



RESPONSABILIDAD CIVIL POR DAÑOS DERIVADOS DEL USO DE INTELIGENCIA ARTIFICIAL¹

Laura Vanessa CORDERO LÓPEZ*

SUMARIO: I. *Introducción.* II. *Aproximación a la noción de “inteligencia artificial”.* Rasgos características y definición. III. *La inteligencia artificial y sus desafíos frente a los modelos jurídicos tradicionales;* IV. *Tipos de daños generados por sistemas de Inteligencia Artificial; Daños patrimoniales.* V. *Daños extrapatrimoniales.* VI. *Imputación jurídica y problemas probatorios en los daños derivados de Inteligencia Artificial.* VII. *El régimen civil aplicable a la Inteligencia Artificial.* VIII. *La responsabilidad civil subjetiva aplicada a la Inteligencia Artificial.* IX. *La responsabilidad objetiva aplicada a la Inteligencia Artificial.* X. *La responsabilidad por productos defectuosos y sistemas de Inteligencia Artificial.* XI. *Derecho comparado sobre regulación de la Inteligencia Artificial: México e instrumentos internacionales.* XII. *Estándares y criterios internacionales relevantes.* XIII. *Conclusiones.* XIV. *Bibliografía.*

Resumen: El presente artículo analiza el régimen de responsabilidad civil aplicable a los daños derivados del uso de sistemas de Inteligencia Artificial (IA) en México. Examina los desafíos que estas tecnologías plantean a los modelos jurídicos tradicionales debido a su autonomía, complejidad técnica (cajas negras algorítmicas) y la multiplicidad de actores involucrados en su desarrollo y operación. Se exploran los daños patrimoniales y

¹ Trabajo recibido el 1 de mayo de 2026 y aprobado el 29 de junio de 2026

* Licenciada en derecho, estudiante de la especialidad de derecho civil de la disciplina responsabilidad civil de la Facultad de Derecho de la UNAM.

extrapatrimoniales generados por la IA, así como la viabilidad de aplicar la responsabilidad civil subjetiva, la responsabilidad objetiva por riesgo creado y la responsabilidad por productos defectuosos. Apoyándose en el derecho comparado y estándares internacionales, el trabajo concluye que es necesario reinterpretar el marco jurídico nacional mediante figuras como la carga dinámica de la prueba y el deber de colaboración procesal, garantizando así el acceso a una reparación integral ante los nuevos riesgos tecnológicos.

Palabras clave: Caja negra algorítmica, Carga dinámica de la prueba, Inteligencia artificial, Reparación integral, Responsabilidad civil objetiva, Riesgo creado.

Abstract: This article analyzes the civil liability regime applicable to damages resulting from the use of Artificial Intelligence (AI) systems in Mexico. It examines the challenges these technologies pose to traditional legal models due to their autonomy, technical complexity (algorithmic black boxes), and the multiplicity of actors involved in their development and operation. The patrimonial and extra-patrimonial damages generated by AI are explored, along with the feasibility of applying subjective civil liability, objective liability for created risk, and product liability. Drawing on comparative law and international standards, the paper concludes that it is necessary to reinterpret the national legal framework through concepts such as the dynamic burden of proof and the duty of procedural collaboration, thereby ensuring access to comprehensive reparation in the face of new technological risks.

Keywords: Algorithmic black box, Artificial intelligence, Comprehensive reparation, Created risk, Dynamic burden of proof, Objective civil liability.

I. INTRODUCCIÓN

El avance tecnológico de las últimas décadas ha propiciado la incorporación gradual de sistemas de Inteligencia Artificial en sectores estratégicos de la vida económica y social.

La utilización de Inteligencia Artificial ha incrementado la posibilidad de generar daños de naturaleza civil. Entre ellos destacan pérdidas económicas ocasionadas por decisiones automatizadas incorrectas, afectaciones al honor o reputación derivadas de la creación o difusión de contenido falso, prácticas discriminatorias atribuibles a errores en las

instrucciones ordenadas a la Inteligencia Artificial, bloqueos indebidos de servicios esenciales, así como daños físicos en actividades de alto riesgo, como la medicina o el transporte.

En este contexto, surge un problema relevante al pretender encuadrar tales afectaciones dentro del régimen tradicional de responsabilidad civil. En el Derecho Civil mexicano, la responsabilidad civil se estructura a partir de elementos clásicos, una conducta, la existencia de un daño, un nexo causal y un factor de imputación, usualmente basado en la culpa o el dolo. Sin embargo, los daños producidos por sistemas de Inteligencia Artificial presentan una dificultad particular ya que pueden materializarse sin una intervención humana inmediata o identificable, debido a que el resultado se origina en procesos automatizados que operan de manera autónoma o semi-autónoma. A ello se suma que, en muchos casos, el funcionamiento interno del sistema resulta opaco o técnicamente complejo, lo cual dificulta explicar con claridad el origen de la decisión incluso para quienes lo desarrollan o implementan.

El objetivo del presente trabajo consiste en analizar el régimen de responsabilidad civil aplicable a los daños derivados del uso de sistemas de Inteligencia Artificial en México. A partir de ello, se busca determinar si el marco civil vigente ofrece herramientas suficientes para garantizar una reparación efectiva del daño, o si resulta necesario recurrir a interpretaciones más amplias mediante figuras como la responsabilidad objetiva por riesgo creado, la obligación de seguridad u otras categorías jurídicas que permitan responder adecuadamente ante este tipo de afectaciones.

II. APROXIMACIÓN A LA NOCIÓN DE “INTELIGENCIA ARTIFICIAL.

RASGOS CARACTERÍSTICAS Y DEFINICIÓN

La Inteligencia Artificial es una tecnología que permite a las computadoras y máquinas simular el aprendizaje humano, la comprensión, la resolución de problemas, la toma de decisiones, la creatividad y la autonomía.

