

LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL
EN LA UNIÓN EUROPEA Y SU REPERCUSIÓN EN EL
CONTRATO DE SEGURO*

*THE REGULATION OF ARTIFICIAL INTELLIGENCE IN THE
EUROPEAN UNION AND ITS IMPACT ON THE INSURANCE
CONTRACT*

Actualidad Jurídica Iberoamericana N° 16 bis, junio 2022, ISSN: 2386-4567, pp. 3612-3641

* Este trabajo se ha realizado en el marco del Proyecto de investigación "Nuevos retos en el Derecho de seguros: hacia un mercado asegurador más transparente y competitivo" (ref.: DER2017-87993-P), financiado por FEDER/ Ministerio de Ciencia, Innovación y Universidades – Agencia Estatal de Investigación/ Proyecto.

Pablo
GIRGADO
PERANDONES

ARTÍCULO RECIBIDO: 28 de noviembre de 2021

ARTÍCULO APROBADO: 22 de febrero de 2022

RESUMEN: Los sistemas de inteligencia artificial (IA) desempeñan cada día más una función destacada en el desarrollo de la actividad económica. No obstante, su aplicación suscita riesgos en las empresas y miedos en los consumidores. Por ello, la Unión Europea promueve un marco jurídico fiable y común, que genere confianza entre los ciudadanos. En una primera parte, el artículo analiza su proceso de elaboración y dedica una atención especial a la Propuesta reciente de Reglamento comunitaria -de 21 de abril de 2021-, calificada como "Ley de Inteligencia Artificial". En la segunda parte, se aborda las implicaciones jurídicas que estos sistemas tienen en el negocio asegurador, poniéndose de manifiesto cuáles son sus riesgos, especialmente para los consumidores, y postulando el establecimiento de medidas de control y protección útiles para alcanzar la necesaria transparencia en la contratación de seguros.

PALABRAS CLAVE: Inteligencia artificial; riesgos; regulación comunitaria; contrato de seguro; transparencia y protección.

ABSTRACT: Artificial intelligence (AI) systems play an increasingly prominent role in the development of economic activity. However, its application raises risks in companies and fears in consumers. For this reason, the EU authorities promote a reliable and common legal framework to gain trust among European citizens. In the first part, the article analyzes its developing process and pays special attention to the recent Proposal of Community Regulation -of April 21, 2021-, classified as "Artificial Intelligence Law". In the second part, the legal implications that these systems have on the insurance business are addressed, showing what their risks are, especially for consumers, and postulating the establishment of control and protection measures useful to achieve the necessary transparency in the insurance policies.

KEY WORDS: Artificial intelligence (AI); risks; regulation in the European Union; insurance; transparency and protection.

SUMARIO.- I. INTRODUCCIÓN.- II. LOS INTENTOS DE ELABORACIÓN DE UN MARCO COMÚN REGULADOR DE LA INTELIGENCIA ARTIFICIAL (IA).- I. Primeros pasos.- 2. Las propuestas regulatorias del Parlamento Europeo .- A) La propuesta relativa a los aspectos éticos de la IA, la robótica y las tecnologías conexas.- B) La propuesta relativa al establecimiento de un régimen de responsabilidad civil por la actuación de los sistemas de IA.- III. EL REGLAMENTO DE ARMONIZACIÓN EN MATERIA DE IA (“LEY DE INTELIGENCIA ARTIFICIAL”).- I. Contexto jurídico. Razones y objetivos.- 2. Notas características de la propuesta.- IV. LAS IMPLICACIONES JURÍDICAS DE LA INTELIGENCIA ARTIFICIAL (IA) EN EL SEGURO.- I. Significación jurídica.- 2. Transparencia y protección del consumidor de seguros.- 3. La exigencia de un control de los riesgos.- 4. Nuevos riesgos ligados a la aplicación de la IA.-

I. INTRODUCCIÓN.

La inteligencia artificial (IA) es uno de los fenómenos más relevantes y con mayor repercusión en la sociedad actual. El riesgo inherente a su aplicación y el peligro de su funcionamiento sin control requiere de la intervención del legislador a fin de prevenir y enfrentar la amplia variedad de interrogantes que, sin duda, suscita en la actividad empresarial. No obstante la referencia habitual a su carácter disruptivo, los principios básicos empleados para su regulación se mantienen, lo cual hace siquiera más necesario la consulta de obras clásicas como las del “professore” Cesare Massimo Bianca, a cuyo magisterio homenajeamos en las siguientes líneas¹, y de quien siempre destacó su permanente interés por las cuestiones más novedosas².

Más bien, la influencia decisiva que tiene en nuestros días el fenómeno de la IA radica en la dimensión internacional inherente a los sistemas que la aplican. En especial, porque un tratamiento jurídico individual por cada Estado resultaría una solución claramente insuficiente y parcial y, en consecuencia, supondría que la industria dedicada a la IA se traslade a aquellos países no reguladores, que actuarían a modo de paraísos fiscales para la IA³. Por ello, y como se pone de manifiesto a lo largo de este trabajo, está justificada la necesidad de una regulación a nivel supranacional, como la que es objeto ahora de atención en el ámbito de la Unión Europea.

1 Entre muchas, cabe destacar su obra en varios volúmenes *Diritto Civile*, ed. Giuffrè.

2 Especialmente, por lo que ahora interesa reseñar, son bien conocidas sus relevantes aportaciones en temas relativos a la firma digital y el derecho de las tecnologías de la información; entre muchas, v. la obra realizada bajo su dirección, *La protezione dei dati personali*, CEDAM, Padova, 2007.

3 LÓPEZ ONETO, M.: *Fundamentos para un Derecho de la inteligencia artificial*, ed. Tirant lo Blanch, Valencia, 2020, p. 20.

• Pablo Girgado Perandones

Profesor titular de Universidad, Universitat Rovira i Virgili (Tarragona). Correo electrónico: pablo.girgado@urv.cat.

Por otro lado, a la hora de analizar esta nueva tecnología, no podemos tampoco obviar la ideología -el trashumanismo- que la trasciende y de cuyas graves consecuencias se ha advertido por los expertos en la materia⁴. En cierta medida, su regulación -recientemente calificada como “Derecho de la IA”- es un freno a los excesos de esta nueva ideología y, además, sirve como mecanismo imprescindible para ajustarla a un uso correcto y respetuoso con la dignidad de la persona⁵.

Al mismo tiempo, el desarrollo exponencial de las nuevas tecnologías, calificado como la cuarta revolución digital⁶, y su incorporación progresiva a la actividad empresarial ha supuesto un impacto en todas las actividades económicas, especialmente las financieras⁷. La digitalización se instrumentaliza a través de la IA, y se sirve de los algoritmos como recurso para la elaboración de una ingente cantidad de datos, que convenientemente, ordenada permite las más diversas actuaciones. Entre muchas, cabe destacar la modulación que permite en la contratación a través de los llamados “contratos inteligentes” (“smart contracts”)⁸. Un riesgo inherente a esta actuación explica el intento de delimitación de la responsabilidad civil -y de su cobertura- por las entidades aseguradoras a fin de emplearlo en el proceso de digitalización de los productos financieros que elaboran para sus clientes, como se verá más adelante.

Durante los últimos años, el Derecho del seguro en España se encuentra inmerso en un proceso modernizador que ha permitido consolidar las bases para una mayor transparencia y competitividad en la actividad aseguradora. Claro reflejo de ello son los cambios legislativos en la ordenación⁹ y en la distribución de seguros¹⁰.

4 Sobre los peligros de esta nueva ideología, v. LÓPEZ ONETO, M.: *Fundamentos*, cit., pp. 20 ss.

5 Aunque puede parecer algo obvio, entendemos que es importante puntualizar el significado auténtico de la calificación como “artificial” a esta “inteligencia”. Frente a una aparente ajenedad -incluso separación- de la inteligencia humana, la realidad es que, tanto en su origen como en su configuración, procede del ingenio humano. La traducción inglesa de “artificial” puede suscitar algunas dudas en este sentido, a diferencia de otras lenguas que identifican claramente esta procedencia (así, en el caso alemán se denomina como “Künstliche Intelligenz”, KI). No obstante, como resalta el DRAE, en sus acepciones primera y tercera del adjetivo “artificial”: “hecho por mano o arte del hombre”, “producido por el ingenio humano”. La correspondiente a inteligencia artificial se remite al ámbito informático (“Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico”).

