

La Incidencia de la Inteligencia Artificial en el Seguro de Responsabilidad Civil

LA INCIDENCIA DE LA INTELIGENCIA ARTIFICIAL EN EL SEGURO DE RESPONSABILIDAD CIVIL

AUTORES:

Felisa Baena Aramburo

Carolina Gómez González

José López-Oliva

Ana María Ramírez Peláez

Andrés Felipe Villegas García

Lisana Carolina Villota

Grupo de Trabajo de Responsabilidad Civil

Asociación Colombiana de Derecho de Seguros — ACOLDESE

Asociación Internacional de Derecho de Seguros — AIDA Colombia

Colombia 2026

RESUMEN

La inteligencia artificial (IA) representa uno de los mayores desafíos que el derecho de daños y la industria aseguradora han enfrentado en su historia reciente. La presente obra colectiva, estructurada en cuatro capítulos, examina de manera sistemática y desde perspectivas complementarias la incidencia de la IA en el seguro de responsabilidad civil (RC), tanto en el ordenamiento jurídico colombiano como en el contexto iberoamericano e internacional.

El primer capítulo sienta las bases dogmáticas de la responsabilidad civil aplicables a los sistemas de IA, analizando cómo los elementos estructurales del derecho de daños —conducta, nexo causal e imputación— se ven profundamente perturbados por la autonomía, la opacidad algorítmica y la multiplicidad de actores que caracterizan a estos sistemas. El segundo capítulo profundiza en la interacción entre la IA y el contrato de seguro de RC en Colombia, examinando el régimen de los artículos 1127 a 1133 del Código de Comercio, las principales líneas de cobertura y exclusiones en el mercado internacional, el marco regulatorio europeo del AI Act (Reglamento UE 2024/1689) y el estado del ordenamiento colombiano. El tercer capítulo aborda el impacto de la IA y el Internet de las Cosas en el régimen de responsabilidad por productos defectuosos, con especial atención a la Directiva (UE) 2024/2853 y sus implicaciones para el seguro de RC, así como los riesgos cibernéticos como frontera difusa entre defecto algorítmico y ataque externo. El cuarto capítulo propone una lectura del seguro de RC desde su función social, como mecanismo de protección de derechos fundamentales en la era tecnológica, y postula la creación de un seguro obligatorio para la atención de incidentes derivados del uso de la IA.

Las principales conclusiones apuntan a la necesidad de reformas estructurales en el ordenamiento colombiano: la consagración de un régimen de responsabilidad objetiva para operadores de IA de alto riesgo; el diseño de productos aseguradores específicos para riesgos de

IA; la creación de un seguro obligatorio para sistemas de IA de alto riesgo; y la adopción de lineamientos regulatorios por parte de la Superintendencia Financiera de Colombia, inspirados en el modelo europeo y adaptados a las particularidades del sistema jurídico y del mercado asegurador nacional.

Palabras clave:

inteligencia artificial; seguro de responsabilidad civil; responsabilidad civil; actividades peligrosas; productos defectuosos; riesgos cibernéticos; AI Act; regulación; Colombia; opacidad algorítmica; función social del seguro; seguro obligatorio.

RESUMO

A inteligência artificial (IA) representa um dos maiores desafios que o direito de danos e a indústria seguradora já enfrentaram na sua história recente. A presente obra coletiva, estruturada em quatro capítulos, examina de forma sistemática e a partir de perspectivas complementares a incidência da IA no seguro de responsabilidade civil (RC), tanto no ordenamento jurídico colombiano como no contexto ibero-americano e internacional.

O primeiro capítulo estabelece as bases dogmáticas da responsabilidade civil aplicáveis aos sistemas de IA, analisando como os elementos estruturais do direito de danos — conduta, nexo causal e imputação — são profundamente perturbados pela autonomia, pela opacidade algorítmica e pela multiplicidade de atores que caracterizam esses sistemas. O segundo capítulo aprofunda a interação entre a IA e o contrato de seguro de RC na Colômbia, examinando o regime dos artigos 1127 a 1133 do Código de Comércio, as principais linhas de cobertura e exclusões no mercado

internacional, o quadro regulatório europeu do AI Act (Regulamento UE 2024/1689) e o estado do ordenamento colombiano. O terceiro capítulo aborda o impacto da IA e da Internet das Coisas no regime de responsabilidade por produtos defeituosos, com especial atenção à Diretiva (UE) 2024/2853 e suas implicações para o seguro de RC, bem como os riscos cibernéticos como fronteira difusa entre defeito algorítmico e ataque externo. O quarto capítulo propõe uma leitura do seguro de RC a partir da sua função social, como mecanismo de proteção de direitos fundamentais na era tecnológica, e postula a criação de um seguro obrigatório para a cobertura de incidentes decorrentes do uso da IA.

As principais conclusões apontam para a necessidade de reformas estruturais no ordenamento colombiano: a consagração de um regime de responsabilidade objetiva para operadores de IA de alto risco; o desenho de produtos seguradores específicos para riscos de IA; a criação de um seguro obrigatório para sistemas de IA de alto risco; e a adoção de orientações regulatórias pela Superintendência Financeira da Colômbia, inspiradas no modelo europeu e adaptadas às particularidades do sistema jurídico e do mercado segurador colombiano.

Palavras-chave:

inteligência artificial; seguro de responsabilidade civil; responsabilidade civil; atividades perigosas; produtos defeituosos; riscos cibernéticos; AI Act; regulação; Colômbia; opacidade algorítmica; função social do seguro; seguro obrigatório.

Nota: El presente artículo de investigación es resultado del trabajo colectivo del Grupo de Trabajo de Responsabilidad Civil de ACOLDESE y AIDA Colombia. Todos los autores han contribuido a la obra en su conjunto.. Esta investigación fue presentada en el marco del XIX Congreso CILA-AIDA el cual se realiza conjuntamente con el Encuentro No.33 de ACOLDESE en la ciudad de Cartagena, del 26 al 28 de agosto de 2026

INTRODUCCIÓN GENERAL

El advenimiento de la inteligencia artificial como tecnología de propósito general constituye, sin lugar a dudas, uno de los desafíos jurídicos más profundos que ha enfrentado el derecho de daños y la industria aseguradora en su historia. No se trata únicamente de una revolución tecnológica o económica: es, en un sentido preciso, una revolución de la responsabilidad. Las máquinas que aprenden, que deciden y que actúan de manera autónoma desafían los fundamentos más arraigados de la responsabilidad civil y, con ellos, la arquitectura del seguro de responsabilidad civil (RC) tal como ha sido concebida y desarrollada por siglos de evolución jurídica.

La presente obra colectiva surge de la preocupación compartida por los autores —todos ellos miembros del Grupo de Trabajo de Responsabilidad Civil de la Asociación Colombiana de Derecho de Seguros (ACOLDESE) y de la Sección Colombiana de la Asociación Internacional de Derecho de Seguros (AIDA)— de contribuir al debate académico y regulatorio sobre la incidencia de la IA en el seguro de RC, con especial énfasis en el ordenamiento jurídico colombiano y en el contexto iberoamericano e internacional. El trabajo que el lector tiene en sus manos integra cuatro investigaciones que abordan el problema desde ángulos complementarios, formando en conjunto una arquitectura analítica coherente y exhaustiva.

El Capítulo I sienta las bases dogmáticas indispensables para el análisis que sigue. Partiendo de los fundamentos generales de la responsabilidad civil —concepto, funciones reparatoria, preventiva y distributiva; distinción entre responsabilidad contractual y extracontractual; elementos estructurales de daño, nexo causal e imputación—, el capítulo examina la naturaleza jurídica de la IA y sus implicaciones para la determinación de los sujetos responsables, los regímenes de imputación aplicables y los desafíos probatorios que presenta la

opacidad algorítmica. La principal conclusión de este capítulo es que la responsabilidad civil derivada de los sistemas de IA no constituye una ruptura con el derecho de daños tradicional, sino su evolución más exigente: los fundamentos permanecen vigentes, pero la complejidad de su acreditación y la distribución de responsabilidad entre actores que operan en múltiples jurisdicciones exigen adaptaciones normativas e interpretativas sustanciales.

Comentado [FB1]: Sería bueno explicar aquí qué es la opacidad algorítmica.

En el Capítulo II se analiza propiamente el impacto de la IA en el seguro de responsabilidad civil. A través de un método analítico y de derecho comparado, los autores estudian la naturaleza jurídica del seguro de RC conforme al Código de Comercio colombiano (artículos 1127 a 1133), los presupuestos clásicos de la responsabilidad civil y su tensión con los rasgos definitorios de los sistemas de IA —autonomía, opacidad algorítmica y capacidad de aprendizaje—. El capítulo analiza las principales líneas de cobertura, los clausulados emergentes y las exclusiones específicas en materia de IA introducidas por el mercado asegurador internacional, el marco regulatorio europeo (Reglamento UE 2024/1689 y Directiva de Productos Defectuosos 2024/2853) y el estado del ordenamiento jurídico colombiano. La conclusión central es que la IA exige una revisión estructural del seguro de RC, la creación de productos específicos de aseguramiento y una actualización normativa urgente que, en Colombia, debería orientarse por los referentes europeos adaptados a las particularidades del sistema jurídico nacional.

El Capítulo III examina la intersección entre la IA, el Internet de las Cosas (IoT), los productos defectuosos y los riesgos cibernéticos, y su incidencia en el seguro de RC. A partir del análisis de la Directiva (UE) 2024/2853, el capítulo estudia la ampliación del concepto de producto para incluir el software y los sistemas de IA, la noción de defecto dinámico en sistemas evolutivos, las dificultades probatorias que genera la opacidad algorítmica y la línea —frecuentemente difusa— entre defecto algorítmico y ataque externo de ciberseguridad. El capítulo concluye que la

interacción entre IA, productos defectuosos y riesgos cibernéticos **confirma que el derecho de daños contemporáneo ya no puede ser examinado de manera aislada del derecho de seguros**; ambos conforman una arquitectura integrada orientada a gestionar el riesgo tecnológico sin frenar el impulso innovador.

Comentado [FB2]: Es una afirmación con mucho peso, tal vez convendría suavizarla.

El Capítulo IV propone una lectura del seguro de RC desde su función social, como mecanismo de protección de derechos fundamentales en la denominada "sociedad del riesgo tecnológico". El capítulo postula la creación de un Seguro Obligatorio para la Atención de Incidentes derivados del uso de la IA, diseñado conforme al marco regulatorio europeo más avanzado, y concibe el mercado asegurador como un co-regulador técnico que sirve de eje de convergencia para el logro de un equilibrio social - funcional entre innovación y dignidad humana.

La lectura integrada de estas cuatro perspectivas conduce a un diagnóstico claro: el ordenamiento jurídico colombiano —y en general el iberoamericano— no está preparado para responder adecuadamente a los riesgos que generan los sistemas de inteligencia artificial. Los marcos de responsabilidad civil existentes son insuficientes para resolver los problemas de imputación, causalidad y prueba que plantea la IA. Los productos aseguradores vigentes presentan vacíos y exclusiones que dejan sin cobertura a empresas y ciudadanos. La regulación pública es escasa, fragmentada e incompatible con la velocidad de adopción de la tecnología. Y la doctrina jurídica, aunque creciente, no ha logrado aún articular propuestas normativas concretas con el grado de sistematicidad que el problema requiere.

Esta obra aspira a contribuir a cerrar esa brecha, ofreciendo al lector —sea abogado, asegurador, regulador o académico— un marco conceptual coherente, un diagnóstico riguroso y un conjunto de propuestas de reforma concretas y viables para el ordenamiento colombiano. Los autores son conscientes de que el derecho de la IA es, por definición, un derecho en construcción:

la tecnología evoluciona a una velocidad que ningún sistema jurídico puede seguir por completo. Pero esa incertidumbre no es excusa para la inacción; es, precisamente, el argumento más poderoso para comenzar ya a construir los instrumentos jurídicos que la sociedad necesita.

CAPÍTULO I

RESPONSABILIDAD CIVIL E INTELIGENCIA ARTIFICIAL: MARCO CONCEPTUAL PARA LA INDUSTRIA ASEGURADORA

Resumen del Capítulo

El presente capítulo examina los fundamentos generales de la responsabilidad civil y su aplicabilidad a los sistemas de inteligencia artificial, con especial énfasis en las implicaciones para la industria aseguradora colombiana. Se analizan los elementos estructurales de la responsabilidad civil —daño, nexo causal y hecho generador—, la naturaleza jurídica de la IA, la identificación de los sujetos potencialmente responsables en la cadena de valor tecnológica, los regímenes de imputación disponibles y los desafíos probatorios que genera la opacidad algorítmica. El capítulo concluye que los sistemas de IA no rompen con las categorías del derecho de daños, sino que exigen su aplicación más sofisticada, representando para la industria aseguradora una oportunidad estratégica en el desarrollo de productos de responsabilidad civil tecnológica robustos y adaptados.

Palabras clave del capítulo:

responsabilidad civil; inteligencia artificial; nexo causal; opacidad algorítmica; actividades peligrosas; productos defectuosos; imputación; carga de la prueba; industria aseguradora.

1. Fundamentos generales de la responsabilidad civil aplicables a la inteligencia artificial

1.1. Concepto y funciones de la responsabilidad civil

La responsabilidad civil constituye el mecanismo jurídico a través del cual quien causa un daño a otro queda obligado a repararlo. Cabe preguntarse si los daños con ocasión de la IA desafían el concepto mismo de responsabilidad civil. En el marco de los sistemas de inteligencia artificial, esta figura adquiere especial relevancia, dado que los daños generados por estas tecnologías pueden presentar características que desafían las categorías tradicionales del derecho de daños.

