganos de índole judicial de las distintas jurisdicciones (art. 178.I de la Constitución); el constituyente confió en el *iura novit curia*, y no en el *novit curia artificialis intelligentia* para la tutela de los derechos, la definición de los deberes de las personas, y la racionalización del ejercicio del poder público vía control de constitucionalidad.

Las actividades que integran la administración de justicia son por consiguiente indelegables a otros órganos de poder y a la inteligencia artificial.

Sin ánimos de demeritar lo aseverado, se estima que los jueces constitucionales pueden utilizar estos dispositivos inteligentes

para la búsqueda de jurisprudencia constitucional nacional o comparada; de hecho, esta acción ya se realiza tanto por jueces como por abogados cuando se consulta a Aletheia y Génesis, que podrían ser consideradas inteligencias artificiales básicas para la búsqueda de resoluciones judiciales del Tribunal Constitucional Plurinacional y el Tribunal Supremo de Justicia, respectivamente.

¿Puede entonces la judicatura constitucional esgrimir ChatGPT y Gemini3? Sí, pero solo para cometidos jurisprudenciales básicos, no para las actuaciones interpretativas y deliberativas sobre cómo entender el significado de una disposición, cómo valorar los argumentos de hecho y derecho, y cómo fallar una acción de defensa u otro proceso constitucional: dado que las personas tienen *derecho a ser juzgados* por personas y no por la inteligencia artificial, sería inconstitucional e ilegal que los jueces introduzcan la argumentación del accionante y la contraargumentación del accionado a esta para que resuelva la concesión o denegación de la tutela impetrada.

Si el juez constitucional abdica a su deber de administrar justicia en favor de la *artificial* intelligence, se agravaría la despectiva concepción de la función judicial como “máquina tragamonedas” (Radín, 1925, p. 358); en virtud a que los jueces ya no serían siquiera la máquina que se acciona con una moneda: se reducirían a ser el “asistente” de la máquina tragamonedas.

6. Conclusiones

Las inteligencias artificiales, como ChatGPT y Gemini3, son dispositivos que han acreditado receptor la capacidad para emular las actividades humanas de interpretación y búsqueda de jurisprudencia, operaciones racionales que ejecutan los abogados y jueces en procesos constitucionales, con considerable eficiencia: celeridad en la resolución de casos hipotéticos con argumentación razonable, y exhaustividad en la remisión de la información requerida.

En virtud a la calidad de las respuestas reportadas, la *artificial intelligence* puede fungir como un asistente letrado por la coadyu-

vancia idónea que concede para la redacción de acciones de defensa –y otros procesos– más sustentadas y sentencias constitucionales –y otras resoluciones judiciales– más fundamentadas y motivadas; pero, que tenga la vis para cometidos interpretativos y cometidos jurisprudenciales, no significa que su utilización esté exenta de directrices y limitaciones.

Para los abogados no existe mayores restricciones en su uso, ya que al no existir una ley que regule la inteligencia artificial en el litigio constitucional y al no ser autoridades judiciales, a estos no les está prohibido esgrimirla (norma de clausura del derecho constitucional de la libertad). Empero, para obtener información fidedigna de estos dispositivos inteligentes transportable al caso a patrocinar, deberá introducir con precisión y claridad las directrices –o *prompts*– así como verificar la verosimilitud de los datos remitidos antes de plasmarlos en sus memoriales.

Para el juez constitucional, la formulación adecuada de las directrices y las limitaciones de aplicación son de relevancia. Los *prompts* a utilizar para la realización de encargos interpretativos y jurisprudenciales deben ser planteados de forma objetiva, con independencia e imparcialidad; y solo pueden hacer uso de ella si se dispone de habilitación constitucional o legal, ya que el principio de legalidad o juridicidad prohíbe a las autoridades judiciales efectuar lo que no les está expresamente autorizado (norma de clausura del derecho constitucional del poder).

No obstante lo afirmado, se juzga que aun si existiese permisión por el constituyente y el legislador la inteligencia artificial no debería sustituir al hombre en la empresa de administrar justicia, en cuanto esta no es un ser con inteligencia en sentido estricto. Y, razonando más allá de las permisiones o prohibiciones jurídicas, se juzga que la abogacía y la judicatura inmersos en procesos constitucionales tienen adscrito la obligación ética de constante formación y la responsabilidad de no dejarse encandilar por la “sabiduría” de la inteligencia artificial, ya que esta es solo una herramienta al servicio de los intereses de sus catalizadores.

Los clientes y los impetrantes de justicia confían en las limitaciones del *iura novit advocatus* y el *iura novit curia*, no en la *iura novit artificialis intelligentia*.

7. Referencias

- Acosta Yparraguirre, E. M. (2024). La inteligencia artificial y el fin del Estado Constitucional y la Democracia... ¿o no? *Eunomía. Revista en Cultura de la Legalidad*, 27, 137-154.
- Álvarez Cantalapiedra, S. (2023). Luces, sombras y riesgos de la inteligencia artificial. *Papeles de relaciones ecosociales y cambio global*, 164, 5-12.
- Andaluz, H. (2011). *La aplicación judicial de la Constitución*, 1ª reimpresión. Editorial El País.
- BBC News Mundo. (20 de abril de 2023). La entrevista falsa con el expiloto de F1 Michael Schumacher que causa indignación en Alemania. *BBC News Mundo*. <https://www.bbc.com/mundo/noticias-65341966>.
- Cabello Ayzama, A. (2024). Implementación de inteligencia artificial en el derecho boliviano: análisis comparativo de Chat GPT y Gemini AI. YUYAY: *Estrategias, Metodologías & Didácticas Educativas*, 3 (2), 120-138.
- Cáceres Nieto, E. (2023). La inteligencia artificial aplicada al Derecho como una nueva rama de la teoría jurídica. *Anales De La Cátedra Francisco Suárez*, 57, 63-89.
- Cámara de Diputados. (2025). Proyecto de Ley PL-558/24: *Ley General de Inteligencia Artificial*. Asamblea Legislativa Plurinacional.
- Cámara de Senadores. (2025). Proyecto de Ley PLS N.º 178/2024-2025: *Ley de Promoción, Gestión y Uso de la Inteligencia Artificial*. Asamblea Legislativa Plurinacional.
- Casanovas Combalia, X. (2023). De la Inteligencia Artificial a la inmortalidad del alma. *Suplemento del Cuaderno CJ*, 234, 1-4.

Conferencia Iberoamericana de Justicia Constitucional. (2022).

Cuestionario del seminario “Estructura y lenguaje de las resoluciones de los tribunales constitucionales”.

Correo del Sur. (18 de abril de 2023). ¿Fallo judicial a través de ChatGPT?: Vocales utilizaron una inteligencia artificial en una audiencia. *Correo del Sur*. <https://correodelsur.com/seguridad/20230418/fallo-judicial-a-traves-de-chatgpt-vocales-utilizaron-una-inteligencia-artificial-en-una-audiencia.html>.

Correo del Sur. (5 de enero de 2026). Presidente del TSJ a Paz: “Lo que usted hizo es constitucional y lo está haciendo por el bien de Bolivia. *Correo del Sur*. <https://correodelsur.com/politica/20260105/presidente-del-tsj-a-paz-lo-que-usted-hizo-es-constitucional-y-lo-esta-haciendo-por-el-bien-de-bolivia.html>.

Cossío Díaz, J. R. (1989). *Estado social y Derechos de prestación*. Centro de Estudios Constitucionales.

Cruz Apaza, R. R. (2021). *Ensayos de Derecho Constitucional y Procesal Constitucional*. Estandarte de la Verdad.

Cumbre Judicial Iberoamericana XXI Edición: “Por una Carrera Judicial Independiente y Eficaz”. (2023). *Aplicaciones de inteligencia artificial en los poderes judiciales de Iberoamérica*. Propuesta del Grupo de Trabajo N.º 4 “Hecho tecnológico y su función jurisdiccional”.

De Ballón, J. (2004). *Métodos y técnicas de Investigación*. Universidad Mayor de San Simón.

Dworkin, R. (1992). *El Imperio de la Justicia. De la teoría general del derecho, de las decisiones e interpretaciones de los jueces y de la integridad política y legal como clave de la teoría y práctica*. Gedisa Editorial.

Fix-Zamudio, H. (2001). *Justicia Constitucional, Ombudsman y Derechos Humanos*. (2da. ed). Comisión Nacional de los Derechos Humanos.

Gadamer, H. (2003). *Verdad y método*. (10ma. ed., Vol. I). Ediciones Sígueme.

González Quirós, J. L. (2019). La inteligencia artificial y la realidad restringida: Las estrecheces metafísicas de la tecnología.

- Naturaleza y Libertad*, 12, 127-158.
- Grupo Europeo sobre Ética de la Ciencia y las Nuevas Tecnologías. (2018). *Declaración sobre Inteligencia artificial, robótica y sistemas autónomos*. Comisión Europea.
- Guastini, R. (2001). *Estudios de Teoría Constitucional*. Universidad Nacional Autónoma de México.
- Hernández, J. A., Conde, J., Querol, B., Martínez, G., y Reviriego, P. (2023). *ChatGPT, tus primeros prompts con 100 ejemplos*.
- Herrera Áñez, W. (2021). *Derecho Procesal Constitucional boliviano, Procesos y procedimientos*. Kipus.
- IEEE. (2017). *Ethically Aligned Design. A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems*. IEEE
- Kant, I. (2002). *Fundamentación para una metafísica de las costumbres*. Alianza.
- Lopezosa, C. (2023). La Inteligencia artificial generativa en la comunicación científica: retos y oportunidades. *Revista de investigación e innovación en ciencias de la salud*, 5 (1), 1-5.
- McCarthy, J. (2007). *What is artificial intelligence?* Stanford University, Computer Science Department.
- Nino, C. S. (2001). *Introducción al análisis del Derecho*. (10ma. ed.). Editorial Ariel.
- Oberg Yáñez, H. (2017). *Iura novit curia. Actualidad jurídica*, 36, 443-448.
- Radin, M. (1925). The theory of judicial decision: or how judges think. *American Bar Association Journal*, 11 (6), 357-362.
- Reale, M. (1997). *Teoría Tridimensional del Derecho. Una visión integral del Derecho*. Tecnos.
- Reyes Ortiz, L. Y. (2024). *Reflexión sobre la aplicación de la inteligencia artificial en procesos penales en el ordenamiento jurídico boliviano*.

(Tesis de Maestría, Universidad Mayor de San Andrés).

Romero Cárdenas, F. (2025). La Brecha entre la Constitución y la Realidad: Los Derechos Digitales Emergentes en Bolivia frente a la Inteligencia Artificial (2019-2024). *Revista Veritas De Difusão Científica*, 6 (2), 2084-2112.

Russell, S. y Norvig, P. (2004). *Inteligencia artificial. Un enfoque moderno*. (2da. ed.). Pearson Prentice Hall.

Sagüés, N. P. (2017). *Derecho Constitucional. Teoría de la Constitución*, T. 1. Astrea.

San Miguel, E. (2025). *La influencia de la Revolución francesa en la legislación boliviana (1825-1828)*. Plural editores.

Schmitt, C. (1983). *La defensa de la Constitución*. Tecnos.

Stippel, J. (2010). Lo que Liberia puede aprender de Bolivia: refundación y pluralismo jurídico. Una propuesta para la reflexión. En: V. Blickwede y M. E. Zegada (Eds.), *Hacia la Construcción del Tribunal Constitucional Plurinacional* (pp. 275-288). Programa de Fortalecimiento a la Concertación y al Estado de Derecho CONCED – GTZ.

Tribunal Constitucional Plurinacional. (10 de marzo de 2024). *“sIac Sistema de inteligencia artificial constitucional”, propuesta presentada por el presidente del TCP en la “Conferencia Mundial IA 2024” realizada en Medellín – Colombia*. <https://tcpbolivia.bo/2024/03/10/siac-sistema-de-inteligencia-artificial-constitucional-propuesta-presentada-por-el-presidente-del-tcp-en-la-conferencia-mundial-ia-2024-realizada-en-medellin-col/#:~:text=Paul%20Enrique%20Franco%20Zamora%2C%20particip%C3%B3,de%20las%20tecnolog%C3%ADas%20de%20informaci%C3%B3n>.

Tribunal Constitucional Plurinacional, *Sentencia Constitucional Plurinacional N.º 0846/2012 de 20 de agosto*.

Tribunal Constitucional Plurinacional, *Sentencia Constitucional Plurinacional N.º 0469/2019-S2 de 9 de julio*.

Tribunal Constitucional Plurinacional, *Sentencia Constitucional Plurinacional N.º 0104/2024-S3 de 29 de abril.*

Tribunal Constitucional Plurinacional, *Sentencia Constitucional Plurinacional N.º 0052/2025-S2 de 25 de febrero.*

UNESCO. (2022). *Recomendación sobre la ética de la inteligencia artificial.*
UNESCO.

Artículos de opinión

Opinion Articles

La firma digital en una cultura procesal analógica

Digital Signatures in an Analog Procedural Culture

► **Pablo Escóbar Ascarrunz**

Universidad Católica Boliviana “San Pablo” • La Paz, Bolivia

<https://orcid.org/0009-0008-9810-6888> • pablo@pabloescobarlaw.com

Revista de Derecho de la UCB – UCB Law Review, Vol. 10 N° 18, abril 2026, pp. 139-155

ISSN 2523-1510 (en línea), ISSN 2521-8808 (impresa).

DOI: <https://doi.org/10.35319/lawreview.202618138>

Recibido: 29 de octubre de 2025 • Aceptado: 10 de abril de 2026

Resumen

La firma digital ha sido celebrada como un hito de modernización jurídica con la Ley 164. Se presentó como un instrumento capaz de garantizar autenticidad, identificación y trazabilidad, inclusive frente a la firma estampada ante Notaría de Fe Pública. Sin embargo, este avance tecnológico tropieza con una limitación conceptual: en materia probatoria, procesal y registral, su validez puede depender de interpretaciones y analogías, ya que ni el Código Civil ni el Código Procesal Civil reconocen expresamente a los documentos firmados digitalmente como públicos. En un entorno jurídico obsesionado con el papel y la tinta, el sistema exige, todavía, una firma física. El artículo analiza esta omisión de bautizar expresamente tales documentos y propone una reforma al Código Civil y al Código Procesal Civil.

Palabras clave: Firma digital, derecho procesal civil, documento público, eficacia probatoria, formalismo procesal.

Abstract

Digital signatures have been celebrated as a milestone in Bolivia's legal modernization following the enactment of Law 164. They were introduced as tools capable of ensuring authenticity, identification and traceability with a level of precision that often exceeds the traditional handwritten signature, even one notarized. Yet this technological advance runs into a classification problem: in evidentiary, procedural and registry matters, its effectiveness often depends on judicial interpretation because neither the Civil Code nor the Rules of Civil Procedure expressly recognizes digitally signed documents as public instruments. In a legal culture where paper instruments retain their presumptive primacy, the system continues to demand a physical signature. This article examines that omission and proposes targeted reforms to align Bolivia's civil and procedural codes with its digital framework.

Keywords: Digital signature; civil procedural law; public document; electronic evidence; procedural formalism.

1. Introducción

El derecho procesal civil boliviano se construye sobre un principio de legalidad y taxatividad particularmente estricto. Las formas, los medios de prueba y, de manera especial, los títulos que habilitan la ejecución forzosa no se presumen ni se infieren con libertad, sino que deben encontrarse expresamente previstos en la ley. Esta lógica, que cumple una función esencial de seguridad jurídica y protección de los intereses de las partes involucradas en procesos judiciales, se vuelve problemática cuando el sistema normativo debe interactuar con instrumentos tecnológicos que no existían al momento de la codificación civil de la década de los setenta.

En este marco, la firma digital plantea un desafío que no es técnico, sino dogmático. Su validez como mecanismo de identificación y autenticación se encuentra reconocida por la legislación especial. Sin embargo, su encaje dentro de las categorías clásicas del

derecho probatorio, del régimen del documento público y de los presupuestos del proceso ejecutivo no ha sido objeto de una adecuación expresa en el Código Civil ni en el Código Procesal Civil. Ello resulta particularmente llamativo si se considera que el Código Procesal Civil es mucho más reciente que el Código Civil y, de manera casi contemporánea, fue promulgado en el mismo contexto normativo que la Ley de Telecomunicaciones y Tecnologías de la Información, norma que ha creado la firma digital.

El resultado es un espacio de incertidumbre porque se tiene un instrumento jurídicamente válido desde el punto de vista sustantivo pero cuya eficacia procesal depende de construcciones interpretativas antes que de una habilitación normativa directa. Esta situación revela una fractura entre dos realidades: por un lado, se tiene a la tecnología que privilegia la automatización, la trazabilidad y la eliminación del error humano y que debería generar confianza; y por otro, la lógica procesal tradicional, estructurada sobre la materialidad del documento físico, la tinta y las huellas, así como la intermediación de funcionarios investidos de fe pública que, pese a distar de las ventajas de la tecnología, son las que las autoridades prefieren analizar a tiempo de evaluar la validez y verdad de un documento.