6 Expresión acuñada por Klaus SCHWAB, fundador del Foro Económico Mundial en su edición de 2016.

7 Más en detalle, v. FERNÁNDEZ DE LIS, S./ URBIOLA ORTÚN, P.: “Transformación digital y competencia en el sector financiero”, *Información Comercial Española (ICE)*, núm. 905, 2018, pp. 73 ss.

8 Cabe considerar otras opciones, como el aseguramiento a medida (*on demand*) o también las coberturas dinámicas (*wearables*), como indica TAPIA HERMIDA, A.J.: “Insurtech”, cit., pp. 553-554.

9 Con la Ley 20/2015, de 14 de julio, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras). Entre muchos, v. los trabajos dedicados en AA. VV.: *Un Derecho del seguro más social y transparente* (dir. por J. BATALLER GRAU y M. J. PEÑAS MOYANO), Aranzadi, Cizur Menor, 2017. Recientemente, sobre el tema, v. BENITO OSMA, F.: *La transparencia en el mercado asegurador*, Comares, Granada, 2021.

10 Como es objeto de crítica generalizada por la doctrina, la norma de distribución de seguros no reside en un texto específico y con título propio, sino que, desgraciadamente, se encuentra comprendida en un Real Decreto-Ley de medidas urgentes -el núm. 3/2020, de 4 de febrero- con una denominación aséptica

En esta tesitura, la industria aseguradora se encuentra inmersa en un período de transformación y de adaptación a un entorno digital de gran envergadura tanto en su actividad negocial como en su organización empresarial. Claro ejemplo de ello es la reciente aprobación de la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero¹¹. Cabe advertir que este fenómeno -tecnoseguros o “insurtech”¹²- se despliega, de manera indistinta, por las entidades exclusivamente digitales o por las entidades aseguradoras tradicionales. Del mismo modo, ambas realizan esta actividad de forma alternativa o cumulativa a las tradicionales del seguro¹³.

Igualmente, la tecnología no sólo está sirviendo como una herramienta para la eficiencia en la industria aseguradora, sino que también está transformando los diferentes aspectos de “la cadena de valor”¹⁴. Ello implica nuevos retos -no exclusivos de la actividad aseguradora- derivados de la utilización de los datos personales y la IA que reclaman, por un lado, la adaptación de la legislación vigente a las cuestiones de carácter ético y jurídico relacionadas con la IA y, además, un marco regulador europeo, efectivo y con visión de futuro, que evite el exceso de regulación, limitándose a subsanar aquellas lagunas jurídicas existentes y aumentar la seguridad jurídica para las empresas y para los ciudadanos.

Este escenario de nuevos retos en el sector asegurador supone la necesidad de un análisis en profundidad de las previsiones europeas en la regulación de la IA

a las diversas Directivas de la Unión Europea que son objeto de incorporación a nuestro ordenamiento jurídico. Así, el RD-L 3/2020 comprende materias tan dispares -al margen de la distribución de seguros- como la contratación pública, los fondos de pensiones, el fomento de la implicación a largo plazo de los accionistas, la armonización del IVA, los mecanismos de resolución de litigios fiscales, etc. Sobre el tema de distribución, v. AA. VV.: *La distribución de los seguros privados* (dir. por J. BATALLER GRAU y M. R. QUINTANS EIRAS), Marcial Pons, Madrid, 2019, AA. VV., *El contrato de seguro y su distribución en la encrucijada* (dir. por P. GIRGADO PERANDONES), Aranzadi, Cizur Menor, 2018.

- 11 Sobre su itinerario legislativo, v. TAPIA HERMIDA, A. J.: “Anteproyecto de Ley de medidas para la transformación digital del sistema financiero”, *RDBB*, núm. 152, 2018, pp. 355 ss.
- 12 Sobre el tema, v. recientemente LANDINI, S.: “Insurtech: Innovation in production, distribution, governance and supervision in the insurance market”, en AA. VV.: *Transparencia y competitividad en el mercado asegurador* (coord. por GIRGADO PERANDONES, P./ GONZALES BUSTOS, J. P), Comares, Granada, 2021, pp. 9 ss. Desde la perspectiva profesional, URÍA FERNÁNDEZ, F./ REQUEJO TORCAL, Á.: “Insurtech. Retos y desafíos de cara a la nueva distribución y contratación de seguros”, *RES*, núm. 169, 2017; FERNÁNDEZ MANZANO, L. A.: “Insurtech: ¿revolución o evolución? una aproximación a los desafíos regulatorios y contractuales que plantea la aplicación de la tecnología en el sector asegurador”, en AA. VV.: *Retos y desafíos del contrato de seguro: del necesario aggiornamento a la metamorfosis del contrato. Libro Homenaje al profesor Rubén Stiglitz* (dir. por A. B. VEIGA COPO), Civitas, 2020, pp. 955 ss.
- 13 TAPIA HERMIDA, A. J.: “Insurtech”, en AA. VV.: *Revolución digital, derecho mercantil y Token economía* (dir. por A. F. MUÑOZ PÉREZ), Tecnos, Madrid, 2019, p. 546.
- 14 Este impacto de las nuevas tecnologías -“insurtech”- en las nuevas tecnologías, se observa, de manera detallada, en el Informe elaborado en marzo de 2019 por la Autoridad Europea de Seguros y Fondos de Pensiones (EIOPA, en las siglas en inglés: “European Authority on Insurance and Pensions Funds”). El citado Informe -titulado “Report on best practices on licencing requirements, peer-to-peer insurance and the principle of proportionality in an insurtech context”- pretendía hacer un análisis y evaluación de las mejores prácticas que se venían empleando en el sector asegurador mediante las nuevas tecnologías -“insurtech”- y así ofrecer una información relevante y útil sobre este tema a las autoridades nacionales de supervisión.

y las propuestas planteadas en la búsqueda de soluciones eficaces. A continuación, se aborda cuáles son las implicaciones jurídicas que tiene en el Derecho del seguro.

II. LOS INTENTOS DE ELABORACIÓN DE UN MARCO COMÚN REGULADOR DE LA INTELIGENCIA ARTIFICIAL (IA).

I. Primeros pasos.

En los últimos años, la IA es objeto de un profundo debate en las políticas comunitarias. Entre otros documentos de trabajo, cabe destacar las orientaciones políticas comprendidas bajo el título “Una Unión que se esfuerza por lograr más resultados” para el período 2019-2024¹⁵. A dicho documento, le siguió un “Libro Blanco sobre la inteligencia artificial” en el que se pretendía promover y desarrollar la IA y los sistemas que la emplean en la UE y, al mismo tiempo, abordar los complejos riesgos que la acompañan¹⁶. Todo ello con la finalidad de crear a nivel europeo un marco jurídico fiable -un “ecosistema de confianza”- que permita la implementación y desarrollo de la IA, que, como es bien sabido, representa la palanca de esta revolución digital.

De entre esta documentación, a continuación, vamos a tratar las referidas a dos propuestas de Reglamento formuladas por el Parlamento Europeo. El primero relativo a los principios éticos para el desarrollo, el despliegue y el uso de la IA, la robótica y las tecnologías conexas. La segunda Resolución, con un objetivo más delimitado, promueve la elaboración de un régimen de responsabilidad civil en materia de IA. Posteriormente, se examina la reciente propuesta de la Comisión de un Reglamento comunitario para establecer una regulación armonizadora en materia de IA (denominada como “Ley de Inteligencia Artificial”).

En todas estas propuestas, se pone el acento en el potencial de la IA para transformar nuestro entorno y la necesidad de abordar los retos y las oportunidades que le son inherentes. Igualmente, reclaman una solidez y seguridad técnicas, así como los mecanismos de protección -por ej., su aseguramiento- para dotarla de seguridad jurídica, imprescindible para incorporarlo al proceso negocial.

Como señala el propio comité de expertos, para que la IA sea fiable requiere de tres componentes: la conformidad con la ley, el respeto a los principios éticos y la solidez en su configuración. Además, el desarrollo y la utilización de la IA

¹⁵ Elaborada por la presidente de la Comisión Europea -entonces candidata-, la Dra. Ursula von der Leyen. Se puede consultar en la página web: https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_es_0.pdf.

