

Colección ESTUDIOS DE DERECHO MERCANTIL • MERCATURA
Dirigida por JOSÉ MIGUEL EMBID IRUJO

INTELIGENCIA ARTIFICIAL Y PRIVACIDAD EN EL DERECHO DE SEGUROS

IRENE HERNÁNDEZ BATISTA

PRÓLOGO

PABLO GIRGADO PERANDONES

Editorial Comares



IRENE HERNÁNDEZ BATISTA

INTELIGENCIA ARTIFICIAL Y PRIVACIDAD EN EL DERECHO DE SEGUROS

PRÓLOGO
PABLO GIRGADO PERANDONES

GRANADA, 2026

BIBLIOTECA COMARES DE CIENCIA JURÍDICA

•
MERCATURA

Colección Estudios de Derecho Mercantil

dirigida por

José Miguel Embid Irujo

69

CONSEJO EDITORIAL

Prof. Niccolò Abriani (*Universidad de Florencia, Italia*)

Profesora María Fernanda Vásquez Palma (*Universidad de Talca, Chile*)

Prof. Pablo Girgado Perandones (*Universitat Rovira i Virgili, Tarragona*)

Prof. Ángel García Vidal (*Universidad de Santiago de Compostela*)

Esta monografía se incardina en el marco del Proyecto de Investigación Derecho del Seguro y Cambio Climático (PID2024-162466OB-I00), y su publicación se realiza gracias a la financiación del Ministerio de Ciencia, Innovación y Universidades, la Agencia Estatal de Investigación y el Fondo Europeo de Desarrollo Regional (MICIU/AEI/10.13039/501100011033/ FEDER, UE).



© Irene Hernández Batista

© Editorial Comares, 2026

Polígono Juncaril

C/ Baza, parcela 208

18220 Albolote (Granada) España

Tlf: 958 46 53 82

E-mail: libreriacomares@comares.com • <http://www.comares.com>
<https://www.facebook.com/comares> • <https://twitter.com/comareseditor>
<https://www.instagram.com/editorialcomares>

ISBN: 979-13-7033-087-3 • Depósito legal: Gr. 302/2026

IMPRESIÓN Y ENCUADERNACIÓN: COMARES

*La determinación de la voluntad después
de hecha una investigación
es seguir las direcciones de esa guía,
y quien tenga la potencia de obrar o de no obrar
de acuerdo con el dictado de semejante
determinación es un agente libre (...)
Porque, por más frecuentemente que se equivoque,
no puede admitir otro guía que no sea la razón (...)
La razón tiene que ser nuestro juez en última instancia
y nuestro guía en todo.*

John Locke
Ensayo sobre el entendimiento humano, 1690

SUMARIO

AGRADECIMIENTOS	XIII
RESUMEN	XV
PRÓLOGO <i>por Pablo Girgado Perandones</i>	XVII
LISTADO DE ABREVIATURAS	XXIII
INTRODUCCIÓN	1
Capítulo I. ELEMENTOS CLAVE DE UN NUEVO PARADIGMA: LA 4. ^a REVOLUCIÓN INDUSTRIAL.....	9
I. IDEA INDIVIDUAL E IDEA SOCIAL DEL DERECHO.....	9
1. Un derecho justo y un derecho válido: moralidad y ética en el derecho.....	10
2. La seguridad jurídica como ingrediente fundamental.....	12
3. La adaptabilidad del derecho y el intervencionismo público.....	13
II. PRIVACIDAD	26
1. Introducción histórica.....	26
2. Interpretación constitucional. Alcance y límites del derecho.....	31
III. EL SECTOR ASEGURADOR.....	36
1. El riesgo y su incertidumbre.....	37
2. Condiciones generales, particulares y limitativas del seguro.....	39
3. Principio de solidaridad.....	42
4. Nuevas necesidades que asegurar.....	44
IV. NOTAS CARACTERÍSTICAS DE LA NORMATIVA DE REFERENCIA: ESPECIAL IMPACTO DEL DEBER DE INFORMACIÓN.....	48
1. Regulación paternalista o libertaria.....	50
2. Situación regulatoria del deber de información en España.....	54
Capítulo II. LA INTELIGENCIA ARTIFICIAL EN EL SECTOR ASEGURADOR.....	63
I. DEFINICIÓN DE DATO PERSONAL.....	63
II. CONCEPTO DE INTELIGENCIA ARTIFICIAL Y BIG DATA	66
1. Introducción. Nuevas fuentes de datos.....	66
2. La IA.....	70