En este sentido, la Real Academia Española ha señalado que la Inteligencia Artificial comprende funciones tales como razonar, emplear el lenguaje, ya sea para traducir entre idiomas, mantener una conversación oral o escrita con una máquina para resolver una tarea, clasificar documentos, crear imágenes a partir de descripciones en lenguaje natural,

reconocer objetos en fotografías e, incluso, aprender de nuestra conducta o costumbres, y de esa forma recomendar la compra de un producto o seleccionar la siguiente canción, por mencionar solo algunas de esas múltiples posibilidades.²

En el contexto de la regulación de la Inteligencia Artificial, la propia Organización para la Cooperación y el Desarrollo Económicos (OECD) ofrece una descripción operativa de lo que constituye un sistema de Inteligencia Artificial. Según esta institución, un sistema de Inteligencia Artificial es un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir de los datos de entrada que recibe, cómo generar información de salida como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos reales o virtuales. Una vez implementados, los distintos sistemas de Inteligencia Artificial presentan diversos niveles de autonomía y varían en su capacidad de adaptación.³ En el ámbito europeo, el Parlamento de la Unión Europea ha advertido tempranamente la necesidad de construir un marco conceptual claro para el análisis jurídico de la robótica y la inteligencia artificial. En particular, en su Resolución con recomendaciones a la Comisión sobre normas de Derecho Civil en materia de robótica, se reconoce que la ausencia de definiciones uniformes constituye un obstáculo para el desarrollo de criterios regulatorios coherentes. Por ello, se enfatiza que cualquier concepto jurídico de robot o de inteligencia artificial debe formularse de manera suficientemente amplia y flexible, a fin de evitar que la regulación limite indebidamente la investigación científica o el avance tecnológico.

Bajo dicha perspectiva, el Parlamento exhorta a la Comisión a impulsar definiciones comunes dentro de la Unión Europea respecto de categorías como los sistemas ciberfísicos, los robots autónomos inteligentes, incluyendo sus posibles subcategorías. Asimismo, propone que tales definiciones se construyan tomando como base ciertas características compartidas por los robots inteligentes: la adquisición de autonomía mediante sensores o mediante el intercambio de información con el entorno; la capacidad de autoaprendizaje a

² GÓMEZ-PÉREZ, Asunción. Discurso de ingreso a la Real Academia Española. Madrid: Real Academia Española, 2023, p. 17. https://www.rae.es/sites/default/files/2023-05/Discurso%20Ingreso%20Asuncion%20Gomez-Perez_0.pdf

³ OECD. OECD Principles on Artificial Intelligence. París: OECD Publishing, 2019. <https://www.oecd.org/en/topics/ai-principles.html>

partir de la experiencia e interacción; la existencia de un soporte físico mínimo; la posibilidad de adaptar su conducta al medio en el que opera; y la ausencia de vida en sentido biológico.⁴ De forma complementaria a la Resolución sobre Derecho Civil y Robótica, la Unión Europea ha concretado su política regulatoria mediante la promulgación de un marco jurídico específico sobre inteligencia artificial, conocido como la Ley de Inteligencia Artificial de la Unión Europea (AI Act). Este instrumento constituye la primera normativa jurídica integral en el mundo destinada a regular de manera sistemática el desarrollo, comercialización y uso de sistemas de Inteligencia Artificial dentro del territorio comunitario. Su propósito es garantizar que el despliegue tecnológico de estas herramientas se realice bajo criterios de seguridad, confiabilidad, transparencia y respeto a los derechos fundamentales, sin obstaculizar el avance de la innovación.⁵

El AI Act adopta un enfoque basado en niveles de riesgo, según el cual los sistemas de Inteligencia Artificial se analizan y clasifican conforme al peligro potencial que pueden generar para las personas y la sociedad. En función de esa clasificación, se establecen obligaciones de cumplimiento diferenciadas: desde la prohibición de prácticas consideradas de riesgo inaceptable hasta requisitos específicos para sistemas de alto riesgo.

Esta lógica de riesgo busca equilibrar la promoción del desarrollo tecnológico con la protección frente a perjuicios que puedan afectar la seguridad, la dignidad humana o los derechos colectivos.⁶

III. LA INTELIGENCIA ARTIFICIAL Y SUS DESAFÍOS FRENTE A LOS MODELOS JURÍDICOS TRADICIONALES

Los análisis doctrinales y legislativos contemporáneos han señalado que ciertas características intrínsecas de los sistemas de inteligencia artificial plantean desafíos significativos frente a los modelos jurídicos tradicionales.

⁴ PARLAMENTO EUROPEO. Resolución de 16 de febrero de 2017 con recomendaciones destinadas a la Comisión sobre normas de Derecho Civil sobre robótica (2015/2103(INL)). Estrasburgo, 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html

⁵ PARLAMENTO EUROPEO. Civil Liability Regime for Artificial Intelligence. Bruselas: Directorate-General for Internal Policies of the Union, 2020, pp. 17-20.

⁶ PARLAMENTO EUROPEO. Ley de inteligencia artificial de la UE: primera normativa sobre inteligencia artificial. Bruselas, 2023. <https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primer-normativa-sobre-inteligencia-artificial>

Según la European Parliamentary Research Service, que ha examinado la relación entre los sistemas de Inteligencia Artificial y el derecho civil, estos desafíos se derivan de rasgos técnicos que dificultan la aplicación de los elementos clásicos de imputación, causalidad y atribución de responsabilidad, tal como los entiende el Derecho Civil tradicional.⁷

En primer lugar, la capacidad de inferencia y decisión autónoma de los sistemas de Inteligencia Artificial implica que estos no funcionan exclusivamente sobre la base de instrucciones humanas directas en cada operación, sino que pueden generar salidas a partir de patrones aprendidos o inferidos de los datos. Esta autonomía operativa contrasta con la noción clásica de conducta humana imputable, ya que el resultado no siempre puede asociarse a una acción u omisión clara de una persona física o jurídica. Dicha independencia funcional complica la determinación del sujeto responsable, puesto que la relación causal entre la acción humana y el daño producido por el sistema no es necesariamente directa o inmediata.⁸

Otra característica que desafía al derecho consiste en la naturaleza compleja de los algoritmos empleados en muchas aplicaciones de Inteligencia Artificial. Los modelos basados en técnicas avanzadas como aprendizaje profundo pueden comportarse como “cajas negras” (conocidas por su nombre en inglés como (Black Box), en las que no resulta sencillo reconstruir o explicar el proceso interno que condujo a una decisión particular, la cual enera dificultades probatorias en los procesos judiciales, pues la carga de acreditar causalidad se ve entorpecida si no es factible determinar con claridad cómo y por qué se produjo el resultado dañino.⁹

Además, los sistemas de Inteligencia Artificial tienden a operar sobre grandes volúmenes de datos y criterios de probabilidad, lo que introduce variabilidad en sus resultados incluso frente a condiciones de entrada similares. Cuando un sistema modifica su output en función de la evolución de los datos o del aprendizaje continuo, se vuelve más

⁷ BERTOLINI, Andrea. Artificial Intelligence and Civil Liability. Bruselas: European Parliament, 2025, p. 9.

⁸ BERTOLINI, Andrea. Artificial Intelligence and Civil Liability, *op. cit.*, pp. 17-20.

