


# La responsabilidad jurídica por daños causados por sistemas de inteligencia artificial autónoma.

## Un marco integrado desde el derecho comparado con énfasis en América Latina


### Jesús E. Villanueva Figueroa<sup>1</sup>

Universidad Santa María  
jesusvillanueva1969@gmail.com

 ORCID 0009-0002-4679-577X


### Shirley Carrizalez Méndez<sup>2</sup>

Universidad Santa María  
scarrizales10@hotmail.com

 ORCID 009-0005-8493-5392


### Joiseth I. Fernández Amoroso<sup>3</sup>

Universidad Santa María  
joifdezamoroso@gmail.com

 ORCID 0009-0009-8105-7669


### Liseth Hidrobo Amoroso<sup>4</sup>

Universidad Santa María  
hidrobo.liseth@gmail.com

 ORCID 0009-0008-7445-5274

### Joselyn Vannesa Fernández A.<sup>5</sup>

Universidad Santa María  
nylesoj251989@gmail.com

 ORCID 0009-0007-3844-305X

<sup>1</sup> Jesús Enrique Villanueva Figueroa (Venezuela), abogado (USM) y doctor en Ciencias de la Educación (ULAC); especialista en Derecho Procesal Civil, con estudios de maestría en Derecho Constitucional Internacional. Juez suplente en tribunales municipales del Área Metropolitana de Caracas.

<sup>2</sup> Shirley M. Carrizales Méndez (Venezuela), abogada adscrita a la Sala Constitucional del TSJ; doctora en Derecho Constitucional y Penitenciario y en Ciencias de la Educación, con maestría en Derecho Constitucional. Docente universitaria; líneas: constitucionalismo, derechos humanos y procesal penal.

<sup>3</sup> Joiseth Ivannet Fernández Amoroso (Venezuela), abogada (USM); doctora en Ciencias Penales y Criminalísticas (UCSAR) y doctorado en Derecho Procesal Constitucional (UCSAR, 2025). Abogada asistente del mag. Edgar Gavidía (Sala de Casación OSocial, TSJ); experiencia en jurisdicción laboral y disciplinaria.

<sup>4</sup> Liseth del Carmen Hidrobo Amoroso (Venezuela), abogada (USM). Formación en derecho constitucional, humanitario y procesal civil (UNED), MASC y derechos humanos; curso internacional de posgrado en Medicina Legal (ULAC).

<sup>5</sup> Joselyn Vanessa Fernández A. (Venezuela), es Abogada egresada de la Universidad Santa María, ejerce el cargo de juez en el sistema judicial venezolano, con participación en el Circuito Judicial de Protección de Niños.



## La responsabilidad jurídica por daños causados por sistemas de inteligencia artificial autónoma.

### Resumen

En el último lustro, las tecnologías han avanzado mucho más rápido que los sistemas de regulación, lo que implica nuevos riesgos y vulnerabilidades. En este artículo se analizan los vacíos legales que existen en la imputación de responsabilidad por daños causados por sistemas de inteligencia artificial (IA) autónomos, especialmente en ausencia de intervención humana directa. Desde una metodología cualitativa basada en el análisis doctrinal, jurisprudencial y comparado, se comentan modelos regulatorios vigentes en la Unión Europea, Estados Unidos y América Latina. Se abordan tanto las perspectivas del derecho civil (indemnización del daño, responsabilidad objetiva) como del derecho penal internacional (tipicidad, imputabilidad, responsabilidad estructural). Se propone un marco jurídico integrado que incluye seguros obligatorios para desarrolladores, fondos de compensación y un órgano internacional de auditoría de IA. Finalmente, se aspira contribuir a la construcción de un modelo normativo para la realidad latinoamericana que sea parte de la educación en derecho comparado.

**Palabras clave:** *Inteligencia artificial; responsabilidad civil; derecho penal internacional; autonomía algorítmica; regulación tecnológica*

# Legal Liability for Damage Caused by Autonomous Artificial Intelligence Systems

## Abstract

In the last five years, technologies have advanced much faster than regulatory systems, implying new risks and vulnerabilities. This article analyzes the legal gaps that exist in the attribution of liability for damages caused by autonomous artificial intelligence (AI) systems, especially in the absence of direct human intervention. Using a qualitative methodology based on doctrinal, jurisprudential, and comparative analysis, it studies current regulatory models in the European Union, the United States, and Latin America. It addresses both civil law (compensation for damages, strict liability) and international criminal law (typicality, imputability, structural liability) perspectives. It proposes an integrated legal framework that includes mandatory insurance for developers, compensation funds, and an international AI audit body. Finally, it aims to contribute to the construction of a regulatory model for Latin America that is part of comparative law education.

*Keywords: artificial intelligence; civil liability; international criminal law; algorithmic autonomy; technological regulation*

## Introducción

La inteligencia artificial (IA) ha trascendido su estatus de promesa futurista para convertirse en una realidad omnipresente y dinámica, penetrando ámbitos tan diversos como la medicina, la administración de justicia y el sector empresarial. En particular, los sistemas de IA autónomos operan con una mínima intervención humana, tomando decisiones complejas basadas en algoritmos, datos de sensores y modelos de aprendizaje automático (Yazdanpanah et al., 2024). Aunque esta capacidad de autodeterminación impulsa el progreso, también introduce una incertidumbre considerable en la atribución de responsabilidad cuando sus acciones derivan en daños.

Al respecto, Gutiérrez Proenza (2022) afirma que debido a las novedades de uso de la IA *“corresponde al derecho empezar a dilucidar problemáticas jurídicas que atañen a esta y buscar las respectivas soluciones”*. Igualmente, acentúa el hecho de que *“al ser situaciones relativamente nuevas, existen vacíos legales y ningún tipo de normativa que permita regular esta interacción entre las personas y las máquinas”* (p. 20). Acerca de dicha problemática, Colombo (2024) asevera: *“La revolución 4.0 tiene un contrapunto inquietante, su innegable lado oscuro. Los sistemas de inteligencia artificial poco a poco se introducen en nuestra cotidianidad, en la esfera más íntima del ser humano”* (párr. 1).

La IA se manifiesta en dos categorías principales: la IA débil, diseñada para tareas específicas, y la IA fuerte, con la capacidad de realizar tareas intelectuales comparables a las humanas, planteando incluso la eventualidad de una conciencia propia, lo que hace aún más complejo el panorama de la imputación de responsabilidad (Gutiérrez Proenza, 2022). El des-

pliegue de la IA no solo afecta aspectos materiales, sino que también puede vulnerar derechos personales fundamentales, como la dignidad, la imagen, el honor, la privacidad y la libertad de contratación (Yazdanpanah et al., 2024).

En este campo, el desafío central radica en la imputación de responsabilidad, dada la ausencia de una intervención humana directa y discernible. En la mayoría de los ordenamientos jurídicos, incluido el venezolano, las normativas no ofrecen respuestas claras sobre quién debe asumir la responsabilidad cuando un sistema de IA autónomo comete un error (Navas Navarro, 2022; Ormazabal Sánchez, 2024). Esta laguna deja a los ciudadanos expuestos a perjuicios cuya trazabilidad es compleja y su reparación resulta esquivada.

La autonomía de la IA desarticula los pilares tradicionales del derecho, donde la responsabilidad civil, por ejemplo, se fundamenta en la acción humana, ya sea dolosa o negligente (Navas Navarro, 2022). La opacidad inherente de muchos sistemas de IA, su complejidad algorítmica y la imprevisibilidad de sus modelos de aprendizaje profundo, dificultan la identificación de la causa o raíz de un daño y, en consecuencia, la atribución de culpa o responsabilidad (Colombo, 2024). Esto apunta a una profunda deshumanización de la causalidad jurídica. Los marcos legales tradicionales, especialmente en el ámbito de la responsabilidad civil, se construyen sobre la acción humana, la intención y un nexo causal directo. La autonomía y opacidad de la IA alteran fundamentalmente este paradigma al generar resultados sin una acción o intención humana directa, en el sentido convencional.