2.1. <i>Aprendizaje automático</i>	77
2.2. <i>IA fuerte e IA débil</i>	82
2.3. <i>Inteligencia Artificial y Big Data en el sector asegurador: Ventajas asociadas a los usos y soluciones empleadas</i>	85
Capítulo III. EL USO DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR ASEGURADOR Y SUS RIESGOS PARA LA PROTECCIÓN DE DATOS PERSONALES	105
I. INTRODUCCIÓN	105
II. RIESGOS PARA EL INDIVIDUO COMO PERSONA FÍSICA	111
1. El uso inadecuado de los datos: cálculo de la prima a través de factores ajenos al riesgo	111
2. Un gobierno inadecuado del dato como principal causante de brechas de seguridad	116
3. Datos excesivos: la problemática de los datos de categoría especial y de los datos inferidos	120
4. Acceso indiscriminado a los propios datos y de terceros	125
5. Monitorización, seguimiento y perfilado constante de individuos	132
6. La modificación del comportamiento y su impacto en la autonomía de la voluntad	138
7. Dificultad en el control de los datos: el principio de limitación del plazo de conservación, terceros destinatarios y transferencias internacionales	142
7.1. <i>Número de intervinientes o destinatarios de los datos personales</i>	142
7.2. <i>El plazo de conservación de los datos personales</i>	147
8. Correlaciones y sesgos: vicios de exactitud	149
9. Dificultad de transparencia e inteligibilidad en la IA: el reto de la explicabilidad y las Black Boxes	153
10. Consentimiento viciado: negociación previa y modificación contractual sobrevenida	160
10.1. <i>El consentimiento en la fase precontractual</i>	161
10.2. <i>El consentimiento ante las modificaciones contractuales sobrevenidas</i>	166
11. Asimetría entre la posición de consumidor y empresario	172
III. RIESGOS PARA LA ENTIDAD ASEGURADORA COMO DESTINATARIA DEL RGPD	174
1. La conculcación del principio de legalidad y de seguridad jurídica en la nueva normativa	174
1.1. <i>Punto de partida: principio de legalidad como elemento clave de un Estado de Derecho</i>	174
1.2. <i>Encargados de tratamiento: la posición de garante del Responsable del Tratamiento</i>	181
1.3. <i>El contenido de la información sobre la lógica aplicada</i>	192
1.4. <i>Inseguridad jurídica derivada de la propia actuación de las administraciones públicas</i>	193
2. El amplio margen sancionador	197
3. Vulneración del secreto empresarial y fraudes a la aseguradora	199
4. La compleja asegurabilidad de nuevos riesgos asociados a la IA	204
5. Situación de monopolio: dificultad para mantener un mercado competitivo	208
IV. RIESGOS SISTÉMICOS. SOCIEDAD Y ESTADO	210
1. Asesoramiento inadecuado en la contratación y responsabilidad derivada	211
2. La determinación del grado de intervención humana para asegurar la supervisión	218
3. Problemas de corte ético-moral. Discriminación y conciencia de la IA	220
4. Dificultad en la determinación del grado de control e intervención estatal ante la IA	230
5. Determinación de responsabilidad administrativa: la sanción económica	237
6. Incierta clasificación de niveles de riesgo de la IA	251