⁹ BERTOLINI, Andrea. Artificial Intelligence and Civil Liability, *op. cit.*, pp. 22-27.

complejo definir qué se entiende por conducta esperada o diligente en su creación y uso, lo que a su vez incide en la evaluación de culpa o negligencia.¹⁰

El funcionamiento de un sistema de Inteligencia Artificial suele involucrar diversos sujetos como desarrolladores, proveedores, implementadores, distribuidores y usuarios finales y esto complica la determinación del responsable jurídico, pues el daño puede derivarse de decisiones técnicas tomadas en distintas fases del diseño, entrenamiento, comercialización o uso del sistema.

IV. TIPOS DE DAÑOS GENERADOS POR SISTEMAS DE INTELIGENCIA ARTIFICIAL

La responsabilidad civil implica el deber de asumir las consecuencias derivadas de un incumplimiento contractual o de un hecho ilícito o riesgoso que produce una afectación a otra persona. En este sentido, la identificación del daño en el uso de sistemas de Inteligencia Artificial resulta determinante para delimitar el alcance de la reparación donde los daños pueden manifestarse tanto en el ámbito patrimonial como en el extrapatrimonial, dependiendo del bien jurídico afectado.

V. DAÑOS PATRIMONIALES

Los daños patrimoniales son aquellos que implican una pérdida o menoscabo en el patrimonio de la víctima, entendido como el conjunto de bienes, dinero o derechos con contenido económico. Se trata de un daño pecuniario susceptible de valoración monetaria, por lo que, en principio, puede ser cuantificado y reparado mediante una indemnización que, en el caso de la Inteligencia Artificial, suele presentarse como consecuencia de decisiones automatizadas erróneas, fallas en procesos de clasificación, ejecución indebida de operaciones o interrupción de servicios digitales esenciales.

- a) *Pérdidas económicas directas*: Este tipo de daño se manifiesta por el menoscabo inmediato y verificable en el patrimonio de la víctima, producido como consecuencia de una decisión, operación o acto que impacta directamente en sus recursos o bienes.

¹⁰ EUROPEAN COMMISSION. White Paper on Artificial Intelligence: A European Approach to Excellence and Trust. Bruselas: European Union, 2020, p. 12.

Estas pérdidas pueden derivar del funcionamiento de sistemas de Inteligencia Artificial financieros automatizados que ejecutan operaciones de compra o venta en lapsos extremadamente breves, sin intervención humana directa. La velocidad y autonomía del sistema amplifican el riesgo, ya que una decisión errónea puede producir un impacto económico inmediato y significativo. Asimismo, pueden presentarse en sistemas de Inteligencia Artificial para la evaluación crediticia o de seguros que, mediante modelos de clasificación, rechazan solicitudes sin una revisión humana efectiva, ocasionando pérdidas asociadas a oportunidades comerciales o financieras frustradas.

- b) *Daños emergentes y lucro cesante*: El daño emergente consiste en la pérdida efectiva, directa y actual sufrida por la víctima, expresada en gastos realizados o en deudas adquiridas como consecuencia del hecho que haya causado el daño. Este supuesto puede observarse cuando una persona incurre en cargos adicionales, comisiones indebidas, multas o gastos derivados de un error automatizado, por ejemplo, el bloqueo injustificado de una cuenta bancaria o de una cuenta de pagos que genera cargos por mora, pagos atrasados o la pérdida de saldo por operaciones no previstas. Por su parte, el lucro cesante se refiere a la ganancia legítima que la víctima dejó de percibir debido al daño sufrido. No implica un egreso, sino una privación de ingresos futuros que razonablemente se habrían obtenido si el hecho no hubiese ocurrido. Esto puede presentarse cuando impide el acceso a un servicio financiero o comercial indispensable para realizar actividades económicas. Por ejemplo, la cancelación automática de una cuenta de pagos o de una plataforma de comercio electrónico puede generar que el usuario deje de recibir ingresos derivados de ventas, pagos recurrentes o contratos que dependían de la disponibilidad de dicho servicio.
- c) *Costos de reparación*: Cuando un sistema inteligente produce una pérdida de información crítica o afecta bases de datos empresariales, la recuperación puede implicar costos elevados de reconstrucción, auditoría o restauración tecnológica. Asimismo, debido a que los sistemas de Inteligencia Artificial suelen operar mediante modelos complejos, la víctima puede verse obligada a contratar especialistas o peritos para intentar demostrar el nexo causal o identificar la falla técnica. Esta situación incrementa el impacto patrimonial del daño, no tanto por el hecho inicial, sino por las

cargas económicas necesarias para lograr una reparación efectiva y jurídicamente exigible.

VI. DAÑOS EXTRAPATRIMONIALES

Los daños extrapatrimoniales son aquellos que afectan bienes jurídicos no económicos, como la dignidad, la reputación, el honor, la integridad moral o la vida privada. Aunque no se traducen de forma inmediata en una pérdida monetaria, su afectación es jurídicamente relevante, pues implica la lesión de derechos fundamentales y de aspectos esenciales de la personalidad.

Este tipo de daños adquiere particular relevancia debido a que los sistemas de Inteligencia Artificial pueden producir afectaciones masivas mediante generación de contenido, difusión de información falsa, decisiones discriminatorias o tratamiento indebido de datos personales.

a) *Daño moral:*

El daño moral constituye una afectación a la esfera personal y extrapatrimonial del individuo, relacionada con bienes jurídicos como la dignidad, el honor, la reputación, la imagen, la vida privada o la estabilidad emocional. A diferencia de los daños patrimoniales, su configuración no depende necesariamente de una pérdida económica cuantificable, sino de la lesión a derechos de la personalidad reconocidos y protegidos por el derecho civil.

En el sistema jurídico mexicano, la reparación de este tipo de afectaciones encuentra fundamento en el artículo 1910 del Código Civil Federal, el cual establece que quien, obrando ilícitamente o contra las buenas costumbres, cause un daño a otro, se encuentra obligado a repararlo, salvo que demuestre que el daño se produjo por culpa o negligencia inexcusable de la víctima.¹¹

En el contexto de la inteligencia artificial, el daño moral adquiere particular relevancia debido a la capacidad de los sistemas automatizados para generar, replicar y difundir contenido de manera masiva e inmediata. Este tipo de afectación puede manifestarse, por ejemplo, mediante la creación automatizada de contenido falso, imágenes manipuladas, audios alterados o deepfakes que atribuyen a una persona conductas, expresiones o

¹¹ MÉXICO. Código Civil Federal, artículo 1910, Diario Oficial de la Federación, última reforma publicada el 26 de marzo de 2024.

hechos inexistentes. Asimismo, puede producirse cuando sistemas algorítmicos difunden información errónea o inexacta que impacta negativamente la reputación profesional, social o personal del individuo afectado.