Cuando ambas se encuentran, el sistema no sabe cómo integrarse a la tecnología sin desnaturalizar sus propias categorías. Desde esta perspectiva, el problema central no radica en si la firma digital es confiable, sino en si el derecho procesal boliviano está conceptualmente preparado para reconocerla como fuente plena de efectos jurídicos, en particular cuando se trata de atribuirle fuerza probatoria reforzada o aptitud ejecutiva.

Sobre esta base, el presente artículo se propone examinar la ubicación dogmática del documento firmado digitalmente dentro del sistema civil y procesal vigente, identificar las limitaciones que surgen de la ausencia de un reconocimiento expreso como documento público y fundamentar la necesidad de una reforma normativa que permita superar un derecho procesal diseñado para el papel y la tinta en un entorno que ya es, de hecho, digital.

2. El régimen del documento público en el Código Civil boliviano

El Código Civil boliviano estructura su régimen probatorio, más allá de las disposiciones de la norma adjetiva, en su Libro Quinto, Título I, dedicado a las pruebas en general. En cuanto a la prueba documental, que es de lo que se ocupa este artículo, hace una distinción entre documento público y documento privado (Art. 1287 y ss., Código Civil, Decreto Ley 12760, 1975). Esta distinción no es meramente formal sino que constituye una pieza central del sistema de valoración probatoria.

El documento público es aquel autorizado por funcionario competente con las formalidades establecidas por ley. Su naturaleza se sustenta en la intervención de un sujeto investido de fe pública. La consecuencia jurídica de esta intervención es que le otorga plena fe respecto de los hechos que este consigna salvo prueba en contrario. Se trata de una presunción de autenticidad y veracidad que traslada la carga de la prueba hacia quien pretende desconocerlo, así lo señalan a grandes rasgos los Arts. 1287 y 1289.

El Código es menos generoso con el concepto de *documento privado* ya que no lo define (un problema recurrente para los estudiantes de derecho civil que quieren apoyarse en él como un diccionario en el que, algunas veces, como con el documento público, lo es) y, por el contrario, describe directamente su utilidad cuando ya ha sido reconocido. El Art. 1297, desde su *nomen juris*, ya adelantan esa descripción en vez de noción: “*Eficacia del documento privado reconocido*”. Sin definirlo, directamente salta a volverlo ya público: “...reconocido por la persona a quien se opone o declarado por la ley como reconocido...” tiene la fuerza del documento público. Es decir que el Código Civil en realidad no versa sobre el documento privado sino que lo hace sobre el documento privado *ya reconocido*, y ese documento es, ergo, el documento público.

Con estas porciones normativas, el Código establece un estándar probatorio tácito: mientras no esté reconocido, el documento privado (no definido legalmente) no tiene fuerza probatoria. O, en

otras palabras, sólo el documento público será válido como prueba. Y aún en otras más: para demandar y acompañar su documento como prueba, quien quiera probar un hecho basado en un documento deberá hacerlo reconocer, si es que antes no lo hubiera sido, como documento público.

Este diseño, a criterio del autor, responde a una lógica histórica en la que la seguridad jurídica se vinculaba a la intervención humana cualificada. La fe pública notarial se concebía como garantía institucional frente a la falsificación o la simulación. El soporte material de papel firmado, manuscritos, sellos, huellas y protocolos, operaba como complemento visible de esa garantía. Casi como un billete o un cheque con medidas de seguridad para evitar su falsificación.

Sin embargo, esta arquitectura normativa fue construida en un contexto tecnológico determinado. El Código Civil de 1975 no contemplaba la posibilidad de mecanismos criptográficos de autenticación ni infraestructuras de certificación digital porque, por supuesto, no existía la alternativa de que esos documentos puedan tener otro soporte. La autenticidad era una cuestión de percepción y certificación humana, con tacto y vista, que hoy puede ser una cuestión de verificación técnica automatizada. Si el Código fuera escrito hoy, es altamente probable que los legisladores no se limiten a esa calidad de documentación sólo físicamente verificable.

De hecho, han existido modificaciones a normas de la misma década de los setenta incorporando y sustituyendo costumbres “anticuadas” por modernidad. Es el caso, por ejemplo, de la obligatoriedad de la publicación a través de gaceta electrónica de las convocatorias a asambleas y juntas en sociedades comerciales, sustituyendo al periódico. Y ni siquiera como alternativa sino que excluyendo y básicamente prohibiendo, a gusto del autor de forma exagerada, que una sociedad comercial pueda convocar por medios de prensa escritos¹.

El punto crítico no es que el Código Civil desconozca la firma digital (de hecho, no podría hacerlo por razones cronológicas), sino que su definición de documento público está casada con la intervención de un funcionario investido de fe pública. La firma digital sustituye la

firma manuscrita, pero no sustituye, en principio, al notario o a ese funcionario público que se requiere.

Surge entonces una interrogante dogmática central: si la firma digital garantiza identidad, integridad y no repudio con estándares técnicos superiores a los de la firma manuscrita, ¿puede afirmarse que el documento firmado digitalmente merece, por coherencia, una fuerza probatoria mínimamente equivalente a la del documento público – dar fe de que su contenido es verdadero y ejecutable? ¿O debe mantenerse dentro de la categoría del documento privado, pese a ofrecer mayores garantías técnicas? ¿Y si se mantiene como documento privado cómo lograr su ascenso a la categoría de documento público cuando no es posible reconocerlo una vez fuera de los sistemas tecnológicos?

La Ley 164 reconoce la equivalencia funcional de la firma digital respecto de la firma manuscrita (Art. 6, Ley 164, 2011). No obstante, esa equivalencia se refiere al acto de firmar, no a la categoría documental en la que el instrumento debe ser enmarcado. El Código Civil no ha sido modificado para integrar expresamente al documento firmado digitalmente dentro del régimen del documento público. Tampoco se ha beneficiado, como sí el Código de Comercio, de procesos de desburocratización.

Esta omisión genera un espacio interpretativo. El operador jurídico puede sostener que la equivalencia funcional permite asimilar el documento digital al documento público cuando concurren determinadas condiciones.

- 1 La Ley N° 779 de Desburocratización para la Creación y Funcionamiento de Unidades Económicas (2016) modifica el Código de Comercio que, al igual que el Código Civil, es de 1975, incorporando mediante su Artículo Adicional Único disposiciones relativas a la publicidad de los actos de comercio. En la práctica, incluso el intento de mantener la publicación de una convocatoria a junta por medio de periódico suele ser observado por el Registro de Comercio y devuelto in limine para su adecuación, desplazando en los hechos la autonomía de la voluntad de los socios que quisieran conservar ese medio de publicación en lugar de adoptar las modalidades modernas. Pero ese debate es materia de otro artículo.

Pero también puede sostener que, al no existir reforma expresa, el documento digital permanece en la órbita del documento privado, perdiendo toda utilidad la propia firma digital.

En un sistema que otorga efectos jurídicos diferenciados a cada categoría, esta falta de definición no es menor. De ella depende la intensidad de la presunción probatoria, la carga de la prueba y, en última instancia, la posición procesal de las partes.

3. El proceso ejecutivo y la lógica de la taxatividad

La cuestión probatoria adquiere mayor intensidad en el ámbito del proceso ejecutivo.

El Código Procesal Civil establece que la vía ejecutiva procede cuando se funda en un título que contenga una obligación clara, líquida y exigible, y que esté expresamente reconocido por la ley (Art. 379 y ss., Ley 439, 2013). La enumeración de títulos ejecutivos no es abierta sino taxativa.

Este principio cumple una función garantista porque la ejecución implica el uso de la coerción estatal-judicial sobre el patrimonio del ejecutado, con un salto de ciertos aspectos de protección o igualdad de las partes en litigio. A diferencia del proceso ordinario, antes de permitirle el derecho de defensa y antes de ser escuchado, si el título ejecutivo en el que se basa pasa una prueba meticulosa del juez, se dicta la sentencia inicial y el demandado toma conocimiento del proceso una vez que ésta ha sido dictada. El demandado puede no tomar conocimiento de que está siendo demandado y tampoco de que pesa una sentencia en su contra que, probablemente, contendrá medidas cautelares otorgadas a favor del acreedor contra su patrimonio que aseguren el pago de la obligación pendiente analizada por la autoridad.

Por ello, el legislador delimita estrictamente los instrumentos que habilitan ese procedimiento expedito, justamente para sólo permitir esta ocasional velocidad que desprotege a los deudores con

base en documentos legítimos y que le produzcan fe de que lo que se afirma sea cierto. Adicionalmente, el proceso ejecutivo requiere del pago de una suma calculada en proporción a la demanda así como para las anotaciones, pidiendo al acreedor una inversión de seriedad en lo que pide.

En este contexto, la ubicación del documento firmado digitalmente se vuelve decisiva. Si el documento digital es considerado documento privado, debe requerirse su reconocimiento previo antes de adquirir fuerza ejecutiva. Si se lo considera documento público, su aptitud ejecutiva sería inmediata, siempre que cumpla con los requisitos materiales y tecnológicos de la obligación.

El problema podría ser aún mayor: tal vez tampoco se lo pueda reconocer como documento privado porque no lleva tinta ni un trazo manuscrito que permita, siquiera previamente, someterlo al proceso de elevación a la calidad de documento público mediante el reconocimiento previsto por el Art. 1298 del Código Civil (Código Civil, Decreto Ley 12760, 1975). Y no por mala fe o por una estrategia procesal de la parte a quien puede no convenirle que la firma sea verificada, sino porque la propia forma prevista por la ley para elevar un documento privado a documento público consiste en oponerle al autor de la firma cuando éste se rehúsa a reconocerlo. En ese sentido, conforme al Art. 1300 del mismo Código, el supuesto autor “está obligado a confesar o negar formalmente si es de su letra o firma”.

La lógica de estas disposiciones supone necesariamente la existencia de una firma manuscrita susceptible de ser atribuida visualmente a una persona determinada, circunstancia que no se presenta cuando el documento ha sido firmado digitalmente.

En efecto, tratándose de documentos firmados digitalmente que son presentados en soporte impreso, el procedimiento físico y analógico de verificación previsto por el Código Civil se vuelve impracticable. El juez no puede examinar la firma en los términos previstos por la ley ni el supuesto autor puede confesar o negar que se trate de su letra o firma, porque aquel trazo manuscrito que la norma supone verificable simplemente no existe en el soporte físico.

Lo que aparece en el papel son únicamente códigos, sellos o leyendas de validación que no permiten verificar por sí mismos la correspondencia entre el documento y el certificado digital del firmante conforme al régimen de la Ley 164 (Ley 164, 2011). La verificación técnica solo puede realizarse sobre el archivo electrónico original, mientras que el procedimiento probatorio previsto por el Código Civil está construido sobre la inspección directa del documento físico.

El resultado es que el documento firmado digitalmente, aun ofreciendo mayores garantías objetivas de autenticidad e integridad, puede encontrarse en una posición probatoria inferior a la de un documento firmado con bolígrafo sobre cualquier soporte material, incluso el más precario, porque ese último sí permite seguir el procedimiento de reconocimiento previsto por los Arts. 1298 y 1300 del Código Civil, mientras que el primero no puede someterse a ese mismo proceso una vez que ha sido extraído del sistema electrónico para su presentación en papel conforme a las reglas generales de la prueba documental (Art. 147 y ss., Ley 439, 2013).

La Ley 439 no contiene una referencia explícita a documentos firmados digitalmente dentro de su catálogo de títulos ejecutivos. Tampoco el Código Civil ha sido modificado para reconocer expresamente que el documento firmado digitalmente puede ostentar carácter de documento público.

Ello obliga a realizar un ejercicio interpretativo. Puede sostenerse que, si la Ley 164 reconoce equivalencia funcional y el documento cumple con los requisitos técnicos de autenticidad, nada impide considerarlo apto como título ejecutivo cuando el contenido obligatorio sea claro y exigible. Sin embargo, esta conclusión no surge de una habilitación expresa, sino de una inferencia lógica que se trazará en el siguiente numeral de este texto.

En un sistema procesal caracterizado por la legalidad estricta, la integración por analogía puede generar resistencia. Algunos operadores pueden inclinarse por una interpretación restrictiva, entendiendo que solo los instrumentos tradicionalmente concebidos como documentos públicos pueden habilitar la vía ejecutiva.

La consecuencia es una paradoja práctica: un instrumento que ofrece mayores garantías técnicas de autenticidad puede enfrentar mayores obstáculos procesales que un documento firmado en papel y certificado por un funcionario. No porque sea menos seguro, sino porque el sistema no ha ajustado sus categorías.

El problema, nuevamente, no es tecnológico sino estructural. La firma digital cumple su función. El proceso ejecutivo, diseñado bajo parámetros analógicos, no ha sido reformulado para integrarla sin fricciones.

4. La verificabilidad técnica de la firma digital: ¿en el fondo puede un documento firmado digitalmente ser considerado un documento público?

La firma digital consiste en información electrónica vinculada al documento firmado que permite identificar al titular del certificado y verificar la integridad del documento conforme al régimen establecido por la Ley 164 (Ley 164, 2011). A diferencia de la firma manuscrita, cuya autenticidad depende de la percepción humana o eventualmente de una pericia caligráfica, la firma digital permite comprobar objetivamente si el documento ha sido firmado por el titular del certificado y si su contenido ha sido alterado con posterioridad a la firma.

Esta verificabilidad técnica forma parte esencial del valor jurídico de la firma digital. El documento electrónico firmado contiene elementos que permiten comprobar la correspondencia entre el certificado digital y el firmante, así como la integridad del documento suscrito. La identificación del firmante y la autenticidad del documento dejan de depender de la apreciación subjetiva de una firma manuscrita y pasan a hacerlo de mecanismos técnicos verificables y cercanos a la infalibilidad.

Sin embargo, esta verificabilidad sólo puede realizarse sobre el documento electrónico original. Cuando el documento firmado digitalmente es trasladado a soporte físico para su presentación en un proceso judicial, los elementos electrónicos que permiten verificar autenticidad e integridad dejan de ser accesibles. Lo que queda en el papel es únicamente una representación gráfica de la firma digital que no permite comprobar por sí misma la correspondencia entre el documento y el certificado del firmante conforme al régimen de la Ley 164.

Se produce entonces una tensión estructural entre el instrumento tecnológico y el procedimiento probatorio. Mientras la autenticidad del documento digital depende de la verificación electrónica del certificado y de la integridad del archivo original, el sistema probatorio tradicional se construye sobre la inspección directa del documento físico. El juez puede examinar el papel, pero no puede verificar técnicamente la firma si no tiene acceso al archivo electrónico original. Lo mismo ocurre con la parte a quien se le opone la firma: por más que sepa que firmó digitalmente el documento que ve impreso, no puede (y no es que no quiera) verificar a ciencia cierta que esa firma digital le corresponde: la única manera de verificarlo es a través del sistema tecnológico construido para ello que, en nuestra realidad, está lejos de las impresoras.

El resultado es que el documento firmado digitalmente pierde gran parte de su utilidad precisamente cuando ingresa al proceso judicial. El instrumento diseñado para permitir una verificación objetiva termina siendo evaluado mediante procedimientos que presuponen la existencia de tinta y trazo manuscrito. La tecnología ofrece un mecanismo más preciso de identificación, pero el proceso continúa operando sobre categorías concebidas para documentos físicamente verificables.

Puede interpretarse que, pese a las dificultades y con un escrutinio más moderado, un documento firmado digitalmente sea considerado, por trazabilidad normativa, como un documento público o, al menos, como un documento con valor, autenticidad y eficacia

equiparables a documento público, precisamente porque su verificabilidad técnica está prevista por el propio ordenamiento.