¹⁶ Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza, COM (2020) 65 final, 2020. Sobre el tema, v. ZURITA MARTÍN, I.: “Las propuestas de reforma legislativa del Libro Blanco Europeo sobre inteligencia artificial en materia de seguridad y responsabilidad civil”, *Actualidad Jurídica Iberoamericana (AJI)*, núm. 14, 2021, pp. 438 ss.

requiere de unas directrices éticas que se deben de incorporar a las líneas de actuación de la Unión Europea y cumplir una serie de requisitos esenciales que confirmen su fiabilidad (en concreto, se señalan las siguientes: “intervención y supervisión humanas”, “solidez y seguridad técnicas”, “privacidad y gestión de datos”, “transparencia”, “diversidad”, “no discriminación y equidad”, “bienestar social y medioambiental”, “rendición de cuentas”)¹⁷.

2. Las propuestas regulatorias del Parlamento Europeo.

A) *La propuesta relativa a los aspectos éticos de la IA, la robótica y las tecnologías conexas.*

Respecto a las dos propuestas regulatorias formuladas por el Parlamento Europeo a la Comisión Europea en materia de IA de 20 de octubre de 2020, analizaremos en este primer apartado la primera de ellas¹⁸. Así, el Parlamento Europeo promueve el impulso de un marco regulador común para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas, basado en la legislación y los valores de la Unión. Este marco regulatorio pretende evitar la fragmentación del mercado interior y así integrar en el Derecho comunitario una serie de obligaciones jurídicas comunes y principios éticos en todo su territorio. Es evidente la inquietud que esta materia suscita en muchos ámbitos de la actividad económica, entre otros, en relación con la protección de los consumidores, la seguridad de los productos o la protección de datos. Pero también en sectores más específicos, como el de los seguros, pues conviene no olvidar las repercusiones que el empleo de estas nuevas tecnologías supone sobre su contratación y distribución en el mercado.

Este marco regulador de la IA en la Unión Europea debe ser adecuado y proporcionado sin que pueda implicar un obstáculo en la innovación y el crecimiento, especialmente de las pequeñas y medianas empresas. Así, se ha de contar con una minuciosa evaluación de los riesgos lo que requiere un enfoque específico en cada una de sus variadas aplicaciones sin que pueda alcanzarse una solución única para todos ellos. Igualmente, la Resolución pretende que cada Estado miembro designe una autoridad nacional de control encargada de garantizar, evaluar y supervisar que el empleo y el desarrollo de la IA, la robótica y las tecnologías conexas cumplan con este marco común y garantice un enfoque armonizado en toda la Unión Europea, especialmente cuando sean de naturaleza transfronteriza. En este último punto no podemos olvidar cómo los nuevos riesgos tienen lugar en un mercado donde la subcontratación o externalización de las actividades -“outsourcing”- es

17 Desde la perspectiva española, conviene, además, tener como referencia el informe de 2019 publicado por el Grupo de trabajo en I+D+i en Inteligencia Artificial del Ministerio de Ciencia, Innovación y Universidades (<https://cpage.mpr.gob.es/producto/estrategia-espanola-de-idi-en-inteligencia-artificial/>).

18 https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html.

práctica habitual, incluso con empresas domiciliadas en otros países; en tal caso, la normativa aplicable dependerá de dónde se encuentre el prestador del servicio.

La Recomendación comunitaria propone a la Comisión la elaboración de un Reglamento sobre principios éticos para el desarrollo, el despliegue y el uso de la IA, la robótica y las tecnologías conexas. Con tal finalidad, aporta una serie de recomendaciones detalladas en su anexo y sistematizadas en una propuesta legislativa que deberá respetar plenamente la dignidad, la autonomía y la seguridad humanas y los demás derechos fundamentales establecidos en la Carta de los Derechos Fundamentales de la Unión Europea (art. 5 Propuesta)¹⁹.

La Propuesta establece una serie de obligaciones aplicables sólo a la IA, la robótica y las tecnologías conexas calificadas como “de alto riesgo”²⁰, garantizando que no se vulneran los principios éticos establecidos en la Propuesta (art. 6)²¹.

Una de las primeras exigencias radica en que el desarrollo, despliegue y utilización de las mencionadas tecnologías de alto riesgo deberán garantizar, en todo momento, una supervisión humana integral (art. 7). Es decir, en cualquier caso, habrá de ser posible el restablecimiento del control humano sobre la tecnología, bien mediante la alteración o la desactivación de la instrumentación empleada.

Con la finalidad de favorecer la seguridad y la transparencia en su empleo, la propuesta pretende que, en el desarrollo, despliegue y utilización de estas nuevas tecnologías, se garanticen las siguientes medidas (art. 8):

- la capacidad de adaptación a circunstancias adversas y que se garantice un nivel de seguridad acorde a unos parámetros mínimos de ciberseguridad en relación

19 v. Diario Oficial de la Unión Europea, de 7 de junio de 2016, C 202/389-405.

20 Se considera como tal el “... riesgo significativo, derivado del desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas, de causar lesiones o daños a las personas o a la sociedad, vulnerando los derechos fundamentales y las normas de seguridad establecidas en el Derecho de la Unión, teniendo en cuenta su uso o finalidad específicos, el sector en el que se desarrollan, despliegan o usan y la gravedad de las lesiones o daños que cabe esperar que se produzcan” (art. 4, letra e). La exigencia de delimitar con exactitud que se entiende por “alto riesgo” ya se ponía de manifiesto en las Conclusiones del Consejo de 9 de junio de 2020 al analizar la configuración del futuro digital de la Unión Europea y, más adelante, en el de 5 de octubre del mismo año. Se trata, en definitiva, de conocer cuáles son los recursos clave definidos como críticos y sensibles en la evaluación coordinada de riesgos de la UE.

21 La Propuesta de reglamento se basa en los siguientes principios: “una inteligencia artificial, una robótica y unas tecnologías conexas antropocéntricas, antropogénicas y controladas por seres humanos; evaluación de la conformidad obligatoria de la inteligencia artificial, la robótica y las tecnologías conexas de alto riesgo; seguridad, transparencia y rendición de cuentas; salvaguardias y vías de recurso contra el sesgo y la discriminación; derecho de resarcimiento; responsabilidad social e igualdad de género en la inteligencia artificial, la robótica y las tecnologías conexas; una inteligencia artificial, una robótica y unas tecnologías conexas ambientalmente sostenibles; respeto de la intimidad y restricciones al uso del reconocimiento biométrico; buena gobernanza relativa a la inteligencia artificial, la robótica y las tecnologías conexas, incluidos los datos utilizados o producidos por dichas tecnologías”. Sobre esta nueva perspectiva económica sostenible, v. PASTOR SEMPERE, M. C.: *Economía digital sostenible*, Pamplona, Aranzadi, 2020, RB I-I.

con el riesgo correspondiente, evitando la explicación fines malintencionados o ilícitos de cualquier vulnerabilidad técnica (letra a);

- el establecimiento de mecanismos de salvaguarda que prevean un plan alternativo frente a posibles riesgos de seguridad o protección (letra b);

- un rendimiento fiable que permita al usuario alcanzar, de manera razonable, los objetivos y las actividades previstas y garantice la posibilidad de su reproducción (letra c);

- la exactitud en la realización de las actividades previstas, y, en caso de imposibilidad de evitar inexactitudes ocasionales, la información a los usuarios y desplegados de la probabilidad de tales errores (letra d);

- la comprensión y explicación accesible de su funcionamiento que permita realizar una revisión del proceso técnico empleado (letra e);

- la información a los usuarios y desplegados del empleo de sistema de IA que les permite conocer sus capacidades, exactitud y limitaciones (letra f);

- la posibilidad de desactivar temporalmente estas nuevas tecnologías y volver a unas funcionalidades seguras en caso de incumplimiento de las medidas de seguridad de los puntos anteriores (letra g).

Además, estas medidas a adoptar se deberán implementar de manera transparente y rastreable por los propios desarrolladores, desplegados y usuarios de estas tecnologías (art. 8.2). Ello permitirá que tales medidas sean auditadas por las autoridades competentes de velar por su cumplimiento (art. 8.3).