7. Comercialización y patrimonialización de los datos personales.....	259
8. Retos para el principio <i>non bis in idem</i> : duplicidad de autoridades, controles y regulación.....	268
8.1. <i>Plano nacional</i>	268
8.2. <i>Plano europeo</i>	276
9. La asegurabilidad de los datos personales en el metaverso.....	279
10. Responsabilidad civil.....	283
10.1. <i>Opacidad y autonomía de los sistemas de IA</i>	288
10.2. <i>Clasificación de la IA: su consideración como producto</i>	290
10.3. <i>RGPD y LIA: clasificación y compatibilidad de la responsabilidad civil</i>	292
10.4. <i>Compleja y opaca cadena de responsables e intervinientes en sistemas de IA</i>	299
10.5. <i>Dificultades para aplicar la normativa de productos defectuosos</i>	301
10.5.1. <i>La inaplicabilidad de las causas de exoneración previstas en el artículo 140 del Real Decreto 1/2007</i>	302
10.5.2. <i>La diversidad de términos y conceptos para designar al responsable</i>	302
10.5.3. <i>Daños morales</i>	304
10.5.4. <i>Uso privativo: ámbito restringido de aplicación del TRLGDCU</i>	305
10.5.5. <i>Producto defectuoso y prueba del defecto</i>	307
10.5.6. <i>Plazo para la manifestación de ausencia de conformidad y plazo para reclamar el daño</i>	309
10.6. <i>Determinación y clasificación de los sistemas de IA de alto riesgo</i>	312
10.7. <i>Diferencias entre la propuesta del Parlamento y la Directiva de la Comisión</i>	312
10.8. <i>Seguro de responsabilidad civil obligatorio</i>	315
 Capítulo IV. INTERPRETACIÓN DE LAS OBLIGACIONES NORMATIVAS DE IA Y PROTECCIÓN DE DATOS PARA LA REDUCCIÓN DE RIESGOS EN EL SECTOR ASEGURADOR.....	 319
I. ASPECTOS GENERALES DE LA NORMATIVA ACTUAL.....	319
1. Enfoque actual: obligación de medios.....	319
2. Ámbito subjetivo de aplicación de la normativa.....	322
II. OBLIGACIONES ESPECÍFICAS DE LA NORMATIVA DE INTELIGENCIA ARTIFICIAL.....	336
1. Sistemas de alto riesgo y plazo para su adecuación.....	336
2. Elementos y definiciones clave para el entendimiento de la LIA.....	340
3. Obligaciones concretas del responsable del despliegue.....	348
3.1. <i>Utilización y vigilancia del sistema de acuerdo con las instrucciones de uso que acompañen al mismo</i>	350
3.2. <i>Vigilar el funcionamiento del sistema de IA encomendando la supervisión humana a personas físicas con competencia, formación y autoridad necesarias</i>	352
3.3. <i>En caso de ejercer control sobre los datos de entrada que alimentan el algoritmo, deberá asegurarse la pertinencia de estos y de que sean suficientemente representativos para la finalidad prevista para el sistema de IA</i>	356
3.4. <i>Obligaciones de comunicación ante la detección de determinados riesgos generales o incidentes graves o defectos de funcionamiento</i>	357
3.5. <i>Conservar por tiempo adecuado los archivos de registro generados por los sistemas de IA siempre que los mismos se encuentren bajo su control</i>	360
3.6. <i>Realización de una evaluación de impacto en materia de protección de datos personales empleando para ello la información que el proveedor está obligado a facilitar</i>	364