Cuatro razones sostienen este juicio de valor: *primero*, la Ley 164 reconoce validez jurídica y probatoria al acto o negocio jurídico realizado en documento digital y aprobado por las partes a través de firma digital, así como a la firma digital misma (Art. 78.I.1 y 78.I.3, Ley 164, 2011). Segundo, el Reglamento aprobado por el Decreto Supremo N° 1793 establece que, cuando una firma digital ha sido inscrita en un documento digital o mensaje electrónico de datos, se presume la voluntad del titular de la firma digital para acreditar ese documento, y que dicha firma se adscribe y vincula con el contenido de la información, de modo que la autenticidad e integridad dejan de depender de la inspección material del trazo manuscrito y pasan a depender de la verificación técnica (Art. 4, Decreto Supremo 1793, 2013). Tercero, la Ley 164 define el certificado digital como un documento digital firmado digitalmente por una entidad certificadora autorizada (Agencia para el Desarrollo de la Sociedad de la Información en Bolivia – ADSIB, en el caso de nuestro país que, además, funge, a interpretación propia, como el funcionario autorizado y que coincide con los requerimientos del 1287 del Código Civil “...*extendido con las solemnidades legales por un funcionario autorizado para darle fe pública...*”) que vincula datos de verificación de firma a un signatario y confirma su identidad, lo que permite afirmar normativamente que la firma digital es susceptible de verificación y que esa verificación está vinculada a una persona determinada (Art. 6.IV.1, Ley 164, 2011). Cuarto, el sistema probatorio civil admite que el documento privado tenga valor, autenticidad y eficacia de documento público cuando es presentado en el proceso afirmándose estar suscrito por la parte contra quien se opone sin tacha oportuna de falsedad, y reconoce además el documento digitalizado o electrónico en los términos que señale la ley, lo que habilita la integración sistemática de la Ley 164 como norma especial para dotar de eficacia probatoria plena al documento electrónico firmado digitalmente (Art. 148.II.4 y 148.III, Código Procesal Civil, 2013). En este marco, la firma digital no solo es

válida: es verificable conforme a ley, y esa verificabilidad es la que permite sostener su fuerza probatoria reforzada.

En síntesis: la verificación técnica conforme a Ley 164 y su reglamento, realizada por autoridad competente dentro del sistema de certificación (ADSIB) como entidad pública autorizada para darle fe, permite tratar al documento firmado digitalmente como documento con valor, autenticidad y eficacia de documento público. Pero no está así escrito en los códigos Civil ni Procesal Civil.

Ergo, la taxatividad puede sobreponerse a esta deducción: puede ser razonable y tecnológicamente coherente, pero no está expresamente consagrada en las categorías que el sistema procesal exige para producir efectos plenos.

5. La práctica judicial y los efectos concretos del vacío normativo

La omisión legislativa de reconocer expresamente al documento firmado digitalmente como documento público no es solamente un problema de teoría jurídica, sino también un problema de funcionamiento práctico del sistema probatorio y procesal.

En teoría, si un documento firmado digitalmente cumple los requisitos técnicos y legales previstos por la Ley 164, debería producir efectos jurídicos plenos. En la práctica, el documento suele verse sometido a cuestionamientos que rara vez se formulan frente a un documento en papel: cómo se verifica, cómo se sabe que es auténtico, dónde está el original o cómo puede comprobarse que no ha sido alterado. Son preguntas razonables dentro de una cultura jurídica acostumbrada a la tinta y al papel, pero resultan desproporcionadas frente a una tecnología precisamente diseñada para responderlas de manera objetiva.

Aquí aparece con claridad la tensión que atraviesa todo este análisis: la tecnología garantiza certeza, pero el sistema institucional no siempre confía en esa certeza. Se prefiere la certeza visible del

papel aun cuando esa certeza visible sea muchas veces menos fiable que la verificación técnica de un documento electrónico.

Este entorno jurídico del país todavía se encuentra fuertemente orientado hacia el papel y la tinta, y en esa orientación termina desaprovechando ventajas que el propio sistema normativo ha puesto a su disposición. El problema no es la firma digital sino la manera en que las autoridades y los operadores jurídicos determinan qué consideran confiable.

Las consecuencias de este vacío normativo son concretas.

En materia probatoria, el documento digital puede quedar atrapado en discusiones preliminares que consumen energía procesal. Se abre la puerta a observaciones formales, exigencias de reconocimiento o requerimientos adicionales que terminan castigando al litigante que optó por un medio más seguro y moderno.

En materia ejecutiva, el efecto puede ser todavía más delicado. El acreedor que cuenta con un documento firmado digitalmente puede ver debilitada la rapidez que caracteriza al proceso ejecutivo, no por falta de obligación sino por falta de una etiqueta normativa clara que permita ubicar al documento dentro del sistema de títulos ejecutivos.

Existe además un costo sistémico. Cuando el derecho no integra con claridad instrumentos digitales, incentiva el retorno al papel. Ante la incertidumbre, las partes vuelven a los documentos que el juez puede entender sin discusión. De este modo, el sistema termina promoviendo indirectamente el abandono de la firma digital pese a haberla reconocido normativamente.

Se produce así una contradicción institucional. El ordenamiento jurídico crea la firma digital como instrumento destinado a fortalecer la seguridad jurídica, pero el sistema procesal mantiene estructuras que reducen su eficacia práctica. El resultado es que el documento firmado digitalmente, pese a ofrecer mayores garantías objetivas de autenticidad e integridad, puede resultar más difícil de utilizar que un documento firmado manuscritamente.

6. Propuesta de reforma: lineamientos concretos para armonizar Código Civil y Código Procesal Civil con la Ley 164

La salida no exige reinventar el proceso civil. Exige coherencia normativa. El sistema ya tomó una decisión de modernización al reconocer la firma digital. Lo que falta es asumir esa decisión en los códigos que ordenan la prueba y la ejecución.

La propuesta puede presentarse en dos líneas:

- Primero, una reforma civil (Código Civil) que incorpore una regla expresa que reconozca que el documento firmado digitalmente, cuando cumpla los requisitos previstos por la legislación especial, goza de fuerza probatoria plena y de un tratamiento equivalente al documento público en lo que respecta a autenticidad e integridad.
- Segundo, una reforma procesal (Código Procesal Civil) que incorpore de manera expresa al documento firmado digitalmente dentro de los instrumentos aptos para producir efectos probatorios reforzados y, cuando corresponda por su contenido obligacional, habilite su aptitud ejecutiva en condiciones equivalentes a los instrumentos tradicionalmente aceptados como títulos ejecutivos. Esto es especialmente importante en un régimen de taxatividad, donde lo que no está previsto termina existiendo solo por interpretación.

El punto no es “darle privilegios” a la firma digital. El punto es dejar de tratarla como si fuera un documento de segunda clase. Si el Estado creó el ecosistema normativo para que exista firma digital, lo coherente es que los códigos de base no la miren como una excepción sospechosa, sino como parte del derecho vigente.

Una reforma así no debilita la seguridad jurídica sino que la fortalece porque traslada la confianza desde el hábito hacia la norma, y desde la norma hacia una tecnología diseñada para producir predictibilidad y certeza.

7. Conclusión

La discusión sobre la firma digital en Bolivia suele plantearse como un debate tecnológico, pero el problema real es procesal. La firma digital es, en términos técnicos y normativos, una herramienta sólida: identifica, vincula y permite verificar integridad. Sin embargo, su eficacia jurídica plena tropieza cuando ingresa a un sistema probatorio y ejecutivo construido para una realidad manuscrita en papel.

El núcleo del problema no está en la validez sustantiva de la firma digital, sino en su encaje dentro de categorías que, por diseño histórico, privilegian la fe pública tradicional y la inspección del soporte material. El Código Civil asocia el documento público a un funcionario autorizado y a solemnidades pensadas para papel y tinta; y el Código Procesal Civil organiza la ejecución forzosa sobre la base de títulos expresamente previstos. En ese marco, el documento firmado digitalmente puede ser técnicamente más confiable y aun así ser jurídicamente más frágil en la práctica.

La tensión se vuelve más clara cuando el documento digital se traslada a soporte impreso. Allí se pierde, o al menos se debilita, el rasgo que lo hace valioso: su verificabilidad técnica. El proceso probatorio tradicional pide al juez mirar el documento y al supuesto autor confesar o negar una firma manuscrita; pero cuando lo que existe es una firma digital, ese procedimiento físico y analógico se vuelve impracticable. La paradoja no es menor: el instrumento diseñado para eliminar incertidumbre termina generando más fricción procesal que un documento con bolígrafo en cualquier soporte material.

Esta situación no debería depender de la apertura interpretativa del juzgador ni de la creatividad interpretativa del abogado. Si el ordenamiento jurídico decidió reconocer la firma digital, la coherencia normativa exige que esa decisión tenga un correlato claro en los códigos que definen la prueba y la ejecución. De lo contrario, se perpetúa un escenario en el que la firma digital existe, pero se utiliza menos de lo que debería; y cuando se utiliza, se enfrenta a resistencias que el sistema no impone a documentos menos seguros.

Por ello, una reforma expresa al Código Civil y al Código Procesal Civil no sería un gesto de modernidad, sino un acto de coherencia. No se trata de reemplazar la seguridad jurídica del formalismo, sino de actualizar sus mecanismos y hacer que la certeza no dependa exclusivamente de la tinta y el papel, sino también de herramientas tecnológicas que el propio derecho ya ha validado. Mientras esa armonización no ocurra, seguiremos en una cultura procesal analógica donde la firma digital, aunque válida, continúa confinada.

8. Referencias

Agencia para el Desarrollo de la Sociedad de la Información en Bolivia. (s. f.). *Validación de firmas digitales*. <https://validar.firmadigital.bo>

Decreto Ley N° 12760, Código Civil. 6 de agosto de 1975.

Ley N° 164, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación. 8 de agosto de 2011.

Decreto Supremo N° 1793, Reglamento a la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación. 13 de noviembre de 2013.

Ley N° 439, Código Procesal Civil. 19 de noviembre de 2013.

Naturaleza jurídica de las memecoins

Legal Nature of Memecoins

► **Félix Fabian Espinoza Valencia**

Investigador independiente • La Paz, Bolivia

<https://orcid.org/0000-0002-7682-2102> • fespinoza@ucb.edu.bo

Revista de Derecho de la UCB – UCB Law Review, Vol. 10 N° 18, abril 2026, pp. 157-176

ISSN 2523-1510 (en línea), ISSN 2521-8808 (impresa).

DOI: <https://doi.org/10.35319/lawreview.202618137>

Recibido: 15 de octubre de 2025 • Aceptado: 16 de abril de 2026

Resumen

Análogo a lo que es un gen en biología, un meme es una unidad de transmisión cultural que se replica, muta y compite por atención en el imaginario colectivo, expandido también en el ámbito financiero como una subcategoría de criptoactivo versado en dinámicas especulativas colectivas pseudo lúdicas. Sin certeza de su tratamiento regulatorio, este artículo determina la naturaleza jurídica de las memecoins (MC), exponiendo figuras de riesgo en el mercado y analizando la declaración de la Comisión de Bolsa y Valores de Estados Unidos (SEC) respecto a la acepción de las MC como un valor negociable y su transacción para oferta y venta en relación con un contrato de inversión que se verifica con un test jurisprudencial anglosajón. Cuando se pretende aplicar el examen en el ecosistema de activos virtuales y concordante con el derecho iberoamericano, encuentra deficiencias metodológicas; por lo que se postula un nuevo test que responde a la nueva arquitectura de tecnologías financieras.

Palabras clave: Memecoins; Criptoactivos; Memética; Mercado de valores; Contrato de inversión; Descentralización.

Abstract

Analogous to what a gene represents in biology, a meme constitutes a unit of cultural transmission that replicates, mutates, and competes for attention within the collective imagination, further extended into the financial domain as a subcategory of crypto-asset operating within pseudo-ludic collective speculative dynamics. In the absence of regulatory certainty regarding their treatment, this article determines the legal nature of memecoins (MC), setting forth risk typologies present in the market and analyzing the declaration issued by the U.S. Securities and Exchange Commission (SEC) with respect to the characterization of MCs as a negotiable security and their transaction for offer and sale in connection with an investment contract — a qualification verified through an Anglo-Saxon jurisprudential test. When the application of said exam is sought within the virtual asset ecosystem and read in conjunction with Ibero-American law, methodological deficiencies emerge; accordingly, this article proposes a novel test responsive to the emerging architecture of financial technologies.

Palabras clave: Meme coins; Crypto-assets; Memetics; Securities law; Investment contract; Decentralization..

1. Introducción

La convergencia entre la cultura e internet ha dado lugar a fenómenos tan interesantes como complejos que han alcanzado al sistema financiero desde una perspectiva atípica.

La memética, expresión acuñada por el biólogo evolutivo, etólogo y divulgador científico británico Dawkins R. (1976) es un marco teórico interdisciplinario que propone el análisis de la cultura mediante una analogía explícita con la biología evolutiva, al concebir a los memes como una unidad de información cultural que se reproduce, varía y es seleccionada en función de su capacidad de propagación.

Esta figura adquiere una particular relevancia en el análisis de fenómenos digitales —como los memes de internet— al ofrecer

herramientas teóricas para comprender la difusión acelerada, la mutación semiótica y el impacto sociopolítico de contenidos culturales en entornos de alta conectividad (Blackmore, S., 1999), particularmente en la eclosión de la economía digital que han tenido su expresión cúspide con los activos virtuales.

Se plantea la cuestión de cómo concebir a las *memcoins* (MC) que en sí no son consideradas un valor conforme a la ley, distinguiendo entre instrumentos financieros que tengan una connotación dentro de la nueva categorización de activos virtuales.

Las transacciones con MC no implican oferta y venta de valores y no constituyen un contrato de inversión, a pesar de estar sujetas a uno.

- i. Un valor no es sinónimo de contrato de inversión, por lo que la premisa es: todo contrato de inversión es un valor, pero no todo valor es un contrato de inversión; más bajo las consideraciones de considerar a un MC como instrumentos financiero sujetos a las variables del *test de Howey (TH)* que aplica a cualquier contrato, precisando que: la transacción sí es analizada por este Test, más no así el activo virtual como token. En suma, se estudia si la MC como activo digital es, en sí misma, un valor; y
- ii. Si la oferta de ese activo puede constituir una operación regulada como valor o contrato de inversión.

Un activo que no es valor en sí mismo puede ser ofrecido de manera que configure un contrato de inversión regulado —y viceversa, un activo estructuralmente asimilable a un valor puede ser distribuido en condiciones que lo excluyan de la oferta pública—. El comunicado de la SEC recoge expresamente esta distinción al señalar que la declaración no se extiende a productos que se etiqueten como MC en una gestión por evadir y/o eludir la aplicación de las leyes federales de valores disfrazando un producto que de otro modo constituiría un valor.

2. Etimología de MC

Un MC proviene del latín *meme*: algo imitado y del inglés coin: moneda. El primer MC fue Dogecoin (DOGE) creado el 6 de diciembre de 2013 por Billy Markus y Jackson Palmer. *Doge* es literalmente un meme de un perro de raza *Shiba Inu* con textos gramaticalmente incorrectos.

En la actualidad existen alrededor de 2.300 MC, sin contar que existen plataformas¹ que facilitan la creación de nuevos, y podrían ascender a millones, pero que carecen de relevancia.

Además de las previamente descritas MC, existe, en una categorización enunciativa y no excluyente²:

- a) **Altcoins**. Criptomonedas alternativas al Bitcoin, que fue la inicial con la que surgió esta categoría como criptomoneda (Ej. Ethereum).
- b) **Stablecoins**. Criptomonedas estables, por estar vinculadas a una moneda fiduciaria o valor tradicional estable. (Ej. USDT).
- c) **Tokens**. Una unidad digital gestionada en una cadena de bloques, que también tiene su propia subclasificación y tipología, que pueden o no tener un valor monetario³.

1 pump.fun

2 Inclusive existe una categoría llamada shitcoin (expresión que combinan en inglés las palabras shit que significa mierda, y coin que significa moneda) que es un término peyorativo que se refiere a criptomonedas que no aportan valor al ecosistema, han fracasado o resultan un rotundo fraude. Ahora, es importante aclarar que se torna subjetivo calificar a una criptomoneda como shitcoin.

3 i) **Tokens de intercambio o pago (*payment/exchange tokens*)**: se orientan a la transferencia de valor como medio de pago o intercambio, por lo que su función económica principal es transaccional dentro o fuera de un ecosistema digital.

ii) **Tokens de utilidad (*utility tokens*)**: confieren acceso o uso a un servicio, aplicación o funcionalidad de una red/plataforma (p. ej., consumo de servicios, tarifas internas, habilitación de funciones), sin que su rasgo definitorio sea la promesa de rendimiento financiero.

iii) **Tokens de inversión o valores (*security/asset/investment tokens*)**: incorporan derechos económicos o patrimoniales comparables a instrumentos financieros (p. ej., participación, deuda, derecho a flujos, o expectativas de retorno vinculadas a un emisor/proyecto), por lo que su calificación suele depender de los derechos que estructuralmente atribuye el token.

