

UNIVERSIDAD PONTIFICIA COMILLAS - ICADE

Facultad de Derecho



EL SEGURO FRENTE A LA INTELIGENCIA ARTIFICIAL: TRANSPARENCIA, EQUIDAD Y ASEGURAMIENTO DEL RIESGO ALGORÍTMICO

Trabajo de Fin de Grado en Derecho

Autor: Pablo Loureiro Orejas

Tutor: Iñigo Navarro Mendizábal

Curso académico: 2025-2026

RESUMEN

La inteligencia artificial está transformando el sector asegurador en dos dimensiones simultáneas: como herramienta interna que las entidades aseguradoras utilizan para la suscripción, la tarificación y la gestión de siniestros, y como objeto de cobertura cuando los daños causados por sistemas algorítmicos de terceros son transferidos al mercado asegurador. Frente a esta transformación, el ordenamiento jurídico español dispone de un marco normativo —integrado por la Ley 50/1980 del Contrato de Seguro, el Reglamento General de Protección de Datos, el Reglamento de Inteligencia Artificial de 2024 y los Principios de Gobernanza de la IA de la EIOPA— que, sin embargo, no ha sido articulado sistemáticamente para abordar las consecuencias jurídico-privadas de la opacidad algorítmica.

La tesis central de este trabajo sostiene que la opacidad de los sistemas de IA utilizados en el contrato de seguro constituye una infracción del deber de información y del principio de buena fe que lo fundamentan, y que la explicabilidad algorítmica —convergentemente exigida por el RGPD, el AI Act y los principios de la EIOPA— debe operar como contenido normativo mínimo del propio contrato de seguro, con consecuencias directas sobre su validez y eficacia. Asimismo, el seguro puede y debe ejercer una función de gobernanza indirecta de la IA, condicionando el acceso a la cobertura al cumplimiento de estándares responsables de desarrollo y despliegue algorítmico.

El análisis transita por los grandes desafíos que la IA plantea al Derecho de seguros: la transparencia algorítmica y los derechos del asegurado frente a la decisión automatizada, la discriminación por variable proxy y sus límites jurídicos, el régimen de responsabilidad civil aplicable a los daños causados por IA y los criterios de asegurabilidad del riesgo algorítmico. El ciberseguro se examina como antecedente relevante que ilumina el recorrido probable del seguro de riesgos de IA. El trabajo concluye con propuestas normativas concretas y cinco principios de gobernanza algorítmica orientados al sector asegurador.

Palabras clave: inteligencia artificial · contrato de seguro · explicabilidad algorítmica · opacidad algorítmica · discriminación por variable proxy · gobernanza algorítmica · RGPD · AI Act · buena fe · Ley del Contrato de Seguro · asegurabilidad · ciberseguro

ABSTRACT

Artificial intelligence is transforming the insurance sector along two simultaneous dimensions: as an internal tool that insurers use for underwriting, pricing and claims management, and as an object of coverage when damages caused by third-party algorithmic systems are transferred to the insurance market. Faced with this transformation, the Spanish legal framework —integrating the Insurance Contract Act of 1980, the General Data Protection Regulation, the Artificial Intelligence Act of 2024 and the EIOPA AI Governance Principles— has not yet been systematically articulated to address the private-law consequences of algorithmic opacity.

The central thesis of this work holds that the opacity of AI systems used in insurance contracts constitutes a breach of the duty of information and the good faith principle that underpin the contract, and that algorithmic explainability —convergently required by the GDPR, the AI Act and EIOPA principles— must operate as a minimum normative content of the insurance contract itself, with direct consequences for its validity and enforceability. Furthermore, insurance can and should exercise an indirect governance function over AI, conditioning access to coverage on compliance with responsible algorithmic development and deployment standards.

The analysis addresses the major challenges that AI poses to insurance law: algorithmic transparency and the rights of the insured against automated decisions, proxy discrimination and its legal limits, the civil liability regime applicable to AI-caused damages and the insurability criteria for algorithmic risk. Cyber insurance is examined as a relevant precedent illuminating the likely trajectory of AI risk insurance. The work concludes with concrete legislative proposals and five algorithmic governance principles oriented to the insurance sector.

Keywords: artificial intelligence · insurance contract · algorithmic explainability · algorithmic opacity · proxy discrimination · algorithmic governance · GDPR · AI Act · good faith · Insurance Contract Act · insurability · cyber insurance

ÍNDICE

Tabla de contenido

I. INTRODUCCIÓN	7
II. EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR ASEGURADOR	10
2.1 Contextualización: el sector asegurador como industria predispuesta a la transformación algorítmica	10
2.2 La cadena de valor aseguradora: una anatomía del cambio tecnológico	11
2.2.1 Suscripción automatizada y tarificación individualizada del riesgo	12
2.2.2 Gestión automatizada de siniestros y detección del fraude	13
2.2.3 Distribución personalizada y atención al cliente mediante IA conversacional	14
2.3 El cambio de paradigma: del seguro de compensación al seguro de predicción y prevención	15
2.4 La irrupción de la inteligencia artificial generativa en el sector asegurador	16
2.5 Los límites jurídicos de la transformación: opacidad, asimetría informativa e inicio de la problemática regulatoria	17
III. LA TRANSPARENCIA ALGORÍTMICA Y LOS DERECHOS DEL ASEGURADO	20
3.1 El deber de transparencia como principio estructural del contrato de seguro	20
3.2 El derecho a la explicación en el marco normativo europeo	21
3.3 La inteligencia artificial explicable (XAI): respuesta técnica y límites jurídicamente relevantes	23
3.4 La explicabilidad algorítmica como contenido normativo mínimo del contrato de seguro	25
3.5 La función de la EIOPA y la convergencia normativa sectorial	27
IV. DISCRIMINACIÓN ALGORÍTMICA Y EQUIDAD EN LA TARIFICACIÓN DEL RIESGO	28
4.1 El principio de igualdad de trato y su proyección sobre la tarificación aseguradora	28
4.2 La discriminación algorítmica indirecta: el fenómeno de la proxy discrimination	29
4.3 El marco normativo anti-discriminatorio aplicable al sector asegurador	30
4.4 La tensión entre equidad actuarial e igualdad jurídica	33

4.5 Consecuencias jurídicas y mecanismos de control	34
V. EL SEGURO FRENTE A LOS NUEVOS RIESGOS GENERADOS POR LA INTELIGENCIA ARTIFICIAL	36
5.1 Tipología y características de los daños derivados de sistemas de inteligencia artificial	36
5.2 El problema de la atribución causal y la responsabilidad civil por daños de IA	37
5.3 El marco normativo europeo de responsabilidad por daños de IA	38
5.4 La asegurabilidad de los riesgos de IA: criterios clásicos y nuevas condiciones	39
5.5 El seguro de responsabilidad civil de los operadores de IA: estructura y cobertura	41
VI. MODELOS DE ASEGURAMIENTO DEL RIESGO ALGORÍTMICO Y FUNCIÓN REGULADORA DEL SEGURO.....	43
6.1. El contrato de seguro como instrumento de gobernanza privada de la IA ..	43
6.2. Modalidades de aseguramiento del riesgo algorítmico	44
6.3. Lagunas de cobertura y el problema del "silent AI"	46
6.4. La función reguladora indirecta del seguro y el papel de la EIOPA	47
6.5. Perspectivas de futuro: ¿hacia un seguro obligatorio de IA en Europa?	48
VII. EL CIBERSEGURO COMO ANTECEDENTE DE LA FUNCIÓN REGULADORA DEL SEGURO EN EL CAMPO TECNOLÓGICO	51
7.1 Planteamiento: el seguro como mecanismo de gobernanza tecnológica	51
7.2 La emergencia del riesgo cibernético y la respuesta del mercado asegurador	51
7.3 La función reguladora indirecta del ciberseguro	52
7.4 El fenómeno del «silent cyber» y su proyección al «silent AI»	53
7.5 Límites de la analogía y especificidades del riesgo algorítmico	54
7.6 Proyección: el ciberseguro como hoja de ruta para el seguro de inteligencia artificial	55
VIII. PROPUESTAS NORMATIVAS Y PRINCIPIOS DE GOBERNANZA ALGORÍTMICA EN EL DERECHO DE SEGUROS	57
8.1. La explicabilidad algorítmica como contenido normativo mínimo del contrato de seguro	57
8.2. Propuesta de reforma de la LCS: incorporación del deber de información algorítmica.....	58
8.3. Coordinación entre el AI Act, Solvencia II y la LCS: hacia un marco jurídico integrado.....	59
8.4. Principios de gobernanza algorítmica para el sector asegurador: una propuesta sistemática	61

8.5. Valoración de conjunto y perspectivas de futuro	62
IX. CONCLUSIONES	65

I. INTRODUCCIÓN

La inteligencia artificial ha entrado en el sector asegurador con una velocidad que el Derecho de seguros, como disciplina, no había anticipado. No es que la tecnología sea nueva, los modelos actuariales llevan décadas incorporando datos y probabilidades, sino que la escala, la opacidad y la autonomía de los sistemas actuales representan algo cualitativamente distinto. Hoy, los algoritmos de tarificación deciden si un contrato se emite, a qué precio y con qué exclusiones; los sistemas de gestión de siniestros determinan si una reclamación es fraudulenta antes de que ningún humano la haya leído. Esta transformación, además, opera en dos sentidos a la vez: el asegurador usa IA para tomar decisiones sobre sus asegurados y, simultáneamente, el mercado asegurador es llamado a cubrir los daños que esos mismos sistemas causan en manos de terceros. Esa doble dimensión, el seguro como usuario y el seguro como cobertura de la IA, es el hilo conductor de la presente investigación.

Y es que el fenómeno no ha pasado desapercibido para el legislador europeo. La Unión Europea ha construido en apenas una década un corpus normativo de primera magnitud. El Reglamento General de Protección de Datos de 2016 fue el primero en reconocer que el derecho a no ser objeto de decisiones exclusivamente automatizadas tiene valor jurídico autónomo, y que la explicabilidad algorítmica no es solo un ideal técnico, sino una exigencia legal exigible. El Reglamento de Inteligencia Artificial de 2024 fue un paso más lejos: clasificó como sistemas de alto riesgo, con obligaciones reforzadas de transparencia y supervisión humana, precisamente los empleados en la valoración del riesgo en seguros de vida y salud. Y la EIOPA, con sus Principios de Gobernanza de la IA, ha traducido esas exigencias al lenguaje específico del supervisor asegurador.¹²³

¹Reglamento (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 (Reglamento de Inteligencia Artificial), DO L 2024/1689, 12.7.2024.

²Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD). DO L 119, 4.5.2016.

³EIOPA (2021). *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector*. EIOPA Consultative Expert Group on Digital Ethics in Insurance. <https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa-ai-governance-principles-june-2021.pdf>

El problema es que ninguno de esos instrumentos ha modificado la Ley 50/1980, de 8 de octubre, del Contrato de Seguro. La LCS se redactó cuando el mayor sofisticado instrumento de tarificación era el actuario humano, y su régimen de deberes de información, buena fe y declaración del riesgo sigue operando como si el algoritmo no existiera. El resultado es una brecha real y práctica: el Derecho público europeo impone obligaciones de gobernanza algorítmica sofisticadas, pero el asegurado que recibe una decisión opaca o discriminatoria apenas dispone de instrumentos contractuales privados para cuestionarla. Colmar esa brecha, y proporcionar herramientas jurídicas concretas para hacerlo, es la razón de ser de este trabajo.

La tesis central que aquí se defiende puede enunciarse con precisión: la opacidad algorítmica en el contrato de seguro no es solo un incumplimiento regulatorio, es una infracción del deber de información y del principio de buena fe que fundamentan el propio contrato. Por eso, la explicabilidad algorítmica, convergentemente exigida por el RGPD, el AI Act y los principios de EIOPA, debe funcionar como contenido normativo mínimo del contrato de seguro, con efectos directos sobre su validez y eficacia. Y, a su vez, el seguro puede y debe ejercer una función de gobernanza indirecta de la IA: al condicionar el acceso a la cobertura al cumplimiento de estándares responsables de desarrollo algorítmico, los aseguradores se convierten en actores centrales, no meramente reactivos, de la regulación de la IA. El análisis transita entre dos ejes: el Eje A, que examina el impacto jurídico de la IA utilizada por el asegurador, y el Eje B, que estudia el seguro como instrumento de cobertura de los daños que la IA causa.

Para sostener esta tesis se recurre a una metodología jurídico-dogmática que combina la interpretación de las normas aplicables, RGPD, AI Act, LCS, Solvencia II y Directiva de Distribución de Seguros, con el análisis de la jurisprudencia relevante, en particular la STJUE *Test-Achats* (C-236/09). Se incorporan también los estudios académicos más recientes sobre IA y seguros, así como los informes institucionales de EIOPA y la Geneva Association, cuya perspectiva empírica resulta imprescindible para no quedarse en lo teórico cuando se evalúan propuestas normativas concretas.⁴

⁴Jia, R. A., Eling, M. y Wang, T. (2025). *Gen AI Risks for Businesses: Exploring the Role for Insurance*. Geneva Association Research Report. Geneva Association. <https://www.genevaassociation.org>

El trabajo se estructura en nueve capítulos. El segundo analiza el impacto de la IA en el sector asegurador. El tercero, las exigencias de transparencia y los derechos del asegurado frente a la decisión automatizada. El cuarto, la discriminación algorítmica y sus límites jurídicos. El quinto, los riesgos que la IA genera y cómo el seguro puede cubrirlos. El sexto, los modelos de aseguramiento del riesgo algorítmico y la función reguladora del contrato. El séptimo, el ciberseguro como laboratorio previo para asegurar riesgos digitales. El octavo, las propuestas normativas y los principios de gobernanza que el sector necesita. Y el noveno recoge las conclusiones. Cada capítulo puede leerse como pieza autónoma, pero el argumento solo se sostiene en su conjunto.

II. EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR ASEGURADOR

2.1 Contextualización: el sector asegurador como industria predispuesta a la transformación algorítmica

La inteligencia artificial lleva años prometiendo transformar industrias; en el sector asegurador, esa promesa ya es realidad operativa. Lo que antes hacía un actuario con tablas estadísticas lo hace ahora un algoritmo con millones de datos. Y la diferencia no es solo de velocidad: es de naturaleza. Por eso, comprender qué es técnicamente la IA, y por qué el seguro es terreno especialmente fértil para su expansión, resulta imprescindible antes de valorar sus efectos jurídicos.

El *Reglamento (UE) 2024/1689*, conocido como *AI Act*, define en su artículo 3.1 los sistemas de inteligencia artificial como «un sistema basado en máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede exhibir capacidades de adaptación tras su implantación, y que, a partir de los *inputs* que recibe, infiere, para alcanzar objetivos explícitos o implícitos, *outputs* tales como predicciones, recomendaciones, decisiones o contenidos que pueden influir en entornos reales o virtuales».⁵ Esta definición, deliberadamente amplia, abarca desde sistemas de aprendizaje automático hasta modelos de lenguaje generativo, pasando por algoritmos de clasificación y redes neuronales profundas.

La doctrina académica distingue tres niveles de IA. La inteligencia artificial estrecha (*Artificial Narrow Intelligence* o ANI) ejecuta tareas específicas y predefinidas, juega al ajedrez, detecta fraudes, calcula primas, pero no puede hacer nada fuera de ese dominio. La inteligencia artificial general (*Artificial General Intelligence* o AGI) sería capaz de razonar transversalmente como un humano; hoy no existe. Y la superinteligencia artificial (*Artificial Superintelligence*) es, de momento, ciencia ficción.⁶ Todo lo que

⁵Reglamento (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*). *Diario Oficial de la Unión Europea* L 2024/1689, de 12 de julio de 2024. Art. 3.1.

⁶La distinción entre ANI, AGI y ASI es estándar en la literatura sobre IA. Véase Bhattacharya, S., Meredith, W., DeGuira, H., Singh, H. K. y Nambiar, M. (2025). Explainable AI in insurance: applications, challenges, and future directions. *Frontiers in Artificial Intelligence*, 8, 1568266. <https://doi.org/10.3389/frai.2025.1568266>

opera en el sector asegurador pertenece a la primera categoría. Eso no lo hace menos sofisticado, ni menos jurídicamente relevante.

La razón por la que el seguro ha resultado tan receptivo a la IA no es casualidad: es estructural. La industria aseguradora es, en su esencia más profunda, una industria de información. Su negocio consiste en evaluar probabilidades de eventos futuros inciertos, fijar precios proporcionales a esos riesgos y gestionar reclamaciones cuando los eventos se materializan. Durante décadas, esa evaluación se apoyó en tablas actuariales y datos históricos poblacionales; hoy, con sensores, registros digitales y poder computacional abaratado, el volumen y la granularidad de la información son de otra magnitud.⁷ El algoritmo no viene a sustituir al actuario: viene a hacer lo mismo que el actuario, pero con órdenes de magnitud más datos y en fracciones de segundo.

Con todo, la adopción de la IA en los seguros ha ido más despacio que en la banca o la sanidad. La literatura especializada documenta ese rezago y lo atribuye a la complejidad regulatoria del sector, a los horizontes temporales largos de los contratos de seguro y a cierta resistencia cultural interna.⁸ Pero ese retraso no debe confundir: la transformación que se avecina reconfigurará de raíz las posiciones jurídicas de aseguradora y asegurado, y el proceso ya está en marcha.

2.2 La cadena de valor aseguradora: una anatomía del cambio tecnológico

Para entender las implicaciones jurídicas, hay que bajar al terreno concreto: ver exactamente en qué eslabones de la cadena de valor aseguradora se está produciendo el cambio. Siguiendo el modelo de cadena de valor de Porter adaptado al sector, emergen cuatro actividades primarias sobre las que la IA ejerce un impacto diferencial: la suscripción de riesgos, la gestión de siniestros, la distribución y la atención al cliente.⁹ Cada una merece análisis propio.

⁷Eling, M., Nuessle, D. y Staubli, J. (2020). The insurability of cyber risk: an empirical analysis. *The Geneva Papers on Risk and Insurance — Issues and Practice*, 45(3), 359–396. <https://doi.org/10.1057/s41288-020-00201-7>

⁸Eling, Nuessle y Staubli (2020), op. cit.

⁹Eling, Nuessle y Staubli (2020), op. cit. El modelo de cadena de valor utilizado está basado en la adaptación al sector asegurador del esquema de Porter (1985).

2.2.1 Suscripción automatizada y tarificación individualizada del riesgo

La suscripción de riesgos (*underwriting*) es la función técnica más antigua y central del seguro: decidir qué riesgos son asegurables, en qué condiciones y a qué precio. Durante siglos, esa decisión se apoyó en tablas actuariales derivadas de estadísticas poblacionales, promedios, distribuciones, correlaciones históricas. La irrupción del aprendizaje automático (*machine learning* o ML) ha desplazado ese paradigma hacia algo cualitativamente distinto: la tarificación individualizada, también llamada tarificación comportamental o *usage-based insurance*. El seguro deja de mirar al grupo para mirar al individuo.