Entre las funciones teóricas de la responsabilidad civil se estudian generalmente: (i) su función reparatoria, orientada a restablecer el equilibrio patrimonial afectado; (ii) la función preventiva, que desincentiva conductas dañosas mediante la amenaza de sanción patrimonial; y (iii) la función distributiva, que asigna entre los distintos actores del mercado los costos de los daños. Para el caso de los daños generados con ocasión del uso de la IA y las tecnologías emergentes,

1.2. Responsabilidad contractual y extracontractual

La distinción entre responsabilidad contractual y extracontractual mantiene plena vigencia frente a la IA, aunque su aplicación práctica presenta complejidades propias. En el ámbito contractual, la IA como herramienta en la ejecución de prestaciones puede dar lugar a incumplimientos imputables al deudor contractual, especialmente cuando este ha prometido un resultado que el sistema no alcanza. En el ámbito extracontractual, los daños causados a terceros ajenos a cualquier vínculo negocial con el operador del sistema exigen la construcción de criterios de imputación desde las normas generales del Código Civil y el Código de Comercio. Haciendo

un paralelo entre ambas instituciones encontraríamos, por ejemplo, estas distinciones fundamentales:

Responsabilidad Contractual

- Relación preexistente entre las partes
- Incumplimiento de obligaciones pactadas
- Plazo de prescripción específico
- Cláusulas limitativas de responsabilidad
- Aplica en contratos de licencia de software IA, SaaS, desarrollo a medida

Responsabilidad Extracontractual

- Ausencia de vínculo previo
- Daño a terceros ajenos al contrato
- Rige el régimen general del Código Civil
- Sin límites convencionales
- Aplica a daños causados a terceros no usuarios del sistema (no obstante uno de los puntos de análisis es precisamente establecer si el usuario de la IA en todos los casos será considerado como un tercero, o si esta distinción, como en la relaciones de consumo se difumina y no aplica el principio de la relatividad de los contratos. ¿es igual si un usuario paga o no suscripción? ¿Se modifica el régimen de responsabilidad aplicable?

Para la industria aseguradora, esta distinción es fundamental al momento de estructurar coberturas: los daños a terceros generalmente se enmarcarán en el ámbito extracontractual, mientras que los reclamos del propio asegurado por fallas del sistema tenderán a ser contractuales.

1.3. Elementos estructurales

La configuración de la responsabilidad civil, frente a sistemas de IA o en cualquier otro contexto, exige la concurrencia de los siguientes elementos:

a) Daño. El daño debe ser cierto, directo y personal. En el contexto de la IA pueden presentarse daños patrimoniales —pérdidas económicas derivadas de decisiones automatizadas erróneas— y extrapatrimoniales —afectaciones a la honra, la intimidad o el buen nombre

ocasionadas por sistemas de reconocimiento facial, perfilamiento o decisiones automatizadas discriminatorias—.

b) Hecho generador. El hecho generador puede ser la acción u omisión del operador humano, o bien la conducta autónoma del sistema. La identificación del hecho generador es uno de los principales desafíos en materia de IA, pues la causalidad puede estar distribuida entre múltiples actores de la cadena tecnológica.

c) Nexos causal. La causalidad adecuada exige que el daño sea consecuencia previsible y directa del hecho generador. En los sistemas de IA, la opacidad algorítmica —conocida como el problema de la "caja negra"— puede dificultar gravemente la acreditación del nexo causal, pues los procesos internos del sistema no son siempre rastreables ni explicables.

d) Culpa o régimen objetivo. Dependiendo del régimen aplicable, la responsabilidad podrá exigir la demostración de culpa del agente (responsabilidad subjetiva) o prescindirá de ella cuando el daño sea atribuible al riesgo inherente de la actividad (responsabilidad objetiva). Este debate adquiere especial relevancia frente a sistemas de IA con alta autonomía decisional.

1.4. Responsabilidad por actividades peligrosas y el uso de la inteligencia artificial

En lo que respecta a la consideración del uso de la IA como actividad peligrosa per se, es preciso tener en cuenta que la Corte Suprema de Justicia de Colombia ha construido la doctrina sobre dos criterios: que la actividad tenga potencial de causar daño por su propia naturaleza, y que ese peligro sea inherente a ella, no derivado de un uso incorrecto. La actividad peligrosa no requiere culpa para generar responsabilidad; basta el daño y el nexo causal, y corresponde al demandado probar la causa extraña.

La dificultad radica en que la IA no es una categoría homogénea. Aplicar la etiqueta de "actividad peligrosa" a todo uso de IA sería tan impreciso como calificar de peligrosa cualquier

forma de uso de la tecnología. La doctrina más coherente, y la que está adoptando el derecho comparado, distingue por nivel de autonomía y magnitud del riesgo potencial:

Un chatbot de atención al cliente difícilmente podría calificarse como actividad peligrosa. Un sistema de scoring que niega créditos o seguros de manera masiva constituye una zona gris que exige análisis caso por caso. Un vehículo autónomo o un robot quirúrgico sí puede calificarse como actividad peligrosa, por analogía con los criterios ya consolidados para vehículos y equipos médicos. Un sistema de IA que controla infraestructura crítica es, sin duda, una actividad peligrosa.

La jurisprudencia de la Corte Suprema de Justicia ha establecido que una actividad es peligrosa cuando "escapa al control absoluto del hombre". Los sistemas de IA de alta autonomía encajan perfectamente en esa definición: su comportamiento no es completamente predecible ni controlable por sus operadores, especialmente en modelos con aprendizaje continuo.

El artículo 2356 del Código Civil colombiano establece que quien emprende una actividad que por su naturaleza representa riesgo para terceros responde por los daños causados, con independencia de la culpa. Esta figura, ampliamente desarrollada por la jurisprudencia de la Corte Suprema de Justicia, resulta especialmente pertinente para los sistemas de IA de alto riesgo.

Por lo anterior, será el marco obligacional establecido para cada actividad de forma particular el que permita definir el alcance de la responsabilidad y los responsables. No se considera necesario construir un sistema enteramente nuevo de responsabilidad civil, aunque sí se imponen nuevos retos para los abogados y operadores judiciales. En este análisis resulta además fundamental el estatuto del consumidor (Ley 1480 de 2011).

2. Naturaleza jurídica de la inteligencia artificial

2.1. ¿Es la IA una cosa, un producto, un servicio o un sistema autónomo?

La calificación jurídica de la inteligencia artificial determina el régimen de responsabilidad aplicable y las partes que pueden ser llamadas a responder. No existe en el ordenamiento jurídico colombiano —ni en la mayoría de los ordenamientos latinoamericanos— una regulación específica que defina la naturaleza jurídica de la IA, lo que obliga al operador jurídico a acudir a las categorías existentes por analogía.

La IA puede ser calificada como cosa cuando se encuentra integrada en un dispositivo físico; como producto cuando es comercializada en el mercado; como servicio cuando se presta de manera continua a través de plataformas digitales; y como sistema con autonomía decisional cuando opera sin supervisión humana directa. Cada calificación conduce a regímenes de responsabilidad distintos.

Calificación	Implicación jurídica	Relevancia aseguradora
Cosa / bien mueble	Régimen de responsabilidad por el hecho de las cosas (art. 2347 C.C.)	Cobertura de RC por bienes bajo custodia o control del asegurado
Producto	Responsabilidad por productos defectuosos (Ley 1480/2011)	Cobertura de RC de productos, incluyendo defectos de diseño y fabricación
Servicio	Responsabilidad del prestador de servicios; Estatuto del Consumidor	Pólizas de RC profesional y errores y omisiones (E&O)
Sistema autónomo	Ausencia de encaje normativo claro; debate sobre personalidad jurídica propia	Riesgo no cubierto o exclusión expresa; mercado en desarrollo

2.2. IA como herramienta versus IA con autonomía decisional

La distinción entre IA como herramienta y IA con autonomía decisional es probablemente la más relevante para la imputación de responsabilidad. Cuando la IA actúa como herramienta bajo

supervisión humana, los marcos tradicionales resultan suficientes; cuando el sistema toma decisiones de manera autónoma sin intervención humana significativa, los esquemas clásicos de atribución de culpa resultan insuficientes y deben complementarse con criterios objetivos.

2.3. Tipología de sistemas de inteligencia artificial

A efectos de estructurar adecuadamente los análisis de responsabilidad y cobertura, conviene distinguir entre los siguientes tipos de sistemas:

IA predictiva: sistemas que analizan datos históricos para anticipar resultados futuros. Ejemplos: modelos de suscripción, scoring crediticio, detección de fraude en seguros. El riesgo típico es el daño derivado de predicciones erróneas o discriminatorias.

IA generativa: sistemas que producen contenido nuevo —texto, imágenes, código— a partir de patrones aprendidos. Riesgos: desinformación, violación de derechos de autor, responsabilidad por contenido generado de manera autónoma.

Sistemas autónomos físicos: vehículos autónomos, drones, robots industriales o quirúrgicos. Presentan los mayores riesgos de daños corporales y materiales, y son los que más urgentemente requieren cobertura aseguradora específica.

2.4. El problema de la autonomía algorítmica

A medida que los sistemas de IA ganan en complejidad y capacidad de aprendizaje continuo, surge el interrogante de si sus decisiones pueden atribuirse jurídicamente a algún sujeto de derecho. Esta problemática, denominada "autonomía algorítmica", plantea si el derecho debe reconocer alguna forma de subjetividad jurídica a ciertos sistemas de IA —como ya discute la Unión Europea—, o si debe mantenerse el principio de que toda responsabilidad recae

necesariamente en personas naturales o jurídicas. La posición mayoritaria de la doctrina, y la más consistente con el estado actual del derecho positivo, se inclina por esta última alternativa.

Para la industria aseguradora, el reconocimiento o no de personalidad jurídica a la IA tiene implicaciones directas en la determinación del tomador del seguro, el beneficiario y el régimen de subrogación aplicable.

3. Sujetos potencialmente responsables

La cadena de valor de un sistema de inteligencia artificial involucra múltiples actores cuya contribución al daño puede ser directa, indirecta o concurrente. La identificación correcta del sujeto responsable es determinante tanto para la víctima que busca reparación como para el asegurador que evalúa el riesgo. Los principales sujetos en la cadena son: el desarrollador o investigador del algoritmo, el proveedor de datos de entrenamiento, el integrador del sistema, el distribuidor y el operador o usuario final.

Un mapa de posibles responsables nos podría arrojar escenarios como los descritos a continuación:

Actor	Fundamento de responsabilidad	Cobertura típica
Desarrollador	Defectos de diseño, entrenamiento deficiente, fallas del algoritmo	RC productos / E&O tecnológico
Proveedor / comercializador	Distribución de producto defectuoso, falta de advertencias	RC productos / RC comercial
Propietario	Guarda de la cosa; actividad peligrosa	RC explotación / RC general
Usuario	Uso inadecuado, incumplimiento de instrucciones, negligencia en supervisión	RC explotación / RC profesional

Empresa implementadora	Integración defectuosa, personalización riesgosa, falta de supervisión	RC profesional / RC patronal
Solidaridad potencial	Concurrencia de causas; imposibilidad de individualización	Análisis caso a caso

3.1. Responsabilidad solidaria y cadenas de suministro tecnológicas

En el ámbito de la IA, la responsabilidad solidaria cobra especial relevancia cuando el daño resulta de la actuación concurrente de varios actores de la cadena tecnológica y no es posible —o resulta desproporcionadamente oneroso— individualizar la contribución causal de cada uno. La jurisprudencia nacional e internacional ha tendido a reconocer la solidaridad en estos supuestos, facilitando la reparación de la víctima.

Para los aseguradores, las cadenas de suministro tecnológicas presentan un riesgo de acumulación relevante: un defecto en un componente de IA utilizado por múltiples empresas puede generar reclamaciones simultáneas bajo pólizas distintas, con el potencial de desestabilizar portafolios de RC tecnológica.

3.2. Analogías con regímenes de responsabilidad existentes

a) Responsabilidad por productos defectuosos. La Ley 1480 de 2011 (Estatuto del Consumidor) establece un régimen de responsabilidad objetiva para productores y proveedores por daños causados por productos defectuosos. La aplicación analógica de este régimen a la IA es la tendencia dominante en el derecho comparado y resulta especialmente útil para calificar los defectos de diseño en modelos de aprendizaje automático.

b) Responsabilidad médica por uso de herramientas tecnológicas. El uso de IA en el diagnóstico médico, en la suscripción de riesgos de salud o en la determinación de prestaciones plantea interrogantes sobre la responsabilidad del profesional que delega decisiones en el sistema. La jurisprudencia ha señalado consistentemente que la herramienta tecnológica no exonera al profesional de su deber de supervisión y juicio crítico.

c) Responsabilidad del empleador por hechos del dependiente. La analogía entre la IA y el dependiente o auxiliar humano permite extender al operador de la IA la responsabilidad por los daños causados por el sistema, bajo el entendimiento de que el sistema actúa en su interés y bajo su control, de manera análoga a como lo haría un empleado.

4. Regímenes de imputación aplicables

La determinación del régimen de imputación aplicable a los daños causados por sistemas de IA es uno de los debates más activos en la doctrina jurídica contemporánea. A continuación se presentan los principales esquemas disponibles y los interrogantes que plantean.