3.1. Rug pull

Es una clase de estafa vinculada a criptoactivos, que se caracteriza porque los desarrolladores que realizan un lanzamiento de una nueva criptomoneda, abandonan repentinamente la iniciativa después de recaudar fondos, dejando a los inversores con tokens sin valor, por lo general se caracteriza por valerse de algún suceso o personaje influyente que incrementa la expectativa de la criptomoneda, que hace que los inversores compren y generen una revalorización. El jefe del laboratorio de investigación de ESET, indica que:

- iv) **Tokens no fungibles – NFT (*non-fungible tokens*):** tokens únicos que representan propiedad y/o identidad digital de un activo o derecho específico; la literatura propone taxonomías basadas en propósito, metadatos, escasez, transferibilidad y estructura del proyecto.
- vi) **Tokens semi-fungibles o multi-token (p. ej., estándares tipo ERC-1155):** permiten que un mismo identificador represente una *clase* de activos con múltiples copias, útil para ítems digitales seriadados, gaming y coleccionables con ediciones.
- vii) **Tokens de gobernanza (*governance tokens*):** otorgan derechos de decisión/voto sobre parámetros y políticas de un protocolo o comunidad (frecuentemente en estructuras tipo DAO), por lo que su valor y riesgos se relacionan con el control y el diseño de la gobernanza.
- viii) **Tokens envueltos (*wrapped tokens*):** representaciones de activos “nativos” de otra cadena o sistema, usadas para interoperabilidad y para habilitar su uso en aplicaciones DeFi (p. ej., como colateral, trading o provisión de liquidez).
- ix) **Tokens de proveedor de liquidez (*LP tokens*):** acreditan la participación de un usuario en un fondo y suelen dar derecho a comisiones y a la devolución proporcional de los activos aportados; se analizan junto con fenómenos como impermanent loss y estrategias de *yield farming*.
- x) **Liquid Staking Tokens – LST:** tokens que representan activos en staking y permiten mantener liquidez y transferibilidad mientras se siguen acumulando recompensas, integrándose además como insumo en otros protocolos de finanzas descentralizadas.
- xi) **Tokens no transferibles o “soulbound” – SBT:** tokens diseñados para ser intransferibles, utilizados como infraestructura de confianza y verificación, más que como activos orientados a negociación.
- xii) **Tokens respaldados por activos del mundo real – RWA (*asset-backed / tokenized real-world assets*):** tokens que representan derechos sobre activos fuera de la cadena, donde la clasificación depende del modelo de tokenización y de la estructura legal del derecho subyacente.

Los proyectos diseñados como estafas rug pull no siempre son obvios. Si bien encontraremos casos en los cuales el proyecto mostraba señales claras de ser un engaño (como la promesa de grandes ganancias), no siempre es así. De hecho, gran parte de los criptoactivos que terminaron siendo una estafa de rug pull fueron presentados como proyectos de inversión sólidos y no como oportunidades para obtener ganancias rápidas.” (Gutiérrez Amaya C., 2022, párr. 5).

3.2. Pump and Dump

es una práctica fraudulenta en el ámbito financiero, que consiste en inflar artificialmente el precio de un (cripto) activo, mediante manipulación y desinformación. Una vez que el precio alcanza niveles altos, los perpetradores venden sus activos, provocando el colapso del precio y dejando a los inversores desprevenidos con pérdidas significativas. Coinbase describe:

los organizadores crean o adquieren grandes cantidades de una criptomoneda de bajo valor, la promocionan para inflar artificialmente el precio del token y luego venden sus activos a participantes desprevenidos.

Téngase presente que, existe una gama más amplia de ilícitos relacionados a finanzas descentralizadas, no obstante, las dos figuras desarrolladas son las más concurrentes y con un vínculo estrecho con las MC, de manera referencial, sin ser el objeto de estudio concurrente.

4. Posición de la División de Finanzas Corporativas de la Comisión de Bolsa y Valores (SEC) de los Estados Unidos de Norteamérica

Dada la relevancia del fenómeno, el 27 de febrero de 2025 la División de Finanzas Corporativas de la Comisión de Bolsa y Valores de EE.UU. (SEC) emite una declaración sobre las MC.

4.1. Aspectos relevantes de la declaración

Describe que una MC es un tipo de activo virtual inspirado en memes⁴ de internet, personajes, eventos actuales o tendencias, donde el promotor busca atraer a una comunidad en línea entusiasta para comprar y comerciar la moneda. Aunque cada MC puede tener características únicas, generalmente comparten ciertas particularidades:

- i. Son adquiridas principalmente por entretenimiento, interacción social y propósitos culturales.
- ii. Su valor se basa principalmente en la demanda del mercado y la especulación, asemejándose a coleccionables.
- iii. Típicamente, poseen una funcionalidad limitada o nula debido a su naturaleza especulativa, suelen experimentar una volatilidad significativa en su precio de mercado y, a menudo, se acompañan de declaraciones sobre sus riesgos y falta de utilidad, salvo para fines de entretenimiento u otros propósitos no funcionales.

Lo peculiar es que, para la SEC las transacciones con las MC descritas no implican la oferta y venta de valores⁵ según las leyes federales de valores de EE.UU., motivo por el que quienes participan en esta oferta y demanda no necesitan registrar dichas transacciones bajo la Ley de Valores (1933) ni acogerse a alguna de sus exenciones de registro. En consecuencia, ni los compradores ni los poseedores de MC están protegidos por las leyes federales de valores. ¿Qué se define entonces como valor según la ley de intercambio de valores (1934)?

La ley realiza esta definición enumerando varios instrumentos financieros, incluyendo *acciones, pagarés y bonos*. Una MC no constituye ninguno de los instrumentos financieros comúnmente enumerados en la definición de "valor" porque, entre otras cosas:

4 Un meme es un elemento cultural transmisible que se propaga mediante imitación o adaptación, con dos acepciones principales según su contexto. El término fue acuñado por el biólogo Richard Dawkins en 1976.

- i. No genera un rendimiento
- ii. Ni otorga derechos a ingresos futuros, ganancias o activos de un negocio.

En suma, una MC no es en sí misma un valor.

Tabla 1: Referencias legales de los valores en Bolivia

BOLIVIA	
Definición de "Valor"	Instrumento financiero que representa derechos o participación en el capital de una empresa, deuda o inversión.
Normativa	Ley del Mercado de Valores N° 1834 de 1998
Entidad regulatoria	Autoridad de supervisión del sistema financiero (ASFI)
Clasificación	Se clasifican en valores de renta fija (bonos) y valores de renta variable (acciones). También existen otros instrumentos financieros como los certificados de participación.
Emisión	La emisión de valores debe ser autorizada por la ASFI y la Bolsa Boliviana de Valores (BBV).

Nota: Elaboración propia

4.1.1. El marco normativo boliviano

El ordenamiento jurídico vigente se articula en tres niveles:

- i. La Ley N° 1834 de Mercado de Valores, que define valor como «título o instrumento que representa derechos de participación, crediticios o de deuda»;
- ii. La Ley N° 393 de Servicios Financieros, que regula el sistema de intermediación financiera y define los instrumentos admisibles;
- iii. La normativa de la Autoridad de Supervisión del Sistema Financiero (ASFI), versada en reglamentar las empresas de tec-

nologías financieras con categorías predeterminadas, en concurrencia con resoluciones de Directorio del Banco Central de Bolivia que establecen lineamientos de orden reglamentario a diversas figuras, pero referentes a estructuras financieras.

Si bien en la normativa boliviana no existe una definición de un MC, la figura de *valor* en Bolivia dependería de si su estructura material satisface los elementos de la definición del artículo 2 de la Ley 1834 y configura oferta pública conforme al artículo 9 de la misma norma.

4.2. Tipología del contrato de inversión

La SEC, conforme a la ley de intercambio de valores norteamericana establece que los *contratos de inversión* son valores. Dado que una MC no es en sí misma un valor, se analiza, conforme al pronunciamiento de la SEC, si podría ser ofrecida y vendida como parte de un *contrato de inversión* bajo la prueba del *contrato de inversión* establecida en el caso SEC v. W.J. Howey Co (1946). El TH analiza si ciertos acuerdos o instrumentos son contratos de inversión basándose en sus "realidades económicas"⁶.

Al evaluar las realidades económicas de una transacción, la prueba de Howey considera 4 variables:

- a) Si existe una inversión en una empresa
- b) Con una expectativa razonable de ganancias
- c) Con/desde una empresa común
- d) Derivadas de los esfuerzos empresariales o gerenciales de otros⁷.

La oferta y venta de una MC no implica una inversión en una empresa ni se realiza con una expectativa razonable de ganancias derivadas de los esfuerzos empresariales o gerenciales de otros. Los compradores de MC no están realizando una inversión en una empresa; es decir, sus fondos no se agrupan para ser gestionados por promotores u otros terceros para desarrollar la moneda o una empresa relacionada.

Cualquier expectativa de ganancias que tengan los compradores de MC no se deriva de los esfuerzos de otros; es decir, el valor de las MC se deriva de la especulación comercial y el sentimiento colectivo del mercado, similar a un coleccionable. Además, los promotores de MC no están llevando a cabo (ni indican una intención de llevar a cabo) esfuerzos gerenciales y empresariales de los cuales los compradores podrían razonablemente esperar una ganancia.

No obstante, esta declaración no se extiende a la oferta y venta de MC que sean inconsistentes con las descripciones anteriores, o productos que se etiqueten como MC en un esfuerzo por evadir la aplicación de las leyes federales de valores disfrazando un producto que de otro modo constituiría un valor. Como se señaló anteriormente, la SEC evaluará las realidades económicas de la transacción particular.

Además, aunque la oferta y venta de una MC puede no estar sujeta a las leyes federales de valores, las conductas fraudulentas relacionadas con la oferta y venta de MC pueden estar sujetas a acciones de cumplimiento o enjuiciamiento por otras agencias federales o estatales bajo otras leyes federales y estatales de los Estados Unidos de América.

En consecuencia, cabe postular si el TH⁸, como estándar jurídico anglosajón es aplicable de manera inmutable en el sistema iberoamericano en concordancia con el nuevo paradigma digital, empleando como referencia a Bolivia.

7 Los tribunales federales desde el caso *Howey*, han explicado que el requisito de esfuerzos de otros se cumple cuando "los esfuerzos realizados por personas distintas al inversor son los indudablemente significativos, aquellos esfuerzos gerenciales esenciales que afectan el fracaso o éxito de la empresa".

8 Se ha realizado en base a la Securities Act de 1933.

Tabla 2: Criterio de Howey y la legislación boliviana

CRITERIO DE HOWEY	BOLIVIA
a) Inversión en una empresa	Se reconoce la inversión privada en empresas, pero no hay un marco específico que la regule como un "valor" salvo que implique la emisión de títulos regulados por la ASFI o BBV.
b) Expectativa razonable de ganancias	En contratos de inversión privados, las ganancias pueden ser esperadas, pero no necesariamente hacen que el contrato sea considerado un valor.
c) Empresa común	Conforme a la estructura del Código de Comercio, y a la tipología societaria, se debe establecer la intervención de una persona jurídica con un fin común.
d) Dependencia de esfuerzos de terceros	No existe un criterio similar en la ley, pero podría aplicarse por analogía en casos donde la inversión dependa de la gestión de terceros (por ejemplo, en fideicomisos o fondos).

Nota: Elaboración propia.

El TH aplica a cualquier contrato, esquema o transacción, independientemente de que tenga alguna de las características de los valores típicos. El foco del test no se limita a la forma y términos del instrumento en sí, sino también a las circunstancias del activo y la manera en que es ofrecido, vendido o revendido, incluyendo ventas en el mercado secundario.

El activo virtual que no es un valor (*security*) por sí mismo puede, aun así, estar sujeto a un contrato de inversión.

5. Consideraciones sobre la esencia y contenido del contrato de inversión

Contando con una aproximación de esta tipología contractual, es certero precisar que, en determinadas circunstancias, desde la teoría general del contrato, el contrato como tal sí podría ser considerado un valor; sin embargo, debe existir un nexo de causalidad con su contenido y alcances, más allá de los elementos constitutivos tradicionales. Si se quiere hacer la inferencia directa de que, un contrato de inversión *per se* es un valor, conforme a los criterios de la tabla

precedente no se identificaría congruencia, porque, debiera cumplir con las 4 variables del *TH*.

En Bolivia, el literal d) del párrafo I del Art. 9 de la Ley N° 516⁹ de promoción de inversiones, contempla que la colocación de aportes de inversión también se realiza a través de contratos.

6. Naturaleza jurídica del MC

El profesor Estévez (1956) cita:

pueden decir, no sin razón, que el tema de la naturaleza jurídica desborda su competencia, pues por su carácter general entra de lleno en el ámbito jurisdiccional del filósofo. Y el filósofo del Derecho, a quien, en efecto, correspondería estudiar esta materia, no tendrá más remedio que rendirse a la inculpación, puesto que tampoco ha consagrado su atención al problema. La ausencia de estudio sistemático en una cuestión de tan excepcional importancia basta para probar la necesidad de una investigación *iustificada* tendente a esclarecerla. Lo que no es dado hacer con sagacidad a los juristas positivos compete, y es un deber inexcusable, a los filósofos del Derecho.

Ingresando así en una valoración epistemológica, es preciso comprender qué es *naturaleza*. (Aristóteles, *Física*, II, 1, 192b21-23). apunta: “es la esencia de los seres que poseen en sí mismos principio de actividad”. (Santo Tomás de Aquino, *De ente et essentia*, cap. I). por su parte refiere: “naturaleza designa aquello que significa la definición; ahora bien, esta última indica lo que una cosa es; de donde se deduce que en su acepción ordinaria esta misma naturaleza se llama esencia o *quiddidad*”. Puede ser considerada desde las siguientes vertientes, i) rutinario ingenuo: sin una clara inquietud científica de cuestionarse a qué necesidad responde, ii) esencia: empleado casi como sinónimos, de lo que contiene a nivel epistemológico; iii) estructura: reflejando de algún modo el momento de organización que aquella idea importa; modo como es configurado por obra del derecho; iv) categoría: tipo o género, refi-

riendo al aspecto procesalista puro de la ubicación configuracional de instituto jurídico.

Por ello, para esbozar la naturaleza jurídica de un MC, se deben identificar los factores que hacen a su arquitectura axiomática:

- a) No es considerado un valor, desde la escuela anglosajona.
- b) No es una moneda de curso legal, como regla¹⁰ desde la escuela iberoamericana.
- c) Es de naturaleza especulativa.
- d) Comprende una ambigüedad regulatoria.
- e) Puede ser un medio de pago alternativo, dependiendo de la regulación jurisdiccional.
- f) Es un activo de contenido patrimonial intangible.

7. Hipótesis para establecer un nuevo estándar

El Test de Howey, desarrollado como parámetro jurisprudencial en el marco del common law estadounidense para determinar cuándo una operación financiera constituye un contrato de inversión y, por tanto, cuándo un activo debe considerarse un valor (*security*) sujeto a regulación del mercado de valores; resulta técnica y jurídicamente inaplicable en el ecosistema de activos virtuales dentro de los ordenamientos jurídicos iberoamericanos, debido a sus características configurativas.

9 La Ley precitada en el Art. 4 define la inversión como “*Toda colocación de aportes de inversión en los diferentes mecanismos de inversión de acuerdo con lo señalado en la presente Ley, destinados al desarrollo permanente de actividades económicas y a la generación de rentas que contribuyan al crecimiento y desarrollo económico y social del país.*”, así como la distinción entre inversión boliviana e inversión preferente, inversión estatal productiva, mixta y extranjera.

10 La excepción a la regla es el caso de El Salvador que estableció por ley a Bitcoin como moneda con poder liberatorio ilimitado.

a) Si existe una inversión en una empresa. En el caso de los activos virtuales, ya no es una sola empresa de un solo rubro, por su naturaleza descentralizada, pueden confluir múltiples empresas de diferentes rubros.

b) Con una expectativa razonable de ganancias. La expectativa deja de ser razonable, porque existen activos virtuales que no buscan, necesariamente un fin de lucro, sino más bien una connotación funcional; como acceso a plataformas o canales de pago). O bien, fines lúdicos, sociales y culturales. Implicando un cambio de paradigma al *valor* del activo.

c) Desde una empresa común. Por la naturaleza de una red descentralizada, no es necesario que existan una persona jurídica cerrada y exclusiva del que dependa el valor de su *activo*.

d) Derivadas de los esfuerzos empresariales o gerenciales de otros. El valor de los criptoactivos está dado; desde su intrínseca volatilidad y, al margen de las *stablecoins*; por la confianza colectiva de la gente en la validación de las transacciones a través de operaciones criptográficas.