III. OBLIGACIONES ESPECÍFICAS DE LA NORMATIVA DE RGPD	365
1. Cumplimiento de los principios básicos	365
1.1. <i>Licitud</i>	365
1.2. <i>Lealtad y transparencia</i>	368
1.2.1. <i>Qué debe entenderse por lógica aplicada</i>	370
1.2.2. <i>Cómo facilitar información sobre sistemas que han sido calificados de poco transparentes (black box) incluso para aquellos que los han desarrollado</i>	371
1.2.3. <i>Dónde y en qué momento debe ponerse a disposición del interesado dicha información</i>	373
1.3. <i>Limitación de la finalidad</i>	374
1.4. <i>Minimización de datos</i>	375
1.5. <i>Exactitud</i>	377
1.6. <i>Conservación</i>	378
1.7. <i>Integridad y confidencialidad</i>	382
1.8. <i>Proactividad</i>	385
2. Garantizar los derechos de los usuarios: derecho de acceso, supresión y no ser objeto de elaboración de perfiles	386
2.1. <i>Acceso</i>	387
2.2. <i>Rectificación</i>	389
2.3. <i>Supresión</i>	390
2.4. <i>Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles que produzca efectos jurídicos en él o le afecte significativamente de modo similar</i>	391
3. Adopción de medidas de medidas de seguridad técnicas y organizativas	394
3.1. <i>Privacidad desde el diseño y por defecto</i>	396
3.2. <i>Existencia de políticas y procedimientos</i>	401
3.3. <i>Análisis de riesgos y evaluación de impacto</i>	404
3.3.1. <i>Cómo debo llevar a cabo un análisis de riesgos</i>	410
3.3.2. <i>Cómo debo llevar a cabo una EIPD</i>	412
3.3.3. <i>Cómo saber que un tratamiento entraña un alto riesgo que precisa de EIPD</i>	417
3.4. <i>Procedimiento de notificación de brechas de seguridad</i>	421
3.4.1. <i>Cuando nos encontramos ante una violación de seguridad</i>	423
3.4.2. <i>Cuando debe notificarse a la Autoridad de protección de datos e, incluso, comunicar a los interesados</i>	424
3.4.3. <i>Desde qué momento debe computarse el plazo para notificar la brecha de seguridad</i>	428
3.5. <i>Auditorías</i>	430
4. Nombramiento obligatorio de un DPO para las aseguradoras	436
4.1. <i>Qué rol desempeña esta figura en una organización</i>	436
4.2. <i>La obligatoriedad de su nombramiento para una entidad aseguradora</i>	439
4.3. <i>Los conocimientos específicos que pueden ser exigidos</i>	442
5. Contratos de encargado de tratamiento y evaluación de los mismos: los «gigantes tecnológicos» y las transferencias internacionales y garantías	443
5.1. <i>Imposibilidad de negociar determinadas cláusulas contractuales que vienen impuestas por la cuota de mercado que representan</i>	444
5.2. <i>Dificultad para extraer información suficiente que permita evaluar al Encargado del tratamiento</i>	446
5.3. <i>Dificultad a la hora de controlar dónde se encuentran los datos y con quién se comparten</i>	447

6. La figura de los códigos de conducta y las certificaciones	451
6.1. <i>Códigos de conducta</i>	451
6.2. <i>Mecanismos de certificación</i>	454
7. Contratación de seguros específicos para la cobertura de los riesgos derivados de incumplimiento y/o ataques de terceros	456
7.1. <i>Entidad aseguradora como proveedor</i>	457
7.2. <i>Entidad aseguradora como cliente</i>	460
8. Los programas de Compliance	461
CONCLUSIONES	465
REFERENCIAS BIBLIOGRÁFICAS	473

AGRADECIMIENTOS

Me gustaría agradecer a mi familia su apoyo incondicional, su espíritu crítico, su inconformismo, su humildad, la importancia del amor a uno mismo, la grandiosidad de las pequeñas cosas, el disfrute de los breves momentos y, sobre todo, el aprender a distinguir lo realmente importante para saber vivir. Destaco su fuerza y su guía porque acompañan e iluminan cada día, son y serán mi presente. También agradezco el apoyo del que ha sido mi director de tesis y me ha dado la oportunidad de volver a reencontrarme a mí misma y mi historia familiar.

Por último, mi gratitud a todos aquellos que me lean y que les haga reflexionar y que incluso critiquen su contenido porque contribuirán a su mejora, especialmente a que la razón humana siga siendo un instrumento vivo, consciente y con conciencia que no sucumba a la inmediatez que proporciona una inteligencia que es artificial.