4.1. Responsabilidad subjetiva (culpa probada)

En el régimen subjetivo, la víctima debe acreditar que el agente actuó con culpa —impericia, imprudencia o negligencia— en el diseño, desarrollo, implementación u operación del sistema de IA. Este modelo enfrenta obstáculos significativos frente a la opacidad algorítmica, pues la víctima raramente tiene acceso a los procesos internos del sistema para demostrar la falla específica.

4.2. Responsabilidad objetiva (riesgo creado)

El régimen objetivo prescinde del análisis de la culpa: basta demostrar el daño, el hecho generador y el nexo causal. Este modelo es el más favorable para las víctimas de daños causados por IA de alta autonomía, y es el que con mayor frecuencia proponen los proyectos regulatorios en curso —incluyendo el Reglamento (UE) 2024/1689 (AI Act), que adopta un régimen de responsabilidad objetiva para sistemas de IA de alto riesgo—.

4.3. Actividades peligrosas e inversión de la carga de la prueba

Cuando la actividad que despliega el sistema de IA es calificada como peligrosa, opera la presunción de culpa establecida por la jurisprudencia colombiana: el demandado debe probar causa extraña —fuerza mayor, hecho exclusivo de la víctima o de un tercero— para liberarse de responsabilidad. Esta inversión de la carga probatoria es de enorme relevancia práctica, pues traslada al desarrollador u operador la obligación de demostrar que actuó con toda la diligencia exigible.

4.4. Debate regulatorio: ¿régimen especial o régimen tradicional?

Existe un debate que transita entre la necesidad de establecer un régimen especial de responsabilidad para los daños causados bajo sistemas de inteligencia artificial o la aplicación del régimen tradicional de responsabilidad que podría resultar suficiente para garantizar la reparación o prevención de daños. Al respecto encontramos lo siguiente:

Posición: Régimen tradicional es suficiente

- Los códigos civiles son suficientemente flexibles

Posición: Se requiere régimen especial para IA

- La opacidad algorítmica hace inviable la responsabilidad subjetiva

- La analogía con actividades peligrosas cubre los casos más graves
- Evita sobre-regulación prematura de tecnología en evolución
- Riesgo de rigidez normativa ante cambio tecnológico acelerado

- La distribución de responsabilidad en cadenas complejas exige reglas claras
- Los daños masivos y sistémicos requieren fondos de garantía específicos
- La UE ya avanza en esta dirección con su AI Liability Directive

Para la industria aseguradora, la ausencia de un régimen especial genera incertidumbre en la tarificación y en la definición de coberturas. La tendencia regulatoria global hacia la responsabilidad objetiva para IA de alto riesgo debería reflejarse ya en los condicionados de las pólizas de responsabilidad civil tecnológica.

5. Problemas probatorios

Los desafíos probatorios en los litigios relacionados con la IA son probablemente los más complejos que enfrenta el derecho procesal contemporáneo. La naturaleza técnica de los sistemas, la asimetría de información entre las partes y la falta de estándares de documentación generan un escenario en que la víctima puede encontrarse en una posición de desventaja estructural.

5.1. Opacidad algorítmica ("caja negra")

Los modelos de aprendizaje profundo (deep learning) producen decisiones a través de procesos matemáticos de alta complejidad que incluso sus propios desarrolladores no siempre pueden explicar en términos causales precisos. Esta opacidad puede hacer imposible demostrar cómo el sistema llegó a una decisión específica que causó el daño reclamado.

5.2. Trazabilidad y auditabilidad

La posibilidad de reconstruir la secuencia de decisiones de un sistema de IA —su trazabilidad— depende de que el sistema haya sido diseñado para registrar su proceso decisional.

La auditabilidad, entendida como la capacidad de verificar externamente ese registro, es aún menos frecuente. Ambos requisitos están siendo incorporados como obligaciones legales en los marcos regulatorios más avanzados, y deben ser exigidos en los contratos de implementación y en los requisitos de suscripción de riesgos.

5.3. Prueba pericial informática

La prueba pericial es el mecanismo procesal por excelencia para acreditar el funcionamiento defectuoso de un sistema de IA. Sin embargo, enfrenta desafíos específicos: (i) escasez de peritos calificados; (ii) dificultad para acceder al sistema en condiciones que permitan su análisis; (iii) evolución del sistema entre el momento del daño y el de la pericia, especialmente en sistemas con aprendizaje continuo; y (iv) confidencialidad del código fuente.

5.4. Carga dinámica de la prueba

El artículo 167 del Código General del Proceso colombiano consagra la carga dinámica de la prueba, permitiendo al juez distribuir la carga probatoria según la proximidad de las partes con los medios de prueba. Esta herramienta es especialmente valiosa en litigios de IA: el desarrollador u operador del sistema tiene mayor acceso al código, a los datos de entrenamiento y a los registros del sistema, y puede ser compelido a asumir la carga de demostrar la ausencia de defecto o la ruptura del nexo causal.

5.5. Acceso al código fuente y secretos empresariales

El acceso al código fuente de un sistema de IA en el marco de un proceso judicial genera una tensión entre el derecho de la víctima a la prueba y la protección de los secretos empresariales

del demandado. Las soluciones procesales disponibles incluyen: (i) exhibición bajo cláusula de confidencialidad; (ii) peritos neutrales designados por el juez con acceso restringido; y (iii) inferencias negativas cuando el demandado se niega injustificadamente a entregar la información.

6. Responsabilidad por productos defectuosos e inteligencia artificial

El régimen de responsabilidad por productos defectuosos —consagrado en Colombia en la Ley 1480 de 2011— ofrece un marco particularmente adecuado para algunos de los daños causados por sistemas de IA, especialmente cuando estos se comercializan como productos o son componentes de bienes físicos.

6.1. Concepto de defecto en sistemas inteligentes

Un sistema de IA es defectuoso cuando no ofrece la seguridad que legítimamente puede esperarse de él, teniendo en cuenta su presentación, el uso que razonablemente cabe esperar y el momento de su puesta en circulación. La definición de "defecto" es más compleja en la IA que en los productos físicos, porque las capacidades del sistema pueden variar con el tiempo, y la expectativa legítima del usuario puede ser difícil de establecer frente a tecnologías novedosas.

6.2. Tipología de defectos

a) Defecto de diseño. Existe cuando el error no está en la fabricación de una unidad específica sino en la concepción misma del sistema. En el contexto de la IA comprende: modelos entrenados con datos sesgados que producen resultados discriminatorios de manera sistemática;

arquitecturas que no contemplan mecanismos de seguridad adecuados; y sistemas diseñados sin mecanismos de supervisión humana en decisiones de alto impacto.

b) Defecto de fabricación. Ocurre cuando una unidad específica del producto se aparta del diseño previsto. En sistemas de IA puede manifestarse como errores introducidos durante el proceso de entrenamiento, fallas en la integración del modelo con sistemas de terceros, o corrupción de datos durante el despliegue.

c) Defecto de información o advertencia. Se produce cuando el fabricante o proveedor omite informar adecuadamente sobre los riesgos del sistema, sus limitaciones, los contextos en que no debe utilizarse, o las medidas de supervisión que el usuario debe adoptar. Es probablemente el defecto más frecuente en la comercialización actual de sistemas de IA.

6.3. Actualizaciones y aprendizaje continuo del sistema

Una de las particularidades más desafiantes de la IA frente al derecho de productos es que el sistema puede modificar su comportamiento después de su puesta en circulación, ya sea mediante actualizaciones deliberadas del fabricante o mediante el aprendizaje continuo a partir de nuevos datos. Esto plantea tres problemas jurídicos fundamentales:

(i) La determinación del momento relevante del defecto: ¿el sistema era defectuoso en su puesta en circulación original, o el defecto surgió con una actualización posterior? (ii) La responsabilidad por actualizaciones: ¿quien despliega una actualización que introduce un defecto responde como fabricante de un nuevo producto o como proveedor de un servicio de mantenimiento? (iii) El aprendizaje no supervisado: cuando el sistema aprende de sus interacciones y modifica su comportamiento de manera no prevista por el diseñador, ¿puede considerarse que existe un defecto sobrevenido atribuible al operador que no supervisó adecuadamente la evolución del sistema?

Conclusión del Capítulo I

La responsabilidad civil derivada del uso de sistemas de inteligencia artificial no constituye una ruptura con el derecho de daños tradicional, sino su evolución más exigente. Los fundamentos —daño, nexo causal, hecho generador e imputación— permanecen vigentes; lo que cambia es la complejidad de su acreditación y la distribución de responsabilidad entre actores que, en muchos casos, operan en distintas jurisdicciones y bajo distintos marcos regulatorios.

Para la industria aseguradora, este escenario representa simultáneamente un desafío y una oportunidad: el desarrollo de productos de responsabilidad civil tecnológica robustos, con condicionados adaptados a las particularidades de la IA —trazabilidad, actualizaciones, opacidad algorítmica, cadenas de suministro—, posicionará a las compañías aseguradoras como socios estratégicos en la gestión del riesgo tecnológico de sus clientes.

CAPÍTULO II

INTELIGENCIA ARTIFICIAL Y SEGURO DE RESPONSABILIDAD CIVIL

Resumen

El presente capítulo examina, desde una perspectiva jurídica, las profundas transformaciones que la inteligencia artificial (IA) introduce en el seguro de responsabilidad civil (RC), tanto en el ordenamiento colombiano como en el contexto iberoamericano e internacional. A través de un método dogmático-analítico, se estudia la naturaleza jurídica del seguro de RC conforme al Código de Comercio colombiano (artículos 1127 a 1133), los presupuestos clásicos de la responsabilidad civil y su tensión con los rasgos definitorios de los sistemas de IA: autonomía, opacidad algorítmica y capacidad de aprendizaje. El trabajo analiza las principales líneas de cobertura, los clausulados emergentes, las exclusiones específicas en materia de IA introducidas por el mercado asegurador internacional, las iniciativas regulatorias europeas (Reglamento UE 2024/1689 y Directiva de Productos Defectuosos 2024/2853) y el marco regulatorio colombiano.

Se concluye que la IA exige una revisión estructural del seguro de RC, la creación de productos específicos de aseguramiento y una actualización normativa urgente que, en Colombia, debería orientarse por los referentes europeos adaptados a las particularidades del sistema jurídico nacional.

Palabras clave:

inteligencia artificial; seguro de responsabilidad civil; imputabilidad; cobertura; exclusiones; Colombia; regulación; riesgo algorítmico; CONPES 4144; Reglamento UE 2024/1689.

I. Introducción

La inteligencia artificial como tecnología de propósito general representa, sin lugar a dudas, uno de los mayores retos jurídicos del siglo XXI. No se trata únicamente de una revolución tecnológica o económica: es, en un sentido profundo, una revolución de la responsabilidad. No es nuevo en el contexto del derecho de daños y su asegurabilidad el hecho de que la capacidad humana, al generar nuevas herramientas que permitan mayor eficiencia y calidad en sus actividades domésticas y productivas, genere también nuevos escenarios lesivos. Hoy, las máquinas que aprenden, que deciden y que actúan de manera autónoma desafían los fundamentos más arraigados del derecho de daños y, con ellos, la arquitectura del seguro de responsabilidad civil tal como la conocemos.

El seguro de RC cumple en las sociedades modernas una función social de primer orden: trasladar el peso económico de los daños causados a terceros desde el patrimonio del responsable hacia una comunidad de riesgos gestionada por el asegurador, garantizando así la efectividad del derecho de las víctimas a ser indemnizadas. Esta función reparadora y socializadora del riesgo, consagrada en Colombia en los artículos 1127 a 1133 del Código de Comercio, presupone la existencia de un sujeto responsable claramente identificable, de una conducta susceptible de valoración jurídica y de un nexo causal verificable entre el actuar humano y el daño producido. Todos esos presupuestos se ven severamente cuestionados cuando el agente generador del daño es un sistema de inteligencia artificial.

La pregunta que articula el presente capítulo es la siguiente: ¿puede el seguro de responsabilidad civil, en su configuración actual, absorber los riesgos que genera la inteligencia artificial, o es necesario construir un nuevo paradigma asegurador?

Colombia ocupa el puesto 51 de 83 naciones en el Global AI Index de 2024 y el puesto 55 de 188 en el Government AI Readiness Index, lo que evidencia que la adopción de la IA en el sector productivo y público ya es una realidad en aceleración. El sector asegurador colombiano, por su parte, registra en el ramo de RC una de sus principales fuentes de crecimiento, con primas devengadas que superan los dos billones de pesos anuales según estadísticas de FASECOLDA. En ese contexto, la adecuación del marco asegurador a la realidad de la IA no es una cuestión futura: es una urgencia del presente.

II. La responsabilidad civil y sus presupuestos clásicos: una revisión necesaria

2.1. Concepto y fundamento de la responsabilidad civil

La responsabilidad civil es, en su acepción más depurada, la obligación que tiene quien ha causado un daño a otro de repararlo. Esta institución, de raíces profundas en el derecho romano —*neminem laedere*— y desarrollada por la pandectística francesa y alemana, ha sido recibida en el derecho colombiano fundamentalmente a través de los artículos 2341 y siguientes del Código Civil, que consagran el régimen de responsabilidad extracontractual, y de las normas del Código Civil y el Código de Comercio que regulan el régimen general de los efectos de las obligaciones, construyendo el marco de la responsabilidad contractual.