Se plantea, entonces, un cambio trascendental de un modelo de causalidad centrado en el ser humano, a uno donde el agente del daño es no humano y sus mecanismos internos resultan inescrutables. La implicación es que los sistemas jurídicos deben redefinir, radicalmente, conceptos esenciales como

acción y culpa o, lo que es más probable, orientarse hacia mecanismos que eludan estos requisitos tradicionales, como la responsabilidad objetiva o los fondos de compensación, reconociendo que el quién y el porqué de la responsabilidad clásica, son cada vez más irrelevantes o imposibles de determinar (Glock y von Alemann, 2022). Asimismo, se presenta el dilema de la innovación frente a la protección. La necesidad de una regulación que salvaguarde la dignidad humana, proteja los derechos y garantice la rendición de cuentas, al tiempo que fomente la confianza en la IA, se contrapone con las preocupaciones sobre la posibilidad de asfixiar la innovación y la competitividad (Huang et al., 2024; Yazdanpanah et al., 2024).

La experiencia de la Unión Europea (UE), con su propuesta de Directiva de Responsabilidad por IA, inicialmente presentada, luego retirada y posteriormente reevaluada, ilustra esta tensión de manera elocuente (European Parliament, 2023). En el proyecto de directiva sobre responsabilidad por IA, la comisión propuso complementar y modernizar el marco de responsabilidad de la UE para introducir nuevas normas específicas sobre los daños causados por sistemas de IA. Estas nuevas normas pretenden garantizar que, en la UE, las personas perjudicadas por sistemas de IA disfruten del mismo nivel de protección que las personas perjudicadas por otras tecnologías. La directiva sobre responsabilidad por IA establecería una presunción de causalidad, refutable para facilitar la carga de la prueba a las víctimas a la hora de demostrar los daños causados por un sistema de IA. Adicionalmente, otorgaría a los tribunales nacionales la facultad de ordenar la divulgación de pruebas sobre sistemas de IA de alto riesgo, sospechosos de haber causado daños (European Parliament, 2025; Unión Europea, 2024; Ormazábal Sánchez, 2024).

Esto revela que la IA autónoma requiere el imperativo de la regulación jurídica así que el desafío fundamental para los reguladores no es solo cómo regular, sino cuánto y con qué

celeridad hacerlo, sin obstaculizar el avance tecnológico. La tendencia subyacente es un acto de equilibrio global entre el fomento del crecimiento económico a través de la IA y la salvaguarda de los valores sociales, en el que los órganos legislativos a menudo luchan por encontrar el punto óptimo, lo que genera incertidumbre legislativa y cambios dinámicos en las políticas. En cualquier caso, es evidente que el desarrollo de las herramientas asociadas a la IA, tomando en cuenta las implicaciones sociales, económicas y biológicas relativas a su uso, no parece depender únicamente de las fuerzas del mercado. Corresponde a la ley regular esta tecnología, para orientar su funcionamiento de forma virtuosa y adaptarla a la consecución de los objetivos de interés público que subyacen a las acciones de legisladores y reguladores (Macchia y Mascolo, 2022, p. 98).

Con base en lo anteriormente expuesto, el objetivo general de este trabajo se plantea analizar los vacíos legales presentes en la imputación de responsabilidad por daños causados por sistemas de inteligencia artificial (IA) autónomos, específicamente en ausencia de intervención humana directa. Desde una metodología cualitativa, fundada en el análisis doctrinal, jurisprudencial y comparado, el artículo aborda el estudio de los modelos regulatorios actualmente en vigor en la Unión Europea, Estados Unidos y Latinoamérica. Igualmente, se propone un marco jurídico integrado que incluye seguros obligatorios que garanticen los intereses de los usuarios, así como fondos de compensación y un órgano internacional de auditoría de IA. Finalmente, se aspira contribuir a la construcción de un modelo normativo adecuado a la realidad latinoamericana, que se integre a la formación profesional en derecho comparado.

## **Vacíos legales en la imputación de responsabilidad por daños de IA autónoma**

La irrupción de la IA autónoma ha puesto de manifiesto la ausencia de su tratamiento en los marcos jurídicos existentes, incapaces de abordar eficazmente la imputación de responsabilidad por los daños que estos sistemas pueden causar. Los principios tradicionales de la responsabilidad civil y penal se ven directamente interpelados por las características inherentes de la IA.

En el ámbito de la responsabilidad civil, la identificación del sujeto causante del daño, la existencia de una lesión y el nexo causal entre la acción u omisión y el perjuicio, son elementos esenciales. Sin embargo, la autonomía de la IA difumina estas líneas (Asaro, 2016; Herbosch, 2025). Campillo (2025) advierte que “uno de los principales problemas en la atribución de responsabilidad civil en el ámbito de la IA es la determinación de la relación de causalidad existente entre una acción y sus consecuencias dañosas” (párr. 8). Los agentes de IA autónomos operan con base en algoritmos preprogramados y aprendizaje continuo, a menudo sin una intervención humana en tiempo real, lo que desdibuja las fronteras de la responsabilidad entre personas y máquinas (Herbosch, 2025). La imprevisibilidad de las acciones de los modelos de aprendizaje automático, que pueden surgir de sesgos en los datos de entrenamiento, escenarios no previstos o errores del sistema, complica significativamente la rendición de cuentas (Yampolskiy, 2020). Además, la cadena de intervinientes en el desarrollo y despliegue de la IA, desde desarrolladores y fabricantes hasta integradores de sistemas y usuarios finales, hace extremadamente difícil determinar la responsabilidad por los errores (Sharipov, 2025).

La complejidad, la opacidad y la capacidad de la IA para externalizar beneficios, desafían las nociones convencionales de causalidad, lo que revela la insuficiencia de los regímenes

de responsabilidad actuales (Herbosch, 2025). Se identifican vacíos de responsabilidad donde nadie puede ser considerado un verdadero responsable, cuando la tecnología asume la toma de decisiones, el actor equivocado resulta culpabilizado, o múltiples actores eluden la responsabilidad al culparse mutuamente.

En el campo del derecho penal, los desafíos son aún más complejos. Para que la IA sea objeto de responsabilidad penal, se requeriría que cumpliera con elementos como la acción típica, antijurídica y culpable (Gutiérrez Proenza, 2022). La imputabilidad, un concepto central en la teoría del delito, presupone la facultad de comprender el alcance de las acciones y de dirigir la propia conducta, capacidades intrínsecamente humanas (Benítez-Abarca et al., 2025). La tipicidad, por su parte, se configura por la realización de una conducta objetiva descrita en el tipo penal, acompañada de dolo o imprudencia. La ausencia de estos elementos subjetivos tornaría la conducta atípica (Del Castillo, 2023). La dificultad radica en atribuir la *mens rea*, es decir la intención o conocimiento de la ilicitud, a una máquina, ante el *actus reus*, que viene a ser el acto físico u omisión (Lee, 2025). La complejidad de los algoritmos de IA y su capacidad de aprender y adaptarse, dificultan determinar si un sistema de IA actuó por sí mismo o si hubo intención humana involucrada. En este conflicto, nos interrogamos sobre el hecho de si la tensión entre la autonomía algorítmica y la imputabilidad humana o la capacidad de ser considerado responsable, constituyen los factores de mayor importancia.

El sistema jurídico está diseñado para actores humanos que poseen conciencia, libre albedrío y capacidad de comprender las consecuencias. Cuando un sistema de IA toma una decisión autónoma que causa un daño, la cadena tradicional de la intención humana se rompe o se difumina. Esto genera una tensión fundamental, donde la aplicación de los principios existentes del derecho penal a los daños causados por la IA, a me-

nudo, conduce a un vacío de responsabilidad, en el que nadie puede ser considerado responsable, o la responsabilidad se atribuye incorrectamente. Lo anterior implica que el derecho penal, a diferencia del derecho civil, que puede adaptarse más fácilmente a través de la responsabilidad objetiva, se enfrenta a un obstáculo filosófico y doctrinal más profundo, que podría requerir la creación de nuevas construcciones jurídicas o una redefinición radical de la personalidad para la IA actual, considerada muy compleja (Custers et al., 2025).

Por otra parte, la “caja negra” de la IA se erige como una barrera para la justicia debido a la opacidad y complejidad de los sistemas de IA que se traducen directamente en obstáculos legales significativos para las víctimas que buscan reparación (Blázquez Ruiz, 2022). Si una víctima no puede comprender cómo un sistema de IA tomó una decisión o cuál fue la falla, no puede probar eficazmente la culpa o la causalidad, elementos fundamentales de muchos regímenes de responsabilidad. Esto implica que, sin mecanismos de transparencia, explicabilidad (Explainable AI - XAI) y divulgación de pruebas, se verá seriamente comprometida la capacidad del sistema jurídico para impartir justicia y equilibrar el poder entre víctimas y concededores de IA, en casos de daños inducidos por la IA (Herbosch, 2025).