La gravedad de estas afectaciones se incrementa cuando la información es difundida a través de plataformas digitales y sistemas automatizados con amplio alcance de propagación. En estos supuestos, la lesión no recae primordialmente sobre el patrimonio de la víctima, sino sobre bienes inmateriales cuya tutela corresponde al régimen de daño moral previsto en el derecho civil mexicano.

De igual forma, la utilización de sistemas de inteligencia artificial en procesos de toma de decisiones automatizadas puede generar formas indirectas de discriminación algorítmica. Cuando un sistema reproduce sesgos contenidos en los datos con los que fue entrenado y produce exclusiones injustificadas en ámbitos como empleo, crédito, seguros o acceso a servicios, la afectación trasciende el plano económico y puede constituir una vulneración a la igualdad, dignidad y reconocimiento social de la persona.

La capacidad de la inteligencia artificial para amplificar contenido falso, replicar sesgos o automatizar decisiones con impacto directo en la esfera personal de los individuos demuestra que los daños derivados de estas tecnologías no deben analizarse exclusivamente desde una lógica patrimonial o técnica.

- b) *Afectación a la privacidad y a los datos personales*: La afectación a la privacidad ocurre cuando se vulnera el control que una persona tiene sobre su información personal, su vida privada o sus datos sensibles. Los sistemas de Inteligencia Artificial suelen operar mediante el procesamiento intensivo de datos, lo cual incrementa la probabilidad de uso indebido, filtraciones o perfiles automatizados que exceden el consentimiento otorgado y se presentan cuando sistemas de Inteligencia Artificial recolectan información de navegación, hábitos de consumo, ubicación o preferencias personales para elaborar perfiles predictivos sin transparencia suficiente. Ello puede derivar en exposición indebida de datos, vigilancia algorítmica o explotación de información personal para fines comerciales, sin que el titular tenga un control real sobre el tratamiento.
- c) *Discriminación algorítmica*: La discriminación algorítmica se produce cuando un sistema automatizado reproduce o amplifica sesgos presentes en los datos de entrenamiento o en los criterios de clasificación, generando decisiones que afectan injustificadamente a

ciertos grupos sociales. Este daño se observa en procesos automatizados de selección laboral, evaluación crediticia, asignación de beneficios o acceso a servicios. Si los datos históricos utilizados para entrenar el sistema reflejan desigualdades previas, el modelo puede reproducirlas, afectando derechos fundamentales como la igualdad y la no discriminación.

VII. IMPUTACIÓN JURÍDICA Y PROBLEMAS PROBATORIOS EN LOS DAÑOS DERIVADOS DE INTELIGENCIA ARTIFICIAL

A diferencia de los modelos tradicionales de responsabilidad civil, en los sistemas de Inteligencia Artificial intervienen múltiples sujetos y procesos técnicos que dificultan la individualización del responsable.

La doctrina contemporánea sobre responsabilidad e inteligencia artificial ha señalado que los problemas de imputación no pueden resolverse únicamente mediante criterios clásicos de autoría directa, pues el funcionamiento de la IA implica la participación concurrente de desarrolladores, operadores, proveedores de infraestructura, entrenadores de datos, distribuidores tecnológicos y usuarios finales.¹² En consecuencia, el análisis jurídico debe desplazarse hacia criterios funcionales de atribución que permitan identificar qué sujeto tenía mayor control sobre el riesgo tecnológico y cuál obtuvo el beneficio principal derivado de la utilización del sistema.

Bajo esta lógica, la imputación jurídica del daño puede construirse a partir de diversos criterios complementarios.

En primer término, resulta relevante el criterio de control del sistema. Debe responder prioritariamente quien tiene capacidad real de supervisión, configuración o intervención sobre el funcionamiento de la inteligencia artificial. Este criterio adquiere relevancia porque la capacidad de prevenir, corregir o limitar el daño normalmente recae en el sujeto que administra u opera el sistema, y no en la víctima que únicamente interactúa con él. En la práctica, ello suele colocar en una posición central de responsabilidad a empresas, plataformas digitales, entidades financieras o proveedores de servicios que utilizan IA como mecanismo de decisión automatizada.

¹² EUROPEAN PARLIAMENT. Civil Liability Regime for Artificial Intelligence. op. cit.

De igual forma, puede atenderse al criterio de beneficio económico. Cuando una empresa obtiene ventajas patrimoniales mediante la implementación de inteligencia artificial, resulta jurídicamente razonable que también asuma los riesgos derivados del funcionamiento de dichos sistemas. Este criterio se relaciona directamente con la lógica de la responsabilidad objetiva por riesgo creado, conforme a la cual quien introduce una fuente de riesgo al tráfico jurídico debe responder por las consecuencias dañosas que ésta genere.¹³

Otro elemento relevante es la capacidad técnica y el acceso a la información. En muchos casos, el operador o desarrollador del sistema posee control exclusivo sobre el modelo algorítmico, los datos de entrenamiento, los registros técnicos y las condiciones de funcionamiento interno. Por ello, diversos autores sostienen que la imputación debe considerar quién tiene posibilidad efectiva de auditar, explicar o corregir el funcionamiento del sistema.¹⁴

Asimismo, la imputación puede apoyarse en el criterio de introducción del riesgo tecnológico. Cuando un sujeto decide incorporar sistemas de inteligencia artificial en actividades que impactan directamente derechos o intereses de terceros, asume una posición especial frente a los riesgos inherentes al uso de dicha tecnología. En estos casos, el fundamento de la responsabilidad no radica necesariamente en la culpa individual, sino en la decisión de introducir al entorno social una herramienta capaz de producir daños automatizados de difícil control.

Estos criterios permiten construir una propuesta de imputación más compatible con las características propias de la inteligencia artificial, evitando que la complejidad técnica del sistema termine trasladando indebidamente el riesgo a la víctima.

Problemas probatorios y asimetría de información

En la mayoría de los casos, la víctima no tiene acceso al funcionamiento interno del algoritmo, ni a los registros técnicos necesarios para demostrar cómo se produjo el daño. Esta situación se relaciona con el fenómeno conocido como “caja negra algorítmica”, mediante el

¹³ Suprema Corte de Justicia de la Nación, Tesis P./J. 43/2008 (Novena Época): Responsabilidad patrimonial del Estado. Diferencia entre responsabilidad objetiva y subjetiva, Semanario Judicial de la Federación y su Gaceta, Tomo XXVII, junio de 2008, p. 719.