La doctrina clásica coincide en que la responsabilidad civil cumple tres funciones principales: resarcitoria, preventiva y sancionatoria, siendo la primera la de mayor proyección práctica en el contexto del seguro.

El fundamento de la responsabilidad civil ha transitado históricamente entre tres grandes paradigmas: la culpa, la garantía o promesa de satisfacción del crédito y el riesgo. El primero, de corte subjetivo, vincula la obligación de reparar a la reprochabilidad de la conducta del agente; el

segundo y el tercero, de naturaleza objetiva, la anclan a la inobservancia de típicas obligaciones de resultado o a la creación de un riesgo anormal que se materializa en un daño, con independencia de la diligencia del causante. Este tránsito —que la doctrina denomina "objetivación de la responsabilidad"— no es nuevo, pero adquiere una dimensión inédita frente a la IA, cuyos daños difícilmente pueden atribuirse a la culpa de un ser humano concreto y cuyo potencial lesivo es a menudo consecuencia del funcionamiento normal, no defectuoso, del sistema.

2.2. La estructura

La responsabilidad civil, contractual o extracontractual, requiere la concurrencia de tres elementos: una conducta (activa u omisiva) atribuible a un sujeto, un daño cierto y antijurídico sufrido por la víctima, y un nexo de causalidad adecuada entre ambos. Cada uno de estos elementos es profundamente problematizado por la IA.

En cuanto a la conducta, la IA no es, al menos desde la perspectiva del derecho vigente, un sujeto de derecho. Sus decisiones y acciones no son, en sentido estricto, conductas humanas; son outputs de algoritmos entrenados con datos y funciones de pérdida que ningún ser humano controla en tiempo real. El problema se agudiza en los sistemas de aprendizaje profundo (deep learning), cuya lógica interna es opaca incluso para sus propios desarrolladores —el célebre "problema de la caja negra" (black box problem)—.

En lo que respecta al daño, la IA puede producir perjuicios de naturalezas muy diversas: daños corporales derivados de la actuación de vehículos autónomos o robots quirúrgicos; daños patrimoniales causados por sistemas de decisión crediticia o de gestión de inversiones; daños a la honra y reputación ocasionados por algoritmos de recomendación o de moderación de contenidos; y daños derivados de la discriminación algorítmica en procesos de selección laboral o de

tarificación aseguradora. La heterogeneidad del daño producido por IA implica que ninguna línea clásica del seguro de RC lo cubre integralmente.

El nexo causal es, posiblemente, el elemento de mayor incidencia problemática. Las doctrinas de la equivalencia de condiciones, la causalidad adecuada o el "but for" test anglosajón presuponen la posibilidad de aislar la condición determinante del daño. Pero en un sistema de IA que combina miles de variables, capas ocultas de procesamiento y datos de entrenamiento de origen heterogéneo, establecer que la decisión específica del algoritmo fue la causa adecuada del daño resulta extraordinariamente difícil. La causalidad se diluye en la complejidad del sistema, y con ella, la posibilidad de atribuir responsabilidad a un sujeto determinado.

2.3. La responsabilidad objetiva: la garantía y el riesgo como criterios de imputación

Ante las dificultades que plantea la culpa como criterio de imputación, la doctrina y el derecho comparado han recurrido crecientemente a la responsabilidad objetiva como fundamento para responder a los daños de la IA. En Colombia, esta modalidad se encuentra consagrada, entre otros, en el artículo 2356 del Código Civil (actividades peligrosas), en la Ley 1480 de 2011 (responsabilidad por productos defectuosos) y en múltiples estatutos sectoriales.

La extensión de la responsabilidad objetiva a los operadores de sistemas de IA es la solución más ampliamente propuesta en la doctrina comparada. El profesor Alberto Tapia Hermida, de la Universidad Complutense de Madrid, ha sostenido que "la responsabilidad objetiva sería más adecuada" para los operadores de IA, acompañada de un seguro de carácter obligatorio que garantice la efectividad de la indemnización. Esta postura es compartida, con matices, por el Parlamento Europeo y por la Comisión Europea en sus iniciativas regulatorias de 2022 y 2024.

III. La inteligencia artificial como fenómeno jurídico y asegurador

3.1. Definición y taxonomía de los sistemas de inteligencia artificial

La definición jurídica de la inteligencia artificial es, en sí misma, un problema complejo. El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, la define como "un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales." Esta definición, de marcado carácter funcional, captura los rasgos esenciales de los sistemas de IA modernos: la autonomía, la adaptación y la capacidad de influir sobre la realidad.

Para los efectos del derecho de la responsabilidad y del seguro, resulta útil distinguir al menos tres grandes categorías según el nivel de autonomía y riesgo: (i) sistemas de IA de bajo riesgo o automatización simple, como los chatbots de atención al cliente; (ii) sistemas de IA de riesgo medio o elevado, como los sistemas de diagnóstico médico asistido, los algoritmos de suscripción aseguradora o los modelos de gestión de crédito, clasificados como de "alto riesgo" por el Reglamento europeo; y (iii) sistemas de IA de autonomía elevada, como los vehículos autónomos y los robots quirúrgicos, que representan el mayor desafío para el seguro de RC.

3.2. Los rasgos disruptivos de la inteligencia artificial para el derecho de daños

Más allá de la taxonomía, importa identificar los rasgos específicos de los sistemas de IA que los hacen jurídicamente disruptivos. El primero es la autonomía: los sistemas de IA no se limitan a ejecutar instrucciones precodificadas; aprenden de los datos, adaptan su comportamiento

y toman decisiones que sus propios creadores no pueden prever con exactitud. El segundo es la opacidad algorítmica o "caja negra". El tercero es la escala y ubicuidad de los daños potenciales: un sistema de IA defectuoso o sesgado puede causar daños en masa a millones de personas simultáneamente, lo cual desborda la capacidad de respuesta del seguro individual de RC.

3.3. El problema de la imputación en sistemas autónomos

El problema de la imputación es el verdadero nudo del seguro de RC frente a la IA. En el esquema tradicional, la cadena de responsabilidad es relativamente clara: el fabricante del producto defectuoso, el prestador del servicio negligente o el conductor imprudente son identificables y asegurables. En el ecosistema de la IA, esa cadena se atomiza en múltiples actores: el investigador que diseñó el algoritmo base, la empresa que lo entrenó, el proveedor de infraestructura en la nube, el integrador, el distribuidor y el usuario final. Ninguno de ellos controla el sistema en su totalidad, y todos podrían ser, en mayor o menor medida, responsables del daño causado.

La doctrina ha propuesto diversas soluciones: la responsabilidad solidaria de todos los actores de la cadena de valor, recogida parcialmente en la Directiva europea de Productos Defectuosos 2024/2853; la responsabilidad del operador o desplegador (deployer) como punto de contacto más próximo a la víctima; y la creación de un fondo de compensación alimentado por una tasa sobre los operadores de IA de alto riesgo. En Colombia, ninguna de estas soluciones ha sido legislativamente adoptada, aunque el CONPES 4144 de 2025 instruye a los reguladores sectoriales para que definan "vías de responsabilidad y mecanismos de reparación" para las víctimas de daños causados por IA.

IV. El seguro de responsabilidad civil en Colombia: régimen jurídico y estructura

4.1. Naturaleza jurídica y configuración legal

El seguro de responsabilidad civil está regulado en Colombia en los artículos 1127 a 1133 del Código de Comercio, modificados sustancialmente por la Ley 45 de 1990. El artículo 1127, reformado por el artículo 84 de dicha ley, establece que "el seguro de responsabilidad impone a cargo del asegurador la obligación de indemnizar los perjuicios patrimoniales que cause el asegurado con motivo de determinada responsabilidad en que incurra de acuerdo con la ley."

El artículo 1131, modificado por el artículo 86 de la Ley 45 de 1990, consagra la regla de la ocurrencia del siniestro: "en el seguro de responsabilidad se entenderá ocurrido el siniestro en el momento en que acaezca el hecho externo imputable al asegurado." Esta norma, que se amolda al sistema de "ocurrencia" (occurrence-based), a diferencia del sistema de "reclamaciones" (claims-made) predominante en los mercados anglosajones, tiene importantes consecuencias prácticas en materia de IA: los daños tardíos o diferidos —frecuentes en sistemas de IA que aprenden y evolucionan con el tiempo— podrían no estar cubiertos por las pólizas vigentes al momento de la reclamación si el hecho externo ocurrió durante la vigencia de una póliza ya vencida.

El artículo 1133, reformado por el artículo 87 de la Ley 45 de 1990, consagra la acción directa de la víctima contra el asegurador: "en el seguro de responsabilidad civil los damnificados tienen acción directa contra el asegurador." Esta disposición es fundamental para garantizar la eficacia del seguro de RC frente a los daños de la IA.

4.2. Partes del contrato y sus obligaciones

El contrato de seguro de RC involucra a cuatro sujetos: el tomador, quien contrata el seguro con el asegurador; el asegurado, titular del interés asegurable; el asegurador, que asume el riesgo a cambio de la prima; y el tercero damnificado, beneficiario del seguro con acción directa consagrada en el artículo 1133. En el contexto de la IA, la identificación de quién es el "asegurado" —el desarrollador del algoritmo, el integrador, el distribuidor o el usuario final— es una cuestión de primera importancia que las pólizas actuales no siempre resuelven de manera clara.

4.3. Amparos y coberturas tradicionales

El seguro de RC en Colombia ofrece, en sus pólizas típicas, una estructura de amparos básicos y complementarios. Los amparos básicos comprenden la responsabilidad civil extracontractual por daños corporales y materiales causados a terceros, los perjuicios extrapatrimoniales derivados de tales daños, y los gastos de defensa judicial. Los amparos complementarios más frecuentes incluyen la responsabilidad civil contractual, la responsabilidad civil del empleador, la responsabilidad de administradores y directivos (D&O), la responsabilidad civil profesional y, más recientemente, amparos específicos para riesgos tecnológicos y cibernéticos. Ninguno de estos amparos fue diseñado para cubrir los riesgos específicos de la IA.

4.4. Exclusiones convencionales y legales

Las exclusiones convencionales más frecuentes en las pólizas colombianas de RC incluyen el dolo o culpa grave del asegurado; los daños derivados del incumplimiento deliberado de obligaciones contractuales; los daños por guerra, terrorismo o conmoción civil; los daños ambientales específicos; y, recientemente, los daños derivados de riesgos cibernéticos, que han migrado de la cobertura tácita en las pólizas generales a productos específicos de ciberseguro. La

práctica internacional más reciente muestra una tendencia a excluir expresamente los daños derivados de la IA, especialmente la IA generativa, de las pólizas de RC general, siguiendo el modelo de las exclusiones cibernéticas adoptadas en la última década.

V. Implicaciones de la inteligencia artificial en el seguro de responsabilidad civil

5.1. Redefinición del riesgo asegurable

La primera y más fundamental implicación de la IA en el seguro de RC es la redefinición del riesgo asegurable. Para que un riesgo sea asegurable debe reunir ciertas condiciones técnicas: debe ser incierto, futuro, posible, fortuito y evaluable estadísticamente. La IA plantea dificultades en casi todos estos requisitos: el comportamiento de un sistema de IA en producción es difícilmente predecible con las herramientas actuariales tradicionales, no existen series históricas de siniestros suficientemente largas, y la naturaleza de los daños que pueden causar es heterogénea. La Lloyd's Market Association (LMA) ha reconocido que existe "una falta de datos" que impide desarrollar modelos actuariales robustos.

5.2. Dificultades en la determinación del asegurado y del tercero damnificado

El mercado asegurador internacional ha tendido a distinguir entre dos categorías de asegurados en materia de IA: los proveedores (providers o developers), que diseñan y entrenan los sistemas, y los operadores o desplegados (deployers), que los integran en productos y servicios. El Reglamento UE 2024/1689 adopta precisamente esta distinción y asigna a cada categoría obligaciones diferenciadas. Por el lado de los terceros damnificados, la IA introduce el problema de las víctimas difusas: millones de personas afectadas de manera sistemática e imperceptible por sistemas de IA sesgados, que difícilmente conocen que han sufrido un daño causado por IA, y aún menos pueden probarlo.

5.3. El siniestro en sistemas de inteligencia artificial: ocurrencia y configuración

La configuración del siniestro en sistemas de IA presenta complejidades particulares. Identificar el "hecho externo imputable al asegurado" del artículo 1131 del Código de Comercio resulta difícil porque el comportamiento dañino del sistema puede no ser un hecho puntual y perceptible, sino una serie de micro-decisiones acumulativas que solo producen un daño apreciable a lo largo del tiempo —el denominado daño gradual—. La solución más adecuada para los riesgos de IA es el sistema de cobertura claims-made, cuya validez ha sido reconocida por la jurisprudencia colombiana para ciertos ramos de RC profesional.

VI. Problemas clásicos revisitados y nuevos desafíos: la IA ante el derecho de la responsabilidad civil y su aseguramiento

El encuentro entre la inteligencia artificial y el derecho de la responsabilidad civil no produce una colisión frontal, sino algo más sutil: una erosión silenciosa de las categorías jurídicas que durante siglos han organizado la reparación del daño. Las instituciones no desaparecen de un golpe; se vuelven imprecisas, inadecuadas, porosas. Esta sección sistematiza esa erosión e identifica soluciones doctrinarias y normativas concretas.

6.1. ¿La responsabilidad civil generada por sistemas de IA es subjetiva u objetiva?