El aprendizaje automático abarca diversas modalidades técnicas con distintas implicaciones jurídicas. El aprendizaje supervisado (*supervised learning*) entrena modelos a partir de datos etiquetados para realizar predicciones sobre observaciones nuevas; es la modalidad dominante en la tarificación del seguro de vida y salud. El aprendizaje no supervisado (*unsupervised learning*) detecta patrones y agrupaciones en datos no etiquetados, siendo especialmente relevante en la segmentación de asegurados. El aprendizaje semi-supervisado combina ambos enfoques cuando la disponibilidad de datos etiquetados es limitada. Por último, el aprendizaje por refuerzo (*reinforcement learning*) optimiza estrategias mediante la interacción iterativa con un entorno, con aplicaciones incipientes en la gestión dinámica de carteras.¹⁰

En el seguro de automóvil, la telemática vehicular calcula primas según el comportamiento real del conductor, velocidad, frenadas, kilometraje; en el de salud, los dispositivos *wearable* aportan datos biométricos continuos; y en el del hogar, los sensores de domótica anticipan incendios o inundaciones. Esta granularidad informativa transforma la tarificación en un proceso de predicción individualizada que ya no requiere de la inferencia estadística colectiva que fundamentaba el principio actuarial clásico.

La doctrina ha comenzado a identificar las consecuencias jurídicas de este proceso. Los modelos predictivos de suscripción producen resultados significativamente más precisos que los métodos actuariales convencionales, pero también plantean interrogantes sobre la representatividad de los datos de entrenamiento y la estabilidad

¹⁰Eling, Nuessle y Staubli (2020), op. cit.

predictiva en escenarios no observados.¹¹ Desde la perspectiva del Derecho español, se ha señalado que la sustitución del criterio actuarial por el algoritmo no es jurídicamente neutra: implica una transformación cualitativa en la naturaleza del deber precontractual de declaración del riesgo ex artículo 10 de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro (LCS),¹²¹³ puesto que la aseguradora ya no depende del asegurado para conocer su perfil de riesgo, sino que lo construye unilateralmente a partir de fuentes de datos externas.

2.2.2 Gestión automatizada de siniestros y detección del fraude

Si la suscripción es donde el seguro nace, la gestión de siniestros es donde el seguro se prueba. Las revisiones sistemáticas de la literatura constatan que el 38% de los artículos académicos sobre IA en seguros abordan esta función, frente al 26% dedicados a la suscripción.¹⁴ No es sorprendente: la gestión de siniestros es donde se decide si la aseguradora paga o no, y el fraude representa en ese contexto una carga de impacto económico muy elevado. Detectarlo mejor, y más rápido, vale mucho dinero.

Los sistemas de detección de fraude basados en IA combinan técnicas de análisis de redes (*network analysis*), procesamiento de lenguaje natural (*natural language processing* o NLP) y visión artificial para identificar patrones anómalos en la presentación de reclamaciones. Se documentan aplicaciones en el automóvil, donde la visión artificial analiza daños y detecta manipulaciones fotográficas, y en la salud, donde el NLP procesa historiales y facturas para detectar inconsistencias.¹⁵ La automatización del proceso de liquidación de siniestros (*straight-through claims processing*) permite, en los casos de

¹¹Bhattacharya, S., Boral, P., Das, S. y otros. (2025). Artificial intelligence in insurance: A systematic review. *Frontiers in Artificial Intelligence*, 8, 1568266. <https://doi.org/10.3389/frai.2025.1568266>

¹²Tapia Hermida, A. J. (2021). La responsabilidad civil derivada de la inteligencia artificial y su aseguramiento. *Revista Ibero-Latinoamericana de Seguros*, 30(54), 1–45.

¹³Ley 50/1980, de 8 de octubre, de Contrato de Seguro. *Boletín Oficial del Estado*, núm. 250, de 17 de octubre de 1980. Art. 10: «El tomador del seguro tiene el deber, antes de la conclusión del contrato, de declarar al asegurador, de acuerdo con el cuestionario que éste le someta, todas las circunstancias por él conocidas que puedan influir en la valoración del riesgo.»

¹⁴Owens, E., Sheehan, B., Mullins, M., Cunneen, M. y Ressel, J. (2022). Explainable Artificial Intelligence (XAI) in Insurance: A Systematic Review. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4088029>. La revisión sistemática de 100 artículos publicados entre 2000 y 2021 constata que el 38% de los trabajos abordan la gestión de siniestros y el 26% la suscripción, lo que refleja la mayor madurez tecnológica de esa función en el sector asegurador.

¹⁵Bhattacharya et al. (2025), op. cit.

menor complejidad, la resolución completa sin intervención humana en cuestión de minutos.

Este nivel de automatización plantea problemas jurídicos específicos en el ordenamiento español. El artículo 18 de la LCS establece el plazo de tres meses para el pago del importe mínimo de lo que la aseguradora considere que debe indemnizar, so pena de intereses de demora agravados.¹⁶ La automatización del proceso de liquidación puede, por un lado, facilitar el cumplimiento de este plazo; pero, por otro, puede producir denegaciones o liquidaciones parciales automatizadas que el asegurado no pueda impugnar eficazmente ante la ausencia de una explicación comprensible de los criterios aplicados.

2.2.3 Distribución personalizada y atención al cliente mediante IA conversacional

El tercer frente afecta a la distribución y la relación con el cliente, y es quizás el más visible para el asegurado ordinario: los *chatbots* y asistentes virtuales basados en IA conversacional han alterado los canales de contratación, con implicaciones directas sobre el régimen de información precontractual que exige la Directiva de Distribución de Seguros¹⁷ y su transposición española en el Real Decreto-ley 3/2020.¹⁸ Los sistemas de recomendación algorítmica personalizan la oferta en función del perfil del cliente; pero cuando esa personalización está optimizada para maximizar el margen de la aseguradora más que los intereses del tomador, se produce una tensión, difícilmente disimulable, con el deber de actuar de manera honesta, imparcial y profesional que la norma impone al distribuidor de seguros.

La Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA) ha reconocido expresamente, en sus principios de gobernanza de la inteligencia artificial en

¹⁶Ley 50/1980, de 8 de octubre, de Contrato de Seguro, op. cit. Art. 18: la aseguradora tiene el deber de satisfacer la prestación al término de las investigaciones y peritaciones necesarias; transcurridos tres meses desde la producción del siniestro sin pago, incurre en mora con los efectos del art. 20 LCS.

¹⁷Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros. *Diario Oficial de la Unión Europea* L 26/19, de 2 de febrero de 2016.

¹⁸Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales. *Boletín Oficial del Estado*, núm. 28, de 5 de febrero de 2020.

el sector asegurador,¹⁹ que los sistemas de distribución automatizados pueden vulnerar este deber de idoneidad si la personalización algorítmica no está sujeta a controles de calidad y supervisión humana suficientes. Esta advertencia regulatoria anticipa una tensión estructural entre la eficiencia económica que persigue la aseguradora y la protección del consumidor que el Derecho de distribución de seguros impone, tensión que los modelos de IA intensifican al escalar y automatizar procesos de decisión que anteriormente requerían el juicio individualizado de un agente o corredor.

2.3 El cambio de paradigma: del seguro de compensación al seguro de predicción y prevención

Lo que la IA está produciendo en el sector asegurador no es solo una mejora de eficiencia, es un cambio de paradigma. La doctrina especializada ha articulado esta tesis con precisión:²⁰ la IA está desplazando al seguro desde el modelo clásico de compensación *ex post*, el seguro interviene cuando el daño ya se ha producido, distribuyendo su coste entre la comunidad de riesgo, hacia un modelo de predicción y prevención *ex ante*, donde la aseguradora anticipa el siniestro, modula la prima en tiempo real e incluso interviene activamente para reducir la probabilidad de que el daño se materialice.

Este cambio tiene consecuencias conceptuales profundas, y no todas han sido todavía absorbidas por el Derecho de seguros. El concepto clásico de mutualización del riesgo, piedra angular de la lógica actuarial, presupone una comunidad de riesgo relativamente homogénea cuyos miembros comparten la incertidumbre de un evento dañoso. La tarificación individualizada, llevada a su extremo lógico, vacía de contenido esa mutualización: si cada asegurado paga exactamente la prima correspondiente a su probabilidad individual de siniestro, ¿qué queda de la función distributiva? La doctrina española ha planteado ya la pregunta: el contrato resultante, ¿sigue siendo en sentido técnico-jurídico un contrato de seguro, o se acerca más a una garantía personal o a un

¹⁹European Insurance and Occupational Pensions Authority (EIOPA). (2021). *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector*. EIOPA-BoS-21/001. Frankfurt: EIOPA.

²⁰Eling, Nuessle y Staubli (2020), op. cit.

contrato de servicios de gestión del riesgo, con todo lo que eso implicaría sobre el régimen aplicable?²¹

Desde la perspectiva del Derecho de la Unión Europea, el principio de mutualidad ha sido históricamente la justificación de las prohibiciones de discriminación en la tarificación. La Sentencia del Tribunal de Justicia de la Unión Europea de 1 de marzo de 2011, *Test-Achats*,²² anuló el artículo 5.2 de la Directiva 2004/113/CE que permitía la utilización del sexo como variable actuarial, precisamente porque vulneraba el principio de igualdad de trato consagrado en la Carta de los Derechos Fundamentales de la Unión Europea. La IA no introduce el sexo como variable explícita, pero puede correlacionar variables aparentemente neutras, patrones de comportamiento digital, ubicación geográfica, hábitos de consumo, con el género o el origen étnico, produciendo discriminaciones indirectas tan o más lesivas que las prohibidas expresamente por la jurisprudencia del Tribunal de Justicia.

La función preventiva que la IA habilita transforma también el rol social del seguro: si la aseguradora puede predecir con precisión qué asegurados van a siniestrar y ofrecerles incentivos, primas reducidas, monitorización activa, para reducir esa probabilidad, se convierte en agente de gobernanza del comportamiento individual, un poder que el ordenamiento jurídico no ha diseñado para controlar.

2.4 La irrupción de la inteligencia artificial generativa en el sector asegurador

Hasta aquí se ha analizado la IA que el sector conocía desde hace una década: los modelos de aprendizaje automático. Pero desde 2022 algo nuevo está cambiando el panorama a una velocidad inusitada. La proliferación de modelos de lenguaje de gran escala (*large language models* o LLM) y de sistemas de inteligencia artificial generativa (*Generative AI* o GenAI) ha abierto una dimensión adicional con características propias que no pueden analizarse con los mismos parámetros que el ML clásico.

²¹Tapia Hermida (2021), op. cit.

²²Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 1 de marzo de 2011, asunto C-236/09, *Association Belge des Consommateurs Test-Achats ASBL y otros contra Conseil des ministres*. ECLI:EU:C:2011:100. El Tribunal declaró inválido el artículo 5.2 de la Directiva 2004/113/CE por ser contrario al principio de igualdad de trato entre hombres y mujeres reconocido en los artículos 21 y 23 de la Carta de los Derechos Fundamentales de la Unión Europea.

La Asociación de Ginebra (*The Geneva Association*) identifica los principales vectores de impacto de la IA generativa en el seguro: la automatización de la redacción y revisión de pólizas, la generación de respuestas personalizadas en atención al cliente, el análisis de documentación jurídica y médica en la gestión de siniestros y la producción de informes actuariales y de modelización del riesgo.²³ Al mismo tiempo, señala riesgos específicos no reducibles a los del ML clásico: la alucinación (*hallucination*), generación de contenidos plausibles pero incorrectos, la opacidad multiplicada de un proceso ya opaco, y los riesgos de manipulación adversarial mediante *prompt injection*.

El informe corporativo de MAPFRE sobre IA generativa²⁴ aporta evidencia sobre el grado de implementación real de estas tecnologías en el sector asegurador español, identificando aplicaciones operativas en la gestión de siniestros, la detección de fraude y la atención al cliente. Este dato tiene relevancia jurídica directa: si las aseguradoras ya emplean IA generativa en procesos con efectos sobre los derechos de los asegurados, la pregunta sobre el marco normativo aplicable es ya práctica y urgente.

Desde el punto de vista jurídico, la IA generativa plantea interrogantes adicionales a los ya señalados para el ML. La generación automatizada de documentos contractuales, incluidas cláusulas de exclusión o condicionados particularizados, mediante LLM sin revisión humana sistemática podría vulnerar los deberes de transparencia e información precontractual que la LCS y la normativa de distribución de seguros imponen a las aseguradoras. Cuando un asistente virtual basado en IA generativa proporciona al tomador información sobre el alcance de su cobertura, cabe además plantear si dicha información constituye asesoramiento técnico con eficacia jurídica vinculante y quién responde si resulta incorrecta.

2.5 Los límites jurídicos de la transformación: opacidad, asimetría informativa e inicio de la problemática regulatoria

Y aquí es donde el análisis jurídico se vuelve incómodo. La magnitud de la transformación descrita contrasta con la insuficiencia del marco jurídico disponible para

²³Jia, X., Eling, M. y Wang, Z. (2025). Generative AI and insurance: Risks, opportunities and regulatory implications. *The Geneva Association Research Report*. The Geneva Association.

²⁴MAPFRE. (2024). *GenAI: Explorando el mañana. Informe sobre inteligencia artificial generativa*. Fundación MAPFRE.

regularla. Los instrumentos clásicos del Derecho de seguros, diseñados para un modelo de decisión humana, transparente, individualizada y controlable, no estaban preparados para este escenario. La velocidad del cambio tecnológico ha vuelto a superar, una vez más, la del legislador.

El problema central tiene un nombre: opacidad algorítmica. Los modelos de mayor capacidad predictiva, en particular las redes neuronales profundas (*deep learning*), son sistemas que ni sus propios creadores pueden explicar del todo. Esta característica, conocida en la literatura como el problema de la «caja negra» (*black box*), no es una curiosidad técnica, tiene consecuencias jurídicas concretas y serias. Si la aseguradora no puede explicar por qué el sistema ha calculado una prima determinada o ha denegado una cobertura, resulta imposible verificar si esa decisión infringe el deber de información del artículo 3 LCS, el principio de buena fe contractual ex artículo 1258 del Código Civil o las prohibiciones de discriminación que impone el Derecho de la Unión Europea. La opacidad técnica se convierte, así, en impunidad jurídica de facto.

A la opacidad se superpone algo igualmente perturbador: la inversión de la asimetría informativa clásica del contrato de seguro. En el esquema tradicional, la asimetría beneficiaba al asegurado, él conocía mejor que la aseguradora su propio perfil de riesgo, y de ahí nacía el deber de declaración del artículo 10 LCS. Los sistemas de IA han dado la vuelta a esa lógica: ahora es la aseguradora quien construye, mediante el análisis de datos masivos, una representación del riesgo individual que el propio asegurado desconoce por completo. No puede cuestionarla ni verificarla, ni sabe siquiera qué variables la determinan. Eso afecta tanto al equilibrio de prestaciones del contrato como a la posibilidad misma de un consentimiento verdaderamente informado.

A ello se añade el riesgo de discriminación algorítmica indirecta. Los modelos predictivos, entrenados sobre datos históricos que reflejan desigualdades sociales, pueden reproducirlas y amplificarlas, penalizando a grupos de asegurados según características correlacionadas, sin que la correlación sea explícita ni deliberada, con variables protegidas. Este fenómeno, que la doctrina anglosajona denomina *proxy discrimination*,

ha sido documentado en la literatura científica²⁵ y será objeto de análisis específico en el Capítulo 4 del presente trabajo.

El ordenamiento jurídico de la Unión Europea ha reaccionado ante estos desafíos con dos instrumentos de alcance general. El artículo 22 del Reglamento General de Protección de Datos (RGPD)²⁶ reconoce el derecho de los interesados a no ser objeto de decisiones basadas exclusivamente en el tratamiento automatizado que produzcan efectos jurídicos significativos o que les afecten de manera análogamente significativa. El *AI Act* clasifica determinados sistemas de IA como de «alto riesgo» cuando se utilizan en el ámbito de los seguros para la evaluación de riesgos y fijación de precios respecto a personas físicas,²⁷ sometiéndolos a requisitos reforzados de transparencia, documentación técnica y supervisión humana.

Con todo, ni el RGPD ni el *AI Act* contemplan mecanismos específicamente adaptados a la estructura jurídica del contrato de seguro. Reconocer principios generales es importante; traducirlos en obligaciones concretas para las aseguradoras y en derechos exigibles para los asegurados requiere una labor de integración jurídica que no puede darse por hecha. Es precisamente esa labor la que constituye el objeto central de los capítulos siguientes. Y la pregunta que los articula es esta: ¿debe la explicabilidad algorítmica operar como contenido normativo mínimo del propio contrato de seguro? ¿Con qué consecuencias sobre su validez y eficacia? Esa es la tesis que este trabajo se propone articular y defender.

²⁵Bhattacharya et al. (2025), op. cit.

²⁶Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD). *Diario Oficial de la Unión Europea* L 119/1, de 4 de mayo de 2016. Art. 22.

²⁷Reglamento (UE) 2024/1689 (*AI Act*), op. cit. Anexo III, punto 5.b: se consideran de alto riesgo los sistemas de IA utilizados en seguros de vida y de salud y seguros en general para la evaluación de riesgos y fijación de precios con respecto a personas físicas.

III. LA TRANSPARENCIA ALGORÍTMICA Y LOS DERECHOS DEL ASEGURADO

3.1 El deber de transparencia como principio estructural del contrato de seguro

El contrato de seguro lleva siglos funcionando, y su arquitectura descansa sobre un principio que el Derecho anglosajón bautizó con una expresión sin traducción perfecta, pero que lo dice todo: *uberrimae fidei*, buena fe máxima. Las partes contratan sobre la base de información asimétrica, cada una sabe cosas que la otra ignora, y la ejecución del contrato depende de que esa asimetría no se abuse. El principio de buena fe, consagrado en el artículo 1258 del Código Civil como norma general de integración contractual,²⁸ adquiere en el seguro una proyección específica y reforzada que el ordenamiento español ha convertido en norma positiva a lo largo de varias disposiciones de la Ley 50/1980, de 8 de octubre, del Contrato de Seguro.

La LCS articula el principio de transparencia mediante dos mecanismos que se refuerzan mutuamente. El artículo 3 impone que las condiciones generales de la póliza sean redactadas con claridad y precisión, y que las cláusulas limitativas de los derechos del asegurado sean específicamente destacadas y aceptadas por escrito.²⁹ El artículo 2 consagra el carácter imperativo de las disposiciones de la Ley en cuanto favorezcan al tomador, asegurado o beneficiario, cualquier pacto en contrario que reduzca esos derechos será nulo.³⁰ Juntos, ambos preceptos configuran un estándar de transparencia material, no

²⁸Código Civil, aprobado por Real Decreto de 24 de julio de 1889. *Gaceta de Madrid*, núm. 206, de 25 de julio de 1889. Art. 1258: «Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan, no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley.»

²⁹Ley 50/1980, de 8 de octubre, de Contrato de Seguro. *Boletín Oficial del Estado*, núm. 250, de 17 de octubre de 1980. Art. 3: «Las condiciones generales, que en ningún caso podrán tener carácter lesivo para los asegurados, habrán de incluirse por el asegurador en la proposición de seguro si la hubiere y necesariamente en la póliza de contrato o en un documento complementario, que se suscribirá por el asegurado y al que se entregará copia del mismo. Las condiciones generales y particulares se redactarán de forma clara y precisa. Se destacarán de modo especial las cláusulas limitativas de los derechos de los asegurados, que deberán ser específicamente aceptadas por escrito.»

³⁰Ley 50/1980, de Contrato de Seguro, op. cit. Art. 2: «Las distintas modalidades del contrato de seguro, en defecto de Ley que les sea aplicable, se regirán por la presente Ley, cuyos preceptos tienen carácter imperativo, a no ser que en ellos se disponga otra cosa. No obstante, se entenderán válidas las cláusulas contractuales que sean más beneficiosas para el asegurado.»

meramente formal; el asegurado debe poder comprender, en términos razonables, los criterios que rigen su relación contractual con la aseguradora.