Igualmente, se impone la imparcialidad y la no discriminación en el desarrollo, despliegue y utilización de las nuevas tecnologías (art. 9). No obstante, de manera excepcional, sí se admite un trato diferenciado entre personas o grupos de personas cuando concurren dos requisitos. Primeramente, la existencia de “una finalidad objetiva, razonable y legítima que sea proporcionada y necesaria. Y, en segundo lugar, no exista otra alternativa que pueda ser menos lesiva al principio de igualdad de trato.

En la misma línea, el proyecto incorpora el cumplimiento de otros puntos fundamentales en la regulación europea de los últimos años al desarrollo, al despliegue y a la utilización de las nuevas tecnologías. Así, en relación con la responsabilidad social y la igualdad de género, se prohíbe que interfieran en los procesos electorales o difundan informaciones confusas o erróneas que generen desinformación. Y se exige el respeto a los derechos de los trabajadores, la

promoción de la educación de calidad y de la alfabetización digital; sin que, en modo alguno, puedan contribuir a incrementar la desigualdad de oportunidades en la conocida como “brecha de género”, ni vulnerar los derechos de propiedad intelectual, o cualesquiera de sus limitaciones o excepciones.

Y, en relación con la sostenibilidad medioambiental, las autoridades competentes evaluarán y velarán -conforme al art. 11- datos personales por el cumplimiento de las medidas que mitiguen y remedien el impacto que puedan ocasionar estas nuevas tecnologías en el medio ambiente (“...los recursos naturales, el consumo de energía, la producción de residuos, la huella de carbono, la emergencia climática y la degradación del medio ambiente...”).

El respeto de la intimidad y la protección de los datos personales también es objeto de atención en el proyecto por los riesgos que puede entrañar para los derechos fundamentales de los ciudadanos de la Unión. Por ello, especialmente en relación con el uso y la recogida de datos biométricos con fines de identificación remota, se establece que su despliegue o utilización sólo es admisible por las autoridades públicas y siempre que cumplan con fines de interés público esencial (art. 12)²².

Finalmente, un punto muy relevante a tener en cuenta en la propuesta se aprecia en el reconocimiento de un derecho de resarcimiento (art. 13). Así, tiene derecho a ser resarcida toda persona física o jurídica que haya sufrido daños o lesiones por el desarrollo, el despliegue o la utilización de la IA, la robótica o las tecnologías conexas, incluyendo también a los programas informáticos, los algoritmos y los datos utilizados o producidos por dichas tecnologías. En cualquier caso, el derecho al resarcimiento requiere que se haya infringido el Derecho comunitario y las obligaciones impuestas en esta propuesta de Reglamento.

B) La propuesta relativa al establecimiento de un régimen de responsabilidad civil por la actuación de los sistemas de IA.

A diferencia de la primera Resolución ya examinada, la segunda²³ no demanda, en cambio, un nuevo régimen de responsabilidad sino que considera suficiente una intervención más delimitada a través de adaptaciones específicas y coordinadas

22 De igual modo, el proyecto se remite al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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 y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento General de Protección de Datos, RGPD) y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (en adelante, Directiva sobre la Privacidad y las Comunicaciones Electrónicas, DPCE).

23 https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ES.html#title1.

de los regímenes de responsabilidad ya existentes en los Estados miembros²⁴. La finalidad perseguida por tal medida radica en la voluntad de evitar que el empleo de la IA pueda acabar sin indemnización cuando el resultado de su empleo sea la causación de un daño o menoscabo a las personas²⁵.

Desde la perspectiva aseguradora, la propuesta reconoce el papel clave de la cobertura del riesgo en el éxito del recurso a las nuevas actividades entre el público destinatario. Con ello, se permite no sólo aprovechar las ventajas derivadas de los sistemas de IA sino también establecer mecanismos sólidos de salvaguardia. En el caso específico de la circulación de vehículos automóviles, se propone que todos los operadores de sistemas de IA de alto riesgo sean titulares de un seguro de responsabilidad civil, equivalente al vigente y obligatorio para todos los vehículos²⁶. Al respecto, la propuesta advierte del más que probable encarecimiento de las pólizas con tal cobertura debido a la incertidumbre que suscitan estas nuevas tecnologías. Sin duda, ello implicaría un serio obstáculo a su establecimiento y, por tanto, a la innovación e investigación inherentes al desarrollo de estos sistemas.

Respecto de este último punto, la propuesta tiene serias dudas sobre cuál sea el mecanismo indemnizatorio idóneo. Por un lado, no es partidaria de un mecanismo que recurra a la financiación con fondos públicos; por otro, tampoco le parece aconsejable que sea el mercado exclusivamente el que se ocupe de su desarrollo. En este último caso, la falta de datos suficientes sobre los riesgos inherentes a las nuevas tecnologías y la incertidumbre sobre su implementación conducen, irremediablemente, a un modelo único de póliza con una prima muy elevada. Al final, los destinatarios acabarían recurriendo a la póliza más económica, pero con una cobertura muy reducida. Ello tendría un impacto negativo sobre la innovación en estas nuevas tecnologías.

Por otro lado, una de las cuestiones más complejas en la utilización de los sistemas de IA se revela a la hora de identificar quién es la persona que controla el riesgo asociado a dicho sistema o cuál es el código o entra responsable del funcionamiento lesivo. La opacidad y el gran número de agentes intervinientes en estos sistemas son las causas principales de esta dificultad. Al mismo tiempo, la utilización de los sistemas de IA puede causar daños graves en diversos ámbitos,

24 En este caso, no se trata de una cuestión nueva, la Resolución del Parlamento Europeo, de 16 de febrero de 2017, planteó un conjunto de recomendaciones destinadas a la Comisión sobre normas de Derecho civil, entre otros temas, sobre los robots inteligentes y su responsabilidad.

25 La propuesta destaca como uno de sus pilares fundamentales la Directiva comunitaria en materia de responsabilidad del fabricante por los daños causados por productos defectuosos. Sobre el tema, entre nosotros, v. ATIENZA NAVARRO, M. L.: "La responsabilidad civil por daños causados por sistemas de inteligencia artificial", en AA. VV., *Retos y desafíos*, cit., pp. 1093-1104.

26 Sobre el tema, v. BENITO OSMA, F.: "Vehículos y sistemas inteligentes en la circulación: responsabilidad civil y seguro", *RES*, núm. 173, 2018, pp. 43 ss.

como por ejemplo en sede de seguros, a la hora de adoptar decisiones sobre la contratación de seguros de enfermedad.

Desde la perspectiva de la responsabilidad civil, la propuesta parte de la ausencia de personalidad jurídica y de conciencia humana de los sistemas de IA, en tanto su función es la de servir a la actividad humana²⁷. En tal sentido, y a fin de dotarle de una mayor claridad jurídica, la propuesta entiende la IA como equivalente al término “toma de decisiones automatizada”. Con ello, lo que se pretende es identificar a la persona que crea, controla e interfiere en el sistema y, de tal modo, hacerle responsable del daño o perjuicio que pueda causar el mismo, en cualquier momento de su actividad. Esta idea de hacerle responsable del daño es conforme con la normativa europea, en concreto con la Directiva sobre la responsabilidad causada por productos defectuosos²⁸. Ello explica que no sea necesario una revisión completa de las normas en materia de responsabilidad civil sino adecuarlas a las especificidades de los sistemas de IA.

Dos cuestiones son relevantes a juicio de la propuesta. La primera está relacionada con la identificación del operador u operadores que intervienen en el sistema de IA. El usuario sólo asumiría responsabilidad si, además, interviene como operador. En caso contrario, su responsabilidad no sería de naturaleza objetiva -como los operadores-, sino subjetiva, derivada de su negligencia o dolo en el empleo del sistema de IA.

La segunda cuestión relevante se corresponde al tipo de sistema de IA, distinguiendo entre los que son de alto riesgo y los que no. La propuesta se preocupa no sólo por definir qué entiende por tal, sino también por establecer un listado exhaustivo de los sistemas que asumen tal condición²⁹. Igualmente, reglamenta la revisión periódica de tal lista para acomodarlo a los continuos avances e innovaciones tecnológicas, incluso creando un Comité técnico de sistemas de alto riesgo, dedicado a estas labores de mantenimiento y adecuación del listado.