## **La responsabilidad civil ante la IA autónoma: perspectivas y desafíos**

La responsabilidad civil, cuyo propósito primordial es la indemnización del daño causado, se enfrenta a un escrutinio sin precedentes ante la emergencia de la IA autónoma. Doctrinal y jurisprudencialmente, se han explorado diversas vías para adaptar este ámbito del derecho. Una de ellas es la responsabilidad proporcional, que propone distribuir el daño entre los posibles causantes, en función del grado de probabilidad de su intervención. Otra aproximación es la inversión de la carga de

la prueba, que exigiría a los desarrolladores y operadores de IA demostrar que su tecnología no fue la causante del daño, aliviando de este modo la carga de la víctima (Álvarez Olalla, 2021). En países como Argentina, la actividad desplegada por sistemas de IA, como el machine learning y el deep learning, se ha considerado una actividad riesgosa conforme al Artículo 1757 del Código Civil y Comercial, lo que permite la atribución de responsabilidad objetiva (Colombo, 2024). Asimismo, la obligación tácita de seguridad, arraigada en el principio de la buena fe contractual, impone un deber de preservar la integridad de los bienes y las personas, configurando una obligación de resultados que, por su naturaleza, genera responsabilidad objetiva (Colombo, 2024; Zabala Leal y Gómez McFarland, 2024).

La aplicación de la responsabilidad objetiva, fundamentada en el riesgo creado o en la realización de una actividad riesgosa, se perfila como el modelo más idóneo y cada vez más adoptado para la IA. Este enfoque responsabiliza a las organizaciones por los daños relacionados con la IA, independientemente de la culpa (Romero Boue, 2024). La Directiva de Responsabilidad por Productos Defectuosos de la Unión Europea, actualmente aplica un régimen de responsabilidad objetiva a los fabricantes de productos defectuosos, incluyendo explícitamente software y sistemas de IA integrados (European Parliament, 2025; Scott et al., 2024). Bajo este modelo, la víctima no necesita probar la negligencia o culpa de la empresa; solo se requiere demostrar que el producto era defectuoso, que se sufrió un daño y que existía un nexo causal entre el defecto y el daño (Ormazábal Sánchez, 2024). La responsabilidad objetiva, al basarse en la creación de un riesgo o en el beneficio obtenido de una actividad, consideramos que resulta más aplicable a la IA que el propio concepto de culpa, por cuanto es sumamente difícil establecer la intencionalidad o negligencia directa en sistemas autónomos y que no tienen un juicio humano.

Esta tendencia representa una convergencia hacia la responsabilidad objetiva como solución pragmática. La dificultad para probar la culpa o la negligencia debido a la opacidad y autonomía de la IA ha llevado a un cambio hacia la imposición de responsabilidad independientemente de la culpa, lo que simplifica la reclamación de la víctima y fomenta que los desarrolladores y operadores prioricen la seguridad. Ello significa que el sistema tradicional basado en la culpa es inadecuado para la IA, lo que hace necesario un cambio pragmático para asegurar la compensación de las víctimas y promover la prevención de riesgos, en lugar de intentar encajar la IA en moldes legales centrados en el ser humano.

En cuanto a los tipos de daños, la IA puede causar perjuicios que se manifiestan directamente sobre la persona humana o que repercuten en su patrimonio, incluyendo la esfera íntima y el daño extrapatrimonial (Arroyo Moreno, 2025; Colombo, 2024). Estas acciones han llevado a la nueva Directiva de Responsabilidad por Productos de la UE a ampliar la definición de daño, para incluir expresamente los efectos sobre la salud psicológica y la destrucción o corrupción de datos no utilizados con fines profesionales. Además, la IA puede ser fuente de daños derivados de la discriminación o la violación de otros derechos fundamentales (Arroyo Moreno, 2025; Colombo, 2024; Scott et al., 2022).

Esta misma Directiva de Responsabilidad por Productos de la UE, incluye explícitamente el software y los sistemas de IA en la definición de producto y amplía la definición de daño para abarcar el perjuicio psicológico y la corrupción de datos (European Parliament, 2024). Esto indica una tendencia más amplia en la adaptación legal, es necesario llegar a reconocer la forma en que las entidades digitales hasta el software pueden ser productos sujetos a responsabilidad y que el daño se extiende más allá de la lesión física o la pérdida directa de propiedad, para incluir el bienestar psicológico y los activos digitales. Esto

tiene implicaciones significativas sobre cómo se concibe y se reclama la responsabilidad en la era digital, trascendiendo las nociones tangibles tradicionales.

## **La responsabilidad penal ante la IA autónoma: límites y nuevos paradigmas**

El derecho penal, con su arraigado principio de personalidad de la pena, enfrenta obstáculos aún mayores que el derecho civil en la atribución de responsabilidad por los actos de la IA autónoma. La responsabilidad penal es, por definición, personal e intransferible. Resulta impensable sancionar a un individuo por la conducta autónoma de un tercero y, menos aún, por la de una máquina (Mongillo, 2024). La imputabilidad, piedra angular de la culpabilidad penal, exige que el sujeto posea la facultad de comprender el alcance de sus acciones y de dirigir su conducta que son capacidades absolutamente humanas. De igual modo, la tipicidad de un delito requiere la presencia de dolo o imprudencia, elementos subjetivos que son imposibles de atribuir a un algoritmo que opera de forma autónoma (Reyes Alvarado, 2024) La complejidad y la capacidad de adaptación de los algoritmos de IA, dificultan la determinación del momento preciso en que las acciones de un sistema transitaron de lo aceptable a lo ilícito, y si existió alguna intención humana involucrada en dicho proceso (Mangi et al., 2025).

En el caso de que una máquina como vehículos terrestres, barcos, drones, que estén dotadas de IA participen en un delito, la cuestión fundamental es quién asume la responsabilidad jurídica. Al respecto, la situación que se presentó con un vehículo autónomo de la empresa Uber, en 2018, resulta emblemático, según lo registran Andrade dos Santos et al. (2024). La capacidad de goce es universal para los seres humanos, mientras que la capacidad de ejercicio es para personas determinadas, lo que plantea un desafío para la personalidad jurídica de

la IA (Gutiérrez Proenza, 2022). Custers et al. (2025) comentan que incluso existe la propuesta de crear una “persona artificial” como categoría jurídica para la IA fuerte, pero su complejidad ha impedido su avance en la Unión Europea.

Ante la imposibilidad de atribuir mens rea e imputabilidad a la IA, el derecho penal está experimentando un cambio de enfoque, del actor individual al sistema y a la organización (Del Castillo, 2023). Por este motivo, la tendencia se está desplazando de centrarse únicamente en el actor humano individual, a considerar la responsabilidad de la entidad jurídica de una corporación y las fallas sistémicas que permitieron que la IA causara daño. Las personas jurídicas, aunque carentes de consistencia psicofísica, ya son sujetas de responsabilidad penal en muchos ordenamientos jurídicos nacionales. Igualmente, las organizaciones pueden ser responsabilizadas por no haber implementado programas de cumplimiento (compliance programs) o procedimientos adecuados para prevenir la comisión de delitos específicos (Mongillo, 2024).

Las empresas pueden incurrir en responsabilidad penal por negligencia o imprudencia, por ejemplo, al no supervisar adecuadamente los sistemas de IA que generan contenido ilegal o facilitan crímenes, o bien por complicidad, al habilitar o asistir actividades delictivas mediante el mal uso de herramientas, la supervisión insuficiente o la inacción deliberada (Singh, 2025). Asimismo, comenta Singh (2025) que la responsabilidad estructural definida como la responsabilidad por los daños causados por la IA, se vincula a los detalles técnicos del diseño del algoritmo, por lo que la IA no debería gozar de inmunidad categórica.