En el paradigma pre-digital, estas exigencias eran razonablemente satisfacibles: el asegurado podía leer el condicionado, compararlo entre compañías y, si hacía falta, someterlo a control judicial. La doctrina especializada en Derecho del seguro y digitalización ha advertido que los sistemas algorítmicos quiebran ese esquema de raíz.³¹ Cuando la aseguradora usa un modelo de aprendizaje automático para calcular la prima o gestionar un siniestro, la decisión no está recogida en ninguna cláusula: emerge de un proceso computacional cuya lógica no se traduce en ningún texto que el asegurado pueda leer. La transparencia deja así de ser un problema de forma contractual para convertirse en un problema de opacidad técnica, para el que los instrumentos del Derecho de seguros clásico no estaban pensados.

Desde la perspectiva del Derecho español, se ha señalado que esta opacidad configura una vulneración del deber de información que el artículo 3 LCS y el artículo 22 RGPD imponen a la aseguradora, en la medida en que el asegurado no puede conocer los criterios que determinan su prima o la denegación de su siniestro y, por tanto, no puede ejercer eficazmente los derechos que el contrato le reconoce. Esta situación introduce una asimetría informativa invertida de nuevo cuño que el Derecho de seguros clásico no prevé ni articula.

3.2 El derecho a la explicación en el marco normativo europeo

El ordenamiento de la Unión Europea ha reaccionado ante la expansión de la toma de decisiones automatizada con un conjunto de instrumentos normativos que, aplicados al sector asegurador, configuran un derecho a la explicación de alcance progresivo y creciente.

³¹ Como afirma Abel Veiga Copo, “Conviene, sin embargo, no dejar de lado que los procesos de tomas de decisiones de los sistemas basados en IA son, hasta cierto punto, absolutamente opacos y desconocidos por las personas sobre las que los datos arrojan información” Veiga Copo, A. (2023). *Seguro e inteligencia artificial*. El impacto de la digitalización en el contrato de seguro. Editorial Aranzadi: p 130.

El artículo 22 del Reglamento General de Protección de Datos (RGPD) reconoce el derecho del interesado a no ser objeto de decisiones basadas exclusivamente en el tratamiento automatizado de sus datos que produzcan efectos jurídicos significativos o que le afecten de manera análogamente significativa. Su aplicación al sector asegurador es directa: la decisión automatizada sobre la prima de un seguro de vida o la denegación de una cobertura de salud produce efectos jurídicos evidentes sobre el asegurado. El artículo 22(2)(a) admite la excepción cuando la automatización es necesaria para la celebración o ejecución de un contrato, pero el Comité Europeo de Protección de Datos ha interpretado esa excepción de forma estrictamente restrictiva. No basta con que la automatización sea conveniente o económicamente eficiente: debe ser necesaria. Y en cualquier caso, el asegurado conserva, cuando menos, el derecho a obtener intervención humana.

El alcance del artículo 22 RGPD en el ámbito del *scoring* algorítmico fue precisado por el Tribunal de Justicia en la sentencia de 7 de diciembre de 2023, *SCHUFA Holding* (C-634/21).³² El Tribunal declaró que la elaboración automatizada de un valor de probabilidad de solvencia constituye por sí misma una «decisión» del artículo 22.1 RGPD cuando el tercero que lo recibe lo utiliza de manera determinante. La proyección sobre el contrato de seguro es directa: la fijación algorítmica de la prima o la denegación de cobertura basadas en un *scoring* de riesgo quedan comprendidas en el artículo 22, con sus garantías, intervención humana, impugnación, justificación, sin que la aseguradora pueda ampararse en la excepción del artículo 22(2)(a) si la automatización es meramente eficiente y no estrictamente necesaria.

Los artículos 13(2)(f) y 14(2)(g) del RGPD imponen al responsable del tratamiento el deber de informar proactivamente al interesado sobre la existencia de decisiones automatizadas, la lógica aplicada y la importancia prevista de dicho tratamiento para el interesado. El artículo 15(1)(h), que regula el derecho de acceso del interesado, añade el derecho a obtener «información significativa sobre la lógica

³²STJUE de 7 de diciembre de 2023, *SCHUFA Holding AG y otros*, C-634/21, ECLI:EU:C:2023:957, apdos. 49–62. El Tribunal declara que la elaboración automatizada de un valor de probabilidad sobre la solvencia del interesado constituye por sí misma una «decisión» en el sentido del art. 22.1 RGPD cuando el tercero que lo recibe lo utiliza de manera determinante para adoptar sus propias resoluciones con efectos jurídicos sobre el interesado. La excepción del art. 22(2)(a) RGPD —necesaria para la celebración o ejecución de un contrato— debe interpretarse de forma estricta y no ampara la automatización meramente conveniente o económicamente ventajosa.

aplicada» en las decisiones automatizadas. Esta referencia es especialmente relevante: no exige divulgar íntegramente el algoritmo, que podría ser secreto empresarial, sino ofrecer una explicación significativa y comprensible del proceso decisional.

El *AI Act* profundiza en estas exigencias con tres disposiciones de alcance sucesivo. El artículo 13 impone a los sistemas de IA de alto riesgo, entre los que se incluyen explícitamente los utilizados por aseguradoras para la evaluación de riesgos y la fijación de precios, requisitos de transparencia que permitan al operador comprender las capacidades y limitaciones del sistema. El artículo 14 impone la supervisión humana efectiva como requisito de diseño, asegurando que una persona pueda comprender, supervisar y, en su caso, corregir las decisiones del sistema. Por último, el artículo 86³³ reconoce un derecho específico a la explicación de la toma de decisiones individual: toda persona afectada por una decisión adoptada sobre la base de un sistema de IA de alto riesgo tiene derecho a obtener del operador «explicaciones claras y significativas sobre el papel del sistema en el procedimiento de toma de decisiones y los principales elementos de la decisión adoptada». Esta disposición es, hasta la fecha, el reconocimiento más explícito del derecho a la explicación en el Derecho positivo de la Unión.

3.3 La inteligencia artificial explicable (XAI): respuesta técnica y límites jurídicamente relevantes

El reconocimiento normativo del derecho a la explicación presupone la existencia de una capacidad técnica para proveer esa explicación. Esta capacidad es objeto de la subdisciplina denominada inteligencia artificial explicable (*Explainable Artificial Intelligence* o XAI), cuyo desarrollo ha respondido simultáneamente a las demandas regulatorias y a la necesidad práctica de contar con sistemas de IA auditables y revisables.

³³Reglamento (UE) 2024/1689 (*AI Act*), op. cit. Art. 86(1): «Toda persona afectada por una decisión que adopte el responsable del despliegue basándose en gran medida en el resultado de sistemas de IA de alto riesgo incluidos en el anexo III [...] y que produzca efectos jurídicos o que afecte a esa persona de manera significativamente similar tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas sobre el papel del sistema de IA en el procedimiento de toma de decisiones y los principales elementos de la decisión adoptada.»

La primera revisión sistemática de la literatura académica sobre XAI específicamente aplicada al sector asegurador³⁴³⁵ analiza 100 artículos publicados entre 2000 y 2021 e identifica cinco categorías de métodos XAI: la interacción e importancia de características (*Feature Interaction and Importance*), el mecanismo de atención (*Attention Mechanism*), la reducción de dimensionalidad (*Dimensionality Reduction*), la destilación del conocimiento y extracción de reglas (*Knowledge Distillation and Rule Extraction*), y los modelos intrínsecamente interpretables. siendo la destilación del conocimiento y extracción de reglas la técnica predominante en el sector, por su capacidad de generar reglas comprensibles a partir de modelos complejos.

Estos métodos se clasifican, además, según la dimensión de la explicación, *local* o *global*, y según su origen: *intrínsecas*, propias del diseño del modelo, o *post-hoc*, aplicadas retrospectivamente para aproximar el comportamiento de un modelo opaco ya entrenado. Esta distinción es jurídicamente relevante: una explicación *post-hoc* no es una descripción del proceso real de decisión, sino una aproximación externa; su suficiencia como explicación en el sentido del artículo 86 del *AI Act* o del artículo 15(1)(h) del RGPD es, en consecuencia, discutible cuando la exactitud de la aproximación no ha sido verificada de forma independiente.

En el plano del Derecho blando europeo, el Grupo de Expertos de Alto Nivel sobre IA (EU HLEG) identificó la explicabilidad como uno de los siete requisitos fundamentales de la IA fiable, encuadrado dentro del requisito de transparencia.³⁶ El documento distingue entre la trazabilidad, documentación técnica del proceso, la explicabilidad propiamente dicha, capacidad de comunicar la lógica del sistema a quienes

³⁴ Owens, E., Sheehan, B., Mullins, M., Cunneen, M. y Ressel, J. (2022). Explainable Artificial Intelligence (XAI) in Insurance: A Systematic Review. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4088029>. El estudio revisa 100 artículos publicados entre 2000 y 2021 e identifica como técnicas predominantes en el sector asegurador la destilación del conocimiento y extracción de reglas (*knowledge distillation and rule extraction*), por su capacidad para generar modelos comprensibles a partir de modelos complejos.

³⁵ Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial (EU HLEG). (2019). *Directrices éticas para una IA fiable*. Comisión Europea. KK-02-19-841-ES-N. Los siete requisitos de la IA fiable son: (1) acción y supervisión humanas; (2) solidez técnica y seguridad; (3) gestión de la privacidad y los datos; (4) transparencia; (5) diversidad, no discriminación y equidad; (6) bienestar ambiental y social; y (7) rendición de cuentas. El requisito de transparencia comprende la trazabilidad, la explicabilidad y la comunicación abierta sobre las capacidades y limitaciones del sistema.

³⁶ Ley 50/1980, de Contrato de Seguro, op. cit. Arts. 2 y 3. Véase también el art. 8, que establece los requisitos mínimos de contenido de la póliza y cuya inobservancia puede determinar la nulidad de las cláusulas afectadas.

se ven afectados, y la comunicación abierta sobre las capacidades y limitaciones del sistema. Esta distinción ayuda a precisar el contenido exigible del derecho a la explicación: no se exige que el asegurador revele el código fuente del algoritmo, sino que sea capaz de comunicar, en términos comprensibles para el asegurado, qué factores determinaron la decisión que le afecta.

3.4 La explicabilidad algorítmica como contenido normativo mínimo del contrato de seguro

Los tres planos normativos analizados, el Derecho español del contrato de seguro, el RGPD y el *AI Act*, convergen en exigir que el asegurado pueda conocer y comprender los criterios que determinan las decisiones que le afectan. Esta convergencia no es accidental: refleja la respuesta del ordenamiento ante la asimetría informativa que los sistemas algorítmicos generan en detrimento de la parte más débil del contrato de seguro.

Aquí está el núcleo del argumento que este trabajo defiende. La exigencia convergente de explicabilidad no debe calificarse únicamente como obligación regulatoria externa, cuyo incumplimiento acarrea sanciones administrativas o responsabilidad frente al supervisor. Debe operar, además, como contenido normativo mínimo del propio contrato de seguro, con consecuencias directas sobre su validez y eficacia en el plano jurídico-privado. El fundamento de esta calificación reside en la articulación del artículo 2 de la LCS con los derechos reconocidos en el RGPD y el *AI Act*. La tesis no es solo teórica: tiene consecuencias prácticas para cualquier asegurado que sea objeto de una decisión algorítmica opaca.

El artículo 2 LCS establece el carácter imperativo de las disposiciones legales sobre contrato de seguro en cuanto favorezcan al tomador, asegurado o beneficiario.³⁷ Los derechos reconocidos en los artículos 13, 14, 15(1)(h) y 22 del RGPD y en los artículos 13, 14 y 86 del *AI Act* favorecen inequívocamente al asegurado como parte afectada por las decisiones automatizadas.

Pero la tesis va más allá de la simple aplicación de la regla de imperatividad. Si la aseguradora utiliza un sistema de IA opaco para tomar decisiones contractualmente

³⁷Código Civil, art. 6.3: «Los actos contrarios a las normas imperativas y a las prohibitivas son nulos de pleno derecho, salvo que en ellas se establezca un efecto distinto para el caso de contravención.»

relevantes, cálculo de prima, denegación de cobertura, liquidación de siniestro, y no está en condiciones de proveer, a requerimiento del asegurado, una explicación significativa de esa decisión, no se produce meramente un incumplimiento regulatorio: se produce una insuficiencia estructural del consentimiento contractual. La decisión aseguradora que no puede ser explicada no puede tampoco ser eficazmente impugnada por el asegurado, lo que vacía de contenido su derecho a la tutela judicial del contrato. En consecuencia, la explicabilidad opera como una condición de la eficacia jurídica plena de la decisión algorítmica en el contexto del contrato de seguro.

Esta calificación tiene consecuencias prácticas precisas. En primer lugar, impone a la aseguradora la obligación contractual, y no solo regulatoria, de implementar únicamente sistemas de IA que sean técnicamente capaces de generar explicaciones significativas de sus decisiones. El coste de esa obligación recae sobre la aseguradora, que elige y despliega el sistema, en línea con el principio, propio del Derecho de contratos por adhesión, de interpretar la oscuridad de las cláusulas en contra de quien las redacta. En segundo lugar, hace que la decisión automatizada que no pueda ser explicada carezca de pleno valor contractual frente al asegurado, reconociéndole a este el derecho a impugnarla y a obtener una revisión por intervención humana. En tercer lugar, y con mayor proyección sistémica, convierte el cumplimiento de los estándares de XAI en un elemento de validez del contrato de seguro y no solo en una condición de licitud de la actividad aseguradora.

Conviene, no obstante, distinguir estas categorías jurídicas, que no son intercambiables ni producen los mismos efectos. La consecuencia de primer orden es la ineficacia relativa de la decisión algorítmica concreta, no la nulidad del contrato de seguro en su totalidad; el asegurado tiene derecho a impugnarla y a obtener revisión humana, mientras el contrato subsiste con las coberturas pactadas. La nulidad ex artículo 6.3 del Código Civil opera, en un segundo plano, sobre las cláusulas del condicionado que excluyan o restrinjan expresamente el derecho a la explicación, por ser contrarias a normas imperativas del RGPD y del *AI Act*. La calificación de vicio del consentimiento, concretamente dolo omisivo del artículo 1269 del Código Civil en su modalidad de reticencia, requiere además acreditar que la aseguradora ocultó deliberadamente la naturaleza algorítmica de la decisión, y conduciría a la anulabilidad del contrato ex

artículo 1300 CC, consecuencia de mayor intensidad pero de más difícil prueba en el plano procesal.

3.5 La función de la EIOPA y la convergencia normativa sectorial

Esa estructura normativa se completa, en el plano sectorial, con las directrices de gobernanza de la IA de la EIOPA. Son *soft law*, no crean obligaciones jurídicas directamente aplicables, pero constituyen una interpretación autorizada de cómo los principios del RGPD y del *AI Act* deben traducirse al lenguaje del supervisor asegurador. Y en ese lenguaje, la EIOPA es muy clara: la transparencia y la explicabilidad son el primero de los seis principios de gobernanza algorítmica aplicables al seguro. Los sistemas de IA que usen las aseguradoras deben ser explicables para los asegurados y auditables por los supervisores. No es una sugerencia de buenas prácticas. Es la posición oficial del supervisor europeo del sector.

La convergencia de estas tres capas, el RGPD, horizontal; el *AI Act*, sectorial de alto riesgo; la EIOPA, de supervisión prudencial, crea un marco normativo suficientemente robusto para sustentar la tesis de la explicabilidad como contenido normativo mínimo. No obstante, la aplicación efectiva de este marco enfrenta desafíos de implementación relevantes: la naturaleza de *soft law* de las directrices EIOPA no garantiza su aplicación uniforme en los distintos Estados miembros, y la brecha entre las exigencias normativas y las capacidades técnicas reales de muchos sistemas de IA desplegados en el sector asegurador es aún amplia.

Y es que la opacidad no produce solo déficits de información: genera también riesgos de discriminación sistemática, muchas veces invisible. Los modelos de aprendizaje automático entrenados sobre datos históricos pueden reproducir, y amplificar, las desigualdades sociales existentes, produciendo discriminaciones indirectas que afectan de forma desproporcionada a determinados grupos de asegurados, sin que nadie lo haya programado así. Este fenómeno, que la literatura especializada designa como *proxy discrimination* o discriminación algorítmica indirecta, es objeto de análisis específico en el capítulo siguiente. Y es, quizás, la consecuencia más perturbadora de la opacidad algorítmica en el sector asegurador.

IV. DISCRIMINACIÓN ALGORÍTMICA Y EQUIDAD EN LA TARIFICACIÓN DEL RIESGO

4.1 El principio de igualdad de trato y su proyección sobre la tarificación aseguradora

Hay una tensión que el Derecho de seguros arrastra desde siempre y que la inteligencia artificial ha vuelto a poner sobre la mesa con nueva urgencia: el principio de igualdad ante la ley, consagrado en el artículo 14 de la Constitución Española³⁸ y en los artículos 20 y 21 de la Carta de los Derechos Fundamentales de la Unión Europea,³⁹ prohíbe tanto la discriminación directa, trato diferenciado explícito por razón de una característica protegida, como la indirecta, práctica aparentemente neutra que produce desventaja desproporcionada sobre un grupo protegido. Pero el seguro se funda en diferenciar primas según el riesgo individual: tratar diferente a quien tiene un perfil de riesgo diferente no es discriminación, sino la esencia del negocio actuarial. La pregunta difícil es cuándo esa diferenciación cruza la línea.

El Derecho de la Unión Europea trazó esa línea, al menos parcialmente, hace más de una década. La Directiva 2004/113/CE prohibió en su artículo 5.2 la utilización del sexo como variable actuarial en el cálculo de primas y prestaciones.⁴⁰ La Sentencia *Test-Achats* del Tribunal de Justicia fue aún más lejos: declaró nula esa excepción por vulnerar los artículos 20 y 21 de la Carta de los Derechos Fundamentales, y fijó un principio de alcance general, la especificidad técnica del negocio asegurador no justifica la vulneración de la igualdad de trato cuando el factor diferenciador es una característica protegida. El argumento de que «el mercado lo requiere» no basta frente a un derecho fundamental.

³⁹Carta de los Derechos Fundamentales de la Unión Europea (2016/C 202/02). *Diario Oficial de la Unión Europea* C 202/389, de 7 de junio de 2016. Art. 20 (igualdad ante la ley) y art. 21 (no discriminación): «Se prohíbe toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual.»

⁴⁰Directiva 2004/113/CE del Consejo, de 13 de diciembre de 2004, por la que se aplica el principio de igualdad de trato entre hombres y mujeres al acceso a bienes y servicios y su suministro. *Diario Oficial de la Unión Europea* L 373/37, de 21 de diciembre de 2004. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 1 de marzo de 2011, asunto C-236/09, *Test-Achats*, ECLI:EU:C:2011:100.

El problema que plantea la inteligencia artificial es más sutil y, por ello, más difícil de combatir: las aseguradoras que utilizan sistemas de ML no incorporan explícitamente el sexo o el origen étnico como variables de entrada, pero no necesitan hacerlo, pues el algoritmo puede llegar al mismo resultado utilizando variables aparentemente neutras que, estadísticamente, funcionan como sustitutos de las características protegidas. Eso es la discriminación *indirecta* algorítmica, y trasciende la estructura de la norma tal como fue diseñada para el mundo analógico. Requiere, en consecuencia, una reinterpretación del principio de igualdad de trato que incorpore las especificidades técnicas del aprendizaje automático.