En otro orden, la propuesta tiene en cuenta los riesgos que, en materia de responsabilidad civil, implica la inclusión de un sistema de IA en un producto o servicio. Riesgos que no sólo repercuten en el destinatario final sino también

27 En este sentido, cabe recordar el rechazo al reconocimiento de personalidad jurídica a los robots, como puso de manifiesto el “Informe sobre responsabilidad derivada de la inteligencia artificial y otras tecnologías digitales emergentes” (“Report from the Expert Group on Liability and New Technologies”) emitido por el Grupo de Expertos el 12 de noviembre de 2011. El Grupo se había creado por la Comisión Europea el 9 de marzo de 2018 con la finalidad de analizar las consecuencias jurídicas que suscitaban la IA y otras nuevas tecnologías en materia de responsabilidad. El grupo de expertos consideraba innecesario y superfluo dotarles de personalidad propia cuando, a continuación, la actuación iba a repercutir irremediabilmente sobre una persona física o jurídica ya existente.

28 Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos.

29 En concreto, la propuesta de Reglamento tiene un anexo enumerativo.

en las empresas, en sus capacidades, en su aseguramiento y financiación para incorporarlos a sus proyectos de investigación y desarrollo basados en las nuevas tecnologías. En este sentido, la propuesta pone el acento, de modo especial en la repercusión -negativa- que pudiera tener sobre el recurso a la innovación en las empresas de tamaño medio o reducido (PYMES).

Por último, cabe indicar que la propuesta atiende al papel del seguro en esta modalidad de responsabilidad civil y la función que desempeña a fin de que los perjudicados puedan recibir una indemnización efectiva. En este sentido, reconoce las dificultades que ofrece la configuración de un seguro nuevo que dé cobertura a las nuevas tecnologías. La escasez de información suficiente o su calidad aún precaria afecta, de un modo considerable, a la evaluación de los riesgos y supone un importante hándicap a la hora de ofertar tales seguros. Por ello, la Resolución pretende implementar una serie de medidas que permitan a las entidades aseguradoras aumentar su capacidad para configurar el riesgo inherente a los sistemas de IA y, así, ofrecer una cobertura más innovadora. Entre ellas, destaca el objetivo de incrementar el acceso a los datos generados por las nuevas tecnologías, la búsqueda de los instrumentos más oportunos para mejorar sus resultados, y la pretensión de facilitar información bien documentada a fin de impedir los fallos antes mencionados en su tratamiento por los sistemas de IA.

Así, la propuesta entiende que labor de las entidades aseguradoras debería estar orientada a conocer cómo y en qué condiciones es asegurable la responsabilidad, si bien no vinculada a la relación con la persona responsable sino con el producto objeto de cobertura. De este modo, las pólizas ofertadas en el mercado no seguirán un patrón único en su configuración -solución "de talla única"- sino que, trascurrido un tiempo prudencial, se adaptarán y especializarán conforme las peculiaridades de cada producto o servicio que emplee los sistemas de IA.

El hecho de que la indemnización pueda superar significativamente los máximos fijados en la propuesta de Reglamento ha servido de justificación para que la Resolución promueva la creación de un Fondo especial de indemnización de carácter temporal. Así, y de manera excepcional, en aquellos supuestos con indemnizaciones muy elevadas, como por ejemplo al tratarse de daños colectivos, se configura un fondo específico que pueda dar cobertura a las necesidades del momento. Incluso se llega admitir que algunos países puedan constituir tales fondos, aunque el sistema de IA no esté calificado de alto riesgo. En cualquier caso, sí se destaca la importancia de publicar, de manera clara y exhaustiva, las condiciones exigidas para acogerse a tal fondo.

III. EL REGLAMENTO DE ARMONIZACIÓN EN MATERIA DE IA (“LEY DE INTELIGENCIA ARTIFICIAL”).

I. Contexto jurídico. Razones y objetivos.

Con posterioridad a las propuestas del Parlamento Europeo analizadas en los epígrafes precedentes, la Comisión ha presentado una nueva propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, con el fin de establecer normas armonizadas en materia de inteligencia artificial³⁰. Al respecto, conviene poner el acento en el instrumento jurídico elegido por el legislador europeo. Si bien es cierto que no concurre la existencia de una previa normativa nacional en cada Estado miembro, la elección del Reglamento revela una intención uniformadora y la búsqueda de una norma común, alejada de los riesgos posibles de fragmentación inherentes a otros recursos normativos, como sucede con las Directivas.

El reconocimiento de los beneficios económicos y sociales generados por la IA en los diversos ámbitos socio-económicos conduce al establecimiento de una serie de pautas que puedan evitar los riesgos inherentes a su aplicación. En realidad, la norma pretende superar uno de los obstáculos más significativos con los que se encuentra la implementación de la IA entre los operadores del mercado (empresas, consumidores), que no es otro que la falta de confianza.

Como se afirma en la Exposición de Motivos de esta reciente propuesta, “la mejora de la predicción, la optimización de las operaciones y de la asignación de los recursos y la personalización de la prestación de servicios” supone indudables ventajas competitivas a quienes los sepan aprovechar, poniéndose de manifiesto su importancia dentro de determinados sectores como el financiero, dentro del cual se comprende el de seguros objeto de nuestra atención. Pero también puede dar lugar a desventajas y perjuicios tanto a personas concretas como a la propia sociedad. Ello justifica la adopción de medidas, como la de este Reglamento, que pretender “buscar un enfoque equilibrado”, a fin de que el ejercicio de estas nuevas tecnologías sea conforme a los valores, los derechos fundamentales y los principios de la Unión Europea.

De esta nueva propuesta cabe destacar una mayor concreción de los objetivos respecto de las propuestas del Parlamento Europeo, centrándose ahora en el establecimiento de un marco jurídico que implemente un ecosistema de confianza para la IA. Este ecosistema focaliza su reglamentación en las personas, en su seguridad y en el respeto de los derechos fundamentales. Además, pretende

30 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM/2021/206 final).

garantizar una seguridad jurídica en beneficio de un mayor desarrollo e inversión en los sistemas de IA. De este modo, se podría compatibilizar la mejora en la aplicación de los derechos fundamentales y el desarrollo de un mercado único y no fragmentado con unos estándares legales, seguros y comunes a todo el territorio de la UE.

Sin embargo, la propuesta no persigue una reglamentación excesivamente detallada, sino que se limita a establecer unos requisitos mínimos necesarios para solventar los riesgos y conflictos vinculados a su empleo en el mercado. Lo contrario podría suponer inconvenientes e impedimentos en el desarrollo de estas nuevas tecnologías y su implementación en toda la UE.

Con tal finalidad, se articula un marco jurídico sólido y flexible, por un lado, a través de normas y principios que puedan resistir el paso del tiempo sin necesidad de una reforma continua. Y, por otro, mediante un sistema regulatorio enfocado en los riesgos, claramente delimitados, y que no imponga restricciones innecesarias para su implementación en el mercado. Estas medidas se concretan en una definición única de la IA resistente al paso del tiempo, en la prohibición de prácticas de la IA significativamente perjudiciales para los valores de la UE y en la adopción de determinados límites a los sistemas de IA de identificación biométrica. Ello se consigue mediante la imposición de una serie de obligaciones -proporcionadas y previsibles- a los usuarios y proveedores de los sistemas de IA.

La normativa propuesta, sin embargo, no crea nuevas estructuras, sino que aprovecha las ya existentes de supervisión y gobernanza, configurando un mecanismo específico de cooperación entre los Estados Miembros y un seguimiento continuado de su aplicación; en concreto, articulado a través del *Comité Europeo de Inteligencia Artificial*. Al mismo tiempo, se facilita la creación de espacios controlados de prueba para los sistemas de IA, que hagan posible disminuir la carga normativa y fomentar su desarrollo por las pymes y las llamadas empresas emergentes.