También, los riesgos de responsabilidad penal para las empresas de IA generativa, abarcan delitos relacionados con un determinado contenido como la explotación infantil, la incitación a la violencia, la difamación o las noticias falsas, o los

ciberdelitos en donde se incluyen las brechas de seguridad, así como violaciones de la propiedad intelectual y la privacidad de datos. Este cambio de enfoque es una adaptación crucial para el derecho penal, reconociendo que la culpa no reside en una mente, absolutamente inexistente, de la máquina, sino en el entorno gestionado por humanos que permitieron sus acciones perjudiciales, eludiendo así el debate filosófico sobre la personalidad de la IA (Herrera de las Heras, 2022; Pietropaoli y Campione, 2024, entre otros).

La jurisdicción y la incertidumbre regulatoria también se presentan como riesgos penales significativos. La naturaleza global y sin fronteras del despliegue de la IA genera una considerable incertidumbre jurídica para las empresas, lo que aumenta su exposición a la responsabilidad penal (Lidstone, 2024). El rápido avance de la IA supera el ritmo del desarrollo legislativo, lo que crea ambigüedad. Esto implica la necesidad de cooperación internacional y armonización en el derecho penal (Cordini, 2020) o, al menos, fundar directrices claras, para evitar un escenario caótico, en el que las empresas se enfrenten a una exposición jurídica impredecible en diferentes jurisdicciones, lo que podría obstaculizar el desarrollo responsable de la IA.

## **Modelos regulatorios vigentes y propuestas en el derecho comparado**

El análisis comparado de los modelos regulatorios para abordar la responsabilidad por daños causados por la IA autónoma, en la Unión Europea, Estados Unidos y América Latina revela enfoques diversos y en constante evolución.

La Unión Europea ha liderado el proceso en la regulación de la IA, con la entrada en vigor de su Reglamento de IA (AI Act) en agosto de 2024, la primera normativa integral de este tipo a nivel mundial (Álvarez Olaya, 2021; Madiega, 2023; Unión

Europea, 2024). Su objetivo es garantizar la seguridad y el cumplimiento de los valores europeos en el desarrollo y uso de la IA. El AI Act adopta un enfoque basado en el riesgo, clasificando los sistemas de IA en categorías: inaceptable se llama a lo prohibido, alto riesgo que viene a estar sujeto a requisitos estrictos, riesgo limitado y sin riesgo evidente (Unión Europea, 2024). Es fundamental destacar que, si bien el AI Act establece un sólido marco regulatorio para el uso de la IA, no aborda directamente las cuestiones de responsabilidad por daños. Para complementar este marco, la Directiva de Responsabilidad por Productos Defectuosos (PLD), en su versión actualizada (2024/2853), es crucial. Esta directiva establece la responsabilidad objetiva para los fabricantes por daños causados por productos defectuosos, incluyendo explícitamente software y sistemas de IA integrados (Unión Europea, 2024). Su alcance se ha ampliado para cubrir daños a la salud psicológica y la corrupción de datos (European Parliament, 2024).

Paralelamente, la Unión Europea propuso la Directiva de Responsabilidad por IA (AILD) en septiembre de 2022, con el fin de adaptar las normas de responsabilidad civil no contractual a la IA. Sus principios fundamentales incluían facilitar las reclamaciones de las víctimas mediante una presunción refutable de causalidad y facultar a los tribunales nacionales para ordenar la divulgación de pruebas sobre sistemas de IA de alto riesgo (European Parliament, 2023). Sin embargo, el 12 de febrero de 2025, la Comisión Europea anunció la retirada de esta propuesta, generando preocupación por la protección de las víctimas (Centre for Democracy and Technology, 2025, párr. 2). Esta decisión se produjo, en parte, por la presión de la industria, que argumentaba que la AILD añadiría complejidad legal y perjudicaría la competitividad, a la vez que se sugería que la PLD, recientemente adoptada, debía ser implementada y evaluada primero (MedTech Europe, 2025).

A pesar de la retirada inicial, las discusiones sobre el expediente se reanudaron y, en julio de 2024, la Comisión envió una versión actualizada de la propuesta (European Parliament, 2025). En este último documento también se plantea la posibilidad de que la AILD se transforme en un reglamento, aplicable directamente, en lugar de una directiva, además de que su alcance se extienda a software no-IA y que se establezca una responsabilidad conjunta a lo largo de la cadena de valor de la IA. Siempre es conveniente mantenerse alertas y en constante exigencia de estos reglamentos para establecer responsabilidades y proteger a las víctimas ante las grandes empresas.

Estados Unidos, como una de las economías más grandes del mundo y cuna de una fuente clave de innovación en IA, en Silicon Valley, sin duda es un campo de pruebas para nuevas ideas sobre la elaboración de políticas y un régimen regulatorio, centrado en abordar el papel de la tecnología de IA en la vida cotidiana de la población (Parinandi et al., 2024). En ese país, el enfoque federal ha sido menos prescriptivo y más centrado en la aplicación de las leyes existentes, como las de responsabilidad por productos y por negligencia, a las tecnologías de IA. La responsabilidad por productos se basa en la existencia de defectos de fabricación, diseño o la ausencia de advertencias adecuadas. La negligencia se aplica cuando hay una falta de diligencia razonable en el diseño, despliegue o mantenimiento de los sistemas de IA (Custers et al., 2025; Gil de Zúñiga et al., 2024; Navas Navarro, 2022).

El panorama regulatorio en Estados Unidos se caracteriza por ser fragmentado ya que continúa un debate sobre la conveniencia de establecer una moratoria en la regulación estatal de la IA para evitar una colcha de retazos o patchworks de leyes inconsistentes (Parinandi et al., 2024.) Sin embargo, los estados han tomado la iniciativa en la regulación de la IA, promulgando leyes que abordan la transparencia, la protección del consumidor y la discriminación algorítmica (Bryson, 2025).

El gobierno federal, por su parte, busca coordinar esfuerzos para promover la consistencia entre las regulaciones federales y estatales.

Como ejemplo de esta confusa situación, diversos casos judiciales han comenzado a sentar precedentes. Se han conocido incidentes con vehículos autónomos, como los de Tesla, Uber y otros, que han dado lugar a reclamaciones por defectos de producto y negligencia. Algunos casos han culminado en acuerdos extrajudiciales, mientras que otros han resultado en fallos a favor de los fabricantes, lo que subraya la complejidad de atribuir responsabilidad en estos escenarios (Parinardi et al., 2025). Adicionalmente, se registran al menos 11 casos de responsabilidad por productos que involucran IA generativa en los tribunales estadounidenses, con alegaciones de defectos de diseño, falta de advertencia y negligencia, así como potencial de causar daños físicos o lesiones corporales, como en el ya mencionado caso de los servicios de transporte de Uber (Andrade dos Santos et al., 2024). En el ámbito de los derechos de autor, se han presentado demandas contra desarrolladores de IA por el uso de material protegido en el entrenamiento de modelos, con resultados variados que demuestran que la legislación en esta área aún no está consolidada (Scoble y Acevedo, 2025).

En lo que respecta a América Latina, la mayoría de las jurisdicciones están adoptando un enfoque para la regulación de la IA con base en el riesgo, similar al modelo de la Unión Europea. Ello implica la prohibición de aplicaciones de riesgo inaceptable y el establecimiento de requisitos específicos para las de alto riesgo. Se observa una clara tendencia a inspirarse en marcos regulatorios de otras regiones, siendo el AI Act el más influyente (Ramírez Plascencia y Alonzo González, 2025).

Se ha conocido que, en Brasil, el Proyecto de Ley No. 2.338 de 2023 sigue siendo el más avanzado en la región. Adopta el

enfoque de riesgo de la UE, por lo que impone obligaciones a los agentes de IA sean desarrolladores, distribuidores o usuarios; se suma a esto la prohibición de sistemas de riesgo excesivo. La propuesta brasileña enfatiza la supervisión humana, los derechos a la explicación y contestación de las decisiones de IA, y establece marcos de responsabilidad civil con responsabilidad objetiva para sistemas de alto riesgo. Además, designa a la Autoridad Nacional de Protección de Datos (ANPD) como la autoridad competente para la supervisión (Atanasovska y Robeli, 2025).

En lo que respecta en Argentina, se busca un ecosistema de IA menos regulado, para fomentar la innovación y atraer inversión extranjera. Sin embargo, su Código Civil ya contiene disposiciones de responsabilidad objetiva para lo que denominan “actividades peligrosas” (Artículo 1757), que podrían aplicarse a los daños causados por la IA (Colombo, 2024; Ramírez Plascencia y Alonzo González, 2025).