4.2 La discriminación algorítmica indirecta: el fenómeno de la proxy discrimination

La discriminación algorítmica indirecta, *proxy discrimination* en la literatura anglosajona, se produce cuando un modelo de ML utiliza variables que, sin ser características protegidas, están estadísticamente correlacionadas con ellas, de modo que incluirlas reproduce exactamente los efectos discriminatorios que la prohibición pretende evitar. La variable neutra actúa como sustituto funcional de la prohibida; el resultado práctico es idéntico al de la discriminación directa, pero sin intención, sin culpable identificable y, a veces, sin conciencia siquiera de que está ocurriendo.

Los ejemplos documentados en el sector asegurador son numerosos. La geolocalización del asegurado puede correlacionarse con el origen étnico o la composición racial del vecindario, replicando algorítmicamente el *redlining* que el ordenamiento estadounidense combatió desde la Fair Housing Act de 1968. El rastro digital del asegurado, historial de navegación, compras en línea, uso de redes sociales, puede correlacionarse con el género, la condición socioeconómica o el estado de salud. Las investigaciones disponibles han identificado estos riesgos como uno de los principales desafíos éticos y regulatorios de la IA en seguros,⁴¹ poniendo de manifiesto que la capacidad de los modelos para detectar patrones complejos en datos masivos

⁴¹Bhattacharya, S., Boral, P., Das, S. y otros. (2025). Artificial intelligence in insurance: A systematic review. *Frontiers in Artificial Intelligence*, 8, 1568266. <https://doi.org/10.3389/frai.2025.1568266>. El estudio identifica la equidad y la mitigación del sesgo como uno de los principales desafíos técnicos de la aplicación de la IA en el sector asegurador.

aumenta también su capacidad para capturar, de forma no intencional, correlaciones con características protegidas.

Lo más perturbador de esta forma de discriminación es, precisamente, que no es intencional: el modelo no «decide» discriminar, sino que aprende correlaciones estadísticas a partir de datos históricos que reflejan las desigualdades estructurales del mercado, convirtiendo la injusticia histórica en un rasgo predictivo que no solo perpetúa, sino que puede amplificar. La doctrina ha advertido que este mecanismo genera un bucle de retroalimentación difícil de romper:⁴² el modelo aprende que ciertos grupos históricamente infrarrepresentados presentan mayor riesgo estadístico, les asigna primas más elevadas, lo que reduce su acceso al seguro, lo que a su vez reduce la muestra de datos disponible de ese grupo, lo que refuerza la percepción de riesgo. La desigualdad se alimenta a sí misma.⁴³

El Grupo de Expertos de Alto Nivel de la Comisión Europea identificó la equidad como uno de los siete requisitos fundamentales de la IA fiable, señalando expresamente la necesidad de prevenir «sesgos injustos que podrían discriminar de forma indirecta o directa, en particular, a los grupos vulnerables».⁴⁴ Esta advertencia cobra especial relevancia en el sector asegurador, donde las decisiones algorítmicas afectan al acceso a bienes esenciales como la cobertura de salud o la responsabilidad civil del automóvil.

4.3 El marco normativo anti-discriminatorio aplicable al sector asegurador

El ordenamiento europeo dispone de un conjunto de instrumentos anti-discriminatorios cuya aplicación al fenómeno de la *proxy discrimination* algorítmica

⁴² A. Veiga copo afirma, “Las predicciones sobre lo que es probable que ocurra se generan primero calculando cómo se han correlacionado las diferentes cualidades entre sí en el pasado y, a continuación, utilizando estas correlaciones para hacer proyecciones sobre lo que ocurrirá en el futuro. Veiga Copo, A. (2023). Op cit: 334

⁴³Eling, M., Nuessle, D. y Staubli, J. (2020). The insurability of cyber risk: an empirical analysis. *The Geneva Papers on Risk and Insurance*, 45(3), 359–396. <https://doi.org/10.1057/s41288-020-00201-7>. Los autores analizan la tensión entre la precisión predictiva de los modelos de ML y los imperativos de equidad (*fairness-accuracy tradeoff*).

⁴⁴Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial (EU HLEG). (2019). *Directrices éticas para una IA fiable*. Comisión Europea. KK-02-19-841-ES-N. El requisito 5 (diversidad, no discriminación y equidad) exige «evitar resultados injustos, especialmente por lo que respecta al impacto de sistemas de IA en la distribución de riqueza, recursos, información o capacidades o en el acceso a productos o servicios» y prevenir «sesgos injustos que podrían discriminar de forma indirecta o directa, en particular, a los grupos vulnerables».

presenta, sin embargo, dificultades de encaje que requieren una labor de interpretación sistemática.

La Directiva 2000/43/CE,⁴⁵ relativa a la igualdad de trato con independencia del origen racial o étnico, prohíbe expresamente la discriminación indirecta en el acceso a bienes y servicios, incluyendo los seguros. Su aplicación al caso de la discriminación algorítmica no requiere probar que la aseguradora pretendía discriminar, lo que sería imposible ante un modelo de ML cuyo funcionamiento es opaco incluso para sus diseñadores, sino que la práctica produce un efecto de desventaja desproporcionada sobre el grupo protegido. Esta distinción entre la prueba de la intención y la prueba del efecto es jurídicamente crucial: abre la posibilidad de impugnar decisiones algorítmicas discriminatorias sin necesidad de acreditar el elemento subjetivo.

La doctrina especializada ha advertido que esta dificultad de encaje es estructural. Xenidis (2020) sistematiza tres incompatibilidades nucleares entre el mapa conceptual del Derecho de igualdad de la UE y la discriminación algorítmica:⁴⁶ la concepción unidimensional de la no discriminación frente al carácter compuesto e interseccional de las clasificaciones de ML, que permite que el algoritmo discrimine simultáneamente por varios motivos sin que ninguno de ellos alcance por sí solo el umbral de la discriminación jurídicamente relevante; la lógica causal que exige una conexión directa entre el factor discriminatorio y la categoría protegida, frente al mecanismo de la variable *proxy* que opera mediante correlación estadística sin relación causal explícita; y el carácter taxativo del elenco de motivos protegidos frente al dinamismo de las clasificaciones algorítmicas, que pueden generar patrones de discriminación emergentes basados en combinaciones de

⁴⁵Directiva 2000/43/CE del Consejo, de 29 de junio de 2000, relativa a la aplicación del principio de igualdad de trato de las personas independientemente de su origen racial o étnico. *Diario Oficial de las Comunidades Europeas* L 180/22, de 19 de julio de 2000. Art. 2(2)(b): existe discriminación indirecta «cuando una disposición, criterio o práctica aparentemente neutros sitúe a personas de un origen racial o étnico concreto en desventaja particular con respecto a otras personas».

⁴⁶Xenidis, R. (2020). Tuning EU equality law to algorithmic discrimination: Three pathways to resilience. *Maastricht Journal of European and Comparative Law*, 27(6), 736–758. <https://doi.org/10.1177/1023263X20982173>. La autora identifica tres incompatibilidades estructurales entre el mapa conceptual del Derecho de igualdad de la UE y la discriminación algorítmica: la concepción unidimensional de los motivos de discriminación frente al carácter compuesto e interseccional de las clasificaciones algorítmicas; la lógica causal que vincula la discriminación a categorías protegidas tasadas frente al carácter estadístico-correlacional del aprendizaje automático; y el carácter taxativo de los motivos protegidos frente a la naturaleza emergente de las clasificaciones algorítmicas, que exige una relectura finalista del principio de no discriminación orientada a su resiliencia frente a la discriminación mediada tecnológicamente.

atributos no contempladas en las directivas. Superarlas exige, según la autora, lecturas estructurales, no esencialistas, de los motivos protegidos, como instrumentos para capturar la producción de desventaja social.

El RGPD aporta una capa de protección adicional y específica para las decisiones automatizadas. El artículo 22(4)⁴⁷ prohíbe que las decisiones automatizadas se basen en categorías especiales de datos en el sentido del artículo 9,⁴⁸ que incluyen el origen racial o étnico, los datos relativos a la salud y las características genéticas, salvo que medie consentimiento explícito del interesado o concurra un supuesto de habilitación legal. La relevancia de esta prohibición en el contexto de la *proxy discrimination* es, sin embargo, limitada: el modelo no procesa formalmente estas categorías, sino variables correlacionadas con ellas. La prohibición solo se activa directamente cuando el dato especial está presente en el conjunto de entrenamiento, no cuando está implícitamente codificado en variables proxy.

El *AI Act* introduce la respuesta normativa más directa a este problema a través de su artículo 10,⁴⁹ que impone a los proveedores de sistemas de IA de alto riesgo prácticas de gobernanza de datos orientadas a garantizar que los conjuntos de datos de entrenamiento sean representativos, libres de errores y exentos de sesgos injustos. Significativamente, el artículo 10(5) permite, en la medida estrictamente necesaria, el procesamiento de categorías especiales de datos *con el fin de detectar y corregir sesgos*, reconociendo así la paradoja técnica de que la eliminación de la discriminación algorítmica puede requerir tomar en consideración precisamente las características que la norma prohíbe utilizar para discriminar. El artículo 5(1) del *AI Act* prohíbe, por su parte,

⁴⁷Reglamento (UE) 2016/679 (RGPD), op. cit. Art. 22(4): «Las decisiones a que se refiere el apartado 1 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.»

⁴⁸Reglamento (UE) 2016/679 (RGPD), op. cit. Art. 9(1): quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, salvo en los supuestos previstos en el apartado 2.

⁴⁹Reglamento (UE) 2024/1689 (*AI Act*), op. cit. Art. 10(2) y (3): los proveedores de sistemas de IA de alto riesgo deberán aplicar prácticas de gobernanza de datos que garanticen que los conjuntos de datos de entrenamiento sean pertinentes, representativos, libres de errores y completos en la medida de lo posible. El art. 10(5) añade que, en la medida en que sea estrictamente necesario, los proveedores podrán procesar categorías especiales de datos con el fin de garantizar la monitorización de sesgos y la corrección de discriminaciones injustas.

los sistemas de puntuación social que produzcan tratos perjudiciales injustificados o desproporcionados,⁵⁰ lo que incluye aquellos modelos de tarificación cuyo efecto real sea penalizar a grupos protegidos sin justificación actuarial suficiente.

4.4 La tensión entre equidad actuarial e igualdad jurídica

La discriminación algorítmica en el seguro expone, en su versión más aguda, una tensión que el Derecho no ha resuelto: la que existe entre la *equidad actuarial*, que postula que la prima debe reflejar fielmente el riesgo individual, pues cobrar a todos lo mismo es ineficiente y genera selección adversa, y la *igualdad jurídica*, que exige que las diferencias de trato no respondan a características protegidas, con independencia de su correlación estadística con el riesgo.

La doctrina ha dado nombre a esta contradicción: el *fairness-accuracy tradeoff*.⁵¹ Los modelos más precisos tienden a capturar, precisamente, las correlaciones con características protegidas que producen discriminación indirecta, mientras que los que imponen restricciones de equidad (*fairness constraints*) sacrifican precisión a cambio de un impacto diferencial reducido. No hay solución técnica universal: las definiciones matemáticas de equidad son en general mutuamente incompatibles, y elegir entre ellas no es una cuestión técnica sino una decisión de política jurídica que no puede dejarse únicamente al algoritmo.

Desde el punto de vista del Derecho español, la resolución de esta tensión está orientada por el principio de proporcionalidad. La diferenciación actuarial basada en variables correlacionadas con características protegidas es admisible únicamente si: (i) la variable utilizada sirve a un objetivo actuarial legítimo, (ii) la correlación con la característica protegida es residual o inevitable dada la naturaleza del riesgo, y (iii) el efecto diferencial sobre el grupo protegido es proporcional a la diferencia real de riesgo. La inversión de la carga de la prueba que impone el artículo 8 de la Directiva 2004/113/CE, conforme al cual corresponde a la parte demandada demostrar que no hubo

⁵⁰Reglamento (UE) 2024/1689 (*AI Act*), op. cit. Art. 5(1)(c): queda prohibido el uso de sistemas de IA para clasificar a las personas físicas basándose en su comportamiento social o características personales con fines de puntuación social que provoque un trato perjudicial en ámbitos no relacionados con los que se generaron los datos, o que sea injustificado o desproporcionado con respecto al comportamiento social.

vulneración del principio de igualdad de trato una vez que el demandante haya aportado indicios de discriminación, es aplicable a las decisiones algorítmicas con las adaptaciones que su naturaleza técnica requiere.

4.5 Consecuencias jurídicas y mecanismos de control

La conexión entre discriminación algorítmica y opacidad de los sistemas de IA convierte la explicabilidad, analizada en el capítulo precedente, en una condición necesaria, aunque no suficiente, del control anti-discriminatorio. Si la aseguradora no puede explicar qué variables determinaron una decisión de tarificación, tampoco puede demostrar que esa decisión no reproduce el efecto discriminatorio prohibido.⁵² La explicabilidad opera, así, no solo como derecho del asegurado, sino como condición procesal del control de validez anti-discriminatoria de las decisiones algorítmicas.

Las directrices de la EIOPA establecen que las aseguradoras deben monitorizar activamente los indicadores de equidad a lo largo de todo el ciclo de vida del sistema de IA, establecer procedimientos de recurso para los asegurados que consideren haber sido objeto de una decisión discriminatoria, y documentar las decisiones de diseño relacionadas con las restricciones de equidad implementadas.⁵³ Estas exigencias de supervisión prudencial se añaden a las obligaciones de gobernanza de datos del artículo 10 del *AI Act* y a los derechos de acceso y explicación del RGPD, creando un régimen de control multi-nivel cuya coherencia depende de la coordinación entre autoridades supervisoras de seguros, de protección de datos y de IA.

En el plano del Derecho privado, la decisión aseguradora que produzca un efecto discriminatorio contrario a las normas imperativas anti-discriminatorias será nula de pleno derecho ex artículo 6.3 del Código Civil, en tanto acto contrario a normas prohibitivas, sin perjuicio de la responsabilidad de la aseguradora frente al asegurado

⁵²Tapia Hermida, A. J. (2021). La responsabilidad civil derivada de la inteligencia artificial y su aseguramiento. *Revista Ibero-Latinoamericana de Seguros*, 30(54), 1–45.

⁵³European Insurance and Occupational Pensions Authority (EIOPA). (2021). *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector*. EIOPA-BoS-21/001. Frankfurt: EIOPA. El principio de equidad de la EIOPA exige que los sistemas de IA no generen resultados discriminatorios, que se monitoricen los indicadores de equidad durante todo el ciclo de vida del sistema y que se establezcan procedimientos de recurso para los asegurados afectados.

afectado.⁵⁴ La dificultad probatoria que impone la opacidad algorítmica podrá ser suplida mediante la presunción de discriminación que activa la inversión de la carga de la prueba prevista en las Directivas anti-discriminatorias, una vez que el asegurado acredite prima facie la existencia de un trato diferencial desfavorable.

Las cuestiones abordadas en este capítulo, discriminación, opacidad, asimetría informativa, son difíciles de resolver jurídicamente porque son difíciles de ver: ese es, en el fondo, el nudo del problema. Pero la transformación algorítmica del seguro tiene también una dimensión más visible y urgente: los daños que los sistemas de IA causan a terceros y el régimen de responsabilidad civil aplicable. ¿Quién responde cuando un algoritmo se equivoca, y cómo puede asegurarse ese riesgo? Esas preguntas ocupan el capítulo siguiente.

⁵⁴Ley 50/1980, de Contrato de Seguro, op. cit. Art. 2, y Código Civil, art. 6.3. La nulidad de pleno derecho de la cláusula o criterio discriminatorio no afecta a la validez del resto del contrato (art. 9 LCS), salvo que la nulidad sea de tal entidad que no pueda subsistir sin la parte nula.

V. EL SEGURO FRENTE A LOS NUEVOS RIESGOS GENERADOS POR LA INTELIGENCIA ARTIFICIAL

5.1 Tipología y características de los daños derivados de sistemas de inteligencia artificial

Los daños que puede causar un sistema de inteligencia artificial son tan variados que resulta difícil encuadrarlos sin perder matices esenciales. La doctrina española especializada distingue entre tres categorías principales:⁵⁵ en primer lugar, los daños materiales causados por la actuación física de sistemas robóticos dotados de IA, como vehículos autónomos, drones de reparto o robots quirúrgicos, que pueden producir lesiones corporales, daños a bienes y muerte; en segundo lugar, los daños económicos resultantes de decisiones algorítmicas erróneas en ámbitos como la gestión financiera automatizada, la concesión de crédito, la denegación de cobertura aseguradora o el diagnóstico médico asistido por IA; y en tercer lugar, los daños morales e inmateriales, que incluyen las vulneraciones de derechos fundamentales, privacidad, igualdad, no discriminación, analizadas en los capítulos precedentes, así como los daños reputacionales derivados de contenidos generados por IA.

A esta tipología clásica se añaden, en el momento presente, nuevas categorías de daño vinculadas al desarrollo de la IA generativa y a la sofisticación de los vectores de ataque contra los propios sistemas de IA. La Asociación de Ginebra ha identificado como riesgos emergentes de la IA generativa la desinformación automatizada a escala, la suplantación de identidad mediante *deepfakes* y la perturbación de procesos decisionales en infraestructuras críticas.⁵⁶ Por su parte, los denominados ataques adversariales, manipulaciones deliberadas de los datos de entrada para inducir al sistema de IA a

⁵⁵Tapia 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://doi.org/10.11144/Javeriana.ris54.rcdu>. El autor identifica como riesgos patrimoniales típicos derivados del uso de la IA: los daños materiales por actuación física de robots; los daños económicos por decisiones erróneas de algoritmos en mercados financieros; y los daños personales por diagnóstico médico incorrecto o conducción autónoma defectuosa.

⁵⁶Lior, A. (2025). Insuring the AI age: The role of insurance in artificial intelligence regulation and governance. *Connecticut Insurance Law Journal*, 31(1). <https://doi.org/10.2139/ssrn.5316376>. La autora documenta que la mayoría de las pólizas de responsabilidad civil profesional y de productos tecnológicos existentes no cubren explícitamente los daños causados por sistemas de IA, y propone el desarrollo de seguros obligatorios para operadores de sistemas de alto riesgo como mecanismo de internalización de los costes externos de la IA.

producir resultados incorrectos, constituyen una nueva forma de fraude que afecta tanto a las aseguradoras que utilizan IA como a los terceros que sufren las consecuencias de las decisiones distorsionadas.⁵⁷

Los daños producidos por sistemas de IA presentan singularidades frente a los supuestos clásicos de responsabilidad civil: su origen puede ser opaco e indetectable; pueden producirse con un desfase temporal considerable entre el fallo y la manifestación del daño; pueden afectar simultáneamente a un número elevado de personas cuando el sistema opera a escala; y su potencial catastrófico puede amplificarse por la interconexión de los sistemas afectados. Estas características inciden directamente en la asegurabilidad del riesgo y en el diseño de los productos destinados a cubrirlo.

5.2 El problema de la atribución causal y la responsabilidad civil por daños de IA

El primer instinto del jurista ante un daño causado por IA es acudir al artículo 1902 del Código Civil⁵⁸, que exige acreditar tres elementos: la existencia de un daño, la relación de causalidad entre la conducta del demandado y el daño, y la culpa o negligencia del responsable. Los sistemas de IA introducen dificultades estructurales en cada uno de ellos, que el régimen clásico de la culpa aquiliana no resuelve satisfactoriamente.