¹⁴ European Commission, White Paper on Artificial Intelligence: *op. cit.*

cual incluso los propios desarrolladores pueden tener dificultades para explicar completamente el razonamiento interno del sistema.¹⁵

Frente a ello, exigir a la víctima una prueba técnica exhaustiva sobre procesos algorítmicos complejos podría traducirse en una barrera prácticamente insuperable para acceder a la reparación del daño.¹⁶ Una de las principales respuestas procesales frente a esta problemática consiste en la aplicación de la carga dinámica de la prueba. Conforme a este criterio, la obligación probatoria debe recaer en quien se encuentra en mejores condiciones técnicas, materiales o informativas para aportar evidencia al proceso.

Otro elemento fundamental es el deber de colaboración procesal. Las empresas que utilizan sistemas de inteligencia artificial deberían encontrarse obligadas a conservar y proporcionar información técnica relevante para el esclarecimiento del daño, incluyendo registros de decisiones automatizadas, datos de entrenamiento, parámetros de funcionamiento y mecanismos de supervisión implementados. La negativa injustificada a proporcionar dicha información podría generar consecuencias procesales adversas o fortalecer presunciones de responsabilidad.

VII. EL RÉGIMEN CIVIL APLICABLE A LA INTELIGENCIA ARTIFICIAL

La responsabilidad civil constituye una institución fundamental del derecho privado, en la medida en que impone a quien causa un daño la obligación de repararlo o, cuando ello no sea posible, de indemnizarlo.

El análisis de los daños ocasionados por sistemas de inteligencia artificial exige partir del régimen general de responsabilidad civil en México, cuya estructura dogmática se construye sobre dos modelos principales la responsabilidad subjetiva y la responsabilidad objetiva.

Según lo señalado en la tesis P/J. 43/2008 (novena época) de la Suprema Corte de Justicia de la Nación, la responsabilidad civil se configura como la obligación de reparar los daños que se causen a terceros, bajo una distinción clara entre responsabilidad subjetiva y objetiva. De acuerdo con este criterio jurisprudencial, la responsabilidad subjetiva se actualiza cuando el daño deriva de hechos culposos atribuibles al agente, lo que implica la

¹⁵ European Parliament, Civil liability and artificial intelligence in the EU, op. cit., pp. 34-38.

¹⁶ OECD, OECD AI Principles, OECD Publishing, 2021.

existencia de negligencia, dolo o intención en la acción u omisión que genera la lesión. Por su parte, la responsabilidad objetiva se funda en la teoría del riesgo, de modo que puede surgir aun en ausencia del elemento culpa cuando el daño deriva del uso o propiedad de una cosa o actividad que, por sus características, representa un riesgo para terceros, sin requerir la demostración de negligencia o dolo por parte del sujeto obligado.¹⁷

VIII. LA RESPONSABILIDAD CIVIL SUBJETIVA APLICADA A LA INTELIGENCIA ARTIFICIAL

La responsabilidad civil subjetiva es aquella en la que la obligación de reparar el daño surge a partir de la conducta humana (acción u omisión) y se determina atendiendo principalmente a la culpa, es decir, al grado de negligencia o falta de diligencia del autor del daño. En este modelo, el elemento decisivo para la imputación es la valoración jurídica del comportamiento del agente.¹⁸ Para acreditar esta responsabilidad se exige demostrar:

- Conducta antijurídica atribuible al agente.
- Daño cierto.
- Nexos causal.
- Culpa o dolo.

a) Conducta antijurídica atribuible al agente

Esta conducta puede ser una acción u omisión que contravenga normas del derecho civil o principios generales como la obligación de no dañar a otro¹⁹. No basta que una acción haya producido un daño, sino que esta acción debe contravenir una norma jurídica protegida. Identificar una conducta antijurídica atribuible a un agente humano en el supuesto de la Inteligencia Artificial es compleja toda vez que las decisiones que generan daño pueden surgir de procesos algorítmicos automatizados.

¹⁷ SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis P./J. 43/2008, op. cit.

¹⁸ Fernández Fernández, Antonio, “La responsabilidad civil subjetiva”, en Homenaje al Doctor Othón Pérez Fernández del Castillo, Facultad de Derecho-UNAM, 2017, pp. 176-177.

¹⁹ MIRKOUSKI, D. O. La responsabilidad civil en el Código Civil y Comercial. https://www.pensamientopenal.com.ar/system/files/Documento_Editado764.pdf

b) *Daño cierto*

El daño cierto se trata de una lesión efectiva en el patrimonio o en bienes jurídicos de la víctima. El daño debe ser evaluable e individualizable, manifestándose como menoscabo económico, lesión moral o afectación de derechos subjetivos.²⁰

En casos de Inteligencia Artificial, los daños patrimoniales (pérdidas económicas directas, lucro cesante, costes de reparación) y extrapatrimoniales (afectación a la reputación, discriminación algorítmica) pueden manifestarse con claridad, sin embargo, se complica la valoración judicial dentro del esquema subjetivo tradicional, en el cual el daño debe estar claramente vinculado a la conducta antijurídica atribuible.

c) *Nexo Causal*

El nexo causal se refiere a la conexión lógica y eficiente entre el hecho realizado por el agente y la lesión sufrida por la víctima²¹. Esta relación de causalidad solo puede establecerse cuando es posible reconstruir racionalmente cómo la acción u omisión del agente condujo al daño.

Esta reconstrucción se vuelve difícil cuando los sistemas de Inteligencia Artificial operan con procesos de aprendizaje automático o con lógicas internas no transparentes. La denominada “caja negra” hace que el vínculo causal entre la conducta humana (por ejemplo, diseño o entrenamiento del sistema) y el resultado sea menos evidente, lo que limita la eficacia del régimen subjetivo.

d) *Culpa o dolo*

La culpa se presenta cuando el autor del daño omite la diligencia que la naturaleza de su acto exige para evitar producir un resultado, es decir, cuando no actúa con la diligencia mínima exigible en las circunstancias. El dolo implica voluntad de causar el daño o conocimiento de la ilicitud del acto²².

Esta exigencia se encuentra con un límite significativo cuando la víctima debe demostrar que el desarrollo, entrenamiento, programación o supervisión del sistema fue negligente. Sin embargo, la evidencia técnica que permite establecer esa negligencia usualmente está bajo el control exclusivo de la empresa desarrolladora o del operador

²⁰ MIRKOUSKI, D O, *op.cit.*

²¹ MIRKOUSKI, D O, *op.cit.*

²² Elemento subjetivo (culpa y dolo). vLex. <https://vlex.com.co/vid/elemento-subjetivo-culpa-dolo-777555325>

tecnológico. Esta asimetría probatoria obstaculiza la demostración de culpa en muchos casos donde el daño se origina en decisiones automatizadas autónomas.