Amerita en consecuencia, establecer un nuevo estándar que debería contener los siguientes criterios:

a) Grado de descentralización. Existen activos virtuales en diversas arquitecturas del ecosistema de tecnologías de registro distribuido, por sus iniciales en inglés DLT, que corresponden al género. La cadena de bloques es un género, que a su vez tiene otros subgéneros, pero que son ajenos a la problemática jurídica. Estas tecnologías emergentes pueden generar repercusiones económico-financieras que, a su vez cumplen diferentes funciones y tienen distintos grados de (ciber)seguridad. Respondiendo a un criterio de autosuficiencia de su protocolo. Repercutiendo con relevancia en el grado de confianza, para conocer si existe una entidad que controla la *blockchain*.

b) Teleología del token. Token entendido como una representación digital de valor, propiedad o modo de acceso. Se debe responder a ¿con qué finalidad se usa?; y a partir de ello discernir si es:

b.1. fungible o no fungible

b.2. divisible o indivisible

b.3. con contenido patrimonial o no

b.4. Su funcionalidad: de utilidad, toma de decisiones, de gobernanza, de recompensa, lúdica, etc.

b.5. Con o sin respaldo

c) Naturaleza de la expectativa lucrativa. Estando en una red abierta y descentralizada, se debe analizar si las potenciales ganancias son resultado de una actividad comunitaria, operaciones computacionales/algorítmicas y/o gestiones del emisor, sean estas proactivas o de administración.

d) Madurez tecnológica. Identificar la fase de desarrollo y operatividad de un determinado proyecto en una cadena de bloques es necesario para asignarle una ponderación específica.

e) Transparencia algorítmica. Evaluar el grado de acceso a la información que se tiene, métricas disponibles, tratamiento de datos personales y sus modelos de *compliance*.

La insuficiencia del TH para operar en el ecosistema de activos virtuales descentralizado establece la necesidad de un estándar de calificación jurídica alternativo, compatible con arquitecturas descentralizadas y con el sistema jurídico germánico.

El *test de Nakamoto (TN)* es una herramienta de calificación jurídica de aplicación subsidiaria cuando el análisis preliminar del activo, conforme a las normas vigentes del sistema financiero no brinda un resultado conclusivo respecto de si el activo o su oferta constituye un instrumento financiero regulado, implicando un precedente jurisprudencial desde el plano constitucional. Teniendo presente que en el sistema Iberoamericano un contrato de inversión puede ser considerado un valor siempre que existe un nexo causal entre el contenido y los alcances de su teleología.

El TN se estructura en dos fases y cinco criterios:

Fase I: Criterios estructurales que determinan la naturaleza del activo

a. Grado de descentralización efectiva. Se analiza si existe una entidad —persona física, jurídica o grupo identificable— que ejerza control preponderante sobre el protocolo, la emisión o el suministro del token. La descentralización efectiva excluye, en principio, la imputación del valor del activo a «los esfuerzos de terceros» en el sentido del TH. Fuentes verificables: libro blanco del proyecto (*whitepaper*), registros on-chain, documentación de gobernanza. Umbral: si más del 50% de los nodos validadores, del suministro total o de los derechos de gobernanza están concentrados en un solo agente o grupo coordinado, se presume centralización relevante.

b. Teleología del token (finalidad funcional). Se determina si el token incorpora derechos económicos exigibles (participación, dividendo, deuda) o si su uso primario es utilitario, cultural o lúdico. La presencia de derechos económicos exigibles aproxima el activo a un valor negociable con independencia de su denominación. Metodología: análisis del *whitepaper*, los contratos inteligentes (*smart contracts*) y las representaciones públicas del emisor o promotor. Subcriterios: (a) fungibilidad; (b) divisibilidad; (c) contenido patrimonial exigible; (d) funcionalidad predominante; (e) existencia de respaldo.

Fase II: Criterios de oferta que determinan la naturaleza de la operación

c. Naturaleza de la expectativa lucrativa. Se evalúa si las representaciones del emisor o promotor generan en el adquirente una expectativa razonable de rendimiento económico derivada de los esfuerzos de un tercero identificable. La expectativa meramente especulativa o derivada del sentimiento colectivo del mercado no satisface este criterio. Indicadores negativos: ausencia de promesa de retorno; advertencias explícitas de falta de utilidad financiera; ausencia de hoja de ruta (*roadmap*) con compromisos de desarrollo.

d. Madurez tecnológica del proyecto. Se identifica la fase de desarrollo en que se realiza la oferta. Las ofertas en fase de pre-lanzamiento o desarrollo (*pre-mainnet*) con captación de fondos del público presentan un perfil regulatorio de mayor riesgo, toda vez que la expectativa de rendimiento depende necesariamente de la actuación futura del equipo promotor. Este criterio opera como factor de ponderación de los criterios anteriores: a menor madurez tecnológica, mayor peso se asigna a los indicios de expectativa lucrativa.

e. Transparencia algorítmica y de gobernanza. Se evalúa la disponibilidad pública del código fuente, de los mecanismos de gobernanza *on-chain* y de las métricas de actividad de red. La opacidad algorítmica, combinada con representaciones de rendimiento, constituye un indicio calificado de asimetría informativa en perjuicio del adquirente, relevante para la aplicación de normas de protección al inversor y de prevención de fraude.

Este test no pretende desplazar las normas vigentes ni operar como fuente autónoma de derecho, sino constituir una herramienta hermenéutica que permite al operador jurídico navegar la laguna normativa que caracteriza el tratamiento de los activos virtuales en Bolivia y el sistema jurídico iberoamericano, dotando de contenido operativo a los conceptos del derecho financiero en el contexto del ecosistema digital financiero descentralizado.

8. Aplicación del Test de Nakamoto en el derecho occidental

Un criterio relevante es desarrollar la aplicabilidad de la problemática que se establece del TH (de origen jurisprudencial anglosajón) en el sistema jurídico germánico occidental.

Como estándares relevantes, se aborda la cuestión desde un paradigma completamente distinto: el de MiCA y MiFID II¹¹. Las criptomonedas tradicionales son activos volátiles y especulativos que no son activos financieros en sentido estricto.

El derecho germánico-europeo opera con una taxonomía tripartita:

a) Tokens referenciados a activos (ART): *Stablecoins* respaldados por activos reales.

b) Tokens de dinero electrónico (EMT): Vinculados a monedas fiduciarias.

c) Otros criptoactivos (incluyendo memecoins): proporcionan acceso a productos o servicios digitales y, a diferencia de los *security tokens*, no tienen la consideración de instrumento financiero bajo la normativa de valores en muchos países. Los *security tokens* quedan regulados por MiFID II, no por MiCA.

9. Implicancias de un MC como valor en un contrato de inversión en el derecho occidental

Existen implicancias en la aplicación de las consideraciones de la determinación financiera de las MC en el derecho occidental iberoamericano.

9.1. Regulatorio-normativo

El reglamento MiCA está diseñado para crear un marco unificado para todos los activos digitales, con foco en transparencia, protección de inversores y garantía de cumplimiento de normas AML y KYC.

Si un MC estaría en la categoría de otros criptoactivos, su emisor necesita publicar un documento técnico antes de la oferta al público. Si no está alcanzado por MiCA no aplican esas obligaciones, pero tampoco sus protecciones.

11 MiFID II (Directiva 2014/65/UE) es la normativa europea vigente desde 2018 que regula los mercados financieros, servicios de inversión y protección al inversor. Sus objetivos clave son aumentar la transparencia, mejorar la competencia y garantizar que los productos financieros comercializados sean idóneos para el perfil del cliente, evitando malas prácticas

9.2. Conducta de mercado

Si la transacción de MC se estructura como un servicio de inversión bajo MiFID II, entonces ese servicio queda sujeto a la directiva de mercados financieros, aunque el activo subyacente no sea un instrumento financiero *per se*.

9.3. Defensa al consumidor

Se identifica una asimetría jurídica, desde la supletoriedad de la Ley N° 453 de defensa del consumidor y estándares internacionales, que consiste en que ni los compradores ni los tenedores de MC quedan protegidos jurídicamente.

Por ello, la razón de ser de los contratos de inversión es que capturan la realidad económica independientemente de la forma jurídica. Bajo el TH, "la forma se ignora en favor de la sustancia y el énfasis recae en la realidad económica." El Tribunal Supremo Norteamericano ha explicado que el término security o valor "encarna un principio flexible más que estático" para adaptarse a los incontables y variables esquemas ideados por quienes buscan el dinero de otros con la promesa de ganancias, haciendo hincapié a la cuarta variable del TH y su aplicabilidad en subcategorías de activos virtuales.

Así, este nuevo test permite establecer con verosimilitud la naturaleza jurídica de las MC para salvaguardar de manera más óptima la dimensión correspondiente de la seguridad jurídica en el entorno de empresas de tecnologías financieras.

10. Referencias

- Aristóteles. (1995). *Física* (G. R. de Echhandía, Trad.). Gredos. (Obra original ca. 350 a. C.)
- Blackmore, S. (1999). *The Meme Machine*. Oxford University Press.
- Coinbase. (s.f.). *¿Qué es un pump and dump en cripto?* Coinbase Learn. <https://www.coinbase.com/es-la/learn/crypto-glossary/what-is-a>

pump-and-dump-in-crypto

Dawkins, R. (1976). *The Selfish Gene*. Oxford University Press.

Estévez, J. L. (1956). *Sobre el concepto de naturaleza jurídica*. [Documento académico]. <https://dialnet.unirioja.es/servlet/articulo?codigo=2057273>

Gutiérrez Amaya, C. (2022, 26 de julio). *Qué es Rug pull: un modelo de estafa en torno a las criptomonedas*. ESET. <https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/que-es-rug-pull-un-modelo-de-estafa-en-torno-a-las-criptomonedas/>

Swiss Financial Market Supervisory Authority (FINMA). (2018, February 16). *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*. <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>

Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). (2023, abril). *Guía práctica para la identificación, trazabilidad e incautación de cryptoactivos: Consideraciones teórico-prácticas sobre activos virtuales basados en la tecnología de cadena de bloques y su investigación penal*. Ministerio Público Fiscal de la Nación (Argentina).

Tomás de Aquino. (1985). *El ente y la esencia* (A. García Marqués y J. M. García Valverde, Trans.). Cuadernos de Anuario Filosófico, Universidad de Navarra. (Obra original ca. 1252)

U.S. Supreme Court. (1946). *SEC v. W.J. Howey Co.*, 328 U.S. 293. <https://supreme.justia.com/cases/federal/us/328/293/>

U.S. Securities and Exchange Commission. (2025, February 27). *Staff statement on meme coins*. Division of Corporation Finance. <https://www.sec.gov/newsroom/speeches-statements/staff-statement-meme-coins>

Los desafíos de la trazabilidad en la era de las black boxes

The Challenges of Traceability in the Era of Black Boxes

► **Mariana Soria Galvarro Gaillard**

Católica Global School of Law • Lisboa, Portugal

<https://orcid.org/0009-0009-2960-3052> • marianagaillard@gmail.com

Revista de Derecho de la UCB – UCB Law Review, Vol. 10 N° 18, abril 2026, pp. 179-193

ISSN 2523-1510 (en línea), ISSN 2521-8808 (impresa).

DOI: <https://doi.org/10.35319/lawreview.202618139>

Recibido: 31 de octubre de 2025 • Aceptado: 16 de abril de 2026

Resumen

El presente artículo realiza una revisión crítica al AI Act, centrandolo en el análisis de la estructura funcional que éste establece, a través de la cual, asigna roles y responsabilidades diferenciadas a los distintos actores de la cadena de valor de los sistemas de inteligencia artificial. Principalmente, examina la distribución de obligaciones a lo largo del ciclo de vida de dichos sistemas, con especial atención a los contextos de opacidad algorítmica en los sistemas de tipo Black Box, en los que los procesos decisionales internos resultan inaccesibles o complejos de reconstruir incluso para sus propios desarrolladores. Se plantea si el AI Act puede garantizar una atribución efectiva de responsabilidades frente al avance tecnológico y la proliferación de contenido sintético, dado que la trazabilidad técnica se torna progresivamente más difícil. La tesis central sostiene que una posible solución consiste en robustecer el entramado probatorio e incorporar la figura del Logger, lo que permitiría conservar evidencia del proceso decisional y prevenir que las obligaciones establecidas en el AI Act se reduzcan a una categoría formal e ineficaz. Sin embargo, concluye en que la implementación práctica enfrenta un desafío sustancial; pues,

el descomponer exhaustivamente la cadena de decisiones de un sistema de IA, cuando su diseño prioriza la eficiencia sobre la explicabilidad, sería, en muchos casos, incompatible con la propia lógica operativa de eficiencia.

Palabras clave: AI Act; Black Boxes; contenido sintético; opacidad algorítmica; responsabilidad; trazabilidad.

Abstract

This article offers a critical examination of the AI Act, centering its analysis on the functional framework it establishes and the way it allocates distinct roles and responsibilities to the several actors involved in the value chain of artificial intelligence systems. In particular, it examines the distribution of obligations throughout the lifecycle of such systems, with special attention to contexts of algorithmic opacity in Black Box systems, where internal decision-making processes are inaccessible or difficult to reconstruct, even for their own developers. The article questions whether the AI Act can ensure effective attribution of responsibilities in light of technological advancement and the proliferation of synthetic content, given that technical traceability becomes increasingly challenging. The central argument posits that a possible solution lies in strengthening the evidentiary framework and incorporating the figure of the Logger, which would allow for the preservation of decision-making records and prevent obligations from being reduced to a merely formal and ineffective categories. Nevertheless, it concludes that practical implementation poses a significant challenge; because the exhaustive decomposition of an AI system's decision-making chain, when its design prioritizes efficiency over explainability, would, in many cases, be incompatible with the very operational logic of efficiency.

Keywords: AI Act; Black Boxes; synthetic content; algorithmic opacity; responsibility; traceability.

1. Confiar sin cuestionar

Si un modelo de aprendizaje automático ofrece un alto rendimiento, ¿por qué no limitarse a confiar en sus resultados sin cuestionar los motivos detrás de sus decisiones? El problema es que una sola métrica, como la exactitud de clasificación, es una descripción incompleta de la mayoría de las tareas del mundo real (Doshi-Velez & Kim, 2017).

El despliegue masivo de la inteligencia artificial (IA) plantea desafíos concretos para la atribución de responsabilidad en el Derecho contemporáneo. Sin duda, estamos viviendo algo que no se trata propiamente de una crisis ontológica del orden jurídico, pero sí de un desafío esencialmente práctico y probatorio; pues la IA difumina la autoría y erosiona la trazabilidad del contenido, dificultando la identificación del sujeto responsable de los sistemas de IA a partir de sus roles establecidos en el marco principal del presente artículo, que es el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de la Unión Europea, relativo a la inteligencia artificial (en adelante, el AI Act).

Antes de avanzar, conviene precisar que, a lo largo de este artículo, el término “responsabilidad” se emplea exclusivamente en el sentido de atribución de roles, funciones o cargos, y no como responsabilidad civil derivada de la reparación de daños ocasionados por el uso de sistemas de IA. Esta última, a la fecha, no se encuentra configurada como un régimen jurídico específico. En consecuencia, toda referencia que se haga a las responsabilidades de los distintos actores de los sistemas referidos, deberá entenderse exclusivamente como las obligaciones propias derivadas del cargo o rol específico que cada uno ocupa dentro de la cadena de valor, y no como una noción derivada del concepto de *liability* propio del Derecho de daños.

En ese entendido y regresando a la problemática de la referida trazabilidad; en definitiva, si bien la IA desempeña hoy un papel central en la automatización y optimización de la creación de contenidos en múltiples ámbitos, esta transformación digital exige, a su vez, la implementación de salvaguardas que permitan validar

la autenticidad de la información. Especialmente, en un contexto donde crece la producción y circulación de información sintética mediante modelos avanzados como las GANs¹, se requiere de instrumentos técnicos que transformen *outputs* opacos en cadenas de responsabilidad verificables.

En efecto, hoy en día, se están implementando métodos de validación de fidelidad estadística que garantizan que los datos sintéticos reflejen correctamente las relaciones y características de los datos reales. Paralelamente, se están diseñando marcos de auditoría que establecen salvaguardas socio-técnicas críticas, permitiendo evaluar tanto la integridad técnica como el impacto social de los conjuntos de datos sintéticos (Ghiurău & Popescu, 2025). Sin embargo, y pese a dichos esfuerzos, la velocidad y complejidad de los sistemas de IA dificultan significativamente la demostración técnica efectiva de estas salvaguardas o intentos de ellas. La actualización constante de modelos y datos, junto con la opacidad de muchas arquitecturas, limita la trazabilidad y la verificación *ex post* en tiempos compatibles con la supervisión regulatoria.

En línea con lo anterior y en el marco del AI Act, se plantea una problemática compleja: por un lado, se atribuye de forma abstracta una personalidad funcional a sistemas que, sin ser sujetos jurídicos, despliegan capacidades decisorias; por otro, los responsables de sistemas de IA asumen una responsabilidad condicionada por la opacidad algorítmica. En consecuencia, al momento de rendir cuentas, con frecuencia carecen del control o de la comprensión necesarios para explicar y demostrar cómo se generan las decisiones.