El primer problema, no el menor, es identificar al responsable, pues el ciclo de vida de un sistema de IA implica una cadena de actores: el *AI Act* distingue entre el proveedor (*provider*), que diseña y desarrolla el sistema; el operador o responsable del despliegue (*deployer*), que integra el sistema en sus procesos y lo utiliza en contextos concretos; y el usuario final, que interactúa con el sistema. Esta distinción es relevante porque el daño puede deberse a un defecto de diseño, atribuible al proveedor, a una integración o configuración incorrecta, atribuible al operador, o a un uso inadecuado,

⁵⁷Amerirad, B., Cattaneo, M., Kenett, R. S. y Luciano, E. (2023). Adversarial Artificial Intelligence in Insurance: From an Example to Some Potential Remedies. *Risks*, 11(1), 20. <https://doi.org/10.3390/risks11010020>. Los ataques adversariales contra sistemas de IA en el sector asegurador incluyen la manipulación de texto, imágenes y datos de entrada para inducir al sistema a adoptar decisiones incorrectas, como la aprobación de siniestros fraudulentos o la infravaloración del perfil de riesgo de un tomador.

⁵⁸Código Civil, op. cit. Arts. 1902-1910, que regulan la responsabilidad civil extracontractual. Art. 1902: «El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.» El art. 1903 extiende esta responsabilidad a las personas bajo la dependencia del causante del daño, con relevancia para la responsabilidad del operador de un sistema de IA.

atribuible al usuario, lo que hace que la atribución de responsabilidad entre estos actores sea frecuentemente incierta y litigiosa.⁵⁹

El segundo problema, quizás el más desconcertante para el Derecho clásico, es el nexo causal: cuando la decisión dañosa fue adoptada por un sistema opaco, la víctima se enfrenta a la imposibilidad práctica de demostrar qué variable determinó el resultado lesivo. Esta dificultad traduce procesalmente el problema de la opacidad algorítmica analizado en el Capítulo 3: si el propio operador no puede explicar la decisión, la víctima no puede construir su cadena causal. La doctrina especializada ha denominado a este fenómeno la «brecha de responsabilidad» (*accountability gap*) de la IA, señalando que constituye el principal obstáculo para la reparación efectiva de los daños causados por sistemas algorítmicos.⁶⁰

El tercer problema es la culpa. El estándar del «hombre razonable» presupone que el demandado pudo anticipar el daño y adoptar medidas para evitarlo, pero en los sistemas de IA la previsibilidad del daño es frecuentemente limitada incluso para sus diseñadores, dado el carácter emergente y no determinista de algunos comportamientos. Esta imprevisibilidad podría llevar a la exoneración sistemática de los responsables bajo el estándar de culpa, privando a las víctimas de reparación efectiva. La doctrina y el legislador europeo han reaccionado ante esta posibilidad desplazando el régimen de responsabilidad aplicable a los sistemas de IA de mayor riesgo hacia esquemas de responsabilidad objetiva o cuasi-objetiva.

5.3 El marco normativo europeo de responsabilidad por daños de IA

La Unión Europea ha articulado una respuesta normativa dual al problema de la responsabilidad por daños de IA, combinando la revisión del régimen de responsabilidad por productos defectuosos con la elaboración de un instrumento específico de responsabilidad por daños de IA.

⁵⁹Reglamento (UE) 2024/1689 (*AI Act*), op. cit. Arts. 9, 13 y 17: los proveedores de sistemas de IA de alto riesgo deben implantar sistemas de gestión del riesgo, documentación técnica y registros de incidencias que permitan la trazabilidad de las decisiones del sistema. Esta documentación resulta determinante para la acreditación del nexo causal en sede de responsabilidad civil.

La Directiva (UE) 2024/2853, que deroga y sustituye a la Directiva 85/374/CEE sobre responsabilidad por productos defectuosos,⁶¹ extiende el concepto de «producto» para incluir el software y los sistemas de IA, sometiendo a los fabricantes y distribuidores a responsabilidad objetiva, sin necesidad de acreditar culpa, por los daños causados por productos defectuosos. Esta extensión es de notable relevancia práctica: el proveedor de un sistema de IA de alto riesgo que cause daños como consecuencia de un defecto de diseño o de los datos de entrenamiento puede ser considerado responsable sin que la víctima deba probar la negligencia en su desarrollo. La nueva Directiva introduce también reglas de inversión de la carga de la prueba en favor de la víctima cuando exista una asimetría informativa relevante que dificulte la acreditación del defecto.

La interacción entre estos dos instrumentos, responsabilidad objetiva por defecto del producto para los proveedores y presunción de causalidad por incumplimiento del *AI Act* para los operadores, crea un marco de atribución que, aunque imperfecto y en proceso de consolidación, supone un avance sustancial respecto al régimen general de la culpa aquiliana. El seguro de responsabilidad civil de los operadores de sistemas de IA adquiere, en este contexto, una importancia estratégica como mecanismo de canalización y distribución de los costes que este nuevo régimen de responsabilidad genera.

5.4 La asegurabilidad de los riesgos de IA: criterios clásicos y nuevas condiciones

No todo riesgo es asegurable, y si los riesgos de IA lo son, y en qué condiciones, es una pregunta más abierta de lo que parece. La determinación técnica de la asegurabilidad requiere confrontarlos con los criterios clásicos de la doctrina actuarial, retomados en el contexto de la IA por Eling, Nuessle y Staubli (2020), que identifican las condiciones que un riesgo debe reunir para poder ser objeto de cobertura aseguradora: (i) aleatoriedad del siniestro; (ii) posibilidad de valoración de la pérdida; (iii) potencial catastrófico limitado; (iv) existencia de un número suficiente de exposiciones

⁶¹Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo. *Diario Oficial de la Unión Europea* L 2024/2853, de 18 de noviembre de 2024. La nueva Directiva amplía el concepto de «producto» para incluir el software y los sistemas de IA, sometiendo a los fabricantes y distribuidores a responsabilidad objetiva por los daños causados por productos defectuosos, sin necesidad de acreditar culpa.

homogéneas; (v) disponibilidad de datos históricos de siniestralidad; (vi) prima asequible para el tomador; (vii) permisibilidad legal; y (viii) ausencia de riesgo moral excesivo.

La investigación más reciente ha propuesto una clasificación en cuatro niveles que permite ordenar analíticamente el estado actual del mercado asegurador ante los riesgos de IA.⁶² El nivel I comprende los riesgos *afirmativamente asegurados* bajo productos específicos, como las garantías de rendimiento de modelos (*Munich Re aiSure*) y las pólizas de responsabilidad por IA (*Armilla, AIUC*). El nivel II son las denominadas *exposiciones silenciosas (silent-AI)*: daños derivados de IA que quedan comprendidos, sin previsión expresa, en pólizas heredadas de ciberseguro, RC de producto o D&O. El nivel III son los riesgos activamente excluidos mediante cláusulas específicas. El nivel IV son los riesgos fuera de las estructuras convencionales del seguro privado, señaladamente, el riesgo de concentración en modelos fundacionales, cuyo fallo puede correlacionar pérdidas simultáneas en múltiples asegurados, para los cuales se barajan estructuras de reaseguro especializado o mecanismos de respaldo público.

El análisis de los riesgos de IA frente a estos criterios arroja un balance ambivalente.⁶³ En favor de su asegurabilidad concurren: la permisibilidad legal, que está siendo progresivamente establecida por el *AI Act* y los instrumentos de responsabilidad; la posibilidad de valoración económica de los daños materiales y económicos; y la presencia de un riesgo moral que, aunque relevante, no es cualitativamente superior al de otros seguros de responsabilidad civil profesional. En contra de la asegurabilidad concurren tres obstáculos principales: la escasez de datos históricos de siniestralidad, pues el mercado de IA aún no ha acumulado la experiencia estadística necesaria para calibrar modelos actuariales fiables; la naturaleza sistémica y potencialmente correlacionada de ciertos fallos de IA, que puede generar eventos de siniestralidad masiva simultánea difícilmente absorbibles por el sector asegurador; y la dificultad de definir con precisión

⁶²Jia, R. A., Eling, M. y Wang, T. (2025). *Gen AI Risks for Businesses: Exploring the Role for Insurance*. Geneva Association Research Report. Geneva Association. <https://www.genevaassociation.org>

⁶³Tapia Hermida (2021), op. cit., pp. 130–138. El autor analiza las cláusulas *claims made* en el seguro de responsabilidad civil de los operadores de IA, señalando que la delimitación temporal del riesgo cubierto por referencia al momento de la reclamación —y no al momento del hecho generador del daño— es especialmente relevante en el sector de la IA, dado que los daños causados por sistemas algorítmicos pueden manifestarse con un desfase temporal considerable respecto al momento en que se produjo el fallo del sistema.

el riesgo cubierto en las pólizas, dado que la heterogeneidad de las aplicaciones de IA dificulta la estandarización de los condicionados.

No obstante, la historia del sector asegurador muestra que riesgos inicialmente considerados no asegurables han terminado generando mercados específicos una vez acumulada suficiente experiencia técnica y proporcionada la certeza jurídica necesaria por el marco regulatorio. El caso del ciberseguro, analizado en el Capítulo 7, es paradigmático. La convergencia del *AI Act*, de la nueva Directiva de Productos y de la Propuesta de Directiva de Responsabilidad por IA está generando las condiciones regulatorias que el mercado asegurador necesita para desarrollar productos específicos de cobertura del riesgo algorítmico.

5.5 El seguro de responsabilidad civil de los operadores de IA: estructura y cobertura

El instrumento asegurador más directamente aplicable a la cobertura de los daños causados por sistemas de IA es el seguro de responsabilidad civil, regulado en España por los artículos 73 a 76 de la LCS.⁶⁴ Este seguro cubre el nacimiento a cargo del asegurado, proveedor u operador del sistema de IA, de la obligación de indemnizar a un tercero los daños y perjuicios causados por un hecho previsto en el contrato. Su relevancia en el contexto de la responsabilidad por IA es doble: de un lado, garantiza la reparación efectiva del perjudicado, que puede ejercer la acción directa contra el asegurador reconocida en el artículo 76 LCS; de otro, distribuye el riesgo entre la comunidad de operadores asegurados, reduciendo el impacto económico individual de las reclamaciones y desincentivando, en principio, la adopción de sistemas de IA inseguros.

La estructuración de los productos aseguradores de responsabilidad civil por IA plantea cuestiones técnicas específicas que la doctrina ha comenzado a abordar.⁶⁵ En primer lugar, la delimitación del riesgo cubierto requiere precisar qué tipos de sistemas

⁶⁴Ley 50/1980, de Contrato de Seguro, op. cit. Art. 76: «El perjudicado o sus herederos tendrán acción directa contra el asegurador para exigirle el cumplimiento de la obligación de indemnizar, sin perjuicio del derecho del asegurador a repetir contra el asegurado, en el caso de que sea debido a conducta dolosa de éste, el daño o perjuicio causado a tercero.»

⁶⁵Jia, X., Eling, M. y Wang, Z. (2025). Generative AI and insurance: Risks, opportunities and regulatory implications. *The Geneva Association Research Report*. The Geneva Association. El informe identifica como riesgos específicos de la IA generativa: la desinformación automatizada con efectos reputacionales, la generación de contenido nocivo, la suplantación de identidad mediante *deepfakes* y la perturbación masiva de procesos de toma de decisiones en sectores críticos.

de IA quedan incluidos, qué modalidades de daño son asegurables y qué relación debe existir entre el fallo del sistema y el daño para que opere la cobertura. En segundo lugar, la delimitación temporal del riesgo plantea la cuestión de si la póliza debe cubrir los daños cuyo hecho generador se produjo durante la vigencia del contrato, sistema del *occurrence*, o los daños respecto de los cuales la reclamación se presenta durante la vigencia del contrato, sistema de las cláusulas *claims made*. Las cláusulas *claims made* son especialmente frecuentes en el seguro de responsabilidad profesional y resultan de particular relevancia en el seguro de IA, dado que los daños causados por sistemas algorítmicos pueden manifestarse con un considerable desfase temporal respecto al fallo que los originó.

Y es que la doctrina ha señalado, con razón, que el seguro de responsabilidad civil de los operadores de IA puede implementar, en la práctica, la función reguladora del seguro,⁶⁶ convirtiendo el mercado asegurador en un mecanismo de incentivo para el cumplimiento del *AI Act* que opera autónomamente respecto a la supervisión pública. Los modelos concretos de aseguramiento y las implicaciones regulatorias se examinan en el capítulo siguiente.

⁶⁶Leung, A., Zhang, R., Ling, E., Toyoda, K. y Loh, S. M. (2026). The Insurability Frontier of AI Risk: Mapping Threats to Affirmative Coverage, Silent Exposures, and Exclusions. *AIFT Working Paper*, mayo de 2026. Los autores codifican 55 clases de amenazas de IA frente a 26 productos aseguradores e identifican una frontera de asegurabilidad en cuatro niveles: riesgos afirmativamente asegurados; exposiciones silenciosas (*silent-AI*) en pólizas heredadas; riesgos activamente excluidos; y riesgos fuera de las estructuras convencionales del seguro privado. La concentración en modelos fundacionales es identificada como la frontera de asegurabilidad genuinamente nueva, dado que el fallo de un proveedor puede correlacionar pérdidas en múltiples asegurados simultáneamente.

VI. MODELOS DE ASEGURAMIENTO DEL RIESGO ALGORÍTMICO Y FUNCIÓN REGULADORA DEL SEGURO

6.1. El contrato de seguro como instrumento de gobernanza privada de la IA

El contrato de seguro tiene, desde siempre, una función declarada: transferir el riesgo del patrimonio del asegurado al de la aseguradora. Pero la doctrina iusprivatista ha comenzado a reconocer una dimensión adicional, menos evidente pero igualmente real: su capacidad para actuar como instrumento de gobernanza privada. En el contexto de la IA, esta dimensión cobra especial relevancia: el seguro puede condicionar el acceso a la cobertura al cumplimiento de estándares de desarrollo, despliegue y supervisión algorítmica, ejerciendo presión normativa sobre los operadores sin intervención legislativa directa.⁶⁷

El mecanismo es elegante en su sencillez: la aseguradora, al definir exclusiones, deberes preventivos del tomador y requisitos de elegibilidad, está articulando, de forma implícita pero jurídicamente eficaz, un estándar de conducta. Si el tomador no documenta adecuadamente el sistema, no lo somete a auditorías periódicas o carece de protocolos de trazabilidad, la aseguradora podrá denegar la cobertura o reducir la indemnización por inobservancia del deber de prevención y agravación del riesgo (arts. 11 y 12 de la Ley 50/1980, de Contrato de Seguro). De este modo, el contrato de seguro opera como un regulador privado que internaliza en el precio y las condiciones de la póliza los incentivos para una IA responsable.⁶⁸

Lior (2025) ha sistematizado esta función bajo el concepto de "AI Insurance as Governance", sosteniendo que el seguro puede, y debe, incorporar cláusulas de gobernanza que obliguen a los asegurados a adoptar prácticas de gestión del riesgo algorítmico como condición de validez de la cobertura. Estas cláusulas incluirían evaluaciones de impacto algorítmico, responsables internos conforme al AI Act, mecanismos de revisión humana en sistemas de alto riesgo y herramientas de explicabilidad auditables. La lógica subyacente es análoga a la que opera en el seguro de

⁶⁸Lior, A. (2025). AI Insurance. *Connecticut Insurance Law Journal*, 31(1). <https://doi.org/10.2139/ssrn.5316376>

responsabilidad medioambiental o en el seguro de ingeniería: la aseguradora no es indiferente a la calidad del riesgo que asume; al contrario, tiene incentivos económicos para reducir la probabilidad del siniestro exigiendo al asegurado que adopte medidas preventivas.⁶⁹

Esta función reguladora privada no suplanta, sino que complementa, la regulación pública. El Reglamento (UE) 2024/1689, de 13 de junio de 2024, sobre inteligencia artificial, establece un régimen de obligaciones de gobernanza para los sistemas de IA de alto riesgo, entre ellos, los utilizados en la valoración de riesgos en seguros de vida y salud (Anexo III), pero no contempla mecanismos de seguro obligatorio salvo por remisión implícita a los regímenes sectoriales existentes; es justo en ese espacio donde el condicionado asegurador puede operar como régimen complementario de gobernanza.⁷⁰

6.2. Modalidades de aseguramiento del riesgo algorítmico

El mercado asegurador está respondiendo a la irrupción de los riesgos derivados de la IA mediante tres estrategias principales, que coexisten en la actualidad con desigual madurez: la extensión de pólizas existentes, el desarrollo de coberturas modulares y la aparición incipiente de productos *standalone* específicos para riesgos de IA.⁷¹

La vía más inmediata ha sido la extensión o modificación de las pólizas de ciberseguro y de responsabilidad civil profesional para incluir, mediante endorsement o cláusula adicional, los riesgos derivados del uso de sistemas de IA. Aseguradoras como AXA XL o Munich Re ofrecen ya extensiones de sus pólizas ciber que cubren la contaminación de datos de entrenamiento (*data poisoning*), la infracción de derechos de propiedad intelectual por contenido generado por IA y las sanciones regulatorias derivadas del incumplimiento del AI Act. Estas extensiones suelen estar sujetas a

⁷⁰Eling, M., Nuessle, D. y Staubli, J. (2020). The insurability of cyber risk: an empirical analysis. *The Geneva Papers on Risk and Insurance — Issues and Practice*, 45(3), 359–396. <https://doi.org/10.1057/s41288-020-00201-7>

⁷¹Bhattacharya, S., Meredith, W., DeGuira, H., Singh, H. K. y Nambiar, M. (2025). Explainable AI in insurance: applications, challenges, and future directions. *Frontiers in Artificial Intelligence*, 8, 1568266. <https://doi.org/10.3389/frai.2025.1568266>

condiciones de elegibilidad rigurosas que incluyen la verificación de los sistemas de gobernanza del asegurado.⁷²

En segundo lugar, las pólizas de responsabilidad civil de producto y de responsabilidad civil profesional constituyen el vehículo más adecuado para cubrir los daños causados a terceros por decisiones o resultados algorítmicos defectuosos. La Directiva (UE) 2024/2853 sobre responsabilidad por productos, examinada en el capítulo anterior, ha extendido el régimen de responsabilidad objetiva del fabricante a los sistemas de IA como productos, lo que convierte al seguro de RC de producto en la cobertura de referencia para los proveedores de sistemas de IA. Para los operadores, aquellos que despliegan el sistema en un contexto concreto, la cobertura pertinente es la póliza de RC profesional, que ampara los daños derivados de errores u omisiones en la prestación del servicio, incluida la utilización negligente de herramientas algorítmicas.⁷³

Las pólizas de responsabilidad de administradores y directivos (D&O) presentan también un campo de aplicación emergente en el contexto de la IA. Si los órganos de gobierno de una empresa adoptan decisiones estratégicas sobre el despliegue de sistemas de IA que resultan en daños significativos, ya sea por falta de supervisión humana adecuada, por ignorar alertas de sesgo algorítmico o por incumplir las obligaciones de registro en la base de datos europea de sistemas de alto riesgo prevista en el art. 71 del AI Act, la cobertura D&O podría activarse para sufragar los costes de defensa y eventuales indemnizaciones derivadas de acciones de responsabilidad.⁷⁴

Por último, y aun de forma incipiente, están emergiendo productos *standalone* de seguro de IA que pretenden integrar en una sola póliza las diversas exposiciones específicas de los operadores y proveedores de sistemas algorítmicos: errores del modelo, daños por sesgos en la salida, violaciones de privacidad, sanciones administrativas y litigios por infracción de propiedad intelectual. La aseguradora PICC en China y algunas iniciativas piloto en Estados Unidos representan las experiencias más avanzadas en este sentido. Sin embargo, la falta de datos históricos de siniestralidad, la heterogeneidad de

⁷³Jia, Eling y Wang (2025), op. cit., Table 3, pp. 32–33.

los riesgos y la incertidumbre sobre la atribución de responsabilidad dificultan su estandarización y explican que su penetración en el mercado europeo sea aún marginal.⁷⁵

6.3. Lagunas de cobertura y el problema del "silent AI"

A pesar del dinamismo del mercado, el análisis comparado de las coberturas existentes revela importantes lagunas estructurales que pueden dejar sin protección real a las víctimas de daños causados por sistemas de IA. La Geneva Association (2025) ha identificado, en su tabla de análisis de lagunas de cobertura, que riesgos tales como la discriminación algorítmica, la manipulación de mercados por algoritmos autónomos, los daños corporales causados por IA en entornos de movilidad autónoma y las pérdidas de activos financieros derivadas de errores en modelos predictivos carecen, en la mayoría de los productos aseguradores vigentes, de cobertura disponible o tienen cobertura limitada y condicionada.⁷⁶

Particular atención merece el fenómeno conocido como "*silent AI*" o cobertura implícita no intencionada, directamente análogo al "*silent cyber*" documentado en el mercado de ciberseguros. La investigación sobre el *silent cyber* demostró que pólizas concebidas antes de la generalización del riesgo cibernético contenían cobertura o exclusión implícita derivada de redacciones imprecisas, generando incertidumbre jurídica tanto para aseguradoras como para tomadores.⁷⁷ El mismo fenómeno se reproduce ahora con la IA: pólizas de responsabilidad civil general o de RC de producto no incluyen ni excluyen expresamente los daños causados por decisiones algorítmicas, creando una zona gris que perjudica tanto a las víctimas como a las propias aseguradoras. La respuesta del mercado, cláusulas de exclusión expresa de riesgos de IA, traslada el problema hacia el asegurado: si el causante del daño no cuenta con cobertura específica para el riesgo algorítmico, la víctima puede quedar sin compensación.