Al respecto, cabe resaltar que uno de los primeros requisitos de la propuesta es su coherencia con otras disposiciones relacionadas con la aplicación de los sistemas de IA. Así, cabe atender, en primer lugar, a las normas en materia de protección de datos y de consumidores, de no discriminación y de igualdad de género³¹. En segundo lugar, se refiere a la legislación sectorial en materia de componentes de seguridad de productos susceptibles de utilizar los sistemas de IA de alto riesgo. En tercer lugar, se alude a las autoridades supervisoras de los servicios financieros que emplean los sistemas de IA a fin de garantizar el cumplimiento de las obligaciones

31 No obstante, la norma ha sido objeto de serias críticas por la BEUC (“Bureau Européen des Unions de Consommateurs”), que resalta la débil protección de la norma al consumidor, especialmente de seguros. <https://www.beuc.eu/publications/eu-proposal-artificial-intelligence-law-weak-consumer-protection/html>.

previstas. Finalmente, considera también la normativa en materia de servicios de intermediación en el comercio electrónico³² y la futura Ley de Servicios Digitales³³.

Esta coherencia también lo es con el conjunto de medidas anunciadas en el “Libro Blanco sobre la inteligencia artificial”, algunas ya comentadas anteriormente³⁴. Todo ello enlaza con la estrategia digital de la propia Comisión –“Configurar el futuro digital de Europa”³⁵- que pretende garantizar los derechos de las personas -y ganar su confianza- en la utilización de los sistemas de IA, en conexión con las iniciativas de gobernanza y protección de datos en la UE³⁶.

La propuesta pretende adoptar medidas que garanticen el establecimiento y funcionamiento del mercado interior, conforme al art. 114 TFUE. Las diversas iniciativas de algunos Estados miembros tendentes a regular de manera individualizada la IA puede conducir, por un lado, a la fragmentación del mercado interno en cuestiones esenciales (requisitos, comercialización, responsabilidad, supervisión), y, por otro, a la inseguridad jurídica inherente a la diversidad regulatoria y a su interpretación, a la vista de la relevante circulación transfronteriza de productos y servicios entre los diversos Estados de la UE.

Es evidente que los objetivos propuestos no se pueden alcanzar de manera efectiva a través de la actuación individualizada de cada Estado, sino que se requiere de una actuación conjunta como la prevista en la propuesta de Reglamento. Con ello, se trata de establecer herramientas sólidas que favorezcan la circulación de productos y servicios, la igualdad de condiciones y de protección a todas las personas, reforzando la competitividad en el mercado y la innovación de la industrial de IA en el seno de la UE.

Igualmente, la regulación de la Propuesta no actúa sino de manera proporcionada al marco jurídico existente sin que incremente injustificadamente su reglamentación. Pues, atiende a un enfoque basado en los riesgos que despliega los sistemas de IA y sólo interviene dentro de los que sean calificados como

32 Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (“Directiva sobre el comercio electrónico”) (DO L 178 de 17.7.2000, p. 1).

33 Así, está en fase preparatoria una Propuesta de Reglamento, del Parlamento Europeo y del Consejo, relativa a un mercado único de servicios digitales, que modifica la Directiva 200/31/CE [COM (2020) 825]. Sobre el tema, v. BENITO OSMA, F.: “El mercado digital de seguros”, en AA. VV.: *Transparencia y competitividad*, cit., pp. 42 ss.

34 En concreto, nos referimos a la reforma de las Directivas sobre máquinas o sobre seguridad general de los productos, así como a las diversas iniciativas en materia de responsabilidad por la utilización de sistemas de IA.

35 Comunicación de la Comisión «Configurar el futuro digital de Europa» [COM(2020) 67 final].

36 Así, cabe destacar la Propuesta de Reglamento relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos), COM(2020)767, la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público, PE/28/2019/REV/I (DO L 172 de 26.6.2019, p. 56).

significativamente altos respecto a los derechos fundamentales y la seguridad. En otro caso, las obligaciones que establece la Propuesta son muy limitadas y esta fundamentalmente orientada a la exigencia de transparencia en su actuación.

Conforme a la propuesta, cuando los sistemas de IA alberguen la posibilidad de entrañar un alto riesgo es necesario establecer una serie de requisitos –“ los datos de alta calidad, la documentación y la trazabilidad, la transparencia, la vigilancia humana, la precisión y la solidez”- necesarios para reducir tales riesgos para los derechos fundamentales y la seguridad, siempre que no estén cubiertos por otros marcos jurídicos específicos. Ello permite a los proveedores y usuarios de tales sistemas de IA reducir los costes de su implementación a parámetros proporcionales a los objetivos y beneficios esperados.

La Propuesta ha tenido en cuenta, mediante la preceptiva consulta, una amplia variedad de observaciones y opiniones de especialistas y profesionales en la materia, quienes, en su momento, pusieron el acento, especialmente, en la necesidad de evitar duplicidades, contradicciones entre normativas y exceso regulatorio. Al mismo tiempo, y junto a la importancia de delimitar determinados conceptos esenciales, se mostraron favorables a un planteamiento enfocado en el riesgo, centrado en las necesidades de cada sector y en la protección de los derechos fundamentales y la seguridad ante la utilización de los sistemas de IA. Además, los partícipes en la consulta se mostraron partidarios de promover espacios controlados de pruebas calificados como una herramienta útil para la implementación de tales sistemas. Y también se mostraron a favor de una combinación de mecanismos preventivos -*ex ante*- de autoevaluación de riesgos por los operadores con mecanismos de supervisión -*ex post*- para aquellos sistemas de IA calificados de alto riesgo.

En definitiva, el resultado es el establecimiento de un conjunto normativo armonizado que tiene por objetivo introducir, poner en servicio y utilizar los sistemas de IA en el mercado de la UE.

2. Notas características de la propuesta.

La norma propuesta fija un ámbito de aplicación suficientemente amplio que comprenda tanto a los proveedores, con independencia de su establecimiento en algún Estado miembro de la UE, que introduzcan en el mercado o pongan en servicio sistemas de IA (art. 2.1), como a los usuarios de tales sistemas de IA.

Asimismo, delimita concienzudamente cada una las nociones esenciales que serán objeto de atención a lo largo del Reglamento. Cabe destacar por su interés

en sede de seguros el correspondiente a los “sistemas de inteligencia artificial”³⁷ y a los diversos integrantes de la cadena de valor de la IA, englobados bajo el término conjunto de operadores (proveedor³⁸, usuario³⁹, representante autorizado⁴⁰, importador⁴¹, distribuidor⁴²).

La definición de “inteligencia artificial” pretende dos objetivos. El primero, la neutralidad tecnológica. El segundo, la durabilidad en el tiempo. De tal modo, se busca proporcionar la seguridad jurídica necesaria ante la rápida evolución de los cambios tecnológicos y de su aplicabilidad en el mercado.

Las definiciones de los operadores destacan por su amplitud, como se observa en la inclusión entre los proveedores y usuarios “de toda persona física o jurídica ...” y también -conviene remarcarlo- “... autoridad pública, agencia u organismo de otra índole”. Además de ello, las definiciones son claras y sencillas en su redacción, con la misma vocación de permanencia que la correspondiente a la IA.

El enfoque basado en los riesgos de la IA y de los sistemas que la emplean, conduce a clasificarlos en tres grupos:

- los que generan un riesgo inaceptable;
- los que generan un riesgo alto;
- los que generan un riesgo bajo o mínimo;

Los primeros de ellos –“riesgo inaceptable”- se engloban en un listado de prácticas prohibidas y se desarrollan en un título propio (Título II). Se trata de aquellos supuestos en los que se considera que las prácticas de tales sistemas de IA actúan contrariamente a los valores fundamentales que inspiran los derechos de la UE (art. 5).

37 “Sistema de inteligencia artificial (sistema de IA): el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa.

38 “toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que desarrolle un sistema de IA o para el que se haya desarrollado un sistema de IA con vistas a introducirlo en el mercado o ponerlo en servicio con su propio nombre o marca comercial, ya sea de manera remunerada o gratuita”.

39 “toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional”.

40 “toda persona física o jurídica establecida en la Unión que haya recibido el mandato por escrito de un proveedor de un sistema de IA para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor”.

41 “toda persona física o jurídica establecida en la Unión que introduzca en el mercado o ponga en servicio un sistema de IA que lleve el nombre o la marca comercial de una persona física o jurídica establecida fuera de la Unión”.

42 “toda persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercializa un sistema de IA en el mercado de la Unión sin influir sobre sus propiedades”.