- 1 Las redes generativas adversativas (RGAs), también conocidas como GANs en inglés, son una red generativa adversarial. Es un modelo de Machine Learning diseñado para generar datos realistas mediante el aprendizaje de patrones a partir de conjuntos de datos de entrenamiento existentes. Opera dentro de una infraestructura de aprendizaje no supervisado mediante el uso de técnicas de aprendizaje profundo, donde dos redes neuronales trabajan en oposición: una genera datos, mientras que la otra evalúa si los datos son reales o generados (Varughese, 2026).

Si bien el principio antropocéntrico establecido en el AI Act afirma que los sistemas de IA deben servir al ser humano, respetar su dignidad, autonomía y derechos fundamentales, y permanecer bajo control humano efectivo a lo largo de todo su ciclo de vida (Parlamento Europeo y Consejo de la Unión Europea, 2024); este principio rector, requiere que la atribución de responsabilidades sea materialmente verificable, pues la mera asignación formal de deberes resulta insuficiente si no se acompaña de mecanismos probatorios y técnicos que permitan rastrear la procedencia de los *outputs* sintéticos y demostrar el control efectivo de los actores implicados.

¿De qué sirve hablar de personalidad humana si no puedo entender, trazar ni demostrar lo que se me exige?

Por ello, en este artículo, se propone una mirada crítica a la atribución de roles y responsabilidades establecidas por el AI Act; pues, más allá del diseño normativo, el problema aparece cuando esa arquitectura debe operar en contextos donde rastrear, controlar y, sobre todo, probar la influencia sobre resultados – en su mayoría sintéticos – se vuelve cada vez más difícil.

2. La “personalidad” funcional de la IA

En ciertos contextos, resulta legítimo hablar de una “personalidad electrónica” sin el fin, lógicamente, de atribuir conciencia o derechos a la IA, sino para reconocer que muchas decisiones nacen de una interacción compleja entre modelos, datos y operadores humanos, configurando así una hibridación funcional humano-máquina. Esto no supone, desde luego, reconocer personalidad jurídica a la IA ni exonerar a los seres humanos de responsabilidad; más bien pone de manifiesto una crisis en la atribución de obligaciones cuando las operaciones tecnológicas desbordan los parámetros de la práctica tradicional.

Dada la velocidad operativa de los sistemas de IA, la respuesta normativa y doctrinal debería orientarse a reforzar y reconfigurar

los instrumentos probatorios y técnicos que permitan esclarecer la contribución relativa de cada interviniente y evitar así una forma de “responsabilidad a ciegas”.

Una de las razones principales para motivar el desarrollo e implementación de estos instrumentos probatorios técnicos, es que permitirían que los derechos de reclamación y explicación previstos en los artículos 85 y 86 del AI Act no queden en lo meramente formal, sino que se ejerzan de forma efectiva.

En particular, el artículo 86 reconoce el derecho a recibir explicaciones claras sobre cómo un sistema influyó en una decisión, lo que plantea una dificultad de fondo; lo cual nos conduce a la ardua tarea de cómo justificar resultados generados con información mayoritariamente sintética, generada automáticamente, no elaborada por humanos, y que no puede (dada su limitación técnica) ser reconstruida, revisada ni contrastada con un responsable humano identificable (aunque haya un deber de *human oversight*). A ello, se suma el uso de modelos opacos o *Black Boxes* cuyos resultados no permiten comprender de manera clara el razonamiento seguido.

En suma, el problema no es meramente técnico, sino profundamente procedimental, cíclico y de gran magnitud, pues no hay explicación sin responsable, no hay responsable sin capacidad real de comprensión y control del sistema; y, sin todo ello, el derecho a la explicación corre el riesgo de vaciarse de contenido y convertirse en una garantía difícil, cuando no imposible, de materializar.

3. Comprendiendo la opacidad algorítmica en sistemas de aprendizaje automático

Antes de adentrarse en la estructura de roles diseñada por el AI Act, resulta imprescindible precisar qué debe entenderse por opacidad algorítmica a lo largo del presente artículo.

Jenna Burrell, reconocida investigadora y profesora en la *School of Information* de la Universidad de California, Berkeley, la define como la incapacidad para conocer cómo y por qué un sistema algorítmico produce determinados resultados (*outputs*) a partir de sus datos de entrada (Burrell, 2016).

Burrell distingue tres formas de opacidad: (i) secreto corporativo, entendido como protección propietaria o confidencialidad empresarial; (ii) analfabetismo técnico, esto es, la ilegibilidad del código y la falta de competencias de programación en la mayoría de los públicos; y (iii) opacidad intrínseca del *machine learning*, que deriva de la desalineación entre los procedimientos matemáticos de los modelos y las formas humanas de interpretación semántica (Burrell, 2016).

En línea de lo anterior, en el ámbito del aprendizaje automático, los modelos entrenados con grandes volúmenes de datos generan correlaciones complejas que no siempre reflejan relaciones causales, dando lugar a sistemas de tipo *black box* cuya lógica interna permanece opaca e inaccesible (Burrell, 2016). Un modelo *black box* es un sistema que no revela sus mecanismos internos. En el ámbito de *machine learning*, el término *black box* se utiliza para describir un modelo que no se puede entender observando sus parámetros (por ejemplo, una red neuronal). Lo opuesto a un *black box* a veces se llama *white box*, también referidos como modelos interpretables (Molnar, 2019).

Naturalmente, esta opacidad algorítmica dificulta la trazabilidad, complica la auditoría y dispersa la responsabilidad entre múltiples actores; e incrementa riesgos sociales relevantes, como discriminación, exclusión y desinformación. Condicionando la confianza y el uso de la información generada.

4. Sujetos regulados y atribución de responsabilidad en el AI Act

Sentado el necesario preámbulo sobre la opacidad algorítmica y sus inherentes dificultades interpretativas; entremos de lleno en el Reglamento, el cual, conforme habíamos adelantado, despliega una cadena escalonada de responsabilidades entre los distintos actores de los sistemas de IA.

Dentro de la arquitectura establecida en el AI Act, el artículo 3, define las principales categorías de actores regulados en el ecosistema de la IA, incluyendo al proveedor, implantador (o usuario profesional), importador, distribuidor y representante autorizado; que, en conjunto, articulan un sistema integral de control a lo largo del ciclo de vida de los sistemas de IA. Sin embargo, el análisis conjunto revela una tensión estructural; mientras la normativa define con precisión las obligaciones formales de cada sujeto, la verificación material de su cumplimiento se diluye progresivamente, generando una trazabilidad fragmentada y, en última instancia, opaca.

El punto de partida lo constituye el Proveedor. Conforme al artículo 16, este actor asume la carga normativa más intensa, pues debe garantizar los requisitos técnicos y de seguridad, implementar sistemas de gestión de calidad, conservar documentación y registros, realizar evaluaciones de conformidad, emitir la declaración UE de conformidad y colocar el Marcado CE. Esta concentración de obligaciones lo sitúa como el nodo originario de la responsabilidad, desde el cual se proyecta la legitimidad del sistema hacia el resto de la cadena.

Mencionado anteriormente, el Marcado CE es, en primer término, una declaración jurídica de conformidad. Indica que el Proveedor afirma que el producto o sistema cumple los requisitos aplicables de la normativa de la UE. En suma, opera como un régimen de conformidad armonizado. Su función es doble, pues, por un lado, habilita la libre circulación del sistema dentro de la Unión; por otro, opera como punto de anclaje probatorio frente a las autoridades.

Sin embargo, su eficacia debe ser matizada. El Mercado CE se apoya en una presunción de conformidad que descansa en procedimientos de evaluación previos, pero cuya verificación sustantiva es limitada. En la práctica, el control se centra en la existencia de documentación y registros, sin garantizar el acceso a la lógica interna del sistema ni a los flujos de datos que determinan su comportamiento. De este modo, el mercado puede generar una apariencia de seguridad regulatoria que no siempre se corresponde con una trazabilidad efectiva.

A partir de este punto, la cadena de responsabilidades se despliega en actores cuya función es, en gran medida, de verificación y transmisión.

Consiguientemente, el Representante Autorizado, previsto en el artículo 22, actúa como extensión operativa del Proveedor cuando este se encuentra fuera de la Unión. Su papel consiste en servir de interlocutor con las autoridades y ejecutar las tareas delegadas. No obstante, su capacidad de control es estructuralmente limitada: depende de la documentación proporcionada por el propio Proveedor y carece de herramientas autónomas para verificar la conformidad técnica. En consecuencia, más que un garante sustantivo, se configura como un canal formal de comunicación, añadiendo un eslabón adicional a la cadena sin reforzar significativamente la capacidad de supervisión.

El siguiente escalón lo ocupan el Importador y el Distribuidor, cuyas obligaciones, establecidas en los artículos 23 y 24, refuerzan la dimensión documental del control. El Importador, responsable de introducir el sistema en el mercado de la UE, debe verificar la existencia de la evaluación de conformidad, la documentación técnica, la declaración UE de conformidad y el Mercado CE. Esta función es decisiva, pues su actuación habilita la entrada legal del sistema en el mercado. Sin embargo, su capacidad de evaluación es esencialmente formal; no dispone de medios para auditar de manera independiente la conformidad técnica ni la calidad de los procesos subyacentes.

El Distribuidor, por su parte, asume un rol posterior y correctivo. Debe asegurar que el sistema mantiene el Mercado CE y la documentación correspondiente, así como garantizar que las condiciones de almacenamiento y transporte no comprometan su conformidad. Ante indicios de incumplimiento, debe actuar retirando o corrigiendo el producto y colaborando con las autoridades. Aunque introduce una segunda instancia de control, su alcance es igualmente limitado: su intervención se basa en la documentación recibida y en verificaciones externas, sin acceso a auditorías profundas del sistema.

En conjunto, ambos actores evidencian un fenómeno de “traslado de complejidad”; cada nivel de la cadena verifica formalmente lo recibido del anterior, pero ninguno puede penetrar plenamente en la dimensión técnica del sistema. Así, la conformidad se reproduce como una cadena de confianza documental más que como un proceso de validación sustantiva, lo que incrementa la opacidad a medida que el sistema avanza hacia su puesta en el mercado.

Finalmente, el Implantador, regulado en el artículo 26, constituye el último eslabón y, paradójicamente, uno de los más críticos. Como usuario del sistema bajo su autoridad, asume obligaciones operativas relevantes, como: garantizar el uso conforme a las instrucciones del Proveedor, implementar supervisión humana, verificar la idoneidad de los datos bajo su control y monitorear el funcionamiento del sistema, informando sobre riesgos o incidentes. En este sentido, se configura como la última línea de defensa frente a fallos o impactos adversos.

Como se pudo ver, en conjunto, el modelo escalonado del AI Act mantiene una coherencia formal, roles definidos, obligaciones encadenadas y el Mercado CE como una suerte de prueba de conformidad; pero descansa en una lógica predominantemente documental. Esta dependencia debilita su eficacia, pues la trazabilidad se vuelve progresivamente opaca y el sistema se aproxima más a una presunción de cumplimiento que a un control material efectivo, dejando abiertas dudas sobre la atribución real de responsabilidad en entornos de alta complejidad tecnológica.

Como resulta evidente, la cadena de responsabilidades dentro de un sistema de IA, se degrada hasta quedar en una simple transmisión, acompañada de una verificación débil e ineficaz.

5. El rol no contemplado para la trazabilidad de sistemas de IA: el *Logger*

5.1 Un intento fallido: AI Liability Directive (AILD)

En este contexto de tensiones estructurales y limitaciones en la trazabilidad efectiva de responsabilidades, resulta especialmente revelador observar la evolución y eventual abandono de los instrumentos normativos complementarios diseñados para reforzar el sistema.

La retirada de la propuesta de AI Liability Directive (AILD) (Comisión Europea, 2022) evidencia la fragilidad del marco regulatorio de la IA actual. El diseño propuesto del AILD ofrecía, principalmente, una vía práctica para articular presunciones de responsabilidad derivadas del incumplimiento de deberes de diligencia y una posterior reparación de daños civiles.

Su propósito original era abordar deficiencias fundamentales en la legislación de responsabilidad vigente (ahora sí refiriéndonos a *liability*) al tratar los daños causados por sistemas de IA. No obstante, se reconoció que las normas locales de responsabilidad actuales, basadas principalmente en conceptos tradicionales de culpa, resultaban inadecuadas para la compleja realidad de la tecnología de IA moderna (Ashkara, 2025). En suma, no bastaba con afirmar que la responsabilidad seguía siendo humana.

5.2 *Logger*

A la luz de lo anterior, y ante la proliferación de contenido sintético, la dificultad para seguir el rastro de los *outputs* generados por

Black Boxes hace que la mera asignación de roles y la atribución formal de responsabilidad resulten verdaderamente insuficientes cuando los roles designados carecen de control efectivo sobre la generación, procedencia y circulación de dicho contenido, especialmente el sintético.

En el AI Act, los deberes de supervisión y verificación recaen en quienes desarrollan, integran o comercializan sistemas de IA, con el Mercado CE como referencia central. Sin embargo, la opacidad técnica y la fragmentación de la cadena limitan la eficacia de este esquema; los roles definidos carecen de registros verificables que respalden la responsabilidad en caso de infracción. Esto evidencia la necesidad de una figura similar a un *Logger*, encargada de custodiar de manera neutral la integridad, disponibilidad y verificabilidad de los registros de los sistemas de IA.

La idea de un *Logger* para los sistemas de IA encuentra inspiración en experiencias consolidadas en otros sectores altamente regulados, como el financiero o el de pagos electrónicos, donde existen entidades o mecanismos dedicados a la auditoría independiente, la conservación de logs y la verificación ex post de operaciones sensibles. Su papel consiste en materializar y preservar registros inmutables, incluyendo entradas, salidas, versiones, metadatos y condiciones operativas, responder a consultas mediante pruebas verificables (por ejemplo, hashes, firmas digitales o snapshots) y mantener la integridad de la cadena de custodia, garantizando así la trazabilidad y evidencia confiable a lo largo del ciclo de vida del sistema (Alda Rodríguez, Díaz López de la Llave, & Horrillo, 2026).

Estas pruebas retenidas en custodia por el *Logger*, permitirían a los auditores, actuando como verificadores, validar eficientemente los resultados. Como custodio neutral que materializa, sella y preserva registros técnicos verificables, el *Logger* permite reconstruir la génesis y evolución de los outputs sin sacrificar necesariamente la eficiencia operativa.

El *Logger* podría, entre otras potenciales funciones: mantener registros auditables e inmutables (*logs*, *hashes*) con conservación mínima legal. Esto reforzaría el esquema de roles agregando a

este actor como quien materializa y custodia registros que pueda proveer a los auditores (Alda Rodríguez, Díaz López de la Llave, & Horrillo, 2026). Recopilando documentación como resultado de los deberes de conservación, especialmente la relativa a los sistemas de IA de alto riesgo; preservando, por ejemplo, las *Model Cards* y *Data Sheets* como herramientas valiosas para el cumplimiento (Song, 2026).

Para su implementación, los sistemas de IA que opten por adoptar estándares elevados de diligencia podrían institucionalizar la figura del *Logger* como un rol técnico-jurídico clave dentro de la cadena de valor del AI Act, adaptado a sus marcos regulatorios nacionales y asignado a entidades públicas o privadas debidamente acreditadas. Esta función permitiría garantizar la trazabilidad y conservación verificable de los procesos decisionales de los sistemas de IA, condición indispensable para auditorías y ejercicio efectivo del derecho al reclamo y justificación de decisiones previsto en el Reglamento.

En efecto, aunque el AI Act se concibe como un marco esencialmente preventivo, su verdadera eficacia se dirime en el ámbito *ex post*, donde la posibilidad de atribuir responsabilidades y evaluar consecuencias, revela si la gobernanza algorítmica cumple, o no, su promesa regulatoria.

6. Conclusión

¿De qué sirve invocar la personalidad humana si no es posible comprender, rastrear ni demostrar aquello que se exige? La IA opera con una suerte de personalidad funcional; actúa, decide y ejecuta, mientras que el ser humano, en muchos casos, se limita a traducir sus efectos.

En definitiva, sin instrumentos que traduzcan la exigida centralidad humana en control verificable y trazabilidad causal, las responsabilidades asignadas por el AI Act se tornan meramente formales.

La retirada de la AILD es muestra clara de la fragilidad del marco regulatorio vigente, ya que los sistemas de IA generan decisiones y realidades sintéticas con una complejidad y velocidad que superan los límites de los tradicionales regímenes de culpa y responsabilidad. Así, mientras hoy podemos hablar de atribuciones y responsabilidades, con las complejidades que eso implique, en el futuro, si hablamos de *liability* plena, nos enfrentaremos a un problema estructural, pues no habrá medios probatorios suficientes para asegurar que los daños civiles sean reparados.