También en Chile se siguen los lineamientos recomendados por la UNESCO (2023), por lo que se comenzó a desarrollar una política nacional de IA y un proyecto de ley para regular esta tecnología, igualmente con un enfoque basado en el riesgo. El proyecto de ley chileno abarca a proveedores e implementadores de IA (nacionales y extranjeros), así como importadores y distribuidores. Establece principios como la intervención humana, la privacidad, la protección de los derechos del consumidor y clasifica los sistemas de IA por su nivel de riesgo. Propone la creación de un Consejo Asesor Técnico de IA y asigna las facultades de supervisión y sanción a la Agencia de Protección de Datos Personales.

En Colombia, el Proyecto de Ley No. 422 de 2025 establece directrices para la regulación de la IA, con la inclusión de incentivos para la investigación y el desarrollo. A la par ofrece la clasificación de riesgos y medidas de responsabilidad civil y penal

para quienes impacten negativamente los sistemas de IA, con la obligación de compensar a las víctimas (Ramírez Plascencia y Alonzo González, 2025; Vanegas et al., 2024).

La situación de México, hasta el presente es diferente, pues no existe en este país una ley específica para la IA. Se han debatido modificaciones al Código Penal Federal con el propósito de criminalizar ciertas conductas relacionadas con la IA, pero estas iniciativas se encuentran en fase de análisis. Recientemente, la autoridad de privacidad de datos (INAI) ha emitido recomendaciones sobre el tratamiento de datos personales por parte de la IA (Ramírez Plascencia y Alonzo González, 2025).

En nuestro país, Venezuela, en noviembre de 2024, la Asamblea Nacional aprobó, en primera discusión el Proyecto de Ley de Inteligencia artificial. Este marco regulatorio plantea la creación de una Agencia Nacional de IA para supervisar y controlar el uso de la IA, con el propósito de promover la educación y el desarrollo ético. En su fase inicial, este instrumento legal se propone “proteger, evaluar e impulsar el desarrollo, uso y aplicaciones de la IA, garantizando el cumplimiento de los principios y derechos fundamentales que permita el desarrollo del país” (Villalta, 2024, párr. 3).

Está visto, por ende, que la polarización regulatoria global y sus implicaciones para la armonización son indudables. El análisis comparativo revela una clara dicotomía: el enfoque proactivo, integral y armonizado de la UE sobre la base del riesgo en sus diferentes etapas, frente a la dependencia más fragmentada y reactiva de los Estados Unidos en el derecho de daños y las iniciativas estatales. A su vez, es evidente que los países latinoamericanos se muestran influenciados, en gran medida, por el modelo de la UE. Esto sugiere un panorama regulatorio global que no converge de manera uniforme. La implicación para América Latina es que, si bien la adopción del marco basado en el riesgo de la UE ofrece un camino estructurado,

también supone heredar los desafíos e incertidumbres actuales de la UE. Esta polarización podría conducir a un arbitraje regulatorio o crear barreras para las empresas que operan en diferentes bloques, lo que destaca la necesidad de considerar cuidadosamente cuál modelo se adapta mejor al contexto legal y económico específico de la región latinoamericana.

Por otra parte, existe una brecha entre la regulación de la IA y la regulación de la responsabilidad. Es importante señalar que el AI Act de la UE, a pesar de ser una regulación integral de la IA, no aborda la responsabilidad por daños, como se ha apuntado (European Parliament, 2025). Esto revela una tendencia crítica subyacente: los organismos reguladores a menudo crean marcos que norman cómo debe desarrollarse y desplegarse la IA en cuanto a la seguridad, gestión de riesgos, transparencia, etc., todos desvinculados de las responsabilidades inherentes (Lund et al., 2025). Tal separación sugiere un reconocimiento de los distintos desafíos legales que plantea cada aspecto. Esto indica que un marco sólido de gobernanza de la IA, requiere no solo una ley reguladora de los sistemas de IA en sí mismos, sino también un régimen de responsabilidad específico y complementario, a fin de garantizar la compensación de las víctimas y fomentar el cumplimiento de las normas de seguridad del AI Act. La dificultad que se le plantea a la UE en lo concerniente a la AILD, pone de manifiesto la complejidad que implica cerrar de manera eficaz esta brecha (Custers et al., 2025).

## **Propuesta de un marco jurídico integrado para la responsabilidad de la IA autónoma**

Un marco jurídico integrado para la responsabilidad de la IA autónoma debe fundamentarse en principios rectores esenciales, que garanticen la seguridad, la transparencia, la explicabilidad, la auditabilidad y, sobre todo, coloque al ser humano como centro de toda ecuación. La regulación debe asegurar que la IA sea una herramienta para el progreso humano, protegiendo la dignidad y los derechos fundamentales. La transparencia y la explicabilidad (Explainable AI - XAI) son cruciales para facilitar la rendición de cuentas y la identificación de fallos (Asaro, 2016). Los sistemas de IA deben someterse a evaluación constante, utilizando datos de calidad, examinando sesgos, realizando pruebas de seguridad y manteniendo una supervisión continua. La seguridad debe garantizar que siempre una persona pueda manipular los sistemas (Gutiérrez Proenza, 2023) y que siempre existirá la supervisión humana efectiva a lo largo de todo el ciclo de vida de la IA (Atanasovska y Robeli, 2025).

En consecuencia, para abordar la complejidad de la atribución de responsabilidad y asegurar la reparación de las víctimas, se proponen dos mecanismos de compensación fundamentales. El primero contempla la creación de seguros obligatorios para desarrolladores y operadores de IA de alto riesgo. La tendencia en la Unión Europea hacia un modelo de responsabilidad objetiva, se complementa con la consideración de seguros de responsabilidad civil para la IA (Farajpour y Gunkel, 2025). La experiencia con vehículos autónomos ya muestra la relevancia de los seguros, como en el caso de algunos fabricantes que adquieren el compromiso de cubrir los daños causados por sus vehículos de ese tipo. El mercado de seguros para la IA está en evolución, reflejando paralelos con la emergencia de los ciberseguros, y reconociendo las limita-

ciones de los marcos de responsabilidad tradicionales (Wang y Wu, 2024). Debería considerarse como ejemplo la nueva implementación de seguros obligatorios como medida esencial para la gestión del riesgo y la protección de las víctimas (European Parliament, 2025).

El segundo mecanismo que apoyamos, firmemente, se refiere al establecimiento de fondos de compensación para víctimas de daños no atribuibles directamente. Esto significa que la creación de los fondos de compensación, financiados por fabricantes y operadores, debería ser una solución para cubrir los daños en aquellos casos en los que no sea posible determinar un responsable directo (Campillo, 2025). Esta estrategia regulatoria es valiosa para la gestión financiera de las pérdidas, especialmente cuando no hay evidencia clara de negligencia o imprudencia por parte de productores o programadores.

Estos mecanismos representan una transición desde la responsabilidad individual a la socialización del riesgo. Las propuestas de seguros obligatorios y fondos de compensación del European Parliament (2025) indican un cambio fundamental de la responsabilidad estrictamente basada en la culpa individual, a un modelo de socialización del riesgo de los daños inducidos por la IA. Si la atribución directa de la culpa es imposible o excesivamente costosa, la carga de la compensación se traslada a un mecanismo colectivo como los fondos de seguros o los fondos de la industria. Esto implica la aceptación social de que la IA, si bien beneficiosa, conlleva riesgos inherentes, a veces no identificables, que deben ser asumidos por la industria que se beneficia de ella, en lugar de dejar a las víctimas sin compensación. Esta es una solución pragmática a lo que puede denominarse “vacío de responsabilidad”, cuando no se puede encontrar una culpa humana específica.

En cuanto a la supervisión y controles efectivos de los sistemas de IA, como parte del marco jurídico integrado, estimamos

que son vitales para mitigar riesgos y garantizar la rendición de cuentas. En primer término, es esencial la creación de un órgano internacional o regional de auditoría y supervisión de IA. Se hace imperativo el establecimiento de una autoridad designada, que cuente con amplios poderes para imponer sanciones (Atanasovska y Robeli, 2025). Ejemplos de esta necesidad se observan en la propuesta de una Agencia Nacional de IA en Venezuela (Villalta, 2024) y la designación de la Autoridad Nacional de Protección de Datos (ANPD) en Brasil, como ente competente (Atanasovska y Robeli, 2025). Un órgano de auditoría garantizaría el cumplimiento de estándares éticos y de seguridad, la evaluación continua y la identificación de sesgos en los sistemas de IA.