El segundo grupo –“de alto riesgo”- comprende aquellos sistemas de IA que comportan un riesgo elevado para la salud y la seguridad de las personas físicas o sus derechos fundamentales. La propuesta de reglamento ha optado por acompañarse de un anexo en el que identifica cuáles son los sistemas de IA calificados como de “alto riesgo”⁴³. Sin menoscabo de las posibles modificaciones que se realizan por la Comisión en un futuro próximo, la propuesta de reglamento clasifica los sistemas de alto riesgo en dos categorías principales, por un lado, aquellos diseñados para utilizarse como componentes de seguridad de productos sujetos a una evaluación previa de conformidad por terceros; y por otro, aquellos que, siendo independientes, tengan implicaciones con los derechos fundamentales expresamente indicados en el anexo III.

Con una finalidad de prevención, se establece un sistema de gestión de riesgos asociado a cualquier sistema de IA de alto riesgo que funcionará “ex ante”. De este modo, se fija una serie de requisitos que han de cumplir durante la vida del sistema. Estos requisitos -recogidos en el capítulo 2, del Título III- se refieren a diversos apartados (datos y gobernanza, documentación técnica, registro, transparencia y comunicación a los usuarios, vigilancia humana, precisión, solidez y ciberseguridad).

Además, se establece un conjunto de obligaciones que habrán de cumplir, por un lado, los operadores (proveedores -arts. 16 ss.-, fabricantes de productos -art. 24-, representantes autorizados -art. 25-, importadores, -art. 26- y distribuidores -art. 27) y los usuarios de estos sistemas de alto riesgo (art. 29). Estas obligaciones se amplían con otras nuevas -de transparencia- cuando los sistemas de IA impliquen riesgos específicos de manipulación. También se exige informar a las personas físicas cuando el sistema de IA interactúa con ellas, se dedique a detectar sus emociones o la asocie con categorías concretas o incluso cuando genere o manipule el contenido de imagen, sonido o vídeo que pueda inducir las a confusión y pensar que son auténticos o verídicos (art. 52).

Estas medidas no se limitan a la introducción y comercialización de los sistemas de IA de alto riesgo, sino que se exige un seguimiento posterior conforme a un plan (art. 61) y el intercambio de información sobre los incidentes graves y fallos de funcionamiento que puedan tener lugar en el mercado (art. 62).

43 En concreto, en el anexo se clasifican los sistemas de IA de alto riesgo en ocho ámbitos diferentes: “Identificación biométrica y categorización de personas físicas”, “Gestión y funcionamiento de infraestructuras esenciales”, “Educación y formación profesional”, “Empleo, gestión de los trabajadores y acceso al autoempleo”, “Acceso y disfrute de servicios públicos y privados esenciales y sus beneficios”, “Asuntos relacionados con la aplicación de la ley” (desde la perspectiva del seguro, suscita un cierto interés el punto b relativo a los “sistemas de IA destinados a utilizarse para evaluar la solvencia de personas físicas o establecer su calificación crediticia, salvo los sistemas de IA puestos en servicio por parte de proveedores a pequeña escala para su uso propio), “Gestión de la migración, el asilo y el control fronterizo”, “Administración de justicia y procesos democráticos”.

Por otro lado, se establecen medidas de apoyo a la innovación, a través de la creación de espacios controlado de pruebas para la IA, frecuentemente conocidos como “sandbox”, de regulación reciente en nuestro ordenamiento (Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero)⁴⁴. Así, antes de su implementación en el mercado, determinados sistemas de IA podrán contar, durante un período limitado, con un entorno operativo controlado que les permita ser objeto de prueba, desarrollo y validación (art. 53). En modo alguno, la creación de tales espacios controlados puede reducir las facultades de supervisión y vigilancia atribuidas a las autoridades competentes⁴⁵. La propuesta fija un marco básico en términos de gobernanza, supervisión y responsabilidad; reduciendo la carga normativa a las pymes y a las empresas emergentes a fin de que también puedan aprovechar estas medidas en favor de la innovación.

Finalmente, la propuesta da cabida a la elaboración de Códigos de Conducta entre los operadores que sirva como mecanismo útil para promover la aplicación voluntaria de los requisitos exigidos en la norma⁴⁶. Especialmente, se está pensando en los sistemas de IA que no son de alto riesgo y, por tanto, no se encuentran obligados a su cumplimiento (art. 69).

IV. LAS IMPLICACIONES JURÍDICAS DE LA INTELIGENCIA ARTIFICIAL (IA) EN EL DERECHO DEL SEGURO.

I. Significación jurídica.

La orientación de este cambio de paradigma está caracterizada por el influjo de la IA y sus múltiples aplicaciones. Por ello, conviene profundizar en su significado y en su repercusión sobre la visión cada vez menos tradicional del sector asegurador.

44 BOE, núm. 300, de 14 de noviembre de 2020.

45 La norma, además, se preocupa, por ordenar los mecanismos de gobernanza y aplicación de las propuestas mencionadas. A nivel europeo, se crea un Comité Europeo de Inteligencia Artificial que tiene como misión facilitar la implementación del Reglamento entre los Estados miembros y la cooperación entre las autoridades nacionales (Título VI, capítulo I, arts. 56-58). A nivel nacional, cada Estado habrá de designar una autoridad competente en la aplicación y ejecución del Reglamento (art. 59). Este órgano tendrá, entre otras, la función de vigilancia del mercado y control de los sistemas de IA, en coordinación con el Comité Europeo y el resto de los órganos propios de cada Estado miembro (arts. 63 ss.).

46 Sin poder ser calificado como un Código de Conducta, no podemos dejar de hacer referencia al Informe recientemente publicado por EIOPA, titulado *Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the european insurance sector. A report from EIOPA's Consultative Expert Group on Digital Ethics in insurance* (Luxembourg, 2021). Como es sabido, EIOPA es una de las tres Autoridades Europeas de Supervisión (junto con la EBA y la ESMA), por lo que tal informe desempeña un papel muy relevante en la elaboración de los futuros Códigos de Conducta. Sin menoscabo de su valor, no deja de llamar la atención la percepción que EIOPA -en este informe- tiene de qué es la ética, fundándola en normas legales y/o en el criterio de la mayoría: “Ethics is thought to mean approaches that are fair based on international and national recommendations, standards and treaties, and of course legislation. Our understanding is that this represents what most people would understand as ethical”.

Es evidente que la IA supone un impulso innovador indiscutible en el diseño, distribución y comercialización de los productos de seguro. Gracias a ello, se consiguen reducir los costes operativos de la actividad aseguradoras y ofrecer al mercado productos más personalizados, en beneficio tanto de las empresas como de los clientes. En este sentido, la tecnología aplicada al seguro dispone de una serie de instrumentos útiles para el asesoramiento automatizado, la evaluación de los riesgos y la gestión de un número ingente de datos en el sector asegurador⁴⁷. De este modo, la compañía aseguradora podrá interrelacionar una gran cantidad de información que le permita predecir eventos futuros y mejorar la calidad del producto asegurador acomodándola a las características del propio cliente.

No obstante, tales instrumentos no dejan de suscitar dudas a la hora de delimitar las implicaciones jurídicas que esta nueva revolución digital implica en el sector asegurador. Así, conviene no olvidar que la mera automatización y acumulación de datos no entraña sustituir el análisis y reflexión imprescindible sobre su contenido⁴⁸. Las consecuencias de su desatención repercuten negativamente en el resultado final, sin que pueda obviarse, por otro lado, las consecuencias jurídicas del recurso a su empleo. De entre ellas, cabe resaltar, por su gran importancia en nuestro estudio, dos muy relevantes, en concreto, nos referimos, por un lado, a la falta de neutralidad de la IA⁴⁹, y, por otro, al riesgo de seguridad jurídica inherente a un empleo sin control de los datos correspondientes a los asegurados.