RESUMEN

La información se ha convertido en motor principal de nuestra sociedad, en particular, aquella que se refiere a una persona física. Aunque esto no es algo nuevo, sí es nueva la forma en la que aquella es manejada y la utilidad que puede extraerse de la misma en beneficio de los que poseen medios adecuados. De entre dichos medios destaca la Inteligencia Artificial. La creciente invasión de privacidad y la dificultad para comprender las nuevas tecnologías han generado a los Estados y sus instituciones la necesidad de regular esta situación. El sector asegurador es un claro destinatario de las normativas que se están desarrollando dada la esencialidad que tienen los datos personales para su actividad. Esta nueva situación genera importantes cambios para todos los actores implicados en una póliza de seguro sin que ninguno de ellos esté siendo plenamente consciente del grave impacto que pueden tener. Dicha inconsciencia viene motivada de una falta de comprensión de los nuevos elementos que se incorporan a nuestra sociedad y de los que el derecho trata de ocuparse sin mucho acierto.

Este volumen pretende hacer reflexionar sobre esta situación y dar luz a esa normativa que, aunque adolezca de claridad, no por ello pierde el sentido coercitivo que exige su cumplimiento. Para la consecución de dicho objetivo se partirá de una concreción y definición de aquellos factores cuya regulación se pretende, en concreto, el dato personal y su interacción con la Inteligencia Artificial; se expondrán los usos para los cuales la actividad aseguradora está destinando aquellos y se evidenciarán los riesgos o peligros que dicha interacción está comportando desde la perspectiva de los distintos actores, en particular derivados de una ineficiente regulación; y, por último, se plantearán posibles soluciones a los riesgos examinados. Todo ello poniendo el foco en la actividad del seguro por su creciente digitalización, por la inherencia que el dato personal tiene en este sector, por la gravosa y amplia regulación que pesa sobre él y por la esencialidad de su existencia en el mercado. Se busca la reflexión meditada sobre esos riesgos y se persigue demostrar la relevancia que tiene el derecho tradicional, colmado de valores y principios a los que se les está dando la espalda y que vienen enmarcados en la seguridad jurídica que todo ordenamiento debe garantizar.

PRÓLOGO

I. El crecimiento exponencial de la aplicación de la inteligencia artificial en el ámbito empresarial se manifiesta claramente en las actividades financieras, entre ellas la aseguradora. Su empleo no sólo está presente en la contratación de seguros sino también en el funcionamiento interno de las propias entidades aseguradoras que asumen esta herramienta digital como un instrumento habitual en su práctica diaria.

El resultado revela, además, un cambio de paradigma en las funciones tradicionalmente desempeñadas por las entidades aseguradoras. Sin menoscabo de la mejora en la eficacia de la gestión empresarial, cabe no desatender la repercusión que su utilización pueda ocasionar en otros intereses igualmente dignos de protección por nuestro ordenamiento jurídico. Al respecto, cabe subrayar el riesgo inherente a la aplicación de la IA sobre la privacidad, como valor jurídico en peligro.

La reciente aprobación del Reglamento de Inteligencia Artificial de la UE supone un paso adelante en la regulación de esta figura, pero son muchos los peligros que, desde la perspectiva de la privacidad, quedan todavía sin una atención suficientemente clara. Se suele decir que los árboles no dejan ver el bosque, y en este caso, los avances muy relevantes, sin duda, de la IA, oscurecen los riesgos que suscita un empleo sin reglas, ni límites, que puede dañar seriamente a instituciones jurídicas bien asentadas entre nosotros, y, en consecuencia, a la seguridad jurídica.

II. La presente monografía responde a esta necesidad de reflexionar sobre el riesgo que el fenómeno de la inteligencia artificial suscita en sede de seguros y el modo en que pueda hacerse compatible este desarrollo tecnológico con la seguridad jurídica y la protección de los diversos intereses en concurso. El trabajo se presentó a la colación del grado de doctor por su autora —Irene Hernández Batista—, quien superó con éxito los obstáculos personales y científicos que se pusieron en su camino. La tesis fue defendida en la Universidad Rovira i Virgili, el ocho de mayo de dos mil veinticinco, en la Sala de Grados de la Facultad de Ciencias Jurídicas, ante un tribunal integrado por las Profesoras Doctoras Lourdes Ferrando Villalba, Paula del Val Talens y Teresa Franquet Sugrañes, quienes le otorgaron la máxima calificación académica, sobresaliente *cum laude*. Las