Con la misma intención deben definirse requisitos de trazabilidad y documentación a lo largo del ciclo de vida de la IA. La Directiva de Responsabilidad por IA de la Unión Europea, en su propuesta contemplaba la facultad de los tribunales de ordenar la divulgación de pruebas, para facilitar las reclamaciones (Madiega, 2023). La implementación de sistemas de registro automático de operaciones es necesaria para evaluar la precisión y solidez de los sistemas, así como para identificar posibles problemas discriminatorios. En este sentido, las empresas deben adoptar políticas de gobernanza de IA, realizar evaluaciones de impacto y auditorías, y documentar los hallazgos de las evaluaciones de riesgos (JDSUPRA, 2025).

Todo ello debe implementarse no solo con posterioridad al hecho, sino también en la prevención y gobernanza proactivas de riesgos. Al exigir estas entradas de rendición de cuentas (National Telecommunications and Information Administration, 2024), el marco propuesto tiene como objetivo reducir la probabilidad de daños en primer lugar y, cuando estos ocurren, lograr que el proceso de atribución sea más factible. Ello requiere un cambio de un sistema legal puramente reactivo, a uno que permita el desarrollo y despliegue de la tecnología, a fin de minimizar futuros daños.

## **Modelo normativo armonizado, con énfasis en la realidad latinoamericana**

La construcción de un modelo normativo armonizado para la IA en América Latina debe partir de la adaptación de las mejores prácticas internacionales a las particularidades jurídicas, económicas y sociales de la región. La influencia de marcos regulatorios como el AI Act de la Unión Europea ya es palpable en Latinoamérica, lo que sugiere que adoptar los enfoques basados en el riesgo, similar al de la UE y Brasil (Atanasovska y Robeli, 2025; JDSUPRA, 2025; National Telecommunications and Information Administration, 2024). También, es oportuno considerar la aplicación de la responsabilidad objetiva para actividades riesgosas, un concepto que ya está presente en el derecho argentino (Colombo, 2024).

Está visto, que la realidad latinoamericana exige una consideración cuidadosa de la capacidad institucional para la supervisión y auditoría, así como la promoción de la innovación en economías en desarrollo. La protección de los derechos fundamentales y la dignidad humana deben ser valores centrales, como ya se observa en las propuestas legislativas latinoamericanas (Breceda Pérez, 2024). En el caso específico de Venezuela, el proyecto de Ley de IA y la propuesta de una Agencia Nacional de IA (Villalta, 2024), representan pasos iniciales que deben integrarse en un marco de responsabilidad más amplio y coherente.

Estas circunstancias permiten a América Latina evitar el ensayo y error observado en la UE, como en el caso de la retirada y revaluación de la AILD (Center for Democracy and Technology, 2025). Puede adoptar los elementos más maduros de los enfoques ya conocidos, evitando sus debilidades, como la separación inicial de la regulación de la IA de la responsabilidad o el enfoque fragmentado a nivel estatal. Esto implica el potencial de desarrollar un marco integrado más coherente y firme

desde el principio, específicamente adaptado a las realidades socioeconómicas y capacidades institucionales de la región, en lugar de limitarse a importar, de manera acrítica, modelos foráneos.

El fomento de la cooperación regional y la creación de estándares comunes son esenciales. La fragmentación regulatoria puede obstaculizar la innovación y el desarrollo tecnológico. La cooperación regional, ejemplificada por la influencia del EU AI Act en Brasil, Chile y Colombia, es un modelo a seguir. La armonización de leyes y la creación de estándares comunes, evitarían la proliferación de patchworks regulatorios, facilitando la inversión y el despliegue de la IA a escala regional (Bryson, 2025; UNESCO, 2023).

Igualmente, se estima conveniente la implementación gradual y flexible del marco normativo con la finalidad de establecer un marco legal que permita la adaptación a los avances tecnológicos, mediante mecanismos como los regulatory sandboxes propuestos en Brasil y Colombia (Atanasovska y Robeli, 2025; Ramírez Plascencia y Alonzo González, 2025). Con esto, es posible fomentar la investigación y el desarrollo de IA responsable a través de incentivos de diversa índole. Asimismo, se debe priorizar la formación de capacidades técnicas y legales para la supervisión y aplicación de la normativa, e implementar mecanismos de monitoreo continuo y revisión periódica de la ley para asegurar su relevancia y eficacia (Lindstone, 2024).

El rol crucial de las agencias de protección de datos en la gobernanza de la IA, es un aspecto fundamental. Varios países latinoamericanos, como Brasil y Chile, están confiando la supervisión y las facultades sancionadoras en materia de IA a sus autoridades de protección de datos ya existentes (Atanasovska y Robeli, 2025). Esto es una tendencia significativa y lógica, por cuanto los sistemas de IA dependen en gran medida de los

datos, y muchos de los perjuicios inducidos por la IA implican la privacidad de la información, los sesgos o las violaciones de los derechos fundamentales que recaen bajo la competencia de la protección de datos.

Así se entiende que las agencias de protección de datos, con sus mandatos y experiencias existentes en la gobernanza de ese tipo de información, se encuentran en una posición única para convertirse en organismos reguladores centrales a los efectos de la IA, especialmente en regiones donde las nuevas agencias dedicadas a la inteligencia artificial podrían tardar en establecerse o carecer de recursos. Esto también sugiere que los principios de protección de datos (privacidad desde el diseño, calidad de los datos, no discriminación) influirán en gran medida en la regulación de la IA en la región. Para tales propósitos, otra experiencia de Unión Europea con este tipo de regulaciones, también proporciona orientaciones aprovechables (European Parliament, 2025).

## **Conclusiones y recomendaciones**

La irrupción de los sistemas de inteligencia artificial autónoma ha expuesto vacíos legales significativos en los marcos de responsabilidad civil y penal existentes, los cuales fueron concebidos para un paradigma de acción y atribución de culpa inherentemente humano. La opacidad algorítmica, la autonomía decisional y la dificultad para imputar mens rea a una máquina, desafían los principios tradicionales de nexos causal, sujeto responsable, factor de atribución, tipicidad e imputabilidad. Esta disrupción exige una evolución jurídica que trascienda los paradigmas convencionales.

El análisis comparado revela una tendencia global hacia la adopción de la responsabilidad objetiva en el ámbito civil, especialmente para sistemas de IA de alto riesgo, como una solución pragmática para garantizar la compensación de las víctimas y fomentar la seguridad, dada la complejidad para probar la culpa. En el ámbito penal, la imposibilidad de atribuir elementos subjetivos a la IA impulsa un cambio hacia la responsabilidad de las personas jurídicas y la responsabilidad estructural, enfocándose en las fallas sistémicas y la falta de supervisión organizacional.

También conocemos los avances de la Unión Europea con un marco regulatorio integral basado en el riesgo (AI Act) y una Directiva de Responsabilidad por Productos Defectuosos que incluye la IA, aunque la propuesta de Directiva de Responsabilidad por IA (AILD) ha enfrentado una ruta incierta. Estados Unidos, por su parte, se apoya en la aplicación de leyes existentes con diferencias entre estados y América Latina sigue los pasos de la Unión Europea con ejemplos notables en Brasil, Chile y Colombia.

En este contexto, es pertinente formular una serie de recomendaciones para América Latina, con énfasis particular en la realidad venezolana: en primer lugar, debe adoptarse el enfoque de riesgo armonizado, con un marco regulatorio basado en el riesgo e inspirado en el modelo de la Unión Europea, pero adaptado a las particularidades jurídicas, económicas y sociales de cada país, así como de la región en su conjunto. Ello implica clasificar los sistemas de IA según su potencial de daño y establecer requisitos proporcionales.