Esta situación es especialmente problemática en el ámbito del seguro de responsabilidad civil del asegurador que utiliza IA internamente para la suscripción y la tarificación, el Eje A de nuestra tesis. Si un asegurado sufre la denegación de cobertura o

⁷⁶Lior (2025), op. cit., pp. 12–15.

⁷⁷Lior (2025), op. cit.

la aplicación de una prima discriminatoria como consecuencia de un sesgo algorítmico en el sistema de tarificación de su aseguradora, no existe en España un producto asegurador específico para ese riesgo, y la reclamación deberá canalizarse por el régimen general de responsabilidad contractual (arts. 1101 y ss. CC) o por las normas de protección del consumidor, sin que el seguro opere como mecanismo de resarcimiento rápido.⁷⁸

6.4. La función reguladora indirecta del seguro y el papel de la EIOPA

La tesis de que el seguro puede operar como instrumento de gobernanza indirecta de la IA ha recibido respaldo institucional de la Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA). En sus Principios de Gobernanza de la IA publicados en 2021, EIOPA estableció que los principios de *accountability* y *fairness* deben aplicarse a todos los sistemas de IA utilizados en el sector asegurador, incluyendo los destinados a la suscripción, la tarificación y la gestión de siniestros. Estos principios, aunque de naturaleza no vinculante, han sido incorporados de facto como criterios supervisores en varios Estados miembros de la UE y han servido de base para la elaboración de la Opinión sobre Gobernanza y Gestión de Riesgos de la IA publicada por EIOPA en agosto de 2025 (EIOPA-BoS-25-363).⁷⁹

La Opinión de 2025 representa un paso significativo en la articulación de la función reguladora del seguro como vector de gobernanza de la IA. EIOPA articula sus objetivos supervisores en torno a dos ejes principales: primero, mitigar los riesgos derivados del uso de sistemas de IA en el sector asegurador, garantizando que las entidades desarrollen prácticas de gestión del riesgo algorítmico adecuadas y proporcionadas; segundo, promover la convergencia supervisora en el ámbito europeo para evitar el arbitraje regulatorio entre Estados miembros. Para ello, vincula esas obligaciones con los requisitos ya existentes en Solvencia II (arts. 41, 46 y 82), la Directiva de Distribución de Seguros (arts. 17, 20 y 25) y DORA (arts. 4-7 y 11),

⁷⁸EIOPA (2025), op. cit., pp. 7–9.

⁷⁹EIOPA (2021). *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector*. EIOPA Consultative Expert Group on Digital Ethics in Insurance. <https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa-ai-governance-principles-june-2021.pdf>

construyendo un marco integrado que sitúa al seguro en la encrucijada de la gobernanza digital.⁸⁰

Desde una perspectiva jurídico-privada, el mecanismo central a través del cual el seguro ejerce esta función reguladora es la fijación de primas en función del perfil de riesgo del asegurado. Una empresa que adopta prácticas robustas de gestión del riesgo algorítmico, auditorías de modelos, mecanismos de supervisión humana, documentación de los sistemas de decisión, representará un riesgo actuarialmente inferior al de una empresa que opera con sistemas opacos y sin controles internos, lo que se reflejará en primas más bajas. Ese diferencial de precio incentiva la adopción voluntaria de buenas prácticas de gobernanza de la IA, en un mecanismo análogo al de las coberturas preventivas en salud o la bonificación por historial de conducción en el automóvil.⁸¹

Los *sandboxes* regulatorios previstos en el art. 57 del AI Act constituyen otro punto de intersección relevante entre la regulación pública y la función de gobernanza del seguro. Son entornos controlados que permiten a los operadores desarrollar y validar sus sistemas bajo supervisión de la autoridad competente antes de su lanzamiento al mercado. La participación en un *sandbox* puede servir como acreditación de due diligence ante las aseguradoras, facilitando el acceso a coberturas o reduciendo las primas, y convierte así al régimen de supervisión pública en un factor de pricing actuarial. En España, la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero, ya contempla un marco análogo aplicable al sector financiero y asegurador.⁸²⁸³

6.5. Perspectivas de futuro: ¿hacia un seguro obligatorio de IA en Europa?

Pocos debates concentran tanta energía en la intersección del Derecho de seguros y la gobernanza de la IA como la pregunta, legítima y urgente, de si debería existir un seguro obligatorio para los operadores de sistemas de alto riesgo. La Propuesta de

⁸⁰EIOPA (2025). *Impact Assessment of Opinion on AI Governance and Risk Management*. EIOPA-BoS-25-363, 6 de agosto de 2025. <https://www.eiopa.europa.eu>

⁸¹Eling, Nuessle y Staubli (2020), op. cit., pp. 375–379 (criterio de "legal permissibility" en el marco de Berliner).

⁸²Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero. BOE, núm. 300, de 14 de noviembre de 2020.

⁸³Tapia Hermida, A. J. (2021). La responsabilidad civil derivada de la inteligencia artificial y su aseguramiento. *Revista Ibero-Latinoamericana de Seguros*, 30(54), 107–146. <https://doi.org/10.11144/Javeriana.ris54.rcdu>

Directiva sobre Responsabilidad en materia de IA, presentada por la Comisión Europea en septiembre de 2022 (COM(2022) 496), no impone directamente un seguro obligatorio, pero establece en su Considerando 14 que los Estados miembros pueden exigir la suscripción de seguros de responsabilidad civil como parte de las medidas nacionales de implementación, y el art. 4 de la propuesta introduce una presunción de causalidad que incrementa significativamente el riesgo de reclamaciones contra los operadores, creando un incentivo indirecto para la cobertura aseguradora.⁸⁴

La analogía con el seguro obligatorio de responsabilidad civil del automóvil resulta iluminadora, aunque imperfecta. El seguro obligatorio de automóviles funciona porque el riesgo es relativamente homogéneo, los vehículos identificables y registrables, la causalidad de los daños generalmente clara, y existe un cuerpo estadístico amplio para fijar primas. Ninguna de estas condiciones se cumple plenamente en el caso de los sistemas de IA: los riesgos son heterogéneos y dependientes del contexto de despliegue, la identificación del sistema dañino puede ser compleja en cadenas de valor con múltiples operadores, la causalidad es frecuentemente incierta, especialmente en sistemas de aprendizaje automático, y los datos históricos de siniestralidad son insuficientes. Las condiciones de asegurabilidad que Eling, Nuessle y Staubli (2020) identifican como requisitos mínimos, aleatoriedad de la pérdida, cuantificabilidad del daño y homogeneidad del pool de riesgo, están ausentes en muchos segmentos del riesgo algorítmico.⁸⁵

A pesar de estas dificultades, la doctrina favorable a un régimen de seguro obligatorio para la IA de alto riesgo señala que la experiencia del seguro de responsabilidad medioambiental y del seguro de instalaciones nucleares demuestra que el legislador puede imponer cobertura obligatoria incluso en contextos de riesgo heterogéneo y difícil cuantificación, siempre que establezca simultáneamente mecanismos de redistribución, como fondos de garantía o pools de reaseguro, que

⁸⁴Wrede, D., Stegen, T. y Graf von der Schulenburg, J.-M. (2020). Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *The Geneva Papers on Risk and Insurance — Issues and Practice*, 45, 657–689. <https://doi.org/10.1057/s41288-020-00183-6>

⁸⁵Lior, A. (2025). Insuring the AI age: The role of insurance in artificial intelligence regulation and governance. *Connecticut Insurance Law Journal*, 31(1). <https://doi.org/10.2139/ssrn.5316376>

permitan absorber el riesgo sistémico. La creación de un fondo europeo de garantía para daños causados por IA de alto riesgo, financiado con contribuciones de los operadores, podría complementar el seguro privado en aquellos segmentos en que la asegurabilidad individual resulte inviable por insuficiencia de datos o por riesgo de pérdidas catastróficas correlacionadas.⁸⁷

En todo caso, cualquier régimen de seguro obligatorio de IA deberá articularse de forma coherente con los requisitos de gobernanza del AI Act, de modo que el condicionado no sea una mera formalidad, sino un instrumento activo de mejora de los estándares de desarrollo y despliegue algorítmico. El seguro no puede convertirse en un mecanismo que facilite la externalización de las consecuencias del riesgo sin internalizar los incentivos para reducirlo: la experiencia del seguro de RC en el sector financiero, donde la cobertura ha sido a veces instrumento de moral hazard más que de gobernanza prudente, es una advertencia que el legislador europeo no puede ignorar al diseñar el futuro régimen.⁸⁸

⁸⁷Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Propuesta de Directiva IA Liability), COM(2022) 496 final, 28 de septiembre de 2022. Art. 4 (carga de la prueba) y Considerando 14 (seguro obligatorio).

VII. EL CIBERSEGURO COMO ANTECEDENTE DE LA FUNCIÓN REGULADORA DEL SEGURO EN EL CAMPO TECNOLÓGICO

7.1 Planteamiento: el seguro como mecanismo de gobernanza tecnológica

Antes de formular propuestas normativas concretas, conviene detenerse en un precedente que el sector asegurador ya ha vivido, y que ilumina, con notable precisión, lo que puede esperarse con la IA. Los capítulos anteriores han construido la tesis de que el seguro puede operar no solo como mecanismo de compensación económica, sino como instrumento de gobernanza indirecta. El ciberseguro no es solo un antecedente histórico: es un laboratorio del que este trabajo extrae lecciones directas. El mercado de ciberseguros constituye el antecedente más directo y mejor documentado de la función reguladora privada del seguro en el campo de las tecnologías de la información.

Y es que la analogía no es superficial.⁸⁹ El ciberseguro ha demostrado que la industria aseguradora es capaz de moldear comportamientos de gestión del riesgo tecnológico de forma más ágil y eficaz que la regulación pública, precisamente porque el incentivo económico, la reducción de la prima o el acceso a la cobertura, actúa de manera inmediata sobre las decisiones empresariales, sin necesidad de procedimientos legislativos ni de infraestructuras de supervisión pública.

7.2 La emergencia del riesgo cibernético y la respuesta del mercado asegurador

El riesgo cibernético, el conjunto de amenazas derivadas de nuestra dependencia de sistemas informáticos y redes de comunicación, comenzó a manifestarse con intensidad en los años noventa, cuando la generalización de Internet transformó la exposición de empresas e individuos a incidentes como la intrusión no autorizada, la destrucción de datos o la interrupción de servicios. En sus inicios, las pólizas de responsabilidad civil general no contemplaban expresamente estos riesgos, lo que generó una situación de incertidumbre jurídica de notable impacto práctico: ni aseguradoras ni

asegurados sabían con certeza si un ataque informático quedaría cubierto bajo las cláusulas de «daños a la propiedad» o «responsabilidad por productos».

Ante esta laguna, el mercado asegurador desarrolló, a partir de finales de los años noventa, productos especializados de cobertura del riesgo cibernético, las denominadas *cyber insurance policies* o ciberpólizas, que ofrecían cobertura específica para los gastos de notificación de brechas de datos, la responsabilidad frente a terceros afectados, la interrupción del negocio y los costes de restauración de sistemas. Este proceso no fue inmediato ni uniforme: durante años coexistieron coberturas parciales y exclusiones ambiguas, hasta que la proliferación de ciberataques de gran escala, los ataques *ransomware* WannaCry y NotPetya de 2017 constituyeron un punto de inflexión paradigmático, impulsó la consolidación de un mercado maduro de ciberseguros con productos estandarizados y condiciones contractuales precisas.

7.3 La función reguladora indirecta del ciberseguro

El aspecto jurídicamente más interesante del mercado de ciberseguros no es el producto en sí: es el efecto normativo indirecto que genera. La mera existencia de condiciones de elegibilidad para la cobertura ha modificado el comportamiento de las empresas aseguradas de una forma que ninguna ley pública había logrado imponer con la misma eficacia. Las aseguradoras, conscientes de que la siniestralidad cibernética está estrechamente correlacionada con el nivel de madurez en seguridad informática del tomador, han incorporado sistemáticamente requisitos técnicos mínimos como condición de elegibilidad para la cobertura o como criterio diferenciador en la tarificación.

Entre estos requisitos se encuentran, con carácter habitual: la implementación de soluciones de autenticación multifactor (MFA) en accesos privilegiados, la realización de auditorías de seguridad periódicas, la existencia de planes de respuesta a incidentes documentados, la segmentación de redes corporativas y la aplicación de parches de seguridad en plazos predefinidos. El incumplimiento de estas condiciones puede dar lugar a la exclusión de la cobertura, a la reducción proporcional de la indemnización o a la rescisión de la póliza. En consecuencia, las empresas que desean beneficiarse de la cobertura cibernética se ven incentivadas, económicamente, y en ocasiones contractualmente obligadas, a elevar sus estándares de seguridad informática con

independencia de lo que la normativa pública de protección de datos o de ciberseguridad les imponga.

Este mecanismo configura lo que la doctrina denomina regulación privada por el mercado de seguros: la aseguradora actúa como un regulador de facto que fija estándares de conducta, los verifica mediante cuestionarios previos y auditorías, y sanciona su incumplimiento mediante la denegación o minoración de la cobertura.⁹⁰ Este modelo regulatorio privado presenta ventajas estructurales sobre la regulación pública en contextos de innovación tecnológica acelerada: su capacidad de actualización es mayor, su aplicación es descentralizada y su eficacia no depende de la dotación presupuestaria de las autoridades supervisoras.

7.4 El fenómeno del «silent cyber» y su proyección al «silent AI»

El desarrollo del ciberseguro no fue un camino recto. Hubo disfunciones jurídicas graves que son hoy de especial interés para quienes tratan de anticipar el recorrido del seguro de IA. El fenómeno denominado «*silent cyber*» o «ciberriesgo silencioso» designa la situación en que pólizas de seguro diseñadas para cubrir riesgos tradicionales, responsabilidad civil general, seguro de daños, interrupción de negocio, no incluían cláusulas explícitas sobre el ciberriesgo, pero tampoco lo excluían expresamente. Esta ambigüedad contractual generó una litigiosidad significativa: ante un incidente cibernético, los asegurados reclamaban cobertura al amparo de redacciones genéricas, mientras las aseguradoras argumentaban que el riesgo informático no estaba incluido en la intención de las partes al tiempo de contratar.

La respuesta del mercado fue la introducción progresiva de cláusulas de afirmación o exclusión explícita del ciberriesgo, las *cyber affirmative* y *cyber exclusion clauses*, y la emisión de guías por organismos como Lloyd's Market Association exigiendo a sus sindicatos clarificar expresamente la posición de cada póliza ante el

ciberriesgo.⁹¹ Este proceso, aunque lento y conflictivo, permitió dotar al mercado de certeza jurídica.

No es difícil ver el patrón repitiéndose. La doctrina ha constatado empíricamente que el riesgo de IA está recorriendo, con notable exactitud, el mismo camino.⁹² La inmensa mayoría de las pólizas existentes ni cubren ni excluyen expresamente los fallos causados por sistemas de inteligencia artificial, situación que se designa como «*silent AI*». Esta laguna genera para los asegurados la misma incertidumbre que generó el «*silent cyber*» en su momento: ante un daño causado por un algoritmo defectuoso, la viabilidad de la reclamación depende de la interpretación judicial de cláusulas redactadas sin tener en cuenta la tecnología de IA. La resolución de esta incertidumbre requiere un proceso de clarificación contractual análogo al que siguió el mercado de ciberseguros, y posiblemente también una intervención regulatoria de alcance similar a la que las autoridades supervisoras promovieron en el contexto del «*silent cyber*».

7.5 Límites de la analogía y especificidades del riesgo algorítmico

La analogía es fértil, pero no puede trasladarse de forma acrítica. El riesgo de IA tiene características propias que lo distinguen del ciberriesgo, y esas diferencias condicionan el diseño del modelo regulatorio-asegurador.

En primer lugar, el riesgo cibernético, aunque complejo, presenta una causalidad relativamente identificable: existe un vector de ataque, un fallo de seguridad y un daño consecuente. El riesgo algorítmico, en cambio, puede manifestarse de forma no determinista y emergente: el mismo modelo, aplicado al mismo conjunto de datos, puede producir resultados diferentes en función de condiciones del entorno difícilmente anticipables. Esta característica dificulta la determinación del nexo causal entre la conducta del operador del sistema de IA y el daño producido, elemento central para la delimitación de la cobertura aseguradora y para la atribución de responsabilidad.

⁹¹Lloyd's Market Association (LMA). (2019). *Cyber War and Cyber Operation Exclusion Clauses*. LMA. Véase también: Lloyd's of London. (2020). *Market Bulletin: Cyber Exposure in Non-Affirmative (Silent) Cyber Policies*. Lloyd's.

⁹²Lior (2025), op. cit. El estudio analiza una muestra de pólizas de responsabilidad civil y de productos tecnológicos y documenta que la inmensa mayoría no incluyen cláusulas explícitas sobre riesgos derivados de sistemas de inteligencia artificial.