miembros de la comisión resaltaron la oportunidad del tema y la necesidad de brindar a la comunidad científica en un plazo breve de tiempo los resultados de la investigación. Impulsada por esta misión, y después de la oportuna revisión, incorporando las mejoras y recomendaciones sugeridas, nos presenta esta su primera obra en la prestigiosa colección *Mercatura* de la editorial Comares, compartiendo un precipitado de soluciones bien fundadas y seguras en una temática tan compleja y llena de incertidumbres ante los peligros inherentes a esta nueva tecnología.

Igualmente, estas líneas breves escritas a modo de prólogo sirven de ocasión propicia para presentar a la Dra. Hernández Batista. Es lugar común —y no por ello menos grave— entre las preocupaciones del *alma mater* manifestar la pérdida sufrida en los últimos años de dar continuidad al relevo generacional en la actividad científica que, como es sabido, representa uno de los pilares básicos de la función de la Universidad. Así, en esta última década del siglo se observa una gran dificultad para atraer a aquellas personas dotadas para tarea tan principal en beneficio de otros sectores. En este contexto, destacamos a la Dra. Irene Hernández quien cuenta con un expediente académico brillante, que le hizo merecedora de una de las ayudas para contratos predoctorales concedidas por el Ministerio de Ciencia e Innovación, si bien, por diversas circunstancias, no pudo disfrutar de ella. Su labor se desempeñó, en cambio, por otros derroteros profesionales en los que ha alcanzado una posición muy relevante en una de las empresas españolas de mayor relieve internacional (*Iberdrola*). No obstante, su vocación universitaria —transmitida por sus padres— le ha animado a encontrar tiempo —un bien tan apreciable como escaso— para llevar a término la labor siempre difícil de culminar una tesis doctoral. Aún más, su interés por la investigación le ha conducido a participar activamente en dos proyectos competitivos sobre el Derecho del seguro, como un miembro más del equipo. No en vano la presente monografía enlaza con esta línea de trabajo y revela su empeño firme y constante en las tareas asignadas, confirmando sus dotes inmejorables para la actividad investigadora, intensificadas notablemente gracias a su experiencia profesional en un ámbito próximo al objeto de estudio.

III. Con la intención de introducir a la lectura de este libro, la Dra. Hernández inicia su estudio en el *capítulo primero* analizando el significado de los elementos clave que esta llamada cuarta revolución industrial suscita en el sector asegurador. Como es sabido, la digitalización ofrece grandes oportunidades mediante el tratamiento masivo de datos (*big data*), si bien —como reverso de una misma moneda— su empleo suscita dudas relevantes en el control de su aplicación o, mejor dicho, en la ausencia de este, poniendo en riesgo la privacidad de sus titulares y, en especial, su impacto en el deber de información. Ante esta tesitura, como nos recuerda la autora, la respuesta del legislador se ha concretado en una pluralidad de regulaciones, directivas, guías y recomendaciones en cuatro áreas normativas, pero interrelacionadas; en concreto, se refiere al seguro, a la protección de consumidores, a la privacidad de los datos y a la inteligencia artificial.

Sin embargo, y a pesar de los intentos del legislador por garantizar un uso correcto de estas nuevas tecnologías, se ve superado por un ámbito técnico que le resulta difícil

de comprender a fin de ofrecer una respuesta jurídica adecuada. Así, esta primera aproximación revela una sensación de falsa seguridad en un legislador excesivamente tecnificado y que termina por abandonarse a la autorregulación por los propios operadores privados. Con el fin de intentar poner un poco de claridad en la relación entre inteligencia artificial y privacidad, la autora emprende un estudio exhaustivo de las definiciones utilizadas en los textos jurídicos, tarea no siempre fácil, y que le permite alcanzar algunas primeras conclusiones, destacando especialmente la relativa al impacto ya señalado de esta normativa en el deber de información.