En segundo lugar, es posible implantar un régimen de responsabilidad civil sólidamente estructurado, a cuyo efecto es conveniente priorizar la adopción de un régimen de responsabilidad objetiva para los daños causados por sistemas de IA de alto riesgo. Este régimen debe complementarse con la creación de seguros obligatorios para desarrolladores y operadores, y los fondos de compensación descritos para socializar el riesgo inherente a la tecnología. En completa correlación, en tercer lugar, podría desarrollarse un marco para la responsabilidad penal de las personas jurídicas, con normativas que responsabilicen a las empresas por la falta de supervisión adecuada, la ausencia de programas de cumplimiento (compliance programs, a la vez que de los fallos sistémicos en el diseño, desarrollo y despliegue de la IA que resulte en conductas delictivas.

En cuarto lugar, se recomienda establecer un órgano nacional o regional de auditoría y supervisión de IA, anclado a las autoridades de protección de datos, dada su experiencia en la gobernanza de datos, a la vez que debe tener facultades claras para exigir transparencia, trazabilidad, auditorías algorítmicas y la divulgación de pruebas en caso de incidentes. Como quinta observación se exhorta a la cooperación regional legislativa y técnica, entre los países latinoamericanos, con lo que se busca evitar la fragmentación regulatoria. La armonización de las leyes y la adopción de estándares comunes, facilitarán la

inversión, el desarrollo y el despliegue responsable de la IA en toda la región.

Es imperativo fortalecer, en sexto lugar, la educación y la capacitación, especialmente en la formación de jueces, abogados, reguladores y profesionales del derecho, con énfasis en las implicaciones técnicas y legales de la IA. Ya no es posible la aplicación justa y eficaz de las leyes sin la comprensión profunda de la tecnología. Estrechamente vinculada a la anterior, se anota como séptima sugerencia la promoción de la innovación ética y responsable, con la creación de incentivos para la investigación y el desarrollo de IA, incluyendo el uso de sandboxes regulatorios, es decir entornos controlados de pruebas que permitan la experimentación controlada y la adaptación normativa a la evolución tecnológica.

Finalmente, es importante resaltar que la IA autónoma representa un cambio de paradigma que exige una respuesta jurídica integrada y adaptable. Al establecer comparaciones entre las experiencias internacionales se puede adoptar un enfoque proactivo, que combine la protección de los derechos con la promoción de la innovación y los valores democráticos (Fornasier, 2021). De este modo, América Latina puede posicionarse como un referente en la gobernanza responsable de la IA, asegurando que esta tecnología sirva al progreso humano de manera segura y equitativa.

## Referencias

- Álvarez Olalla, M. P. (2021). Propuesta de reglamento en materia de responsabilidad civil por el uso de inteligencia artificial, del Parlamento Europeo, de 20 de octubre de 2020. *Revista CESCO de Derecho de Consumo*, (38), 1–10. <https://dialnet.unirioja.es/servlet/articulo?codigo=8001740>
- Andrade dos Santos, L., Minikel de Oliveira, L., Pedrolí Renz, R., & Bastiani Kretzer, T. (2024). Responsabilização penal da inteligência artificial: Uma revisão integrativa sobre a possibilidade de entidades tecnológicas serem criminalmente punidas. *Revista Avant*, 8(2), 98–113. <https://ojs.sites.ufsc.br/index.php/avant/article/view/7653>
- Arroyo Moreno, A. M. (2025). El impacto de la inteligencia artificial en la responsabilidad civil: Necesidad de normativa aplicable. *Revista Aranzadi Doctrinal*, (6), 1–22. <https://repositorio.ual.es/handle/10835/19404>
- Asaro, P. M. (2016, March). The liability problem for autonomous artificial agents. In *AAAI Spring Symposia* (pp. 190–194). <https://cdn.aaai.org/ocs/12699/12699-56141-1-PB.pdf>
- Atanasovska, D., & Robeli, L. (2025). Brazil's AI Act: A new era of AI regulation. *GDPR Local*. <https://gdprlocal.com/brazils-ai-act-a-new-era-of-ai-regulation>
- Benítez-Abarca, A. B., Chafra-Moina, S. P., Manosalvas-Vaca, M. A., & Saltos-Verdezoto, Y. M. (2025). Influencia de la inteligencia artificial en el derecho penal: Una revisión sistemática de la literatura. *Polo del Conocimiento*, 10(3), 3078–3095. <https://polodelconocimiento.com/ojs/index.php/es/article/view/9274/pdf>

- Blázquez Ruiz, F. J. (2022). La paradoja de la transparencia en la IA: Opacidad y explicabilidad. Atribución de responsabilidad. *Revista Internacional de Pensamiento Político*, (17), 261–272. <https://doi.org/10.46661/revintpensampolit.7526>
- Breceda Pérez, J. A. (2024). La dignidad humana frente a la inteligencia artificial: Un análisis ético y normativo en América Latina. *TraHs*, (18), 74–101. <https://doi.org/10.25965/trahs.6367>
- Bryson, D. (2025, July 13). Congress should have taken the federalist approach to AI regulation. *The Carolina Journal*. <https://www.carolinajournal.com/opinion/congress-should-have-taken-the-federalist-approach-to-ai-regulation/>
- Campillo, J. (2025). Impacto de la IA en el ámbito de la responsabilidad civil. *Auris. Strategy, Law and Ethics*. <https://auris.legal/impacto-de-la-ia-en-el-ambito-de-la-responsabilidad-civil/>
- Center for Democracy and Technology. (2025, February 12). *Press release: Withdrawal of the AI Liability Directive proposal raises concerns over justice for AI victims*. <https://cdt.org/press/>
- Colombo, M. (2024). Justificación del factor de atribución objetivo en la responsabilidad civil por daños causados por la inteligencia artificial. *Sistema Argentino de Información Jurídica*. <https://www.saij.gob.ar>
- Cordini, N. S. (2020). La armonización del derecho penal: Un proceso con diversos actores y a distintas velocidades. *Revista Jurídica Derecho*, 9(13), 51–70. <https://dialnet.unirioja.es/servlet/articulo?codigo=8986648>
- Custers, B., Lahmann, H., & Scott, B. I. (2025). From liability gaps to liability overlaps: Shared responsibilities and fiduciary duties in AI and other complex technologies. *AI & Society*, 40, 4035–4050. <https://link.springer.com/content/pdf/10.1007/s00146-024-02137-1.pdf>

- Del Castillo, E. (2023). Sobre la responsabilidad penal, el dolo y la imputabilidad. *Noticias Jurídicas*. <https://noticias.juridicas.com/conocimiento/articulos-doctrinales/18230-sobre-la-responsabilidad-penal-el-dolo-y-la-imputabilidad/>
- European Parliament. (2023). *Artificial Intelligence Liability Directive* (Briefing). European Parliamentary Research Service. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS\\_BRI\(2023\)739342\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf)
- European Parliament. (2024). *Proposal for a directive on adapting non-contractual liability rules to artificial intelligence* (Study). European Parliamentary Research Service. [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS\\_STU\(2024\)762861\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS_STU(2024)762861_EN.pdf)
- European Parliament. (2025). *Legislative Train (06/2025): A new plan for Europe's sustainable prosperity and competitiveness – AI liability directive*. <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-ai-liability-directive>
- Farajpour, R., & Gunkel, D. (2025). Legal and comparative analysis of civil liability of artificial intelligence in automated decision-making. *AI and Tech in Behavioral and Social Sciences*, 3(1), 168–176. <https://www.sid.ir/paper/1496998/en>
- Fornasier, M. O. (2021). Inteligência artificial e democracia: Oportunidades e desafios. *NOMOS: Revista do Programa de Pós-Graduação em Direito da UFC*, 41(1), 171–194. <http://repositorio.ufc.br/handle/riufc/62264>
- Gil de Zúñiga, H., Goyanes, M., & Durotoye, T. (2024). A scholarly definition of artificial intelligence (AI): Advancing AI as a conceptual framework in communication research. *Political Communication*, 41(2), 317–334. <https://doi.org/10.1080/10584609.2023.2290497>