En segundo lugar, la cuantificación actuarial del riesgo cibernético, aunque compleja, se ha desarrollado a medida que el mercado acumulaba datos históricos de siniestralidad. El riesgo de IA, por su novedad y por la heterogeneidad de sus manifestaciones posibles, carece todavía de bases actuariales suficientemente robustas. Se ha señalado que la ausencia de datos históricos de siniestralidad específicos del riesgo algorítmico representa uno de los principales obstáculos para el desarrollo de un mercado asegurador maduro en este ámbito, y que superar este obstáculo requerirá la colaboración entre aseguradoras, reguladores y operadores tecnológicos para la construcción de bases de datos de incidentes compartidas.⁹³

En tercer lugar, el riesgo algorítmico se produce en un contexto regulatorio sustancialmente distinto del que existía en los años formativos del ciberseguro. La aprobación del *AI Act* y la existencia de un marco de supervisión pública con autoridades nacionales competentes introducen una dimensión de Derecho público que el ciberseguro no encontró en sus primeras décadas. Ello implica que el seguro de IA no puede desarrollarse de forma estrictamente autónoma respecto a la regulación pública, sino que deberá articularse coherentemente con las obligaciones que el *AI Act* impone a los proveedores y usuarios de sistemas de alto riesgo. La oportunidad que esto abre es significativa: los requisitos del *AI Act*, documentación técnica, pruebas de robustez, sistemas de gestión de riesgos, supervisión humana, pueden convertirse en los estándares de referencia que las aseguradoras incorporen como condiciones de elegibilidad, de manera análoga a como las ciberpólizas incorporaron los estándares de la norma ISO/IEC 27001 o los marcos del NIST.⁹⁴

7.6 Proyección: el ciberseguro como hoja de ruta para el seguro de inteligencia artificial

El recorrido del ciberseguro desde la ambigüedad del «*silent cyber*» hasta un mercado con productos especializados, condiciones estandarizadas y efectos regulatorios

⁹³Eling, M., Nuessle, D. y Staubli, J. (2020). The insurability of cyber risk: an empirical analysis. *The Geneva Papers on Risk and Insurance*, 45(3), 359–396. <https://doi.org/10.1057/s41288-020-00201-7>

⁹⁴Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (*AI Act*). *Diario Oficial de la Unión Europea* L 2024/1689, de 12 de julio de 2024. Anexo III, punto 5.b. Sobre la norma ISO/IEC 27001 como estándar de referencia en ciberseguros, véase: International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection*. ISO.

reconocidos ofrece una hoja de ruta, imperfecta pero orientadora, para el desarrollo del aseguramiento del riesgo algorítmico. Las etapas de ese recorrido son identificables: primero, la clarificación contractual que elimine las lagunas del «*silent AI*»; segundo, la construcción de una base actuarial a partir de la acumulación sistemática de datos de incidentes; tercero, el diseño de productos especializados que condicionen la cobertura a la observancia de estándares de gobernanza algorítmica verificables; y cuarto, la articulación de estos productos con el marco regulatorio público del *AI Act* y las guías de la EIOPA.

Lo que aquí interesa subrayar es que la experiencia del ciberseguro no solo valida la viabilidad técnica y económica de asegurar riesgos tecnológicos complejos, sino que demuestra empíricamente que el mercado asegurador es capaz de ejercer una función de gobernanza tecnológica efectiva cuando las condiciones regulatorias e informativas son adecuadas.⁹⁵ Las propuestas normativas concretas que permitirían facilitar este desarrollo se abordan en el Capítulo 8 del presente trabajo. Trasladar este modelo al ámbito de la inteligencia artificial no es, por tanto, una propuesta de *lege ferenda* sin arraigo en la realidad, sino la aplicación de un patrón ya consolidado a un contexto tecnológico nuevo.

⁹⁵Lior (2025), op. cit.

VIII. PROPUESTAS NORMATIVAS Y PRINCIPIOS DE GOBERNANZA ALGORÍTMICA EN EL DERECHO DE SEGUROS

8.1. La explicabilidad algorítmica como contenido normativo mínimo del contrato de seguro

Los capítulos anteriores han mostrado que la opacidad de los sistemas de IA empleados por las aseguradoras genera un déficit estructural en el cumplimiento del deber de información precontractual que deriva de la buena fe objetiva consagrada en los artículos 1258 y 1902 del Código Civil y, específicamente en el sector asegurador, de los artículos 3, 10 y 60 de la Ley 50/1980, de 8 de octubre, del Contrato de Seguro (LCS). La tesis que sostiene este trabajo es que la explicabilidad algorítmica, entendida como la capacidad del sistema de IA de generar, a requerimiento del afectado, una explicación comprensible y suficiente de las razones que fundamentan una decisión, debe ser reconocida como un contenido normativo mínimo del contrato de seguro, con independencia de que el sistema empleado sea o no de alto riesgo a los efectos del Reglamento (UE) 2024/1689 sobre inteligencia artificial (AI Act).⁹⁶

La propuesta se sustenta en tres convergencias normativas que ya existen en el Derecho positivo. En primer lugar, el RGPD ya consagra, en su artículo 22, el derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluyendo la elaboración de perfiles, que produzca efectos jurídicos o le afecte significativamente de modo similar. Sus apartados 2 y 3 obligan al responsable habilitado para adoptar tales decisiones a garantizar, al menos, la intervención humana, la expresión del punto de vista del interesado y la posibilidad de impugnar la decisión. Este derecho de impugnación no puede ejercerse eficazmente si el interesado desconoce los factores que han determinado la decisión algorítmica, lo que convierte a la explicabilidad en un presupuesto funcional del derecho reconocido por el RGPD.⁹⁷

⁹⁶Ley 50/1980, de 8 de octubre, del Contrato de Seguro. BOE, núm. 250, de 17 de octubre de 1980. Arts. 3, 10, 12 y 60.

⁹⁷Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD). DO L 119, 4.5.2016. Art. 22 (decisiones individuales automatizadas, incluida la elaboración de perfiles).

En segundo lugar, el AI Act clasifica como sistemas de IA de alto riesgo los destinados a la evaluación de la solvencia y la fijación de precios en seguros de vida y salud (Anexo III, punto 5.b), imponiendo a sus proveedores obligaciones de gestión de riesgos (art. 9), documentación técnica (art. 11), transparencia (art. 13) y supervisión humana (art. 14). El art. 13 exige que estos sistemas sean suficientemente transparentes para que los operadores interpreten y utilicen sus resultados adecuadamente, lo que, proyectado sobre el operador-asegurador, debe entenderse también como una obligación de trasladar al asegurado información comprensible sobre los criterios algorítmicos que han influido en la decisión que le afecta.⁹⁸

En tercer lugar, los Principios de Gobernanza de la IA de EIOPA (2021) y los siete requisitos de la IA fiable elaborados por el Grupo de Expertos de Alto Nivel de la Comisión Europea (2019), entre los que figuran la explicabilidad, la transparencia, la no discriminación y la responsabilidad, ofrecen un marco conceptual que, pese a su naturaleza indicativa, ha comenzado a incorporarse como estándar de diligencia en la supervisión de las entidades aseguradoras. La convergencia de estos tres planos normativos permite afirmar que la explicabilidad algorítmica ha adquirido ya el estatus de principio general del Derecho europeo de seguros digital, con efectos interpretativos sobre los deberes de información previstos en la LCS.⁹⁹¹⁰⁰

8.2. Propuesta de reforma de la LCS: incorporación del deber de información algorítmica

La LCS, promulgada en 1980, concibió su régimen de información precontractual y contractual para situaciones de valoración del riesgo basadas en datos declarados por el propio tomador y evaluados por peritos humanos. La incorporación masiva de sistemas de IA en la tarificación, la suscripción y la gestión de siniestros ha revelado que este régimen resulta insuficiente para garantizar la transparencia y la buena fe que debe

⁹⁸Reglamento (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 (Reglamento de Inteligencia Artificial), DO L 2024/1689, 12.7.2024. Arts. 6, 9, 13 y 17.

⁹⁹EIOPA (2021). *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector*. EIOPA Consultative Expert Group on Digital Ethics in Insurance, junio de 2021, pp. 12–27 (Principios 1-7).

¹⁰⁰EU HLEG (2019). *Directrices éticas para una IA fiable*. Grupo de expertos de alto nivel sobre inteligencia artificial. Comisión Europea. KK-02-19-841-ES-N, pp. 15–27 (requisitos de IA fiable).

presidir la relación aseguraticia cuando la decisión relevante es adoptada o asistida por un algoritmo.¹⁰¹

Se propone incorporar en la LCS un nuevo precepto, modificando el artículo 3 o como nuevo artículo 3 bis, conforme al cual, cuando el asegurador utilice sistemas de IA para determinar la aceptación del riesgo, la prima, la cobertura o la liquidación del siniestro, deberá informar al tomador, antes de perfeccionarse el contrato y ante toda modificación relevante de la póliza, de: (i) el hecho de que la decisión ha sido adoptada o asistida por un sistema de IA; (ii) las variables o categorías de datos que han resultado determinantes para la decisión; y (iii) los mecanismos disponibles para el tomador para solicitar revisión humana de la decisión y para ejercer los derechos que le reconocen el RGPD y el AI Act.¹⁰²

Esta propuesta es coherente con el art. 13 del AI Act y con el derecho a la explicación del RGPD, y los traslada al plano contractual privado, donde tienen efectos más inmediatos para el asegurado. Su infracción debería permitir al tomador, cuando menos, impugnar la cláusula lesiva, nula por inobservancia del requisito de transparencia del art. 3 LCS, y reclamar los daños derivados de la decisión algorítmica opaca sin necesidad de probar la culpa del asegurador, bastando con acreditar el nexo causal entre la falta de explicabilidad y el perjuicio. Esta última consecuencia conecta directamente con la presunción de causalidad que la Propuesta de Directiva de Responsabilidad en materia de IA (COM(2022) 496) introduce para los supuestos en que el operador haya incumplido sus obligaciones de gobernanza algorítmica.¹⁰³

8.3. Coordinación entre el AI Act, Solvencia II y la LCS: hacia un marco jurídico integrado

Uno de los desafíos normativos más complejos que plantea la digitalización del sector asegurador es la articulación coherente de tres bloques que han evolucionado con

¹⁰²Bhattacharya, S., Meredith, W., DeGuira, H., Singh, H. K. y Nambiar, M. (2025). Explainable AI in insurance: applications, challenges, and future directions. *Frontiers in Artificial Intelligence*, 8, 1568266. <https://doi.org/10.3389/frai.2025.1568266>

¹⁰³Directiva (UE) 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II). DO L 335, 17.12.2009. Arts. 41, 44, 46 y 82.

lógicas y ritmos distintos: el AI Act, reglamento horizontal de gobernanza algorítmica; Solvencia II, marco prudencial de las aseguradoras; y la LCS, régimen contractual privado de la relación aseguraticia. Su superposición genera riesgos de incoherencia, duplicidad de obligaciones y vacíos de protección que solo una interpretación sistemática y, de lege ferenda, cláusulas de enlace explícitas pueden resolver.¹⁰⁴

Desde la perspectiva del AI Act, los sistemas de IA utilizados por las entidades aseguradoras en la valoración del riesgo en seguros de vida y salud son de alto riesgo (Anexo III, punto 5.b), lo que impone obligaciones de gobernanza que incluyen el registro en la base de datos europea de sistemas de alto riesgo (art. 71), la designación de un responsable de gobernanza, evaluaciones de conformidad (art. 43) y sistemas de gestión de riesgos auditables (art. 9). Solvencia II, por su parte, impone requisitos de gobernanza interna (art. 41), gestión de riesgos (art. 44) y función actuarial (art. 48) materialmente compatibles con los del AI Act pero no formalmente alineados con él. La EIOPA ha comenzado a abordar esta brecha en su Opinión de agosto de 2025, interpretando las obligaciones de gobernanza del AI Act a la luz de los requisitos de Solvencia II y de la Directiva de Distribución de Seguros, pero sin fuerza normativa vinculante.¹⁰⁵

La propuesta de coordinación tiene tres dimensiones. Primero, de lege ferenda, debería modificarse el art. 46 de Solvencia II, o el Reglamento Delegado (UE) 2015/35, para incluir expresamente la gestión del riesgo de los sistemas de IA en el sistema de gestión de riesgos de las aseguradoras, con las particularidades del AI Act aplicables a los sistemas de alto riesgo. Segundo, la LCS debería remitirse expresamente a los derechos del RGPD y del AI Act, de modo que el asegurado pueda ejercer el acceso, la rectificación y la impugnación directamente en el marco contractual, sin acudir a mecanismos extracontractuales más costosos. Tercero, la supervisión de la DGSFP debería coordinarse formalmente con la autoridad española de IA del art. 70 del AI Act, para evitar arbitrajes regulatorios y garantizar una vigilancia efectiva.

¹⁰⁴Tapia Hermida, A. J. (2021). La responsabilidad civil derivada de la inteligencia artificial y su aseguramiento. *Revista Ibero-Latinoamericana de Seguros*, 30(54), 107–146. <https://doi.org/10.11144/Javeriana.ris54.rcdu>

¹⁰⁵EIOPA (2025). *Impact Assessment of Opinion on AI Governance and Risk Management*. EIOPA-BoS-25-363, 6 de agosto de 2025, pp. 3–9 (objetivos y opciones de política). <https://www.eiopa.europa.eu>

8.4. Principios de gobernanza algorítmica para el sector asegurador: una propuesta sistemática

El trabajo desarrollado permite sistematizar principios de gobernanza algorítmica orientados al sector asegurador, que son a la vez criterios interpretativos de la normativa vigente y guía para la reforma propuesta. Se articulan como estándares de conducta exigibles a las aseguradoras que utilicen sistemas de IA y derivan, convergentemente, del RGPD, del AI Act, de los principios EIOPA (2021), de las directrices HLEG (2019) y de la LCS.

El primer principio es el de **explicabilidad proporcional**. El nivel de explicación exigible debe ser proporcional a la trascendencia de la decisión para el asegurado: mayor ante la denegación de cobertura o el incremento significativo de la prima, menor en funciones auxiliares de back-office. No requiere revelar el código fuente o la arquitectura del modelo, protegible como secreto empresarial, sino identificar las variables determinantes y su peso relativo, en términos comprensibles para un asegurado medio.

El segundo principio es el de **supervisión humana efectiva**. Las decisiones algorítmicas con efectos significativos sobre el asegurado no pueden adoptarse sin posibilidad de revisión por una persona humana cualificada, que no sea mero ratificador automático del resultado. El art. 14 del AI Act exige esto para los sistemas de alto riesgo, pero debe extenderse, por vía contractual o regulatoria, a cualquier sistema de IA usado en la valoración del riesgo o en la gestión de siniestros.

El tercer principio es el de **no discriminación algorítmica auditada**. Las aseguradoras deben implantar protocolos de detección y corrección de sesgos en sus sistemas de IA, con especial atención a las variables proxy que reproduzcan discriminación por género, origen étnico, discapacidad u otras condiciones protegidas. Estos protocolos deben ser auditables por la autoridad supervisora y sus resultados documentados en el expediente de conformidad del art. 9 del AI Act.¹⁰⁶

El cuarto principio es el de **accountability o responsabilidad por el algoritmo**. El asegurador que utiliza un sistema de IA es plenamente responsable de las decisiones

¹⁰⁶ Jia, R. A., Eling, M. y Wang, T. (2025). *Gen AI Risks for Businesses: Exploring the Role for Insurance*. Geneva Association Research Report, pp. 36–39 (conclusiones y recomendaciones). <https://www.genevaassociation.org>

adoptadas o asistidas por él, con independencia de que el modelo haya sido desarrollado por un tercero. La delegación del desarrollo técnico no exime al operador de sus obligaciones de gobernanza, transparencia y no discriminación frente al asegurado. Este principio, enunciado por EIOPA en su Principio 5 sobre *accountability* (2021), conecta con el régimen de responsabilidad del operador previsto en los arts. 25 y 26 del AI Act y con la imputación contractual de la culpa in eligendo reconocida por la jurisprudencia del Tribunal Supremo.¹⁰⁷

El quinto principio es el de **mejora continua y adaptación dinámica**. Dado el carácter evolutivo de los sistemas de IA, en especial los modelos que se reentrenan con nuevos datos, las obligaciones de gobernanza no pueden concebirse como una evaluación única y estática en el despliegue, sino como un proceso continuo de monitorización, revisión y actualización. La Geneva Association ha subrayado que la gestión del riesgo de la IA generativa exige "pasar del cumplimiento estático a la supervisión dinámica", dado que los riesgos evolucionan más rápidamente de lo que las normas pueden formalizarlos.¹⁰⁸

8.5. Valoración de conjunto y perspectivas de futuro

Las propuestas de este capítulo arrancan de un diagnóstico que puede sorprender: el Derecho español y europeo de seguros dispone ya, en gran medida, de los materiales normativos necesarios, RGPD, AI Act, Solvencia II, principios EIOPA y la propia LCS, para construir un régimen coherente y eficaz de gobernanza algorítmica en el sector asegurador. Lo que falta no son instrumentos, sino su articulación sistemática y su coordinación explícita, que solo una reforma legislativa puntual y una supervisión activa y convergente pueden proporcionar.

¹⁰⁷En el plano comparado, el Estado de Colorado (EE. UU.) aprobó en 2021 el Senate Bill 21-169, que prohíbe a las aseguradoras utilizar datos de consumidores de manera que resulte en discriminación injusta basada en criterios protegidos, e impone obligaciones de auditoría algorítmica específicas para el sector. El NAIC (National Association of Insurance Commissioners) publicó en 2023 el Model Bulletin on the Use of Artificial Intelligence Systems by Insurers, que establece estándares de gobernanza, documentación y supervisión humana para los sistemas de IA utilizados en suscripción, tarificación y tramitación de siniestros. Ambos instrumentos son relevantes como referentes comparados del diseño europeo, aunque no son directamente aplicables en el ordenamiento español.

¹⁰⁸Eling, M., Nuessle, D. y Staubli, J. (2020). The insurability of cyber risk: an empirical analysis. *The Geneva Papers on Risk and Insurance — Issues and Practice*, 45(3), 359–396, pp. 373–379 (aplicación del marco de asegurabilidad de Berliner a riesgos emergentes). <https://doi.org/10.1057/s41288-020-00201-7>

La perspectiva de *lege ferenda* más realista en el corto plazo no es la de una ley específica de seguros algorítmicos, sino la de reformas puntuales y coordinadas de la LCS, del Reglamento Delegado de Solvencia II y del régimen de supervisión de la DGSFP, en el marco de la transposición del AI Act y de la Directiva de Responsabilidad en materia de IA. A medio plazo, la Opinión de EIOPA de 2025 tiene vocación de convertirse en base para una Directiva Delegada o en un estándar técnico vinculante que homogenice en toda la UE las obligaciones de gobernanza algorítmica de las entidades aseguradoras.¹⁰⁹

La hipótesis del seguro obligatorio para operadores de sistemas de IA de alto riesgo ha generado debate. Algunos ordenamientos comparados han comenzado a explorarla, pero no es hoy viable en el Derecho europeo por razones que trascienden la voluntad legislativa: la ausencia de una base de datos actuarial suficiente sobre siniestralidad algorítmica, la inexistencia de *pools* de reaseguro especializados en riesgo de IA y la dificultad de cuantificar daños difusos y causalmente complejos hacen que las condiciones mínimas de asegurabilidad identificadas por la doctrina no estén satisfechas. Imponerlo sin estas condiciones estructurales no produciría la cobertura efectiva perseguida, sino pólizas con exclusiones tan amplias que vaciarían de contenido la garantía, lo que es coherente con la cautela expresada al analizar los límites de asegurabilidad del riesgo algorítmico: el seguro obligatorio requiere, como presupuesto, que el mercado correspondiente sea ya funcionalmente posible. A largo plazo, si el mercado alcanza la madurez suficiente, con series históricas de siniestralidad, *pools* de reaseguro sectoriales y fondos de garantía complementarios, la cuestión podrá ser planteada con fundamento actuarial sólido.