En el *capítulo segundo* continúa profundizando en el significado de estas nuevas realidades tecnológicas, prestando una atención detenida a la interdependencia en el sector asegurador entre la inteligencia artificial y el tratamiento masivo de datos (*big data*). Esta tarea pone de manifiesto cómo el entrenamiento de estos últimos a través de la IA ofrece notables mejoras no sólo en la automatización de los procesos sino también en la elaboración de las pólizas de seguro, incluso creando nuevos ramos de explotación de la actividad aseguradora. Como es sabido, esta situación también ha supuesto un cambio muy relevante en las pólizas ya existentes orientadas hacia un modelo más personalizado, en la que se procede a un seguimiento del individuo, pero —como acentúa la Dra. Hernández Batista— queda en peligro su privacidad.

A continuación, el *capítulo tercero* analiza los riesgos que el uso de la inteligencia artificial en el sector asegurador implica para la protección de los datos personales desde una triple perspectiva: el de las personas físicas intervinientes, el de la propia entidad aseguradora y, finalmente, el de la propia sociedad en su conjunto, entendido como «riesgo sistémico».

Desde la perspectiva del asegurado, la autora pone de manifiesto el cambio que esta nueva tecnología representa en la información recibida por el asegurador. De un escenario tradicional basado en el sometimiento del tomador del seguro a un cuestionario, se incorporan nuevas fuentes de información que permiten una mejora sustancial en el conocimiento del asegurador, pero que también implican un desconocimiento por aquel del proceso de tratamiento de sus datos. Incluso cabe afirmar que este conocimiento supera, con claridad, al que tiene el propio tomador de sí mismo. Sin duda, esta manifestación conlleva la aparición de nuevos riesgos para su privacidad como consecuencia tanto de la asimetría en el conocimiento recíproco de las partes en el seguro, como en el surgimiento de fallas en la conformidad prestada al inicio y durante la vida del contrato. Por ello, la autora propone la necesidad de establecer límites sensatos en protección de los derechos e intereses legítimos del tomador y del asegurado.

Como señala seguidamente la Dra. Hernández Batista, este cambio tecnológico representa una oportunidad y, correlativamente, un riesgo que acrecienta el temor de su empleo entre las entidades aseguradoras. Es sabido que la utilización de la información es imprescindible en la contratación de seguros. La incorporación de la digitalización ofrece innumerables ventajas, pero también resulta difícil encajarla con la configuración tradicional de las cláusulas y condiciones de las pólizas. El empleo de la IA en

su actividad empresarial puede suponer la trasgresión de los derechos y libertades de los tomadores del seguro o de las exigencias legales, cuyo contenido —como ya se ha indicado— es ciertamente confuso. Sin menoscabo de los intentos de los legisladores nacional y europeo de proporcionar garantías a los operadores jurídicos, su implementación hasta el momento no ofrece suficiente confianza. Todo ello implica una pérdida de seguridad jurídica en las aseguradoras por falta de conocimiento de la actitud que deben adoptar ante estos nuevos retos tecnológicos.

Finalmente, este capítulo tercero examina la repercusión en la sociedad que supone la introducción de la IA en el negocio asegurador. Al respecto, se ha puesto de manifiesto —y criticado severamente— la aparición de sesgos en los sistemas empleados, que pueden conducir a una situación incluso de exclusión social de determinados colectivos sociales y, con frecuencia, especialmente vulnerables. En este sentido, la autora defiende la necesidad de apostar por la intervención y supervisión del ser humano durante el proceso tecnológico. En este punto, merece que el lector preste atención detenida a sus valiosas reflexiones sobre la superposición de derechos que viene aconteciendo en la práctica y con premisas autónomas en cada uno de ellos. Del mismo modo, la autora resalta la inseguridad jurídica que viene suscitando la normativa específica —tanto el Reglamento General de Protección de Datos como el Reglamento de la UE de inteligencia artificial— por su labor de clasificación de los riesgos y la complejidad en su comprensión.