IX. LA RESPONSABILIDAD OBJETIVA APLICADA A LA INTELIGENCIA ARTIFICIAL

La responsabilidad civil objetiva (también llamada responsabilidad por riesgo creado) es aquella en la que el deber de reparar se genera sin necesidad de analizar la culpa del causante, pues basta con que el daño provenga del uso de mecanismos, instrumentos o sustancias peligrosas. En este supuesto, la responsabilidad se funda en el riesgo inherente a la actividad o cosa utilizada, y no en la conducta subjetiva del agente.²³

En el derecho civil mexicano, este régimen se encuentra expresamente reconocido en el artículo 1913 del Código Civil Federal, que establece que cuando una persona haga uso de mecanismos, instrumentos, aparatos o sustancias peligrosas por su velocidad, energía eléctrica, naturaleza explosiva o inflamable, u otras causas análogas, estará obligada a responder del daño que cause, aun cuando no obre ilícitamente, salvo que pruebe que el daño se produjo por culpa inexcusable de la víctima. De esta disposición se desprende que la responsabilidad objetiva opera como una forma de imputación reforzada, en la que el elemento determinante es la creación del riesgo, no la acreditación de negligencia.

Desde esta perspectiva, la figura del riesgo creado adquiere particular relevancia en el análisis de daños derivados de sistemas de inteligencia artificial. La implementación de Sistemas de Inteligencia Artificial en sectores como servicios financieros, salud, transporte o seguridad implica la introducción de tecnologías capaces de generar afectaciones relevantes sin intervención humana inmediata. En estos casos, el riesgo no depende necesariamente de un actuar negligente, sino de la propia operación del sistema y de la posibilidad de que sus decisiones produzcan consecuencias perjudiciales para terceros. Así, el uso de Inteligencia Artificial puede generar un riesgo estructural ya que la probabilidad de daño se encuentra vinculada al funcionamiento del sistema, aun cuando su utilización haya sido técnicamente correcta.

La adopción de este régimen no elimina el análisis de causalidad. La víctima debe acreditar que el daño se relaciona causalmente con el funcionamiento del sistema

²³ FERNÁNDEZ FERNÁNDEZ, Antonio, *op. cit.* pp. 173-183.

automatizado. No obstante, el régimen objetivo ofrece una ventaja significativa: evita que la reparación quede condicionada a la prueba de culpa en contextos donde ésta puede resultar prácticamente inacreditables por razones técnicas, asimetría informativa o falta de acceso a registros internos del sistema.

X. LA RESPONSABILIDAD POR PRODUCTOS DEFECTUOSOS Y SISTEMAS DE INTELIGENCIA ARTIFICIAL

El desarrollo e incorporación de sistemas de inteligencia artificial en actividades cotidianas ha generado nuevas discusiones sobre la aplicabilidad de las figuras tradicionales de responsabilidad civil.

La responsabilidad por productos defectuosos surge cuando un bien colocado en el mercado no ofrece la seguridad que legítimamente puede esperarse de él y, como consecuencia de ello, produce un daño a terceros. Esta figura se relaciona con el deber de seguridad que recae sobre fabricantes, desarrolladores, distribuidores y proveedores, quienes tienen la obligación jurídica de evitar que los productos introducidos al tráfico jurídico generen riesgos indebidos para los usuarios o personas afectadas por su funcionamiento.²⁴

En el caso de la inteligencia artificial, el problema adquiere características particulares debido a que el “producto” no necesariamente consiste en un objeto físico, sino en sistemas digitales complejos capaces de procesar grandes volúmenes de información o interactuar de manera autónoma con usuarios y entornos tecnológicos.

El defecto puede manifestarse de distintas maneras. Puede existir un defecto de diseño, entendido como una falla inherente en la arquitectura o programación del sistema desde su creación. Esto ocurre, por ejemplo, cuando un modelo algorítmico es desarrollado sin mecanismos mínimos de control, supervisión o validación técnica, permitiendo que produzca decisiones inseguras o discriminatorias incluso cuando funciona conforme a su programación original.

También puede presentarse un defecto de funcionamiento, relacionado con errores operativos o resultados anormales derivados de la ejecución del sistema. En estos supuestos,

²⁴ OECD, OECD Principles on Artificial Intelligence, *op. cit.*

la inteligencia artificial produce decisiones distintas a aquellas que razonablemente deberían esperarse bajo condiciones normales de operación.

A su vez, el defecto puede consistir en una deficiencia de información o advertencia. Este supuesto se configura cuando el desarrollador, proveedor u operador omite informar adecuadamente sobre los riesgos, limitaciones, márgenes de error o alcances reales del sistema de inteligencia artificial.

Dentro de esta categoría también deben considerarse las deficiencias derivadas del entrenamiento algorítmico. Los sistemas de IA dependen de grandes volúmenes de datos para su funcionamiento y aprendizaje; por ello, un entrenamiento basado en datos incompletos, sesgados o insuficientes puede provocar resultados discriminatorios, inexactos o inseguros. En estos casos, el defecto no necesariamente radica en un error técnico visible, sino en las condiciones bajo las cuales el sistema fue desarrollado y entrenado.

Esta problemática resulta particularmente visible en plataformas digitales y sistemas de IA generativa. Herramientas capaces de producir texto, imágenes, audio o video mediante aprendizaje automático pueden generar contenido falso, reproducir sesgos discriminatorios o difundir información inexacta que afecte derechos de terceros. De igual manera, en el sector financiero, la utilización de modelos automatizados para evaluación crediticia, detección de fraude o administración de cuentas puede ocasionar bloqueos indebidos, exclusiones injustificadas o decisiones automatizadas incorrectas con consecuencias patrimoniales relevantes.

En estos supuestos, adquiere especial relevancia la teoría del riesgo creado. Cuando una empresa decide incorporar inteligencia artificial como herramienta principal de operación, automatización o toma de decisiones, introduce al entorno social una fuente de riesgo tecnológico cuyos efectos potenciales pueden afectar a terceros.²⁵

XI. DERECHO COMPARADO SOBRE REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL: MÉXICO E INSTRUMENTOS INTERNACIONALES

La regulación de la inteligencia artificial constituye un desafío jurídico global que ha llevado a diversos países y organizaciones internacionales a desarrollar marcos normativos y principios orientadores para su uso responsable y seguro. A nivel internacional, existen

²⁵ SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis P./J. 43/2008, *op. cit.*

instrumentos que establecen criterios generales sobre ética, derechos humanos y gobernanza de la Inteligencia Artificial, mientras que pocos países han implementado leyes específicas. México, por su parte, se encuentra todavía en una fase inicial de construcción de un marco regulatorio, con múltiples iniciativas legislativas, pero sin una ley federal aprobada que regule de manera integral la Inteligencia Artificial.