Este es uno de los grandes debates dogmáticos que plantea la IA al derecho de la responsabilidad civil, y la respuesta tiene consecuencias directas y determinantes para el seguro de RC. La responsabilidad subjetiva —articulada en Colombia alrededor del artículo 2341 del Código Civil— exige la prueba de culpa del agente. Aplicada a la IA, esta exigencia tropieza con un obstáculo estructural: ¿dónde reside la culpa cuando el sistema actúa de manera autónoma,

aprende de datos que nadie controló individualmente y toma decisiones que ningún programador específico anticipó?

La doctrina ha intentado salvar este obstáculo a través del concepto de culpa algorítmica, definida como la falta de diligencia en el diseño, entrenamiento, supervisión o despliegue de un sistema de IA que, materializada en el comportamiento del sistema, produce un daño a un tercero. El firme defensor del sistema de aprendizaje automático que omite realizar una auditoría de sesgo antes del despliegue, el operador de IA médica que desactiva los mecanismos de supervisión humana para reducir costos, el desarrollador que entrena su modelo con datos desactualizados: todos ellos incurren en culpa algorítmica, aunque en el momento del daño no estén presentes ni lo hayan querido.

La propuesta normativa que se deriva de este análisis es que el legislador colombiano consagre expresamente un régimen de responsabilidad objetiva para los operadores de sistemas de IA clasificados como de alto riesgo, siguiendo la taxonomía del Reglamento UE 2024/1689. Para los sistemas de IA de riesgo bajo o medio, la responsabilidad subjetiva con estándares de diligencia reforzada —culpa algorítmica— sería el régimen aplicable, con la carga de la prueba en cabeza del operador respecto del cumplimiento de dichos estándares.

6.2. Si la conducta no la comete el asegurado sino el sistema de IA: ¿existe hecho amparado por el seguro?

Esta pregunta toca directamente la estructura del contrato de seguro de RC colombiano. El artículo 1127 del Código de Comercio define el objeto del seguro como "los perjuicios patrimoniales que cause el asegurado con motivo de determinada responsabilidad en que incurra de acuerdo con la ley." Si el causante material del daño no es el asegurado sino el sistema de IA, ¿está cubierto el evento?

La respuesta debe ser afirmativa, apoyada en una interpretación sistemática y finalista del contrato de seguro. El seguro de RC no cubre exclusivamente los actos personales y directos del asegurado; cubre su responsabilidad jurídica, que puede surgir tanto de actos propios como de los daños producidos por las cosas que guarda o los sistemas que están bajo su dirección y control. Un sistema de IA operado por el asegurado en el ejercicio de su actividad profesional o empresarial es, jurídicamente hablando, una herramienta a cargo del asegurado, cuyo manejo defectuoso o cuyo resultado dañino genera la responsabilidad de este último.

La advertencia importante es que esta conclusión depende críticamente de la redacción de las condiciones generales de la póliza. Si la póliza contiene una exclusión de "daños causados por sistemas automatizados o de inteligencia artificial", la cobertura puede quedar excluida. Esta es precisamente la tendencia que el mercado internacional está siguiendo: las nuevas exclusiones de IA del ISO (2026) y las exclusiones absolutas de Berkley Insurance eliminan la cobertura para daños causados por IA, lo que obliga a los asegurados a buscar coberturas específicas.

6.3. La actuación de la IA como causa extraña

La causa extraña requiere, según la Corte Suprema de Justicia, la concurrencia de tres requisitos: imprevisibilidad, irresistibilidad y exterioridad. La pregunta que plantea la IA es si el asegurado puede invocar la actuación autónoma e imprevista de un sistema de IA propio como causa extraña que rompa el nexo causal.

La respuesta depende del grado de autonomía del sistema y del nivel de diligencia que el operador haya desplegado. El fallo de ese instrumento no es, en sentido estricto, un evento extraño al asegurado, sino la materialización del riesgo que él mismo creó e introdujo en el tráfico. Como regla general, el operador de un sistema de IA no puede invocar válidamente la causa extraña para

exonerarse de responsabilidad civil cuando el daño se deriva del comportamiento autónomo de ese sistema.

6.4. La causalidad en sistemas de IA y la carga de la prueba

La víctima de un daño causado por IA enfrenta una asimetría informativa estructural: el demandado tiene acceso al código fuente, a los datos de entrenamiento, a los registros de decisiones del sistema y a la documentación técnica; la víctima, en cambio, carece de esos elementos. Las soluciones exploradas por el derecho comparado son: el deber de documentación y trazabilidad para los operadores de sistemas de alto riesgo; la inversión de la carga de la prueba cuando el demandante acredita el daño y la participación del sistema en su producción; y la prueba pericial especializada en inteligencia artificial.

6.5. La cadena de valor de la IA y la distribución de la responsabilidad

El ecosistema productivo de la inteligencia artificial involucra típicamente seis categorías de actores: el investigador que diseña la arquitectura del modelo; el desarrollador que lo entrena; el proveedor de datos de entrenamiento; el proveedor de infraestructura en la nube; el integrador; y el operador o usuario final. Cada uno tiene una influencia distinta sobre el comportamiento del sistema y, por ende, una contribución diferente al riesgo de daño.

El derecho comparado ha convergido hacia la responsabilidad solidaria entre los distintos actores de la cadena de valor como regla general, con la posibilidad de acciones de repetición para la distribución interna del costo del daño. La nueva Directiva de Productos Defectuosos de la UE (2024) establece expresamente que cuando dos o más partes sean responsables del mismo daño, "los Estados miembros velarán para que puedan ser considerados responsables solidariamente."

6.6. La responsabilidad de los administradores y el seguro de directores y administradores (D&O) ante la inteligencia artificial

El seguro de directores y administradores (D&O) fue concebido para amparar a quienes adoptan decisiones estratégicas frente a reclamaciones derivadas de errores, omisiones o actos cumplidos en el ejercicio de sus funciones. La irrupción de la inteligencia artificial transforma el contorno de esa responsabilidad: cuando parte de las decisiones empresariales se delega, se informa o incluso se genera mediante sistemas algorítmicos, surge un deber autónomo de diligencia a cargo del órgano de administración, consistente en comprender la tecnología que la organización despliega, evaluar su impacto y comunicarlo con honestidad a los mercados, los inversionistas y los reguladores.

La práctica corporativa revela una brecha significativa entre la magnitud del riesgo y la atención que efectivamente recibe. Según una encuesta global de Deloitte (2024), el 45% de las juntas directivas no incluye la IA en su agenda y solo el 14% la discute en cada reunión, pese a que los propios directores reconocen como funciones esenciales del órgano de gobierno la supervisión del uso ético de la IA (57%), la definición de la estrategia (44%) y la gestión de riesgos y oportunidades (35%). Esa distancia entre lo que los administradores admiten que deberían hacer y lo que realmente hacen es, precisamente, el espacio donde nace la responsabilidad y, con ella, el siniestro potencialmente amparable bajo la póliza D&O.

Los riesgos que la IA proyecta sobre los administradores se manifiestan en dos planos. De un lado, pueden incurrir en responsabilidad por subestimar el impacto negativo de la tecnología sobre el negocio y omitir su divulgación; del otro, por sobreestimar sus beneficios mediante afirmaciones exageradas dirigidas al mercado, conducta que en su forma extrema configura el

denominado AI washing (atribuir a la empresa capacidades de IA que no posee)¹, hoy perseguido como una modalidad de fraude bursátil. La jurisprudencia de Estados Unidos ofrece ya ejemplos en ambos sentidos, desde demandas por divulgación deficiente² hasta acciones por promesas incumplidas frente a los inversionistas³.

A su vez, el estándar de responsabilidad por el daño directo causado por sistemas autónomos se está redefiniendo. En el caso *Benavides v. Tesla* (Florida, 2025)⁴, un jurado halló que el fabricante había puesto en el mercado un producto defectuoso y distribuyó la responsabilidad entre la empresa (33%) y el conductor (67%), con una condena del orden de USD 329 millones. El precedente sugiere que el fabricante de un sistema de IA puede ser declarado corresponsable cuando lo diseña de modo que no detecta riesgos previsibles, lo comercializa induciendo una confianza excesiva en sus capacidades y ese fallo contribuye causalmente al daño. Trasladado al gobierno corporativo, si los administradores conocían o debían conocer tales riesgos y no adoptaron medidas de mitigación, su inacción puede constituir una negligencia susceptible de activar la cobertura D&O.

¹ Ilustran esta tendencia las demandas colectivas presentadas por Rosen Law Firm contra AppLovin Corporation y Skyworks Solutions, Inc., en las que se alega que ambas compañías formularon afirmaciones sobre sus capacidades de IA que no correspondían a la realidad de sus operaciones, induciendo a los inversores a adquirir acciones a precios inflados.

² El caso paradigmático es la demanda colectiva interpuesta en junio de 2025 contra Reddit, Inc. y sus directores, en la que los inversores alegan que la compañía conocía y omitió divulgar en los documentos de su oferta pública inicial de marzo de 2024 el impacto que los asistentes de IA generativa (ChatGPT, Gemini, Perplexity) producían sobre el tráfico de su plataforma y, por tanto, sobre sus ingresos publicitarios, lo que derivó en una caída del precio de la acción superior al 15% en mayo de 2025. Demandas análogas se han presentado contra DoubleVerify y TripAdvisor.

³ Entre los ejemplos recientes figuran: la demanda colectiva contra Oracle Corporation (5 de febrero de 2026), por afirmar que sus inversiones en infraestructura de IA se traducirían en aumentos sustanciales de ingresos que no se materializaron; la demanda contra Fermi America (5 de enero de 2026), cuya oferta pública inicial captó USD 757,7 millones sobre proyecciones de demanda que se desplomaron tras el retiro de su único cliente, con una caída del 59% frente al precio de salida; y la acción de grupo contra CoreWeave, Inc. (12 de enero de 2026), por afirmaciones presuntamente falsas sobre la fortaleza de la demanda de sus servicios y la ocultación de problemas operacionales.

⁴ *Benavides v. Tesla, Inc.*, Tribunal Federal del Distrito Sur de Florida, veredicto de jurado del 1 de agosto de 2025. Un vehículo Tesla con el sistema Autopilot activado no se detuvo ante una señal de pare y colisionó, causando la muerte de Naibel Benavides León y lesiones graves a Dillon Angulo. El jurado halló que Tesla vendió un producto defectuoso y distribuyó la responsabilidad en un 33% a la empresa y un 67% al conductor, con una condena total del orden de USD 329 millones, incluidos USD 200 millones en daños punitivos.

Para el mercado asegurador, estas tendencias proyectan tres consecuencias. La primera es que el volumen y la diversidad de las reclamaciones vinculadas a la IA anticipan una mayor siniestralidad y presiones sobre las primas y las condiciones de cobertura. La segunda es que la noción de «circunstancia» notificable adquiere una dimensión nueva: los administradores deben evaluar de manera periódica si las condiciones de litigiosidad propias de su industria y de la tecnología que emplean constituyen un hecho que deba comunicarse al asegurador para anclar la cobertura al periodo de póliza correspondiente. La tercera es que el sector debe avanzar hacia productos que aborden el riesgo de IA de forma expresa, precisando tanto los amparos como las exclusiones, entre ellas el AI washing deliberado.

En el contexto colombiano, donde el seguro D&O opera como un amparo voluntario dentro del régimen general de los artículos 1127 y siguientes del Código de Comercio, el desafío es doble: los aseguradores deberán incorporar en la suscripción criterios que valoren la madurez del gobierno corporativo de IA del asegurado, y los administradores deberán integrar la gestión del riesgo algorítmico como un componente sistemático de su diligencia. Así entendida, la póliza D&O deja de ser un instrumento meramente reactivo para convertirse en un incentivo de buena gobernanza, en línea con la función preventiva del seguro que se examina en los apartados siguientes.

6.7. El seguro de RC como instrumento estructural del sistema de responsabilidad

El seguro de responsabilidad civil no es simplemente un instrumento de transferencia individual del riesgo: es, en su dimensión más profunda, un mecanismo de organización social para la gestión colectiva de los daños. Si los sistemas de IA pueden causar daños masivos, seriados e invisibles a millones de personas, y si los operadores individuales no tienen patrimonio suficiente para responder por esos daños, el seguro —individual u obligatorio— es el único mecanismo capaz

de garantizar que la promesa legal de reparación se traduzca en indemnización efectiva para las víctimas.

La función preventiva del seguro merece especial atención en el contexto de la IA. Una póliza bien diseñada, cuya prima refleje fielmente el riesgo del sistema de IA asegurado, tiene un efecto incentivador sobre el comportamiento del operador: el asegurado que implementa mejores controles de gobernanza algorítmica debería obtener primas más bajas, generando un círculo virtuoso entre la buena gestión del riesgo y la reducción de la exposición aseguradora.

6.8. Hacia un modelo integrado: de la cobertura reactiva a la arquitectura aseguradora proactiva

El análisis desarrollado permite identificar un conjunto de propuestas sistémicas para la adecuación del seguro de RC colombiano a los retos de la IA. El primer nivel de esa arquitectura es el seguro obligatorio de RC para operadores de sistemas de IA de alto riesgo, por analogía con el Seguro Obligatorio de Accidentes de Tránsito (SOAT). El segundo nivel es el seguro voluntario específico de IA para riesgos no cubiertos por el seguro obligatorio: daños patrimoniales puros, daños reputacionales, responsabilidad de directores y administradores por decisiones basadas en IA, responsabilidad profesional de los usuarios de IA en sectores regulados. El tercer nivel, para riesgos sistémicos o catastróficos de IA, sería un fondo de compensación alimentado por contribuciones de los operadores de IA de alto riesgo, gestionado por el Estado y activado como mecanismo de último recurso.