Cerrar esta brecha exige complementar la conformidad formal con evidencia técnica verificable e incorporar la figura del *Logger*. De esta manera (si es que acaso existe una salida perfecta frente al fenómeno que estamos viviendo) la conformidad puede transformarse en responsabilidad revisable, por tanto, exigible; y no una mera declaración. Aun cuando la descomposición exhaustiva de la cadena decisoria contradiga la lógica operativa de eficiencia para la cual los sistemas de IA fueron diseñados.

7. Referencias

- Alda Rodríguez, Á., Díaz López de la Llave, G., & Horrillo, P. (2026). Construyendo un log verificable, parte 1: Ideas principales. BBVA. <https://www.bbva.com/es/innovacion/construyendo-un-log-verificable-parte-1-ideas-principales/>
- Ashkara, Z. (2025). AI liability directive withdrawn: EU impact 2025. AI Act Blog. <https://www.aiactblog.nl/en/posts/ai-liability-directive-withdrawal>
- Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1). <https://doi.org/10.1177/2053951715622512>
- Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning (arXiv:1702.08608). arXiv. <https://doi.org/10.48550/arXiv.1702.08608>
- Ghiurău, D., & Popescu, D. E. (2024). Distinguishing Reality from AI:

- Approaches for Detecting Synthetic Content. *Computers*, 14(1), 1. <https://doi.org/10.3390/computers14010001>
- Molnar, C. (2019). *Interpretable machine learning: A guide for making Black Box models explainable*. Leanpub. <https://christophm.github.io/interpretable-ml-book/>
- Comisión Europea. (2022). Propuesta de Directiva del Parlamento Europeo y del Consejo sobre normas de responsabilidad civil extracontractual en materia de inteligencia artificial (COM (2022) 496 final)(AI Liability Directive). <https://eurlex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0496>
- Parlamento Europeo y del Consejo de la Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (AI Act). *Diario Oficial de la Unión Europea*. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689>
- Song, P. (2026). Model cards and data sheets: documentation standards for ML. *ML Journey*. <https://mljourney.com/model-cards-and-data-sheets-documentation-standards-for-ml/>
- Varughese, J. (2026). ¿Qué son las redes generativas adversariales (GAN)? IBM. <https://www.ibm.com/mx-es/think/topics/generative-adversarial-networks>

Políticas Editoriales

Editorial Policies

Revista de Derecho de la UCB

UCB Law Review

Historia y misión

La revista inicia su primera publicación en el año 2017. Está a cargo del Instituto para la Democracia de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Boliviana “San Pablo” (UCB), sede La Paz.

La revista tiene por misión la difusión de investigaciones jurídicas, científicas y originales, con el objetivo de contribuir al conocimiento del Derecho, al desarrollo, al diálogo plural y la generación de buenas prácticas jurídicas en el marco del respeto a los derechos humanos. Está dirigida a académicos, estudiantes y practicantes del Derecho, así como a hacedores de políticas públicas. Las publicaciones de la revista tienen primordialmente naturaleza teórica, deóntica, práctica y aplicada en relación con el análisis jurídico local, regional y global.

Líneas de investigación

Las principales líneas de investigación de la revista son:

1. Derecho social, trabajo, familia, niñez y adolescencia.
2. Filosofía, historia, ética y moral.
3. Derechos humanos, pluralismo, tutela jurídica, justicia y cultura de paz.
4. Derecho patrimonial civil y comercial.
5. Medio ambiente, recursos naturales y energías.
6. Institucionalidad, administración, derecho sancionatorio, relaciones internacionales y soberanía.

Frecuencia de publicación

La revista se publica de forma impresa (ISSN 2521-8808) y digital en lawreview.ucb.edu.bo (ISSN 2523-1510) semestralmente los meses de abril y octubre, aunque también puede publicar números especiales no periódicos.

Política de acceso abierto

La Revista de Derecho de la U.C.B. es una revista de acceso abierto.

La licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0) permite a cualquier persona leer, descargar, copiar, distribuir y adaptar los contenidos publicados, siempre que se otorgue el debido

reconocimiento a la autoría original. No se autoriza el uso de la obra ni de sus derivados con fines comerciales y, en caso de generarse obras derivadas, estas deben difundirse bajo la misma licencia. Este esquema promueve el acceso abierto al conocimiento, garantizando al mismo tiempo el respeto a los derechos de autor y la circulación responsable de la producción académica.

Declaración de privacidad

La Revista de Derecho de la U.C.B no comunicará ni transferirá a terceros los datos personales de sus usuarios sin consentimiento expreso de su titular. Se salva el caso de requerimiento judicial.

Condiciones Generales

Se entiende por *manuscrito* el texto original propuesto para su publicación en la revista.

El envío de un manuscrito para su consideración implica la autorización para su eventual publicación y difusión en formato digital e impreso, la cesión no exclusiva de los derechos de autor para su divulgación, así como la aceptación de las normas editoriales establecidas por la Universidad Católica Boliviana “San Pablo” (UCB) y por la revista, con el correspondiente sometimiento a ellas.

El contenido, los datos y las opiniones expresadas en los manuscritos son de exclusiva responsabilidad de sus autores y no reflejan necesariamente la posición institucional de la UCB, del Instituto para la Democracia, de los editores ni de la revista.

Las investigaciones presentadas deben cumplir con los estándares establecidos para la revisión por pares académicos, ser originales, corresponder en su autoría a quienes figuren en el manuscrito y observar las normas éticas y de integridad académica. Asimismo, los textos no deben haber sido publicados previamente ni estar en proceso de evaluación en otro medio, salvo los casos expresamente permitidos en la sección ética y buenas prácticas.

Las personas autoras deberán identificarse indicando su afiliación institucional. En caso de no tenerla, deberán declararse investigadores independientes. Además, deberán incluir su número de registro ORCID, el cual puede obtenerse en <https://orcid.org>.

Los idiomas oficiales de publicación son el español y el inglés; sin embargo, la revista se reserva el derecho de aceptar publicaciones en otros idiomas.

La revista publicará prioritariamente investigaciones que hayan sido evaluadas de forma anónima y favorable en su mérito formal, sustantivo y metodológico por pares académicos. En cada publicación se consignarán las fechas de recepción y aprobación del manuscrito.

Todas las comunicaciones entre la revista, los autores y las instancias evaluadoras se realizarán por correo electrónico.

La recepción de manuscritos es continua. La revista se reserva la facultad de determinar el orden y el momento de publicación de los textos aprobados, considerando los tiempos naturales del proceso de revisión, corrección y aprobación, así como la organización editorial de cada número, de acuerdo con los criterios que la revista estime pertinentes.

La revista está financiada íntegramente por la Universidad Católica Boliviana “San Pablo”, sede La Paz. El envío, revisión y publicación de manuscritos son totalmente gratuitos.

Presentación del manuscrito

Los manuscritos deberán enviarse en formato digital Microsoft Word al correo electrónico: law.review.lpz@ucb.edu.bo o a través del sitio web de la revista. En caso de incluir gráficos, estos deberán presentarse adicionalmente en formato Microsoft Excel, para facilitar su correcta edición.

Los manuscritos deben ajustarse al formato de la revista y seguir las normas de estilo oficiales de la American Psychological Association (APA), 7ª edición en inglés, con las siguientes particularidades:

- a) No es necesario incluir encabezado.
- b) Los subtítulos deberán estar numerados (1., 2., 3., etc.).
- c) La primera página debe contener:
 - Título,
 - Resumen y palabras clave en español e inglés.

El resumen no debe exceder las 200 palabras. El nombre de las personas autoras deberá incluir una llamada a pie de página con su información profesional, afiliación institucional (cargo e institución), ciudad, país, correo electrónico de contacto e identificación ORCID. Asimismo, deberán declararse las fuentes de financiamiento de la investigación y, en su caso, su pertenencia a un proyecto más amplio.

- d) Las referencias deberán organizarse alfabéticamente con sangría francesa. No se deben incluir fuentes que no hayan sido citadas directamente, salvo aquellas que hayan influido en la definición conceptual o metodológica del trabajo.

- e) Las citas de normas legales deben incluir: artículo, tipo de norma, número o nombre y año.
Ejemplo: (*Art. 1279, Código Civil, Decreto Ley 12760, 1975*) o (*Art. 17, Ley 439, 2013*). El ámbito de origen de la norma deberá especificarse cuando corresponda.
- f) Las citas de jurisprudencia deben incluir: tribunal, denominación de la resolución, número y año.
Ejemplo: (*TCP, Sentencia Constitucional Plurinacional, 1620, 2014*). El ámbito de origen de la jurisprudencia también deberá aclararse cuando corresponda.

La extensión máxima del manuscrito será de 12.000 palabras.

El Formulario de cumplimiento de buenas prácticas académicas de la revista deberá ser completado, firmado y enviado junto con el manuscrito por todas las personas que figuren como autoras.

Proceso de evaluación

El manuscrito será evaluado por el consejo editorial, que podrá aceptarlo o rechazarlo de acuerdo a sus méritos y al perfil de la revista. El consejo editorial podrá ejercer esta potestad en cualquier momento hasta antes de la publicación del manuscrito y no necesita motivar o justificar su decisión. En caso de aceptación, el manuscrito será editado y remitido a un par académico o árbitro.

Para emitir sus evaluaciones, quienes sean pares académicos contarán con un plazo razonable, en el marco de la complejidad y extensión de la investigación.

Las observaciones que se comuniquen a quienes tiene la autoría deberán ser subsanadas en un plazo prudente a establecerse por el editor.

La revista otorgará criterios para la revisión de pares académicos respecto a la claridad, coherencia (entre lo propuesto, analizado y concluido), orden lógico, relevancia y pertinencia, metodología y rigor científico, sustento, fuentes adecuadas, discusión académica sobre hallazgos, conclusiones respaldadas y originalidad (aporte y novedad) de la investigación.

El dictamen sobre la investigación por parte de los pares académicos debe ser motivado. Las posibles decisiones del dictamen sobre el manuscrito son las de:

- a) aceptación para publicación,
- b) publicable con correcciones menores,
- c) publicable luego de una revisión substancial
- d) rechazo de publicación.

El formulario de dictamen de pares académicos de la revista deberá ser llenado, firmado y enviado por los pares académicos.

Formulario de dictamen de pares académicos

Los editores comunicarán la aceptación o rechazo del manuscrito a quien lo hubiese sometido a la revista para su revisión y publicación, pudiendo mantener en reserva la motivación del dictamen.

Ética y buenas practicas

Para los editores

La evaluación de los manuscritos se realizará exclusivamente sobre la base de su mérito académico, considerando su importancia, originalidad, validez del estudio, claridad, coherencia y relevancia para el ámbito temático de la revista.

No se tomarán en cuenta factores ajenos a la calidad académica, como la raza, orientación sexual, religión, origen étnico, filosofía política o afiliación institucional de las personas autoras.

Las decisiones de edición y publicación no estarán influenciadas por las políticas de gobiernos, instituciones u organizaciones externas a la revista.

Los editores conservan plena autoridad sobre el contenido editorial y el momento de publicación, en resguardo de la misión, visión y objetivos académicos de la revista.

El equipo editorial no divulgará información alguna sobre los manuscritos recibidos antes de su publicación, salvo a las personas autoras, revisores, asesores editoriales y editores involucrados en el proceso de evaluación.

Los editores y miembros del Consejo Editorial no harán uso de la información no publicada contenida en los manuscritos para sus propias investigaciones sin el consentimiento explícito de las personas autoras.

Asimismo, toda información privilegiada o idea obtenida durante la gestión editorial será tratada de forma confidencial y no podrá utilizarse para beneficio personal.

Los editores deberán inhibirse de participar en la evaluación de manuscritos en los que exista un conflicto de intereses, derivado de relaciones competitivas, colaborativas o institucionales con las personas autoras o con las entidades vinculadas al trabajo. En tales casos, se asignará la gestión editorial a otro miembro del consejo.

Los editores garantizarán que todos los manuscritos aceptados para evaluación sean sometidos a revisión por pares especializados en el campo correspondiente.

La decisión final sobre la publicación se basará en la validez académica de la investigación, su relevancia científica y social, las observaciones de los revisores y el cumplimiento de los requisitos legales vigentes relativos a difamación, infracción de derechos de autor y plagio. Los editores podrán consultar con otros editores o revisores antes de tomar una decisión definitiva.

Los editores se comprometen a investigar toda denuncia o indicio de conducta contraria a la ética académica. Si se verifican irregularidades, se emitirá la corrección, retractación o nota de preocupación correspondiente, independientemente del tiempo transcurrido desde la publicación original.

Para los pares académicos

La revisión por pares constituye un elemento esencial del proceso editorial y de la comunicación académica formal. Este procedimiento ayuda a los editores a tomar decisiones informadas sobre los manuscritos recibidos y, mediante la interacción editorial con las personas autoras, contribuye al mejoramiento de la calidad de las investigaciones publicadas.

Participar como revisor o revisora es una responsabilidad académica fundamental, inherente al compromiso científico de quienes contribuyen al avance del conocimiento.

Cualquier revisor invitado que se considere no capacitado para evaluar el manuscrito, o que sepa que no podrá hacerlo oportunamente, deberá notificar de inmediato a los editores y rechazar la invitación, a fin de que se pueda asignar el trabajo a otro evaluador.

Los manuscritos enviados para revisión son documentos confidenciales y deben ser tratados como tales.

No deberán mostrarse ni discutirse con otras personas, salvo autorización expresa de los editores en casos excepcionales y justificados. Este principio también se aplica a los revisores invitados que declinen la revisión.

La evaluación del manuscrito debe realizarse de manera objetiva, con observaciones claras, fundamentadas y constructivas, destinadas a mejorar el trabajo académico. La crítica personal es inapropiada y no será admitida.

Las personas revisoras deben identificar trabajos relevantes previamente publicados que no hayan sido citados por las autoras o autores.

Toda observación o argumento sustentado en fuentes previas deberá incluir la referencia bibliográfica correspondiente.

Asimismo, quienes revisan deben informar a los editores sobre cualquier similitud sustancial o coincidencia entre el manuscrito evaluado y otro trabajo (publicado o no) del cual tengan conocimiento.

Los revisores que enfrenten un conflicto de intereses, ya sea derivado de relaciones competitivas, colaborativas o institucionales con las personas autoras o las entidades vinculadas a la investigación, deberán declararlo inmediatamente y rechazar la invitación.

El material no publicado contenido en el manuscrito no podrá ser utilizado en las investigaciones de los revisores sin el consentimiento expreso y por escrito de las personas autoras.

De igual modo, cualquier información privilegiada o idea obtenida durante la revisión deberá mantenerse estrictamente confidencial y no podrá emplearse para beneficio personal. Esta obligación se extiende también a los revisores que declinen participar en el proceso de evaluación.

Para quienes tienen la autoría del manuscrito

En el ámbito de la ciencia e investigación jurídica, las personas con autoría de una investigación original deben presentar una descripción precisa del trabajo realizado y de sus resultados, seguida de una discusión objetiva sobre su relevancia. La investigación debe incluir suficiente detalle y referencias para permitir su replicación, cuando corresponda. Los artículos de revisión deben ser precisos, objetivos y exhaustivos, mientras que las opiniones o piezas de perspectiva editorial deben identificarse claramente como tales. Las declaraciones falsas o inexactas constituyen una conducta no ética e inaceptable.

Podrá solicitarse a las personas autoras que proporcionen los datos primarios de su investigación, tanto para revisión editorial como para su eventual disponibilidad pública. En todo caso, deben garantizar el acceso a dichos datos por parte de otros profesionales competentes durante al menos diez años después de la publicación, siempre que se proteja la confidencialidad de los participantes y los derechos legales asociados.

Las personas autoras deben asegurarse de haber redactado y presentado trabajos completamente originales, citando adecuadamente las fuentes utilizadas y reconociendo las publicaciones que hayan influido en la determinación del objeto de estudio. El plagio, en cualquiera de sus formas –como presentar el trabajo ajeno como propio, copiar o parafrasear partes sustanciales sin atribución, o reclamar resultados de otros– constituye una falta ética grave e inaceptable.

Asimismo, deben reconocer de forma adecuada la información obtenida en privado (por conversación, correspondencia o discusión), la cual no puede ser utilizada ni divulgada sin el consentimiento escrito de la fuente. No se debe emplear información obtenida en procesos confidenciales, como la revisión de manuscritos o solicitudes de financiamiento, sin permiso explícito de sus titulares.

Los trabajos que describan esencialmente la misma investigación no deben publicarse en más de una revista o publicación primaria. En consecuencia, no se debe someter a consideración un manuscrito ya publicado. La presentación simultánea a más de una revista constituye un comportamiento editorial poco ético e inaceptable. De manera excepcional, la publicación secundaria (por ejemplo, traducciones o protocolos) podrá admitirse siempre que exista acuerdo entre las personas autoras y las editoras de las revistas implicadas, se mantenga la fidelidad del contenido y se cite la fuente original.