- Glock, P., & von Alemann, S. (2022). The paradigm shift in AI: From human labor to humane creativity. In *Liquid legal—Humanization and the law: Law for professionals* (pp. 215–230). Springer Nature. [https://link.springer.com/chapter/10.1007/978-3-031-14240-6\\_11](https://link.springer.com/chapter/10.1007/978-3-031-14240-6_11)
- Gutiérrez Proenza, J. (2022). La responsabilidad jurídica de la inteligencia artificial desde el derecho clásico. *Axioma. Revista Científica de Investigación, Docencia y Proyección Social*, (27), 19–25. <https://pucesinews.pucesi.edu.ec/index.php/axioma/article/view/808>
- Herbosch, M. (2025). Liability for AI agents. *North Carolina Journal of Law & Technology*, 26(3), 391–458. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=5236649](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5236649)
- Herrera de las Heras, R. (2022). Aspectos legales de la inteligencia artificial: Personalidad jurídica de los robots, protección de datos y responsabilidad civil. *Dickinson*. <https://doi.org/10.48550/arXiv.2306.02781>
- Huang, K., Joshi, A., Dun, S., & Hamilton, N. (2024). AI regulations. In *Generative AI security: Theories and practices* (pp. 61–98). Springer Nature Switzerland. [https://link.springer.com/chapter/10.1007/978-3-031-54252-7\\_3](https://link.springer.com/chapter/10.1007/978-3-031-54252-7_3)
- JDSupra. (2025). *AI Watch: Global regulatory tracker—Brazil*. <https://www.jdsupra.com/legalnews/ai-watch-global-regulatory-tracker-8973398/>
- Lee, S. (2025). The role of *mens rea* in modern law: Analyzing the impact of *mens rea* on criminal justice and its future directions. *Number Analytics*. <https://www.numberanalytics.com/blog/mens-rea-role-in-modern-law>
- Lidstone, H. K. (2024). Navigating the challenges of generative AI. *BFW Attorneys*. <http://dx.doi.org/10.2139/ssrn.5004973>

- Lund, B., Orhan, Z., Mannuru, N. R., Bevara, R. V. K., Porter, B., Vinaih, M. K., & Bhaskara, P. (2025). Standards, frameworks, and legislation for artificial intelligence (AI) transparency. *AI and Ethics*, 5, 3639–3655. <https://doi.org/10.1007/s43681-025-00661-4>
- Macchia, M., & Mascolo, A. (2022). Intelligenza artificiale e regolazione. In *Intelligenza artificiale e diritto: Una rivoluzione?* (pp. 67–100). Il Mulino. <https://art.torvergata.it/bitstream/2108/315774/1/2022%20Int%20art%20e%20regolaz.pdf>
- Madiega, T. (2023). *Artificial Intelligence Liability Directive* (Briefing). European Parliamentary Research Service (EPRS). <https://courses.ilac.eu/wp-content/uploads/2023/03/AI-DIRECTIVE.pdf>
- Mangi, D., Butro, I., & Memon, T. (2025). AI and criminal liability: Theoretical dilemmas in applying criminal law to artificial intelligence. *The Critical Review of Social Sciences Studies*, 3(2), 2174–2186. <http://thecrsss.com/index.php/Journal/article/view/608>
- MedTech Europe. (2025). *Industry coalition calls for withdrawal of AI Liability Directive*. <https://www.medtecheurope.org/news-and-events/news/industry-coalition-calls-for-withdrawal-of-ai-liability-directive/>
- Mongillo, V. (2024). Responsabilidad penal y extrapenal de las personas jurídicas por delitos relacionados con la inteligencia artificial: Vías de intervención legal y principales obstáculos. *REDEPEC: Revista Electrónica de Responsabilidad Penal de Personas Jurídicas y Compliance*, (4), 2–26. <https://dialnet.unirioja.es/servlet/articulo?codigo=9730873>
- National Telecommunications and Information Administration. (2024). *Liability rules and standards*. <https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report/using-accountability-inputs/liability-rules-and-standards>

- Navas Navarro, S. (2022). Responsabilidad civil e inteligencia artificial. *El Cronista del Estado Social y Democrático de Derecho*, (100), 106–115. [https://www.elcronista.es/sumario\\_numero\\_100.asp](https://www.elcronista.es/sumario_numero_100.asp)
- Ormazábal Sánchez, G. (2024). La prueba en los procesos de responsabilidad civil por daños causados por sistemas de inteligencia artificial. *InDret. Revista para el Análisis del Derecho*, (3), 395–445. <https://doi.org/10.31009/InDret.2024.i3.12>
- Parinandi, S., Crosson, J., Peterson, K., & Nadarevic, S. (2024). Investigating the politics and content of US state artificial intelligence legislation. *Business and Politics*, 26(2), 240–262. <https://doi.org/10.1017/bap.2023.40>
- Pietropaoli, S., & Campione, R. (2024). Los artefactos de la inteligencia jurídica: Personas y máquinas. *Dickinson*.
- Ramírez Plascencia, D., & Alonzo González, R. M. (2025). The rise of artificial intelligence in Latin America. In *Ethical and legal dilemmas of artificial intelligence in Latin America* (pp. 1–18). Springer Nature Switzerland.
- Reyes Alvarado, Y. (2024). Imputabilidad e imputación. *InDret. Revista para el Análisis del Derecho*, (2), 233–266. <https://doi.org/10.31009/InDret.2024.i2.06>
- Romero Boue, H. (2024). Responsabilidad civil en el uso de la inteligencia artificial. *Diálogos y Voces Judiciales*, 2(2), 20–33. <https://doi.org/10.5281/zenodo.14508578>
- Scoblete, G., & Acevedo, M. (2025). GenAI product liability cases are making their way through the courts: Here’s what we’re watching. *Verisk*. <https://core.verisk.com/Insights/Emerging-Issues/Articles/2025/May/Week-4/GenAI-Product-Liability-Cases>
- Scott, G., Tener, O., & Thurbon, R. (2024). The world’s first AI regulation is here. *Goodwin*. <https://www.goodwinlaw.com/en/insights/publications/2024/03/alerts-practices-aiml-series-1-the-worlds-first-ai-regulation-is-here>

- Sharipov, R. (2025). Analysis and reduction of errors in AI models. *The American Journal of Engineering and Technology*, 7(05), 202–210. <https://doi.org/10.37547/tajet/Volume07Issue05-20>
- Singh, C. (2025). Is generative AI (artificial intelligence) the next advent in the evolution of finance and navigating financial crime and regulation? *Journal of Financial Crime*, 32(3), 751–759. <https://www.emerald.com/insight/content/doi/10.1108/jfc-07-2024-0232/full/html>
- UNESCO. (2023). *Readiness assessment methodology: A tool of the Recommendation on the Ethics of Artificial Intelligence*. <https://unesdoc.unesco.org/ark:/48223/pf0000385198>
- Unión Europea. (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo*. Diario Oficial de la Unión Europea. [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401689)
- Vanegas, W. J., Santamaría, M., & Molina, M. (2024). Políticas públicas ante la revolución de la inteligencia artificial en Colombia. *Revista Venezolana de Gerencia (RVG)*, 29(106), 865–883. <https://dialnet.unirioja.es/servlet/articulo?codigo=9394102>
- Villalta, L. (2024, November 11). AN aprueba en primera discusión Proyecto de Ley de Inteligencia artificial. *Asamblea Nacional de la República Bolivariana de Venezuela*. <https://www.asambleanacional.gob.ve/noticias/an-aprueba-en-primera-discusion-proyecto-de-ley-de-inteligencia-artificial>
- Wang, X., & Wu, Y. C. (2024). Balancing innovation and regulation in the age of generative artificial intelligence. *Journal of Information Policy*, 14, 385–416. <https://doi.org/10.5325/jinfopoli.14.2024.0012>
- Yampolskiy, R. V. (2020). Unpredictability of AI: On the impossibility of accurately predicting all actions of a smarter agent. *Journal of Artificial Intelligence and Consciousness*, 7(01), 109–118. <https://doi.org/10.1142/S2705078520500034>

- Yazdanpanah, V., Gerding, E. H., Stein, S., Dastani, M., Jonker, C. M., Norman, T. J., & Ramchurn, S. D. (2023). Reasoning about responsibility in autonomous systems: Challenges and opportunities. *AI & Society*, 38(4), 1453–1464. <https://link.springer.com/article/10.1007/s00146-022-01607-8>
- Zabala Leal, T. D., & Gómez McFarland, C. A. (2024). La responsabilidad civil y la ética en la inteligencia artificial: Una revisión sistemática de las ideas del período 2018–2023. *IUS-*TA**, (60), 66–93. <https://doi.org/10.15332/25005286.9964>