VII. Conclusiones

Primera. La inteligencia artificial introduce perturbaciones estructurales en los tres elementos de la responsabilidad civil —conducta, daño y nexo causal— que los hacen difícilmente

encuadrables en los esquemas tradicionales del derecho de daños colombiano. La autonomía, la opacidad algorítmica y la capacidad de producir daños masivos y seriados de los sistemas de IA exigen una revisión profunda de los criterios de imputación y de la distribución de la carga de la prueba, orientándose hacia la responsabilidad objetiva por riesgo como principio rector.

Segunda. El seguro de responsabilidad civil colombiano, regulado en los artículos 1127 a 1133 del Código de Comercio, presenta limitaciones significativas para dar respuesta a los riesgos de la IA: el sistema de "ocurrencia" del siniestro, la ausencia de una definición de "asegurado" adaptada al ecosistema de la IA, la inexistencia de seguros obligatorios específicos y la falta de cláusulas estándar de cobertura para riesgos de IA hacen que el instrumento asegurador vigente sea insuficiente para garantizar la reparación efectiva de las víctimas.

Tercera. El mercado asegurador internacional ha iniciado, de manera acelerada, un proceso de adaptación a los riesgos de la IA. Las exclusiones de IA generativa del ISO (CG 40 47, CG 40 48 y CG 35 08), adoptadas desde enero de 2026, y la exclusión absoluta de Berkley Insurance para D&O y RC profesional generan una brecha de cobertura que las empresas colombianas que utilizan IA deben gestionar de manera urgente con sus corredores de seguros.

Cuarta. El marco regulatorio europeo —en particular el Reglamento (UE) 2024/1689 y la Directiva de Productos Defectuosos 2024/2853— constituye el referente más avanzado y sistemático para la regulación de la IA y sus implicaciones en materia de responsabilidad civil. Colombia debería inspirarse en este marco para el diseño de su propia legislación, adaptándolo a las particularidades del sistema jurídico colombiano y a la realidad del mercado asegurador nacional.

Quinta. El CONPES 4144 de 2025 representa un avance significativo en la política pública colombiana sobre IA, pero su silencio sobre el papel del seguro y la insuficiencia de los

mecanismos de responsabilidad civil específicos para la IA constituyen una laguna que debe ser colmada con urgencia por el legislador y la Superintendencia Financiera de Colombia.

Sexta. Las propuestas de reforma más urgentes para el ordenamiento colombiano son: la consagración de un régimen de responsabilidad objetiva para operadores de IA de alto riesgo; la creación de un seguro obligatorio de RC para dicha categoría de operadores; la modernización del artículo 1131 del Código de Comercio para permitir el sistema de claims-made en el seguro de RC tecnológico; y el desarrollo por la SFC de lineamientos específicos para el aseguramiento de riesgos de IA.

Séptima. La IA no es solo un desafío para el seguro de RC: es también una oportunidad. Las aseguradoras colombianas que desarrollen productos innovadores de cobertura específica para riesgos de IA estarán mejor posicionadas para capturar los beneficios de la transformación digital del sector y para cumplir la función social que el seguro de RC tiene en la sociedad colombiana.

CAPÍTULO III

INTELIGENCIA ARTIFICIAL, PRODUCTOS DEFECTUOSOS Y RIESGOS

CIBERNÉTICOS:

ANÁLISIS DE SU IMPACTO EN EL SEGURO DE RESPONSABILIDAD CIVIL

Resumen

El presente capítulo examina la incidencia de la inteligencia artificial (IA) y el Internet de las Cosas (IoT) en el derecho de la responsabilidad por productos defectuosos y en el seguro de responsabilidad civil. Se analiza la Directiva (UE) 2024/2853 como respuesta normativa a los nuevos desafíos derivados de los sistemas inteligentes, incluyendo la ampliación del concepto de producto para abarcar el software y los sistemas de IA, la noción de defecto dinámico en sistemas evolutivos, los mecanismos probatorios y presunciones de defectuosidad y causalidad, y los riesgos cibernéticos como frontera difusa entre defecto algorítmico y ataque externo. El capítulo concluye que el seguro de RC se erige como el verdadero mecanismo de estabilización del sistema de responsabilidad por productos defectuosos en la era de la IA.

Palabras clave:

inteligencia artificial; Internet de las Cosas; productos defectuosos; Directiva (UE) 2024/2853; riesgos cibernéticos; defecto dinámico; seguro de responsabilidad civil; causalidad; presunciones.

Introducción

La inteligencia artificial (IA) puede entenderse como un conjunto de herramientas y sistemas computacionales diseñados para reproducir o simular determinadas funciones propias del cerebro humano. Este campo de estudio surgió hacia mediados de la década de 1950 y, desde entonces, ha atravesado distintas etapas caracterizadas por expectativas elevadas, períodos de gran entusiasmo, así como críticas y cuestionamientos acerca de su verdadero alcance y desarrollo (Steels y López, 2018).

Para Nilsson (2000), la inteligencia artificial tiene como finalidad el estudio y desarrollo del comportamiento inteligente en las máquinas, lo que comprende capacidades como percibir, razonar, aprender, comunicarse y actuar dentro de entornos complejos. La irrupción de estas tecnologías en el mercado de bienes y servicios exige una revisión profunda de los regímenes jurídicos de responsabilidad, en especial del régimen de productos defectuosos, y plantea nuevos desafíos para la industria aseguradora.

1. Inteligencia artificial e Internet de las Cosas: del riesgo individual al riesgo

sistémico

El Internet de las Cosas (IoT) hace referencia a entornos en los que la conectividad a redes y la capacidad de procesamiento se incorporan a objetos, sensores y elementos de uso cotidiano, permitiendo que dichos dispositivos puedan generar, compartir y utilizar información con una intervención humana mínima (Rose, Eldridge y Chapín, 2015).

La incorporación de inteligencia artificial en entornos vinculados al IoT no solo incrementa la posibilidad de producción de daños, sino que modifica sustancialmente la propia configuración del riesgo. En el modelo industrial tradicional, el riesgo solía atribuirse a un bien determinado o a

una conducta individual claramente identificable. Sin embargo, dentro de los ecosistemas digitales interconectados, el riesgo se distribuye entre múltiples dispositivos, plataformas tecnológicas, servicios digitales y procesos permanentes de actualización, dando lugar a lo que puede entenderse como un riesgo sistémico descentralizado, en el que el daño puede originarse como consecuencia de la interacción entre diversos componentes que, analizados individualmente, podrían no presentar defectos o fallas.

Las nuevas tecnologías generan un impacto considerable en la dinámica del sector asegurador a nivel global. Entre los principales desafíos que introducen para el sector se encuentran la declaración del estado del riesgo y sus variaciones durante la vigencia del contrato de seguro, reguladas en los artículos 1058, 1059 y 1060 del Código de Comercio colombiano. Los avances tecnológicos transforman la forma en que se evalúa el riesgo y fortalecen la capacidad de las aseguradoras para verificar la información suministrada por el asegurado (Vesga, 2022).

Esta situación evidencia una tensión estructural dentro del derecho de daños: fue concebido para responder frente a daños concretos, individualizados y fácilmente localizables, mientras que la inteligencia artificial y el IoT producen riesgos dinámicos, interdependientes y en constante evolución. En este escenario, la cuestión jurídica ya no se limita a determinar quién debe responder por el daño ocasionado, sino también a establecer de qué manera debe distribuirse jurídicamente un riesgo que no puede atribuirse plenamente a un único sujeto o agente.

2. La Directiva (UE) 2024/2853: ¿adaptación suficiente o respuesta parcial?

La responsabilidad por productos defectuosos busca replantearse frente a los nuevos desafíos derivados de los avances tecnológicos, especialmente aquellos relacionados con la inteligencia artificial, los nuevos modelos de negocio y las transformaciones en las cadenas de suministro. Sin embargo, resulta llamativo que la situación de vulnerabilidad en la que pueden

encontrarse las personas físicas y los consumidores no haya recibido una atención suficiente dentro de este proceso de actualización y adaptación (Meco, 2026).

La Directiva introduce una transformación sustancial en la concepción tradicional tanto del producto como del daño, al incorporar dentro del régimen de responsabilidad objetiva elementos como el software, los archivos digitales y los sistemas de inteligencia artificial, y reconoce como indemnizables los perjuicios ocasionados por la destrucción, pérdida o corrupción de datos (Sancho, 2026).

La principal innovación consiste en la incorporación de excepciones a la causal de exoneración de responsabilidad basada en la inexistencia del defecto al momento en que el producto fue introducido en el mercado. La Directiva limita la posibilidad de excluir responsabilidad cuando exista probabilidad de que el carácter defectuoso que ocasionó el daño no estuviera presente inicialmente o haya surgido con posterioridad, especialmente en contextos tecnológicos en los que los sistemas de IA pueden modificarse, actualizarse o evolucionar después de su comercialización (De la Vega, 2024).

2.1. La ampliación del concepto de producto como avance estructural

Si bien la delimitación jurídica del concepto de "producto" constituye una de las cuestiones centrales para la aplicación del régimen especial de responsabilidad por productos defectuosos, la nueva Directiva aborda esta materia ampliando el concepto tradicional para abarcar elementos tecnológicos y digitales. La incorporación expresa del software y de los sistemas de inteligencia artificial dentro del concepto de producto representa un importante avance normativo, ya que permite superar discusiones meramente formales relacionadas con la naturaleza material o inmaterial del bien, desplazando el eje del análisis hacia el nivel de seguridad que legítimamente el consumidor puede esperar del producto (De la Vega, 2024).

Sin embargo, los datos no siempre quedarán comprendidos dentro de la categoría jurídica de producto, razón por la cual las normas relativas a la responsabilidad por productos defectuosos no resultarán aplicables al contenido de determinados archivos digitales. Cuando el producto permanece bajo control del fabricante a través de actualizaciones permanentes, resulta discutible la existencia de un momento definitivo de puesta en circulación, lo que pone en crisis la concepción clásica del "estado del producto al momento de salir al mercado".

2.2. El defecto dinámico y la seguridad evolutiva

La Directiva (UE) 2024/2853 introduce una novedad parcial respecto al criterio tradicional de defecto. Aunque mantiene el estándar de seguridad legítimamente esperable, añade un segundo parámetro alternativo: el nuevo artículo 7.1 dispone que un producto será considerado defectuoso cuando no ofrezca la seguridad que una persona tiene derecho a esperar o aquella exigida conforme al Derecho de la Unión o al ordenamiento nacional (Pazos, 2025).

Tratándose de sistemas de inteligencia artificial, la seguridad no constituye una condición estática o permanente. Un sistema puede ofrecer condiciones adecuadas de seguridad al momento de su comercialización y, posteriormente, volverse inseguro como consecuencia de su interacción con nuevos datos o a raíz de actualizaciones defectuosas. De allí surge la noción de defecto dinámico, cuya delimitación temporal plantea importantes desafíos jurídicos.

2.3. Facilidad probatoria y equilibrio procesal

La nueva Directiva mantiene la regla según la cual el afectado que reclama indemnización debe asumir la carga de probar el perjuicio, el carácter defectuoso del bien y la relación causal entre ambos. Sin embargo, introduce presunciones relevantes sobre la existencia del defecto y del nexo causal, que pueden adquirir especial relevancia práctica en el ámbito de los productos

digitales cuando estos incumplan las exigencias normativas de seguridad o ciberseguridad aplicables (De la Vega, 2024).

La introducción de presunciones en los supuestos de dificultades técnicas excesivas para acreditar el carácter defectuoso o el nexo causal constituye una respuesta pragmática frente a la opacidad algorítmica. La denominada "caja negra" tecnológica dificulta —y en ocasiones impide— reconstruir el proceso decisional que desembocó en la producción del daño (Wigg, 2024).

Desde una mirada crítica, estas presunciones resultan indispensables para impedir que la complejidad tecnológica se transforme en un obstáculo para el acceso a la justicia. Sin embargo, también implican trasladar el riesgo probatorio hacia el fabricante, lo cual puede repercutir en el incremento de las primas de seguro y en la adopción de cláusulas contractuales más restrictivas.

3. Riesgos cibernéticos: frontera difusa entre defecto y ataque externo

Los productos digitales gestionan nuestros datos personales bajo la premisa de ofrecer mayor comodidad y bienestar. Se estima que para 2025 existirán alrededor de 75.000 millones de dispositivos con componentes digitales capaces de conectarse con otras personas y con objetos del entorno (Friedman, 2018).

Uno de los aspectos más complejos en este ámbito consiste en diferenciar entre un defecto algorítmico y un incidente externo de ciberseguridad. Si la vulnerabilidad frente a un ataque deriva de fallas en el diseño del sistema, esta puede considerarse un defecto conforme a la Directiva (UE) 2024/2853. En cambio, si el ataque resulta extraordinario e imprevisible, podría calificarse como un hecho externo.

La línea divisoria entre defecto y ataque externo resulta frecuentemente difusa. En entornos IoT caracterizados por una alta interconexión, alcanzar una seguridad absoluta es imposible, lo

que plantea hasta qué punto puede exigirse al fabricante la eliminación total del riesgo cibernético. La ampliación del concepto de defecto hacia las vulnerabilidades digitales fortalece la protección del consumidor, pero al mismo tiempo incrementa la responsabilidad jurídica de los fabricantes y, en consecuencia, de sus aseguradoras.