El cuarto y último capítulo desempeña una función esencial en el trabajo, pues cumple con la función de dar respuesta a los interrogantes planteados en los capítulos anteriores, lo que explica que su extensión sea claramente superior a la de estos últimos. Como se ha puesto de manifiesto, la respuesta del legislador ante el fenómeno de la IA se reduce a la autorregulación por el propio sector. Esta situación genera entre las empresas una situación de incertidumbre a la hora de proceder con los sistemas basados en IA. Con la finalidad de despejar dudas y aportar seguridades a los operadores económicos, la autora consagra este capítulo a la interpretación de las obligaciones exigidas por las normas de IA y de protección de datos, que permitan reducir los riesgos en el sector. Así, la Dra. Hernández Batista defiende la urgencia de proceder a un estudio detallado de las obligaciones a cumplir por las empresas y se detiene, pormenorizadamente, en el modo en que se han de llevar a término. Su actuación debe estar presidida por el cumplimiento del derecho de información sobre los usos de la IA y el correlativo deber de información por quien lo emplea. De tal modo, se garantiza la protección de los derechos frente a los avances tecnológicos constantes de la IA. Entre otros temas de interés a debate, cabe resaltar la importancia que se atribuye al control sobre la información que pueda obtenerse del proveedor sobre el sistema empleado de IA. Esta medida le permitirá a quien recurra a la inteligencia artificial detectar los errores que se desencadenen y notificarlo tan pronto acontezcan, asumiendo un compromiso mayor con su responsabilidad. Con tal medida, se mejoraría el resultado final y se conseguiría fortalecer los objetivos perseguidos.

Igualmente, la autora defiende la urgencia de desarrollar e implementar en el mercado asegurador tales medidas a fin de poder contar con una IA responsable y respetuosa con los diferentes intereses en liza, proponiendo ubicar al ser humano en el centro como *leitmotiv* de su actuación.

IV. Como punto final a este prólogo, sólo me queda recomendar la lectura de esta monografía a los interesados en el mercado del riesgo y en la búsqueda de herramientas útiles para mejor afrontar los nuevos retos tecnológicos. Escrita con claridad y precisión, la obra nos ofrece respuestas bien argumentadas a los problemas complejos que el empleo de la inteligencia artificial en el ámbito asegurador suscita en el régimen jurídico de la privacidad y de la protección de datos. Igualmente, no quiero dejar de reiterar mi felicitación a la autora que ha sabido combinar una sólida formación jurídica con su experiencia profesional consolidada en la materia. Corresponde ahora al lector adentrarse en la obra para poder comprobar de primera mano esta valoración y, así, aprovechar los amplios conocimientos que atesora su autora.

PABLO GIRGADO PERANDONES

Inteligencia artificial y privacidad en el derecho de seguros es una obra imprescindible para comprender uno de los debates jurídicos más decisivos de nuestro tiempo: cómo integrar tecnologías cada vez más autónomas en un sector que maneja algunos de los datos más sensibles de la vida de las personas. Lejos de ofrecer un análisis meramente descriptivo, el libro propone una mirada crítica, rigurosa y profundamente original sobre los desafíos que plantea la IA en la actividad aseguradora, desde la tarificación algorítmica hasta la gestión automatizada de siniestros.

Su valor no reside solo en la claridad con la que explica conceptos complejos, sino en la capacidad de anticipar problemas que ya están transformando la práctica jurídica y el propio modelo de negocio del seguro. La obra ilumina zonas grises que suelen pasar desapercibidas: los riesgos de opacidad algorítmica, las tensiones entre eficiencia y derechos fundamentales, la redefinición del consentimiento en entornos automatizados o el impacto real de la regulación europea emergente.

El lector encontrará un enfoque equilibrado entre teoría y práctica, con ejemplos, escenarios y reflexiones que permiten comprender por qué la IA no es simplemente una herramienta más, sino un elemento que reconfigura la esencia misma del contrato de seguro. Este libro es necesario porque ofrece criterios sólidos para navegar un terreno en rápida evolución y, sobre todo, porque invita a pensar con profundidad en cómo preservar la confianza, la equidad y la protección de datos en un sector que depende precisamente de esos valores.