Un referente relevante es la Jurisprudencia 2031640, emitida por la Suprema Corte de Justicia de la Nación, en la que se reconoce que el uso de herramientas tecnológicas por órganos jurisdiccionales no sustituye la función jurisdiccional humana ni exime del deber de fundamentación y motivación de las resoluciones judiciales²⁶. Este criterio no regula la Inteligencia Artificial como tal, pero establece un parámetro constitucional relevante respecto al uso de tecnologías automatizadas debe respetar los derechos fundamentales y no puede desplazar la responsabilidad del juzgador.

En México no existe actualmente una ley federal específica que regule la inteligencia artificial de manera integral. No obstante, se han registrado diversas iniciativas legislativas y propuestas de reforma constitucional para dotar al país de un marco legal en la materia. Según un análisis de proyectos de ley, desde 2021 han surgido múltiples propuestas diseñadas para abordar aspectos como la creación de una agencia nacional de Inteligencia Artificial, la inclusión en la Constitución de facultades para legislar sobre Inteligencia Artificial y ciberseguridad, y conceptos de regulación basados en niveles de riesgo similares a la Ley de Inteligencia Artificial de la Unión Europea. Sin embargo, ninguna de estas iniciativas ha prosperado a ley y muchas han quedado pendientes o desechadas en el proceso legislativo.

Adicionalmente, se ha propuesto una reforma al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos para otorgar al Congreso la facultad expresa de legislar sobre Inteligencia Artificial, ciberseguridad y neuroderechos. Esta reforma, aunque debatida, aún no se ha consolidado como parte del texto constitucional, evidenciando la ausencia de una base constitucional sólida para una regulación federal específica de Inteligencia Artificial en México.²⁷

²⁶ SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. Jurisprudencia 2031640, Semanario Judicial de la Federación, Undécima Época.

²⁷ CÁMARA DE DIPUTADOS. Iniciativa de reforma al artículo 73 constitucional en materia de inteligencia artificial y ciberseguridad, Gaceta Parlamentaria, México, 2024.

Algunas autoridades han emitido guías o recomendaciones sobre tecnologías automatizadas, pero no constituyen normativas obligatorias ni generales para todos los usos de Inteligencia Artificial. Además, la Suprema Corte de Justicia de la Nación (SCJN) ha empezado a pronunciarse sobre aspectos relacionados con responsabilidad civil y tecnología en tesis jurisprudenciales, pero aún no existe un corpus amplio de jurisprudencia directamente vinculada a Inteligencia Artificial.²⁸

Asimismo, en el ámbito financiero, la Comisión Nacional Bancaria y de Valores ha emitido criterios y guías relativas al uso de tecnologías automatizadas en entidades financieras supervisadas, particularmente en materia de modelos automatizados de evaluación de riesgos, prevención de lavado de dinero y fintech²⁹. No obstante, dichas disposiciones no constituyen un marco integral sobre responsabilidad, transparencia algorítmica o evaluación de impacto.

XII. ESTÁNDARES Y CRITERIOS INTERNACIONALES RELEVANTES

Naciones Unidas y derechos humanos: La Organización de las Naciones Unidas ha reconocido la importancia de conectar el desarrollo y uso de la Inteligencia Artificial con la protección de los derechos humanos. En su informe sobre inteligencia artificial y derechos humanos, el sistema de la ONU destaca que la adopción de tecnologías automatizadas debe garantizar el respeto de los derechos fundamentales³⁰ y que la regulación debe orientarse a prevenir daños a estos derechos.³¹ Esta perspectiva internacional subraya la necesidad de incorporar principios de derechos humanos en cualquier marco regulatorio nacional, incluido el mexicano.

Principios de la OCDE sobre Inteligencia Artificial: La Organización para la Cooperación y el Desarrollo Económico (OCDE) formuló en 2019 los Principios de Inteligencia Artificial, que han sido adoptados por múltiples países como referencia para políticas públicas responsables. Estos principios incluyen que la Inteligencia Artificial debe ser confiable, respetar los derechos humanos y libertades fundamentales, garantizar la transparencia y explicabilidad, fomentar la robustez técnica y la seguridad, y promover la rendición de

²⁸ NACIONES UNIDAS, *op. cit.*

²⁹ COMISIÓN NACIONAL BANCARIA Y DE VALORES. Disposiciones Fintech.

³⁰ NACIONES UNIDAS, *op. cit.*

³¹ Naciones Unidas, Informe sobre Inteligencia Artificial y Derechos Humanos (ONU, 2023).

cuentas. Estos estándares internacionales sirven como base para la evaluación de marcos regulatorios comparados y ofrecen criterios que pueden ser adaptados por México en su propia regulación.³²

Ley de Inteligencia Artificial de la Unión Europea (AI Act): La Ley de Inteligencia Artificial de la Unión Europea (AI Act) es hasta ahora el marco regulatorio más avanzado y completo a nivel mundial. Se trata de un reglamento obligatorio para todos los Estados miembros que clasifica los sistemas de Inteligencia Artificial según el nivel de riesgo que representan y establece obligaciones detalladas de transparencia, gestión de riesgos, supervisión humana, documentación técnica y notificación de incidentes, con requisitos distintos según la categoría de riesgo. Los sistemas que representan riesgos inaceptables están prohibidos.³³ Este enfoque basado en niveles de riesgo y en salvaguardias reforzadas ha sido considerado como un referente global para la regulación de Inteligencia Artificial, y varios países latinoamericanos observan este modelo para la construcción de sus propios marcos normativos.³⁴

XIII. CONCLUSIONES

La inteligencia artificial representa uno de los retos contemporáneos más relevantes para el derecho civil, particularmente en materia de responsabilidad por daños. Ello no implica que las categorías tradicionales de responsabilidad civil hayan perdido utilidad o vigencia, sino que las características propias de los sistemas de inteligencia artificial dificultan la aplicación de los mecanismos clásicos de imputación, causalidad y prueba sobre los que históricamente se ha construido el derecho de daños.