4. El seguro de responsabilidad civil en la Unión Europea: estabilización del sistema

La nueva Reglamentación sobre Seguridad General de Productos adoptada por la Unión Europea en 2023 (Reglamento 2023/988), junto con la Directiva sobre responsabilidad por daños derivados de productos defectuosos, generan diversas repercusiones en el mercado asegurador. Su impacto no se limita a la instauración de un régimen de responsabilidad que trasciende la distinción clásica entre contractual y extracontractual, sino que además introduce un sistema autónomo cuyo fundamento jurídico se suma a los regímenes ya existentes en cada Estado miembro (Tabares, 2024).

Desde una perspectiva crítica, el seguro desempeña tres funciones esenciales en este contexto: en primer lugar, actúa como garantía patrimonial; en segundo término, facilita la distribución social del riesgo tecnológico; y finalmente, cumple una función preventiva al incentivar la adopción de medidas técnicas. Sin embargo, también puede generar efectos colaterales: la transferencia del riesgo al asegurador puede derivar en una externalización moral del mismo si no se acompaña de mecanismos de control y franquicias adecuadas.

5. El mercado colombiano frente a la inteligencia artificial

En Colombia, el Estatuto del Consumidor (Ley 1480 de 2011) permite la inclusión de productos inteligentes dentro del régimen objetivo por defecto de seguridad. Sin embargo, a diferencia de la normativa de la Unión Europea, no existe una referencia expresa al software como

producto, lo que puede generar incertidumbre interpretativa. Si bien una lectura evolutiva permitiría incorporar los sistemas inteligentes, la ausencia de precisión normativa podría obstaculizar la uniformidad en la jurisprudencia.

En el ámbito asegurador colombiano, el mercado ofrece pólizas de riesgos cibernéticos que contemplan incidentes digitales, incluyendo fallas de seguridad y vulneraciones de datos. Esto evidencia que la adaptación contractual ha avanzado con mayor rapidez que la evolución normativa. El desafío actuarial en este ámbito resulta considerable: la falta de estadísticas consolidadas sobre siniestros vinculados con la inteligencia artificial dificulta la adecuada tarificación del riesgo, y la coordinación entre pólizas de responsabilidad civil general y pólizas cibernéticas exige un nivel de sofisticación técnica que no siempre está presente en todos los operadores del mercado asegurador.

6. Reflexión final

La Directiva (UE) 2024/2853, que tendrá una alta influencia en el mercado asegurador colombiano, constituye una respuesta técnicamente sólida y sofisticada frente a los retos que plantean la inteligencia artificial y el Internet de las Cosas. No obstante, persiste la dificultad de resolver plenamente la tensión existente entre la concepción del producto como entidad estática y la naturaleza dinámica de los sistemas evolutivos.

El seguro de responsabilidad civil se configura como el verdadero mecanismo de estabilización del sistema. Sin su intervención, la aplicación de la responsabilidad objetiva podría tornarse económicamente inviable para los operadores y carente de efectividad para las víctimas.

En definitiva, la interacción entre inteligencia artificial, productos defectuosos y riesgos cibernéticos confirma que el derecho de daños contemporáneo ya no puede ser examinado de

manera aislada respecto del derecho de seguros. Ambos conforman una arquitectura integrada orientada a gestionar el riesgo tecnológico sin frenar el impulso innovador.

CAPÍTULO IV
FUNCIÓN SOCIAL DEL SEGURO DE RESPONSABILIDAD CIVIL Y
PERSPECTIVAS REGULATORIAS
EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

Resumen

Las dimensiones tradicionales del daño y de la responsabilidad civil se han transformado como consecuencia del avance tecnológico que comprende a la Inteligencia Artificial, a los sistemas automatizados y al ciberespacio. El ciudadano se sitúa en una condición de vulnerabilidad estructural ante la complejidad de los algoritmos y la naturaleza de los riesgos cibernéticos que generan profundas asimetrías técnicas y económicas.

Frente a esta realidad, el presente capítulo analiza la función social del contrato de seguro de responsabilidad civil como instrumento con función preventiva del daño y como mecanismo para garantizar la reparación y la protección de los derechos fundamentales. Asimismo, propone la creación de un Seguro Obligatorio para la Atención de Incidentes con la Inteligencia Artificial, teniendo como marco de referencia las últimas tendencias regulatorias de la Unión Europea, que opere como co-regulador del riesgo y que garantice el equilibrio social funcional entre la innovación y la dignidad humana.

Palabras clave:

función social del seguro; responsabilidad civil; inteligencia artificial; seguro obligatorio; derechos fundamentales; co-regulación; sociedad del riesgo; AI Act; equilibrio social funcional.

Introducción

La falta de regulación normativa relacionada con la inteligencia artificial ha dado especial relevancia a la existencia de un contrato de seguro de responsabilidad civil con función social que garantice la reparación de los daños relacionados con su operación y uso. En Europa se ha resaltado la importancia del seguro considerando que el derecho positivo enfrenta dificultades para garantizar la reparación del daño y para fortalecer la confianza en el desarrollo tecnológico.

Las propuestas de exigir seguros obligatorios para determinados sistemas de inteligencia artificial de alto riesgo han sido analizadas como mecanismos de protección patrimonial de las víctimas. Sin embargo, la doctrina europea ha advertido que esta obligatoriedad debe ser selectiva y proporcional al nivel de riesgo, considerando que su exigencia indiscriminada puede inhibir la innovación (López Sánchez, 2024).

Desde el punto de vista funcional, el seguro de responsabilidad cumple una labor esencial al redistribuir los costos del daño y permitir que los beneficios de la inteligencia artificial no se obtengan a costa de la desprotección jurídica de los afectados. En este sentido, el seguro no solo acompaña al derecho de daños, sino que se consolida como uno de sus pilares estructurales (Wigg Sotomayor, 2024).

El derecho privado contemporáneo se enfrenta a uno de los desafíos más disruptivos de su historia: la asimilación jurídica de la revolución tecnológica. El desarrollo masivo de sistemas de Inteligencia Artificial, el procesamiento de datos a gran escala (big data) y la autonomía progresiva de los entornos ciberfísicos han modificado los linderos tradicionales de la responsabilidad civil contractual y extracontractual. Conceptos dogmáticos clásicos como la culpa, el nexo de causalidad y el defecto del producto resultan insuficientes cuando el daño es el resultado de un

aprendizaje profundo no lineal, de un sesgo algorítmico invisible o de una vulnerabilidad de día cero en una infraestructura crítica (Beck, 1998).

En esta denominada "sociedad del riesgo tecnológico", la asimetría entre las corporaciones desarrolladoras y los ciudadanos comunes se profundiza exponencialmente. La complejidad inherente a los sistemas de vanguardia impone a las víctimas cargas probatorias técnicas y económicas que tornan ilusoria la promesa de una reparación integral. El reto de la responsabilidad civil no se encuentra exclusivamente en la reforma de los códigos sustantivos, sino en la ampliación de la definición ontológica y funcional del contrato de seguro.

I. El seguro de responsabilidad civil como fuente de protección de derechos y justicia social

La vertiginosa transición hacia la automatización algorítmica y la interconectividad digital ha transformado sustancialmente la naturaleza y la dimensión del daño asegurable. En la sociedad contemporánea, caracterizada por la ubicuidad de la Inteligencia Artificial, el big data y los entornos ciberfísicos, los riesgos ya no son puramente materiales o localizables.

La disrupción tecnológica introduce asimetrías entre los desarrolladores u operadores de sistemas complejos y los ciudadanos, quienes a menudo se encuentran en una condición de vulnerabilidad estructural. Ante este panorama, el seguro de responsabilidad civil para nuevas tecnologías trasciende su tradicional función resarcitoria y patrimonial para erigirse en un instrumento fundamental de prevención y contención de riesgos, de justicia social y de protección de los derechos humanos.

Los nuevos desarrollos tecnológicos asociados al desarrollo de la Inteligencia Artificial generan grandes desafíos, entre los cuales se destacan los asociados a la aplicación de los

regímenes de responsabilidad tradicionales y la determinación de las causas del daño, considerando la complejidad algorítmica. El seguro de responsabilidad civil incentiva de manera indirecta las buenas prácticas de diseño ético y seguridad desde el origen, reduciendo drásticamente la probabilidad de que se causen daños a los ciudadanos y procurando que se logre una verdadera justicia social preventiva.

El seguro de responsabilidad civil para las nuevas tecnologías no debe ser interpretado como una simple herramienta de transferencia de costos operativos para las empresas de innovación, sino como una importante garantía institucional que permite diluir la asimetría técnica y económica entre el emisor del riesgo y el ciudadano. El seguro democratiza el acceso a la reparación y asegura que el progreso tecnológico no se construya a expensas de la dignidad humana y los derechos de las mayorías.

II. El seguro obligatorio para la atención de incidentes ocurridos en el uso de la inteligencia artificial

El diseño e implementación de un seguro obligatorio para la atención de incidentes con el uso de la inteligencia artificial se propone considerando los altos riesgos que se derivan de la utilización de esta herramienta tecnológica y los daños que tienen origen en los incidentes por fallas de la IA, ciberataques, vulneraciones masivas de datos y colapsos de infraestructuras en la nube.

Teniendo en cuenta la coherencia y solidez de las normas implementadas en la Unión Europea en relación con la IA —en particular el Reglamento (UE) 2024/1689 y la Directiva (UE) 2024/2853—, el Seguro Obligatorio para la Atención de Incidentes con IA puede diseñarse

tomando como referente estas disposiciones, adaptándolas a las particularidades del ordenamiento jurídico colombiano.

Con este contrato se incorporaría al concepto del seguro un componente de vanguardia promotor del desarrollo y de los derechos humanos. El propósito de su implementación es asegurar los riesgos mínimos que impactan al usuario de la inteligencia artificial y los riesgos determinados y asociados a los bienes jurídicos sujetos a protección constitucional de quien utiliza la inteligencia artificial.

III. El seguro de responsabilidad civil como eje de convergencia para el equilibrio social funcional

El seguro de responsabilidad para el uso de la IA no es visto solo como un instrumento de traslado de riesgos, sino como una herramienta clave para lograr el desarrollo que integre los avances tecnológicos y el respeto por los derechos humanos. La viabilidad de una sociedad tecnológica no depende exclusivamente de su capacidad de invención, sino de su aptitud para asimilar el riesgo sin fracturar la cohesión social.

El mercado asegurador se erige, en este contexto, como un co-regulador técnico que sirve de eje de convergencia para el logro de un equilibrio social funcional. Al imponer condiciones de suscripción que reflejan el nivel real de riesgo —auditorías de algoritmos, evaluaciones de sesgo, mecanismos de supervisión humana documentados—, el asegurador establece estándares de diligencia que complementan y, en ocasiones, anticipan la regulación pública. Esta función co-reguladora del seguro es particularmente valiosa en un contexto de vacío normativo como el que caracteriza hoy al ordenamiento colombiano en materia de IA.

Las propuestas de reforma que se derivan del análisis son concretas y urgentes: la consagración legal de la responsabilidad objetiva para operadores de sistemas de IA de alto riesgo; la creación por vía legislativa de un seguro obligatorio de RC para dichos sistemas; la emisión por la Superintendencia Financiera de Colombia de lineamientos específicos sobre suscripción, cobertura, exclusiones y reservas para riesgos de IA; y la creación de un fondo de compensación para daños catastróficos de IA, siguiendo el modelo del FOGAFIN en el sector bancario. Estas reformas deben ser abordadas de manera coordinada y con participación activa del sector asegurador, la academia y las asociaciones especializadas como ACOLDESE, AIDA Colombia y FASECOLDA.

BIBLIOGRAFÍA

A. Doctrina nacional e iberoamericana

- ACOLDESE. (2023). *Memorias del XIV Congreso Colombiano de Derecho de Seguros*. Bogotá: ACOLDESE.
- Atienza Navarro, M. L. (2022). *Daños causados por inteligencia artificial y responsabilidad civil*. Barcelona: Atelier.
- Badillo Arias, J. A. (2019). Responsabilidad civil y aseguramiento obligatorio de los robots. En Monterroso Casado (Dir.), *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento* (pp. 25-66). Valencia: Tirant lo blanch.
- Bertolini, A. (2016). On robots and insurance. *International Journal of Social Robotics*, 8, 381-391.
- Calderón Villegas, J. J., & Insignares Cera, S. (Eds.). (2022). *Derecho Digital: Retos para el Derecho Colombiano ante la Transformación Digital*. Bogotá: Universidad de los Andes.
- Díez Velásquez, M., & Restrepo Pedroza, S. (2026). Viabilidad jurídica de la aplicación del régimen de productos defectuosos en casos de daños ocasionados por sistemas algorítmicos de Inteligencia Artificial de alto riesgo en Colombia. *Revista de Derecho y Economía*, 65, 173-205. <https://doi.org/10.18601/01236458.n65.07>
- Fundación MAPFRE / CILA. (2019). *Temas relevantes del Derecho de Seguros contemporáneo*. Madrid: Fundación MAPFRE.
- Grupo de Investigación Nuevas Tecnologías y Derecho Privado - UEXTERNADO. (2025). CONPES 4144: IA y Retos del Futuro Digital para la Protección de Datos Personales en

Colombia. Observatorio de Nuevas Tecnologías y Derecho Privado, Universidad Externado de Colombia.