Lo que esta investigación ha puesto de manifiesto es que el seguro, lejos de ser un mero receptor pasivo de las transformaciones que la IA impone al sector, tiene potencial para ser un agente activo de gobernanza: a través del condicionado, la tarificación y los requisitos de elegibilidad, las aseguradoras pueden incentivar buenas prácticas de desarrollo y despliegue de IA mucho antes de que el legislador actúe. Esta función reguladora privada no sustituye a la regulación pública, pero la complementa de un modo que el Derecho de seguros, con su experiencia en la gestión de riesgos complejos, está

¹⁰⁹ EIOPA (2021), op. cit., Principle 6 ("Societal and environmental well-being"), pp. 27–29.

especialmente bien situado para desempeñar. El reto está en que el ordenamiento jurídico proporcione el marco adecuado para que el seguro pueda ejercer esa función de manera justa, eficiente y alineada con los derechos fundamentales de los asegurados.

IX. CONCLUSIONES

El trabajo que aquí concluye ha recorrido un territorio amplio: desde la tarificación algorítmica hasta la asegurabilidad del riesgo de IA, desde la discriminación por variable proxy hasta los principios de gobernanza que el sector necesita. Las conclusiones que siguen no son un simple resumen. Son el destilado de un argumento construido paso a paso:

Primera. La inteligencia artificial no ha llegado al sector asegurador por una puerta lateral: ha entrado por el frente y ha reconfigurado su arquitectura funcional. Lo hace como herramienta interna, tarificación, suscripción, gestión de siniestros, y simultáneamente como objeto de cobertura, cuando los daños causados por sistemas algorítmicos de terceros se transfieren al mercado asegurador. Esa doble dimensión exige marcos analíticos diferenciados que el Derecho de seguros no había contemplado hasta la irrupción de la regulación algorítmica europea.

Segunda. La opacidad de los sistemas de IA utilizados por las entidades aseguradoras en la valoración del riesgo y la fijación de la prima constituye una infracción del deber de información precontractual y contractual derivado del principio de buena fe objetiva consagrado en los arts. 1258 del Código Civil y 3, 10 y 60 de la LCS. La asimetría informativa estructural que genera el algoritmo no transparente impide al asegurado ejercer racionalmente su libertad de contratación y articular una reclamación eficaz frente a decisiones perjudiciales. Las consecuencias jurídico-privadas de esta situación deben ser jerarquizadas: la consecuencia de primer orden es la ineficacia relativa de la decisión algorítmica concreta, con derecho a revisión humana, subsistiendo el contrato; en segundo plano, la nulidad ex art. 6.3 CC de las cláusulas del condicionado que excluyan el derecho a la explicación por ser contrarias a normas imperativas del RGPD y el AI Act; solo en tercer lugar, y cuando concurra ocultación deliberada de la naturaleza algorítmica de la decisión, podrá plantearse la anulabilidad del contrato por dolo omisivo ex art. 1269 CC, consecuencia de mayor intensidad pero de más difícil acreditación procesal.

Tercera. La explicabilidad algorítmica, entendida como el derecho del asegurado a obtener una explicación comprensible de los factores determinantes de la decisión que le afecta, es exigible convergentemente desde tres planos normativos: el art. 22 RGPD,

que reconoce el derecho a no ser objeto de decisiones exclusivamente automatizadas y a obtener intervención humana e impugnar el resultado; el art. 13 del AI Act, que obliga al operador de un sistema de alto riesgo a garantizar transparencia suficiente para interpretar y utilizar adecuadamente sus resultados; y los Principios de Gobernanza de la IA de EIOPA, que configuran la explicabilidad como criterio supervisor en el ámbito asegurador. La convergencia de estos tres planos permite afirmar que la explicabilidad ha adquirido estatus de principio general del Derecho europeo de seguros digital.

Cuarta. La discriminación algorítmica en la tarificación presenta una forma específica y técnicamente compleja: la discriminación por variable proxy, mediante la cual el algoritmo reproduce de facto diferenciaciones prohibidas, por razón de género, origen étnico, discapacidad u otras condiciones protegidas, a través de variables correlacionadas que no están formalmente vedadas. Este fenómeno vulnera el principio de igualdad de trato reconocido en la STJUE Test-Achats (C-236/09) y en las directivas sectoriales de igualdad, y no puede conjurarse mediante la simple eliminación de la variable sensible del modelo, pues el sesgo puede persistir a través de las variables proxy. Su detección y corrección requiere auditorías específicas de impacto discriminatorio como condición de conformidad del sistema de IA.

Quinta. El régimen europeo de responsabilidad civil aplicable a los daños causados por IA se articula sobre dos instrumentos complementarios: la Directiva (UE) 2024/2853 sobre responsabilidad por productos, que extiende la responsabilidad objetiva del fabricante a los sistemas de IA como productos y elimina la carga de la prueba del defecto para el perjudicado en determinados supuestos; y la Propuesta de Directiva de Responsabilidad en materia de IA (COM(2022) 496), que introduce una presunción de causalidad cuando el operador haya incumplido sus obligaciones de gobernanza algorítmica. Ambos instrumentos refuerzan la necesidad de contar con coberturas de responsabilidad civil específicas para los operadores de IA.

Sexta. La asegurabilidad de los riesgos algorítmicos es técnicamente viable, pero presenta dificultades significativas que impiden la plena aplicación del marco de Berliner (1982): escasez de datos históricos de siniestralidad, correlación sistémica de los daños derivados de fallos masivos de IA, dificultad de cuantificación de las pérdidas máximas posibles y asimetría informativa severa entre asegurador y asegurado. Estos obstáculos,

que son en gran medida temporales y resolverán a medida que el mercado madure, justifican estrategias de cobertura graduales que van desde la extensión de pólizas existentes, ciberseguro, RC profesional, RC de producto, D&O, hasta la aparición de productos standalone específicos de IA.

Séptima. El contrato de seguro puede y debe ejercer una función de gobernanza indirecta de la IA, condicionando el acceso a la cobertura, o modulando las primas, en función del perfil de gobernanza algorítmica del asegurado. Esta función, identificada por la doctrina más reciente como "AI Insurance as Governance", convierte al asegurador en un cuasi-regulador privado que internaliza en la estructura económica del contrato los incentivos para la adopción de buenas prácticas de desarrollo, despliegue y supervisión de sistemas de IA. La Opinión de EIOPA de agosto de 2025 (EIOPA-BoS-25-363) representa el primer paso institucional para articular esta función en un marco supervisor coherente.

Octava. El Derecho español y europeo de seguros dispone ya de los materiales normativos necesarios para construir un régimen coherente de gobernanza algorítmica en el sector asegurador. La reforma legislativa necesaria no requiere la creación de un nuevo cuerpo normativo, sino la modificación coordinada de la LCS, para incorporar el deber de información algorítmica como contenido mínimo del contrato, del Reglamento Delegado de Solvencia II, para integrar la gestión del riesgo algorítmico en el sistema de gestión de riesgos de las entidades, y del régimen de supervisión de la DGSFP, para coordinarlo con la autoridad competente en materia de IA designada por España en virtud del AI Act.

Novena. Cinco principios deben guiar tanto la interpretación del Derecho vigente como el diseño de las reformas pendientes. Primero: explicabilidad proporcional a la trascendencia de la decisión para los derechos del asegurado. Segundo: supervisión humana efectiva, no meramente formal ni decorativa. Tercero: no discriminación algorítmica auditada y documentada. Cuarto: accountability plena del operador, con independencia de quién haya desarrollado el modelo. Y quinto: mejora continua mediante monitorización dinámica a lo largo de todo el ciclo de vida del sistema. Estos principios no son aspiraciones: son exigibles ya, a partir del marco normativo vigente.

Décima. La presente investigación presenta limitaciones que deben ser expresamente reconocidas. Desde el punto de vista normativo, el análisis se ha centrado en el ordenamiento de la Unión Europea y su proyección sobre el Derecho español, sin desarrollar el estudio comparado de otros sistemas jurídicos, como el estadounidense, el británico post-Brexit o el de los ordenamientos iberoamericanos, que ofrecen perspectivas valiosas sobre la gobernanza algorítmica en el sector asegurador. Desde el punto de vista técnico, la investigación parte de una caracterización general de los sistemas de IA sin adentrarse en el análisis diferenciado de las distintas arquitecturas algorítmicas, modelos de árboles de decisión, redes neuronales profundas, modelos de lenguaje generativo, cuyas propiedades de explicabilidad difieren significativamente. Finalmente, la acelerada evolución regulatoria del sector, con el AI Act en fase de implementación y la Opinión de EIOPA de 2025 aún en desarrollo, hace previsible que algunos de los análisis aquí desarrollados requieran revisión a medida que se produzcan avances normativos. Estas limitaciones señalan líneas de investigación futura: el estudio comparado de los modelos de gobernanza algorítmica en seguros, la elaboración de estándares técnico-jurídicos de XAI específicos para el sector asegurador, y el análisis empírico de la implementación efectiva de los derechos a la explicación reconocidos en el RGPD y el AI Act.

Décima. La presente investigación presenta limitaciones que deben ser expresamente reconocidas. Desde el punto de vista normativo, el análisis se ha centrado en el ordenamiento de la Unión Europea y su proyección sobre el Derecho español, sin desarrollar el estudio comparado de otros sistemas jurídicos, como el estadounidense, el británico post-Brexit o el de los ordenamientos iberoamericanos, que ofrecen perspectivas valiosas sobre la gobernanza algorítmica en el sector asegurador. Desde el punto de vista técnico, la investigación parte de una caracterización general de los sistemas de IA sin adentrarse en el análisis diferenciado de las distintas arquitecturas algorítmicas, modelos de árboles de decisión, redes neuronales profundas, modelos de lenguaje generativo, cuyas propiedades de explicabilidad difieren significativamente. Finalmente, la acelerada evolución regulatoria del sector, con el AI Act en fase de implementación y la Opinión de EIOPA de 2025 aún en desarrollo, hace previsible que algunos de los análisis aquí desarrollados requieran revisión a medida que se produzcan avances normativos. Estas limitaciones señalan líneas de investigación futura: el estudio comparado de los modelos de gobernanza algorítmica en seguros, la elaboración de estándares técnico-jurídicos de

XAI específicos para el sector asegurador, y el análisis empírico de la implementación efectiva de los derechos a la explicación reconocidos en el RGPD y el AI Act.

El seguro frente a la inteligencia artificial no es una cuestión técnica periférica al Derecho de seguros. Es el centro del debate jurídico que definirá el contrato de seguro del siglo XXI. La opacidad algorítmica no puede ser aceptada como el precio inevitable del progreso tecnológico. La explicabilidad es un derecho que el ordenamiento ya reconoce. El reto, ahora, es convertir ese reconocimiento en instrumentos reales, contractuales, procesales, regulatorios, que funcionen cuando el asegurado los necesita. No en el papel. En la práctica.

BIBLIOGRAFÍA

1. LEGISLACIÓN

1.1 Normativa de la Unión Europea

Carta de los Derechos Fundamentales de la Unión Europea. *Diario Oficial de la Unión Europea* C 202, 7.6.2016.

Directiva 2000/43/CE del Consejo, de 29 de junio de 2000, relativa a la aplicación del principio de igualdad de trato de las personas independientemente de su origen racial o étnico. DO L 180, 19.7.2000.

Directiva 2004/113/CE del Consejo, de 13 de diciembre de 2004, por la que se aplica el principio de igualdad de trato entre hombres y mujeres al acceso a bienes y servicios y su suministro. DO L 373, 21.12.2004.

Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II). DO L 335, 17.12.2009.

Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros. DO L 26, 2.2.2016.

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. DO L 2024/2853, 18.11.2024.

Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, COM(2022) 496 final, 28 de septiembre de 2022.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos). DO L 119, 4.5.2016.

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 (Reglamento de Inteligencia Artificial). DO L 2024/1689, 12.7.2024.

1.2 Normativa española

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. *Gaceta de Madrid*, núm. 206, de 25 de julio de 1889.

Constitución Española. *Boletín Oficial del Estado*, núm. 311, de 29 de diciembre de 1978.

Ley 50/1980, de 8 de octubre, del Contrato de Seguro. *Boletín Oficial del Estado*, núm. 250, de 17 de octubre de 1980.

Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea. *Boletín Oficial del Estado*, núm. 28, de 5 de febrero de 2020.

Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero. *Boletín Oficial del Estado*, núm. 300, de 14 de noviembre de 2020.

1.3 Normativa extranjera e instrumentos no vinculantes

Colorado Senate Bill 21-169, «Concerning the use of external consumer data and information sources in insurance practices» (2021). Estado de Colorado, EE. UU.

National Association of Insurance Commissioners (NAIC) (2023). *Model Bulletin on the Use of Artificial Intelligence Systems by Insurers*. NAIC.

2. JURISPRUDENCIA

2.1 Tribunal de Justicia de la Unión Europea

STJUE de 1 de marzo de 2011, *Association Belge des Consommateurs Test-Achats y otros*, C-236/09, ECLI:EU:C:2011:100.

STJUE de 5 de marzo de 2015, *Boston Scientific Medizintechnik*, asuntos acumulados C-503/13 y C-504/13, ECLI:EU:C:2015:148.

STJUE de 16 de julio de 2015, *CHEZ Razpredelenie Bulgaria*, C-83/14, ECLI:EU:C:2015:480.

STJUE de 7 de diciembre de 2023, *SCHUFA Holding AG y otros*, C-634/21, ECLI:EU:C:2023:957.

STJUE de 27 de febrero de 2025, *Dun & Bradstreet Austria*, C-203/22, ECLI:EU:C:2025:139.

2.2 Tribunales españoles

Sentencia del Tribunal Supremo (Sala de lo Contencioso-Administrativo), de 11 de septiembre de 2025, recurso de casación núm. 7878/2024 (caso BOSCO; Fundación Ciudadana Civio contra Secretaría de Estado de Seguridad Social).

3. OBRAS DOCTRINALES

Amerirad, B., Cattaneo, M., Kenett, R. S. y Luciano, E. (2023). Adversarial Artificial Intelligence in Insurance: From an Example to Some Potential Remedies. *Risks*, 11(1), 20. <https://doi.org/10.3390/risks11010020>

Bhattacharya, S., Meredith, W., DeGuira, H., Singh, H. K. y Nambiar, M. (2025). Explainable AI in insurance: applications, challenges, and future directions. *Frontiers in Artificial Intelligence*, 8, 1568266. <https://doi.org/10.3389/frai.2025.1568266>

Eling, M., Nuessle, D. y Staubli, J. (2020). The insurability of cyber risk: an empirical analysis. *The Geneva Papers on Risk and Insurance, Issues and Practice*, 45(3), 359–396. <https://doi.org/10.1057/s41288-020-00201-7>

- Jia, R. A., Eling, M. y Wang, T. (2025). *Gen AI Risks for Businesses: Exploring the Role for Insurance*. Geneva Association Research Report. Geneva Association. <https://www.genevaassociation.org>
- Leung, A., Zhang, R., Ling, E., Toyoda, K. y Loh, S. M. (2026). The Insurability Frontier of AI Risk. *AIFT Working Paper*.
- Lior, A. (2025). AI Insurance. *Connecticut Insurance Law Journal*, 31(1). <https://doi.org/10.2139/ssrn.5316376>
- Owens, E., Sheehan, B., Mullins, M., Cunneen, M. y Ressel, J. (2022). XAI in Insurance: A Systematic Review. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4088029>
- Tapia Hermida, A. J. (2021). La responsabilidad civil derivada de la inteligencia artificial y su aseguramiento. *Revista Ibero-Latinoamericana de Seguros*, 30(54), 107–146. <https://doi.org/10.11144/Javeriana.ris54.rcdu>
- Veiga Copo, A. (2023). *Seguro e inteligencia artificial*. El impacto de la digitalización en el contrato de seguro. Editorial Aranzadi.
- Wrede, D., Stegen, T. y Graf von der Schulenburg, J.-M. (2020). Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *The Geneva Papers on Risk and Insurance, Issues and Practice*, 45, 657–689. <https://doi.org/10.1057/s41288-020-00183-6>
- Xenidis, R. (2020). Tuning EU equality law to algorithmic discrimination: Three pathways to resilience. *Maastricht Journal of European and Comparative Law*, 27(6), 736–758. <https://doi.org/10.1177/1023263X20940547>

4. INFORMES INSTITUCIONALES Y OTRAS REFERENCIAS

- EIOPA (2021). *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector*. EIOPA-BoS-21/001. EIOPA Consultative Expert Group on Digital Ethics in Insurance. <https://www.eiopa.europa.eu>
- EIOPA (2025). *Impact Assessment of Opinion on AI Governance and Risk Management*. EIOPA-BoS-25-363, 6 de agosto de 2025. <https://www.eiopa.europa.eu>
- EU HLEG (2019). *Directrices éticas para una IA fiable*. Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial. Comisión Europea. KK-02-19-841-ES-N. <https://digital-strategy.ec.europa.eu>
- Lloyd's Market Association (2019). *Cyber War and Cyber Operation Exclusion Clauses*. LMA. <https://www.lma.org.uk>
- MAPFRE (2024). *GenAI: Explorando el mañana. Informe sobre inteligencia artificial generativa*. Fundación MAPFRE.

Declaración de Uso de Herramientas de Inteligencia Artificial Generativa en Trabajos Fin de Grado

Por la presente, yo, Pablo Loureiro Orejas, estudiante de E-3 de la Universidad Pontificia Comillas al presentar mi Trabajo Fin de Grado titulado "educación financiera y planificación económica en familias de personas con discapacidad intelectual: análisis de necesidades y retos", declaro que he utilizado la herramienta de Inteligencia Artificial Generativa ChatGPT u otras similares de IAG de código sólo en el contexto de las

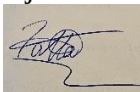
actividades descritas a continuación:

1. **Crítico:** Para encontrar contra-argumentos a una tesis específica que pretendo defender.
2. **Referencias:** Usado conjuntamente con otras herramientas, como Science, para identificar referencias preliminares que luego he contrastado y validado.
3. **Corrector de estilo literario y de lenguaje:** Para mejorar la calidad lingüística y estilística del texto.
4. **Sintetizador y divulgador de libros complicados:** Para resumir y comprender literatura compleja.
5. **Revisor:** Para recibir sugerencias sobre cómo mejorar y perfeccionar el trabajo con diferentes niveles de exigencia.
6. **Traductor:** Para traducir textos de un lenguaje a otro.
7. **Brainstorming de ideas de investigación:** Utilizado para idear y esbozar posibles áreas de investigación.

Afirmo que toda la información y contenido presentados en este trabajo son producto de mi investigación y esfuerzo individual, excepto donde se ha indicado lo contrario y se han dado los créditos correspondientes (he incluido las referencias adecuadas en el TFG y he explicitado para qué se ha usado ChatGPT u otras herramientas similares). Soy consciente de las implicaciones académicas y éticas de presentar un trabajo no original y acepto las consecuencias de cualquier violación a esta declaración.

Fecha: 8 de junio de 2026

Firma:

A small, square image showing a handwritten signature in dark ink on a light-colored background.