La responsabilidad subjetiva continúa siendo jurídicamente funcional en aquellos casos donde el daño puede vincularse con una conducta humana identificable y controlable. Cuando existen fallas de supervisión, configuraciones negligentes, omisiones técnicas relevantes, utilización indebida de sistemas automatizados o incumplimiento de deberes

³² NACIONES UNIDAS, op. cit.

³³ PARLAMENTO EUROPEO, Ley de inteligencia artificial de la UE: primera normativa sobre inteligencia artificial, op. cit.

³⁴ PARLAMENTO EUROPEO, op. cit.

mínimos de cuidado, el modelo basado en culpa conserva capacidad suficiente para justificar la obligación de reparar. En estos supuestos, la intervención humana permanece dentro del ámbito de control del agente responsable y permite mantener la lógica tradicional de imputación subjetiva.

La utilización de inteligencia artificial en sectores sensibles implica la incorporación deliberada de fuentes de riesgo, pues quien decide implementar dichos sistemas y obtiene beneficios derivados de su utilización debe también asumir las consecuencias jurídicas derivadas de los daños que éstos generen, aun cuando no sea posible acreditar una conducta específica.

La denominada “caja negra” genera una asimetría estructural entre la víctima y quienes controlan el sistema, pues normalmente son estos últimos quienes poseen acceso a los registros técnicos, parámetros de funcionamiento, procesos de entrenamiento y mecanismos internos de decisión automatizada y trasladar íntegramente la carga probatoria a la víctima produciría un desequilibrio incompatible con la función reparadora del derecho civil.

La aplicación de mecanismos como la carga dinámica de la prueba, las presunciones judiciales razonables y el deber de colaboración procesal constituye una respuesta necesaria frente a la desigualdad técnica e informativa existente entre las partes. No puede exigirse a la víctima demostrar aquello que resulta material o técnicamente inaccesible para ella, particularmente cuando la información indispensable para esclarecer el origen del daño se encuentra bajo control exclusivo del operador tecnológico o de la empresa responsable del sistema automatizado.

Finalmente, el derecho civil mexicano cuenta con bases doctrinales y normativas suficientes para enfrentar muchos de los problemas derivados de la inteligencia artificial; sin embargo, también evidencia la necesidad de avanzar hacia estándares regulatorios más claros y específicos.

En este sentido, el desafío no consiste en sustituir las categorías tradicionales de responsabilidad civil, sino en reinterpretarlas y complementarlas conforme a las exigencias propias del entorno tecnológico contemporáneo. La evolución de la inteligencia artificial exige que el derecho civil preserve su función reparadora y preventiva frente a nuevas formas de riesgo, garantizando que el avance tecnológico no se traduzca en debilitamiento de

derechos, sino en una adaptación coherente y efectiva de los mecanismos de protección jurídica.

XIV. BIBLIOGRAFÍA

- BERTOLINI, Andrea. Artificial Intelligence and Civil Liability. Bruselas: European Parliament, 2025.
https://www.europarl.europa.eu/RegData/etudes/STUD/2025/776426/IUST_STU%282025%29776426_EN.pdf
- COMISIÓN NACIONAL BANCARIA Y DE VALORES. Disposiciones Fintech.
<https://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20car%C3%A1cter%20general%20aplicables%20a%20las%20instituciones%20de%20tecnolog%C3%ADa%20financiera.pdf>
- EUROPEAN COMMISSION. White Paper on Artificial Intelligence: A European Approach to Excellence and Trust. Bruselas: European Union, 2020.
- EUROPEAN PARLIAMENT. Civil Liability Regime for Artificial Intelligence. Bruselas: Directorate-General for Internal Policies of the Union, 2020. Disponible en: [https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2020\)652773](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)652773) [consulta: 1 de mayo 2026].
- FERNÁNDEZ FERNÁNDEZ, Antonio. “La responsabilidad civil subjetiva”. En: Homenaje al Doctor Othón Pérez Fernández del Castillo. Ciudad de México: Facultad de Derecho-UNAM, 2017, pp. 173-183.
- GÓMEZ-PÉREZ, Asunción. Discurso de ingreso a la Real Academia Española. Madrid: Real Academia Española, 2023. https://www.rae.es/sites/default/files/2023-05/Discurso%20Ingreso%20Asuncion%20Gomez-Perez_0.pdf
- MÉXICO. Código Civil Federal. Diario Oficial de la Federación, última reforma publicada el 14 de noviembre de 2025.
- MIRKOUSKI, D. O. La responsabilidad civil en el Código Civil y Comercial. Disponible en: https://www.pensamientopenal.com.ar/system/files/Documento_Editado764.pdf
- NACIONES UNIDAS. Informe sobre Inteligencia Artificial y Derechos Humanos. Nueva York: ONU, 2023.

- OECD. OECD Principles on Artificial Intelligence. París: OECD Publishing, 2019.
<https://www.oecd.org/en/topics/ai-principles.html>
- OPENAI. ChatGPT (modelo GPT-5.5). San Francisco: OpenAI, 2026. Disponible en:
<https://openai.com/chatgpt>
- PARLAMENTO EUROPEO. Ley de inteligencia artificial de la UE: primera normativa sobre inteligencia artificial. Bruselas, 2023.
<https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial>
- PARLAMENTO EUROPEO. Resolución de 16 de febrero de 2017 con recomendaciones destinadas a la Comisión sobre normas de Derecho Civil sobre robótica (2015/2103(INL)). Estrasburgo, 2017.
https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html
- ROMERO, M. Á. M. “Regulación de la inteligencia artificial: desafíos legales en México”. Revista RIDE, 2025. <https://www.ride.org.mx/index.php/RIDE/article/view/2291>
- SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. Semanario Judicial de la Federación, Undécima Época. <https://sjf2.scjn.gob.mx/detalle/tesis/169428>
- SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. Tesis P./J. 43/2008, Responsabilidad patrimonial del Estado. Diferencia entre responsabilidad objetiva y subjetiva, Semanario Judicial de la Federación y su Gaceta, Novena Época, tomo XXVII, junio de 2008. <https://sjf2.scjn.gob.mx/detalle/tesis/169428>
- vLEX. Elemento subjetivo (culpa y dolo). <https://vlex.com.co/vid/elemento-subjetivo-culpa-dolo-777555325>

Nota: La autora reconoce el apoyo de ChatGPT (modelo GPT-4.1), desarrollado por OpenAI, como herramienta auxiliar en la mejora estilística de partes de este trabajo. Este asistente de lenguaje fue empleado únicamente como apoyo en la organización del texto, sin sustituir el análisis, criterio jurídico, ni las conclusiones originales del investigador.