López de Mantaras, R., & Brunet Crosa, P. (2023). ¿Qué es la inteligencia artificial? Papeles de Relaciones Ecosociales y Cambio Global, 164. <https://dialnet.unirioja.es/servlet/articulo?codigo=9287111>

Martínez Neira, N. H. (2018). Cátedra de Derecho Contractual Societario y de Seguros (3.ª ed.). Bogotá: Legis.

Nilsson, N. (2000). Inteligencia Artificial: Una Nueva Síntesis [Traducido al español de Artificial Intelligence: A New Synthesis]. Madrid: McGraw-Hill.

Novum Jus. (2024). Hacia una adaptación de la responsabilidad civil a la inteligencia artificial y su proyección en Colombia. Novum Jus, 18(3), 179-207. <https://doi.org/10.14718/NovumJus.2024.18.3.7>

Ossa Gómez, J. E. (1991). Teoría General del Seguro. El Contrato (2.ª ed.). Bogotá: Temis.

Solarte Rodríguez, A. (2016). El principio de reparación integral del daño en el derecho contemporáneo. En AA.VV., Tendencias de la responsabilidad civil en el siglo XXI (pp. 125-188). Bogotá: Pontificia Universidad Javeriana / Dike.

Tamayo Jaramillo, J. (2007). Tratado de Responsabilidad Civil (2 vols.). Bogotá: Legis.

Tapia Hermida, A. J. (2021). La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento. Revista Ibero-Latinoamericana de Seguros, 30(54), 107-146. <https://revistas.javeriana.edu.co/index.php/iberoseguros/article/view/33793>

Tapia Hermida, A. J. (2022). La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento. Revista Española de Abogados Especializados en Responsabilidad Civil y Seguro, 76, 79-104.

- Tapia Hermida, A. J. (2021). Actualización y utilidad de los Principios de Derecho Europeo del Contrato de Seguro (PEDCS). *Revista Ibero-Latinoamericana de Seguros*, 30(55).
<https://doi.org/10.11144/Javeriana.ris55.aupd>
- Veiga Copo, A. B. (2021). *Seguro y Tecnología*. Madrid: Civitas-Thomson Reuters.
- Vesga Ariza, R. A. (2022). Nuevas perspectivas del uso de la tecnología en el ámbito del contrato de seguro. *Revista Ibero-Latinoamericana de Seguros*, 57, 13-48.
<https://doi.org/10.11144/Javeriana.ris57.nput>
- Wigg Sotomayor, I. (2024). Panorama del fenómeno de la inteligencia artificial en relación con la responsabilidad civil. *Actualidad Jurídica (Universidad del Desarrollo)*.
<https://derecho.udd.cl/actualidad-juridica/files/2024/09/9-isabel-wigg-sotomayor.pdf>

B. Doctrina internacional

- Adversa AI. (2026). AI Risk Management Insurance: What the New Exclusions Mean for Enterprises. <https://adversa.ai/blog/ai-risk-management-insurance-what-the-new-exclusions-mean/>
- Astegiano-La Rizza, A. (2014). *Les assurances de responsabilité de l'entreprise* (6.^a ed.). L'Argus de l'assurance.
- Ayo Ferrándiz, C. (2024). Responsabilidad civil e inteligencia artificial. Uría Menéndez, AJUM 67-2025. <https://www.uria.com/es/publicaciones/9326-responsabilidad-civil-e-inteligencia-artificial>
- Clyde & Co. (2024). Emerging Risks Series — Artificial Intelligence [Podcast]. 27 de junio de 2024 (N. Beresford, T. Tippet y C. Williams).
- Corvo López, F. M. (2026). Novedades en materia de prueba a la luz de la Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo del 23 de octubre de 2024, sobre

responsabilidad por los daños causados por productos defectuosos. *Actualidad Jurídica Iberoamericana*, 24, 162-187.

De la Vega García, F. (2024). Directiva (UE) 2024/2853, del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y que deroga la Directiva 85/374/CEE. *Ars Iuris Salmanticensis*, 13, 306-311. <https://revistas.usal.es/cuatro/index.php/ais/article/view/32428>

Deloitte Global Boardroom Program. (2024). AI/gen AI Board Governance Survey. Deloitte, junio de 2024.

Ellul, J., Gordon, P., Ioannis, R., & Schneider, G. (2023). When is good enough good enough? On software assurances. *ERA Forum*, 23, 345-346. <https://doi.org/10.1007/s12027-022-00728-3>

Erkan, F., & Biswas, T. D. (2025). Artificial Intelligence and Liability for Damages. *International Journal of Social Sciences*, 9(41).

Fairgrieve, D., et al. (2016). Product Liability Directive. En Machnikowski, P. (Ed.), *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (pp. 17-108). Cambridge: Intersentia. <https://doi.org/10.1017/9781780685243.002>

Friedman, V. (2018). On The Edge: Solving The Challenges Of Edge Computing In The Era Of IoT. <https://www.databank.com/resources/blogs/solving-edge-computing-challenges-in-era-of-iot/>

Geneva Association. (2023). *AI in Insurance: A Risk Perspective*. Zurich: The Geneva Association.

González Beluche, P. (2023). La adaptación de la Directiva 85/374/CEE en materia de responsabilidad por daños causados por productos defectuosos a la cuarta revolución

industrial. Cuadernos de Derecho Transnacional, 15(2), 446-488.

<https://doi.org/10.20318/cdt.2023.8065>

González Beluche, P. (2025). La nueva Directiva (UE) 2024/2853 de 23 de octubre de 2024 sobre responsabilidad por los daños causados por productos defectuosos. La Ley Unión Europea, 132.

Groutel, H., Leduc, F., Pierre, P., & Asselain, M. (2008). *Traité du contrat d'assurance terrestre* (Vol. 1). Litec.

Howells, G., & Weatherill, S. (2005). *Consumer Protection Law* (2.^a ed.). Aldershot: Ashgate.

Hunton Andrews Kurth LLP. (2025). How Insurance Policies Are Adapting To AI Risk. Law360.

<https://www.hunton.com/insights/publications/how-insurance-policies-are-adapting-to-ai-risk>

Insurance Services Office (ISO). (2026). Endorsements CG 40 47, CG 40 48, CG 35 08. Generative Artificial Intelligence Exclusions for Commercial General Liability. New York: ISO.

Juárez Ferrer, M., & Márquez, J. F. (2024). Responsabilidad civil por la utilización de inteligencia artificial. TR La Ley. AR/DOC/2262/2024.

Lloyd's Market Association (LMA). (2024). Understanding Artificial Intelligence Risk in Insurance Products – The Challenges. LMA Market Survey. <https://lmalloyds.com/understanding-artificial-intelligence-risk-in-insurance-products-the-challenges/>

Luna Yerga, A. (2008). Causalidad y su prueba. Prueba del defecto y del daño. <https://dialnet.unirioja.es/servlet/articulo?codigo=2787435>

- Manuel Ortiz, F. (2026). Los daños producidos por sistemas inteligentes defectuosos en la Directiva Europea. *Revista de Derecho Civil*, XIII(1), 201-241.
<https://www.nreg.es/ojs/index.php/RDC/article/view/1164>
- McKinsey & Company. (2026). *State of AI Report / Global AI Survey*. New York: McKinsey & Company.
- Meco Tébar, F. (2026). La transposición de la Directiva (UE) 2024/2853 sobre productos defectuosos: ¿una oportunidad para la protección de los derechos de colectivos en riesgo o situación de vulnerabilidad? *Revista Actualidad Jurídica Iberoamericana*.
<https://doi.org/10.7203/AJI.24.33103>
- Muñoz García, C. (2025). Directiva 2024/2853 sobre responsabilidad por los daños causados por productos defectuosos. Contexto y armonización de máximos para proteger a consumidores y "a otras personas físicas". *La Ley Unión Europea*, 132.
- Naylor, M. (2017). *Insurance Transformed*. Palgrave Macmillan. <https://doi.org/10.1007/978-3-319-63835-5>
- Núñez Zorrilla, M. C. (2019). *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*. Madrid: Editorial Reus.
- Pazos Castro, R. (2025). El carácter defectuoso del producto en la nueva Directiva europea 2024/2853. *Revista de los Estudios de Derecho y Ciencia Política*, IDP, 43.
<https://doi.org/10.7238/idp.v0i43.433093>
- Peña López, F. (2024). Responsabilidad objetiva y subjetiva en las propuestas legislativas europeas sobre responsabilidad civil aplicables a la inteligencia artificial. En Álvarez Lata, N.

(coord.), Derecho de contratos, responsabilidad extracontractual e inteligencia artificial (pp. 411-499). Madrid: Aranzadi. <http://hdl.handle.net/2183/40114>

Risk & Insurance. (2026). Traditional Insurance Leaves Enterprises Exposed as AI Liability Claims Surge. <https://riskandinsurance.com/traditional-insurance-leaves-enterprises-exposed-as-ai-liability-claims-surge/>

Rose, K., Eldridge, S., & Chapín, L. (2015). La Internet de las Cosas – Una Breve Reseña. <https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf>

Sancho López, M. (2026). Cumplimiento normativo en la era de la inteligencia artificial: Directiva (UE) 2024/2853 sobre productos defectuosos y la responsabilidad de bienes intangibles y servicios digitales. *Actualidad Jurídica Iberoamericana*, 24. ISSN: 2386-4567.

Setnor Byer. (2025). New AI-Specific Insurance Exclusions Underscore Risks Associated with Generative Artificial Intelligence. setnorbyer.com.

Steels, L., & López de Mantaras, R. (2018). The Barcelona declaration for the proper development and usage of artificial intelligence in Europe. *AI Communications*, 31, 485-494. <https://content.iospress.com/articles/ai-communications/aic180607>

Tabares Cortés, F. (2024). Nuevas tendencias indemnizatorias para la protección del consumidor: Modificaciones al régimen de productos defectuosos en la Unión Europea. *Revista Ibero-Latinoamericana de Seguros*, 61, 59-98. <https://doi.org/10.11144/Javeriana.ris61.ntip>

University of San Andrés Law Review. (2025). Liability for damages caused by the use of AI: objective, subjective, or hybrid liability? Buenos Aires: UdeSA.

C. Legislación y regulación

Colombia. Congreso de la República. (1971). Decreto 410 de 1971 — Código de Comercio. Diario Oficial N.º 33.339.

Colombia. Congreso de la República. (1990). Ley 45 de 1990. Por la cual se expiden normas en materia de intermediación financiera, se regula la actividad aseguradora, se conceden unas facultades y se dictan otras disposiciones. Diario Oficial N.º 39.607.

Colombia. Congreso de la República. (2011). Ley 1480 de 2011 — Estatuto del Consumidor. Diario Oficial N.º 48.220 de 12 de octubre de 2011.

Colombia. Congreso de la República. (2012). Ley 1581 de 2012 — Ley de Protección de Datos Personales.

Colombia. Corte Constitucional. (2024). Sentencia T-323. Bogotá: Corte Constitucional.

Colombia. Corte Suprema de Justicia. Sala de Casación Civil. Sentencias sobre actividades peligrosas y artículo 2356 del Código Civil.

Colombia. Departamento Nacional de Planeación. (2025). CONPES 4144: Política Nacional para la Inteligencia Artificial. Bogotá: DNP.

Colombia. Superintendencia de Industria y Comercio (SIC). (2024). Circular Externa 002 de 2024. Lineamientos sobre uso de inteligencia artificial en actividades comerciales. Bogotá: SIC.

Comisión Europea. (2022). Propuesta de Directiva sobre responsabilidad en materia de IA (AI Liability Directive). COM(2022) 496 final.

Unión Europea. Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos. DOUE.

Unión Europea. Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo, de 10 de mayo de 2023, sobre seguridad general de los productos. DOUE.

Unión Europea. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (AI Act). DOUE L, 12 de julio de 2024.

D. Jurisprudencia

Benavides v. Tesla, Inc., Case Nos. 1:21-cv-21940-BB y 22-22607-KMM, United States District Court, Southern District of Florida. Jury Verdict Form (Doc. 534), 1 de agosto de 2025.

Disponible en: https://www.govinfo.gov/app/details/USCOURTS-flsd-1_21-cv-21940

Demanda colectiva de inversores de Reddit, Inc. (NYSE: RDDT), junio de 2025. Disponible en:

<https://www.rgrdlaw.com/cases-reddit-inc-class-action-lawsuit-rddt.html>

Demanda colectiva contra Oracle Corporation (NYSE: ORCL), presentada el 5 de febrero de 2026.

Disponible en: <https://zlk.com/cases/oracle-corporation-class-action-lawsuit-orcl>

Demanda colectiva contra Fermi America, Inc., presentada el 5 de enero de 2026. Disponible en:

<https://zlk.com/cases/fermi-inc-class-action-lawsuit-frmi>

Demanda colectiva contra CoreWeave, Inc. (NASDAQ: CRWV), presentada el 12 de enero de

2026. Disponible en: <https://www.rgrdlaw.com/cases-coreweave-inc-class-action-lawsuit-crwv.html>

Rosen Law Firm, demanda colectiva contra AppLovin Corporation (NASDAQ: APP). Disponible

en: <https://rosenlegal.com/case/applovin-corporation/>

Rosen Law Firm, demanda colectiva contra Skyworks Solutions, Inc. (NASDAQ: SWKS).

Disponible en: <https://rosenlegal.com/case/skyworks-solutions-inc/>