Solo quienes cumplan los criterios de autoría deben ser listadas como tales, asumiendo la responsabilidad pública sobre el contenido. Los criterios son:

- a) Haber contribuido significativamente a la concepción, diseño, ejecución, obtención de datos, o análisis e interpretación del estudio.
- b) Haber redactado o revisado críticamente el manuscrito con aportes intelectuales sustanciales.
- c) Haber aprobado la versión final del documento y su presentación para publicación.

Las personas que hayan colaborado de manera relevante (por ejemplo, asistencia técnica, redacción, edición o apoyo general) pero no cumplan los criterios anteriores deben incluirse en los agradecimientos, previo consentimiento escrito. Quien remita el manuscrito debe asegurarse de incluir a todas las personas con coautoría y de que estas hayan revisado y aprobado la versión final.

Las personas autoras deben declarar, en la etapa más temprana posible, cualquier conflicto de intereses que pueda influir en los resultados o interpretación de su investigación –ya sean financieros (honorarios, becas, consultorías, propiedad de acciones, entre otros relacionados) o no financieros (relaciones personales o profesionales, afiliaciones o creencias sobre el tema tratado)–. Asimismo, deben revelar todas las fuentes de apoyo financiero.

El uso de inteligencia artificial en la investigación o en la redacción del manuscrito debe ser declarado en el formulario de autoría.

Si la investigación involucra el uso de animales o participantes humanos, las personas autoras deben garantizar el cumplimiento de las normas éticas vigentes. El manuscrito deberá incluir una declaración al respecto, así como sobre la obten-

ción del consentimiento informado. Los derechos de privacidad de los participantes deben ser respetados en todo momento.

Las personas autoras tienen la obligación de participar activamente en el proceso de revisión por pares, respondiendo de manera puntual y completa a las solicitudes editoriales. En caso de requerirse correcciones o revisiones, deben responder punto por punto y reenviar el manuscrito en los plazos establecidos.

Si después de la publicación descubren errores o inexactitudes significativas, las personas autoras deben notificarlo de inmediato al equipo editorial y colaborar para corregir mediante una fe de erratas o retractación. Si los editores identifican un problema a través de terceros, será responsabilidad de las personas autoras aclararlo o rectificar el documento con prontitud.

La Universidad Católica Boliviana “San Pablo” no se responsabiliza por las opiniones, comentarios o contenidos de los artículos publicados, los cuales son responsabilidad exclusiva de sus autoras y autores.

Para la editorial

En casos de presunta mala conducta científica, publicación fraudulenta o plagio, la persona editora principal, en coordinación con el equipo editorial, tomará todas las medidas pertinentes para esclarecer la situación y actuar conforme a las buenas prácticas académicas. Estas medidas podrán incluir la publicación oportuna de una fe de erratas, una aclaración o, en los casos más graves, la retractación del artículo afectado.

Asimismo, la editorial adoptará medidas razonables para prevenir la publicación de trabajos en los que se haya identificado mala conducta científica, asegurando que tales prácticas no sean promovidas ni toleradas bajo ninguna circunstancia.

La persona editora principal también garantiza la preservación y disponibilidad permanente de las investigaciones publicadas, asegurando su accesibilidad continua y su adecuada conservación en los repositorios institucionales correspondientes.

UCB Law Review

Editorial Policy, Ethic and Good Practices

History and mission

The journal began its first publication in 2017. It is published by the Law School of the Faculty of Law and Political Sciences of the Bolivian Catholic University “San Pablo” (UCB), La Paz region.

The journal’s mission is to disseminate original legal, scientific, and research, with the aim of contributing to legal knowledge, development, pluralistic dialogue, and the generation of good legal practices within the framework of respect for human rights. It is aimed at legal scholars, students, and practitioners, as well as public policymakers. The journal’s publications are primarily theoretical, deontic, practical, and applied in nature, related to local, regional, and global legal analysis.

Lines of investigation

The main lines of research of the journal are:

1. Social law, labor, childhood and family.
2. Philosophy, history, ethics and morals.
3. Human rights, pluralism, legal protection, justice and culture of peace.
4. Civil and commercial law.
5. Environment, natural resources and energy.
6. Institutions, administration, penal law, international relations and sovereignty.

Publication frequency

The journal is published in print (ISSN 2521-8808) and online at lawreview. ucb.edu.bo (ISSN 2523-1510) every six months in April and October, although it can also publish special non-periodic issues.

Open access policy

The U.C.B. Law Review is an Open Access Journal.

The Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International license allows users to read, download, copy, distribute, and adapt the published content, provided that appropriate credit is given to the original author(s). The use of the work and any derivative materials for commercial purposes is not permitted, and any adaptations must be distributed under the same license. This framework promotes open access to knowledge while ensuring respect for authors’ rights and the responsible dissemination of academic work.

Privacy Statement

U.C.B. Law Review will not communicate or transfer to third parties the personal data of its users without the express consent of the owner, except judicial order.

General conditions

A *manuscript* is understood as the original text submitted for publication in the journal.

Submission of a manuscript for consideration implies authorization for its potential publication and dissemination in both digital and print formats, the non-exclusive transfer of copyright for its distribution, and full acceptance of the editorial policies established by the Universidad Católica Boliviana “San Pablo” (UCB) and the journal, including adherence to these policies.

The content, data, and opinions expressed in the manuscripts are the sole responsibility of their authors and do not necessarily reflect the institutional position of the UCB, the Institute for Democracy, the editors, or the journal.

Submitted research must meet the standards required for peer review, be original, belong in authorship to those identified in the manuscript, and comply with ethical and academic integrity principles. Likewise, manuscripts must not have been previously published or simultaneously submitted for consideration elsewhere, except in cases explicitly permitted in the Ethics and Good Practices section.

Authors must identify themselves by indicating their institutional affiliation. Those without one must declare themselves independent researchers. Authors are also required to include their ORCID identification number, which can be obtained at <https://orcid.org>.

The official publication languages of the journal are Spanish and English; however, the journal reserves the right to publish in other languages when appropriate.

The journal primarily publishes research that has been anonymously and favorably evaluated for its formal, substantive, and methodological merit by academic peers. Each publication will include the dates of manuscript submission and approval.

All communication between the journal, authors, and reviewers will be conducted via email.

Manuscript submission is continuous. The journal reserves the right to determine the order and timing of publication for approved manuscripts, taking into account the natural timeframe of the review–correction–approval process, as well as the editorial organization of each issue, according to the journal’s editorial criteria.

The journal is fully funded by the Universidad Católica Boliviana “San Pablo”, La Paz Campus. Submission, peer review, and publication processes are entirely free of charge.

Manuscript Submission and Style

Manuscripts must be submitted in Microsoft Word format via email to: law.review.lpz@ucb.edu.bo or through the journal’s web site. If the manuscript includes graphs or figures, these must also be provided in Microsoft Excel format for editorial purposes.

Manuscripts should follow the journal’s format and comply with the official American Psychological Association (APA) 7th edition (English version) style guide, with the following exceptions:

- a) No header is required.
- b) Subheadings must be numbered (1., 2., 3., etc.).
- c) The first page must include:
 - Title.
 - Abstract and keywords in both Spanish and English.

The abstract must not exceed 200 words. Authors’ names must include a footnote providing their professional information, institutional affiliation (position and institution), city, country, contact email, and ORCID ID. Any funding sources or the connection to a broader research project (if applicable) must also be declared.

- d) The reference list must be organized alphabetically and use hanging indentation. Only works directly cited in the manuscript should be listed, except for those that significantly influenced the conceptualization or design of the study.
- e) Legal citations must include the article, type of norm, number or name, and year.

Example: (*Art. 1279, Civil Code, Decree Law 12760, 1975*) or (*Art. 17, Law 439, 2013*).

The jurisdiction of the legal source must be specified when relevant.

- f) Case law citations must include the court, title of the decision, number, and year.
Example: (*TCP, Constitutional Ruling, 1620, 2014*). The jurisdiction of origin must also be clarified when appropriate.

The maximum manuscript length is 12,000 words.

The Academic Good Practices Compliance Form must be completed, signed, and submitted along with the manuscript by all listed authors.

Evaluation process

The editorial board will evaluate the manuscript and may accept or reject it according to its merits and the profile of the journal. The editorial board may exercise this power at any time until before the publication of the manuscript and does not need to give reasons for its decision. In case of acceptance, the manuscript will be edited and sent to an academic peer reviewer.

To issue their evaluations, the arbitrators will have a reasonable period according to the complexity and length of the manuscript.

The observations communicated to the authors must be corrected within a reasonable time to be established by the editor.

The journal will grant criteria for the academic peer review regarding clarity, coherence (between what is proposed, analyzed, and concluded), structure, relevance and pertinence, methodology and scientific rigor, sustenance, adequate sources, academic discussion on findings, supported conclusions and originality (contribution and novelty) of the research.

The opinion on the research by academic peers must be motivated. The possible decisions of the opinion on the manuscript are

- a) acceptance for publication,
- b) publishable with minor corrections,
- c) publishable after substantial revision, and
- d) rejection of publication.

The journal's Manuscript Evaluation Form for Academic Peers must be completed, signed, and sent by the academic peer.

Academic Peer Review Form

The editor will communicate the acceptance or rejection of the manuscript to whoever submitted it to the journal for review and publication and may keep the motivation of the opinion confidential.

Ethics and Good Practices

For the editors

The evaluation of manuscripts will be based exclusively on their academic merit, taking into account their importance, originality, validity of the study, clarity, coherence, and relevance to the journal's scope.

Considerations such as race, sexual orientation, religion, ethnic origin, political philosophy, or institutional affiliation of the authors will not influence the review or publication process.

Decisions regarding editing and publication are made independently of any governmental or institutional policies external to the journal.

Editors retain full authority over all editorial content and the timing of publication, in alignment with the mission and academic objectives of the journal.

The editorial team will not disclose any information regarding submitted manuscripts prior to publication, except to the authors, reviewers, editorial advisors, and editors directly involved in the process.

Editors and members of the Editorial Board must not use unpublished information obtained through the review process for their own research without the explicit consent of the authors.

Likewise, any privileged information or ideas acquired through manuscript handling will remain confidential and must not be used for personal advantage.

Editors will recuse themselves from handling manuscripts where a conflict of interest exists, whether due to competitive, collaborative, or institutional relationships with any of the authors or their affiliated entities. In such cases, another editorial board member will assume responsibility for the manuscript.

Editors will ensure that all submitted manuscripts under consideration are subject to peer review by qualified experts in the relevant field.

Final publication decisions will be based on the academic validity of the research, its relevance to the scholarly community, the reviewers' comments, and legal requirements related to defamation, copyright infringement, and plagiarism. Editors may consult with additional editors or reviewers in making their final decision.

Editors are committed to investigating any reported or suspected cases of unethical behavior. If misconduct is confirmed, the journal will issue the appropriate correction, retraction, or statement of concern, regardless of the time elapsed since publication.

For Academic Peers

Peer review is an essential component of the editorial process and formal academic communication. It assists editors in making informed decisions regarding submitted manuscripts and, through editorial dialogue with authors, contributes to improving the quality of published research.

Serving as a reviewer is a core academic responsibility and a vital part of the scientific community's collective effort to advance knowledge.

Any invited reviewer who feels unqualified to assess a manuscript, or who knows that a prompt review will not be possible, must immediately notify the editors and decline the invitation so that another reviewer can be assigned.

Manuscripts received for review are confidential documents and must be treated as such. They should not be shared or discussed with others except with explicit authorization from the editors in exceptional and justified cases. This confidentiality rule also applies to reviewers who decline the review invitation.

The evaluation must be objective, and comments should be clear, reasoned, and constructive, providing feedback that can help authors improve their work. Personal criticism is inappropriate and unacceptable.

Reviewers must identify relevant published work that has not been cited in the manuscript. Any comment, claim, or argument based on prior research should include the corresponding citation.

Reviewers should also alert editors to any substantial similarity or overlap between the manuscript under review and other works (published or unpublished) known to them.

Reviewers who have a conflict of interest arising from competitive, collaborative, or institutional relationships with the authors or related entities must declare it immediately and decline the review invitation.

Unpublished material disclosed in a manuscript may not be used in a reviewer's own research without the explicit written consent of the authors.

Likewise, any privileged information or ideas obtained through the review process must remain strictly confidential and may not be used for personal advantage. This obligation also applies to reviewers who decline the review.

For those who have the authorship of the manuscript

Within the framework of legal science and research, authors of an original study must present an accurate description of the work conducted and its results, followed by an objective discussion of its significance. The research should include sufficient detail and references to allow replication, where applicable. Review articles must be precise, objective, and comprehensive, while opinion or editorial perspective pieces must be clearly identified as such. False or misleading statements constitute unethical and unacceptable conduct.

Authors may be required to provide the raw data of their research, either for editorial review or for public access. In any case, they must ensure that such data remain accessible to competent professionals for at least ten years after publication, provided that participants' confidentiality and related legal rights are protected.

Authors must ensure that they have written and submitted entirely original work, have properly cited all sources used, and have acknowledged publications that influenced the study's scope or approach. Plagiarism—in any form, such as presenting another's work as one's own, copying or paraphrasing substantial parts without attribution, or claiming results from others—is an unethical and unacceptable practice.

Authors must also properly acknowledge information obtained privately (through conversation, correspondence, or discussion), which cannot be used or reported without the explicit written consent of the source. Information acquired during confidential processes, such as manuscript review or grant evaluation, must not be used without written authorization from the rights holders.

Works describing essentially the same research should not be published in more than one primary journal or publication. Accordingly, a manuscript previously published elsewhere must not be submitted for consideration. Submitting the same manuscript simultaneously to more than one journal constitutes unethical and unacceptable behavior. Exceptionally, secondary publication (e.g., translations or protocols) may be justified, provided that all involved authors and editors agree, the content remains faithful to the original, and the primary source is cited.

Only individuals meeting the authorship criteria should be listed as authors, as they must be able to assume public responsibility for the content. The criteria are:

- a) Significant contribution to the conception, design, execution, data acquisition, or analysis and interpretation of the study.
- b) Drafting or critically revising the manuscript with substantial intellectual input.
- c) Approval of the final version and agreement to its submission for publication.

Contributors who do not meet these criteria (e.g., technical assistance, writing, editing, or general support) should be acknowledged in the acknowledgments section with written consent. The corresponding author must ensure that all co-authors have reviewed and approved the final version of the manuscript.

At the earliest possible stage, authors must declare any potential conflicts of interest that could influence the results or interpretation of their research—whether financial (fees, grants, consultancies, share ownership, among others) or non-financial (personal or professional relationships, affiliations, or beliefs related to the topic). All sources of financial support must also be disclosed.

The use of artificial intelligence in research or in the writing of the manuscript must be declared in the authorship form.

If the research involves human participants or animals, authors must ensure compliance with all relevant ethical standards. The manuscript must include a statement confirming this compliance and the obtaining of informed consent. Participants' privacy rights must always be respected.

Authors are obliged to participate actively in the peer review process and cooperate fully by responding promptly and thoroughly to editorial requests. In the event of corrections or revisions, authors must address reviewers' comments point by point and resubmit the manuscript within the specified deadlines.

When authors discover significant errors or inaccuracies in their published work, they must promptly notify the editors and cooperate to issue an erratum or retraction. If editors learn of an issue from third parties, it remains the authors' responsibility to clarify or correct the publication promptly.

The Universidad Católica Boliviana "San Pablo" assumes no responsibility for the opinions, comments, or content expressed in the published articles, which are the sole responsibility of their authors.

For the editorial

In cases of alleged scientific misconduct, fraudulent publication, or plagiarism, the Editor-in-Chief, in coordination with the editorial team, shall take all appropriate actions to clarify the situation and act in accordance with good academic practices. Such actions may include the prompt publication of an erratum, a clarification, or, in the most serious cases, the retraction of the affected article.

The editorial team shall also take reasonable steps to prevent the publication of works in which research misconduct has been identified, ensuring that such practices are neither promoted nor knowingly tolerated under any circumstances.

The Editor-in-Chief further commits to ensuring the permanent preservation and accessibility of the published research, guaranteeing its continued availability and proper storage within the corresponding institutional repositories.

UNIVERSIDAD
CATÓLICA
BOLIVIANA
ERIGIDA CANONICAMENTE
POR LA SANTA SEDE DESDE 2023



Carrera de
Derecho



Avenida 14 de septiembre N° 4807 - Obrajes - La Paz

www.ucb.edu.bo

www.lawreview.ucb.edu.bo

law.review.lpz@ucb.edu.bo