Además, la aplicación de los sistemas de IA puede causar no sólo daños sino un tratamiento discriminatorio a los consumidores, excluyendo a los más vulnerables de su cobertura aseguradora. Por ello, la normativa ahora vigente y la pendiente de incorporación a nuestro ordenamiento⁵⁰ no podrán ignorar

47 Así, v. MARTÍNEZ-GIJÓN MACHUCA, P.: “Diseño”, cit., pp. 226-227; FELIU REY, J.: “Tecnología y seguro: la automatización (*smart contracts*)”, RES, núm. 117, 2019, pp. 54 ss. Igualmente, cabe destacar la Resolución aprobada por el Parlamento Europeo, de 17 de mayo de 2017, sobre la tecnología financiera, en la que se pone también de manifiesto la aparición de nuevos riesgos, como por ej. los llamados “riesgos cibernéticos”, que se mencionan más adelante.

48 ALARCÓN FIDALGO, J.: “El futuro Libro Blanco de las insurtech”, *Revista Española de Seguros (RES)*, núm. 180, 2019, p. 374.

49 Como recuerda S. LANDINI: “Insurtech”, cit., p. 10, una de las claves que se suelen destacar en la comunicación electrónica a nivel comunitario es la “neutralidad tecnológica”. Así, se recoge entre los objetivos generales en el art. 3.4.c del “Código Europeo de Comunicaciones Electrónicas” (aprobado por la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018). Además, las Autoridades nacionales cuando regulen el acceso a los operadores al mercado electrónico, deberán tener en cuenta “la necesidad de garantizar una neutralidad tecnológica que permita a las partes diseñar y gestionar sus propias redes” (art. 7.2.c Directiva 2018/1972). En realidad, se trata de velar por la competencia en el mercado y fomentarla, favoreciendo el acceso de nuevos operadores y evitando obstáculos que perjudiquen la libertad de elección de los usuarios, porque se imponga o discrimine el uso de una tecnología en favor de otra.

No obstante, este principio de neutralidad tecnológica difiere de la falta de neutralidad que ahora comentamos. En este punto, nos referimos al hecho de que los sistemas de IA son implementados por las propias entidades aseguradoras, velando por su propio interés, y, por ello, su postura sea subjetiva o no neutral, respecto a los intereses propios de los consumidores de seguros.

50 Tanto la normativa de distribución - Real Decreto-ley 3/2020, de 4 de febrero- como el Reglamento Delegado (UE) 2017/2358 de la Comisión, de 21 de septiembre de 2017 y el más reciente -pendiente de incorporación y que modifica al anterior- Reglamento Delegado de 21 de abril de 2021. Sobre el tema,

estas consecuencias negativas que, en un futuro no tan lejano, implicará esta nueva tecnología digital en el mercado, en los operadores económicos y en sus clientes⁵¹, siendo imprescindible la adopción de medidas tuitivas, especialmente a estos últimos⁵². Al respecto, cabe advertir que tales medidas deben adoptarse en armonía con el papel innovador de estas nuevas tecnologías en el mercado asegurador, sin que puedan significar un obstáculo a su desarrollo.

De tal modo, el objetivo debería consistir en analizar e identificar cuáles son los riesgos que la aplicación de los sistemas de IA puede causar en toda la cadena de valor de los seguros y que, frecuentemente, afectan a los clientes. La innovación de los sistemas de IA es fruto del obrar humano y, por tanto, pueden también corregirse sus efectos -potencialmente- nocivos; así, se consigue aprovechar la innovación en el sentido pretendido por la Unión Europea, es decir, a fin de alcanzar una IA fiable conforme a los principios éticos de respeto de la autonomía humana, prevención del daño, equidad y explicabilidad⁵³.

2. Transparencia y protección del consumidor de seguros.

En conexión con el apartado anterior, la propuesta pone también el foco de atención en la necesidad de seguridad, transparencia y rendición de cuentas en la información facilitada a los clientes⁵⁴. Como se recuerda, la "materia prima" en el mercado asegurador es la información. La digitalización del mercado influye decisivamente en su acceso, empleo y circulación entre los operadores y, de forma especial, en los consumidores y usuarios⁵⁵. La protección de estos últimos es uno

v. MARTÍNEZ-GIJÓN MACHUCA, P.: "Diseño, aprobación, control y distribución de productos de seguro", RES, núms. 185-186, 2021, pp. 217 ss. Más recientemente, del mismo autor, v. "Requisitos en el diseño, aprobación y control de productos de seguro y en materia de gobernanza (a propósito del artículo 185 del real decreto-ley 3/2020, de 4 de febrero)", en AA. VV.: *Transparencia y competitividad en el mercado asegurador*, cit. pp. 86 ss., quien advierte del control más exhaustivo y la exigencia de un mayor desarrollo por los nuevos sistemas de IA.

- 51 Así, cabe destacar, entre los operadores económicos, la aparición de nuevas figuras, como las plataformas de aseguramiento colaborativo (*peer to peer*), los comparadores de seguros, los agregadores de información de seguros, el asesoramiento robotizado, etc. Sobre el tema, v. TAPIA HERMIDA, A.J.: "Insurtech", cit., pp. 549.
- 52 Es cierto, como se ha puesto de relieve entre nosotros (MARTÍNEZ-GIJÓN MACHUCA, P.: "Requisitos en el diseño", cit., p. 96), la resistencia -cuando no el escaso interés- de las entidades aseguradoras por la promoción de los sistemas de IA en las pólizas ya existentes (especialmente, por el aumento del coste que tendría en la prima y su posible perjuicio frente a otros competidores), pero no menos cierto es que el mercado de seguros es abierto y pueden entrar nuevos competidores con un grado mayor de desarrollo en sus seguros con sistemas de IA.
- 53 Así, v. las *Directrices éticas para una IA fiable* elaboradas por el "Grupo de expertos de alto nivel sobre inteligencia artificial" (creado por la Comisión Europea en 2018) y publicadas en abril de 2019. Puede consultarse en: <https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>.
- 54 Esta exigencia de transparencia se recoge en la normativa de distribución respecto de los mismos sujetos implicados en la actividad aseguradora, tanto públicos (así, las exigencias a la DGSFP, v. art. 7.2 norma de distribución), como privados (aparte de las entidades aseguradoras, también a los mediadores de seguros, la misma norma de distribución, art. 8.3).
- 55 Como es sabido, la digitalización se corresponde a una tecnología de información caracterizada por el tratamiento de los datos y de las infraestructuras creadas para su desarrollo ("software" y "hardware"). Sobre este tema, v. HOFFMANN-RIEM, W.: *Big Data. Desafíos también para el Derecho*, Aranzadi, Cizur Menor,

de los pilares fundamentales del Derecho de la Unión Europea y, por ello, la regulación en el empleo de la IA, la robótica y las tecnologías conexas, requieren, en especial, de transparencia en sus mecanismos de actuación internos y externos, entre operadores y con consumidores y usuarios⁵⁶.

La digitalización también afecta a la protección de los consumidores. No se escapa de nuestra atención la “conversión” de las entidades aseguradoras en uno de los principales “consumidores” de big data. Se trata de una herramienta que les va a permitir conocer con un mayor detalle cuál es el perfil de sus posibles asegurados. En cierto modo, se puede hacer referencia a un incremento exponencial de tal información y a su influencia decisiva en la contratación de seguros⁵⁷.

Sin menoscabo de las ventajas que ello puede ocasionar, cabe no olvidar que éstas, en principio, repercutirían sobre la industria aseguradora, pero no necesariamente sobre los usuarios y consumidores de seguros, que incluso pueden ver mermado aún más su posición⁵⁸.

Con tal finalidad, cabe subrayar la importancia de contar con un marco regulador para la IA aplicable en aquellos casos en que los consumidores y usuarios estén sujetos a un sistema algorítmico, sean sus destinatarios o estén orientados a él. La normativa, en aras de la seguridad jurídica, debe aplicarse a todos los desarrolladores y a toda la cadena de valor y garantizar un alto nivel de protección a los consumidores.

3. La exigencia de un control de los riesgos.

Desde la perspectiva aseguradora, cabe destacar, por un lado, que la IA, la robótica y las tecnologías conexas son determinadas por los seres humanos

2018. Suscita especial interés la transmisión de estos datos en las diversas fases contractuales y el empleo de “soportes digitales” duraderos en sustitución del empleo tradicional del papel (v. art. 56 norma de distribución, RD-L 3/2020, de 4 de febrero).

56 Cabe atender al Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y a la normativa española (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, LOPD). En consonancia con el régimen general, y desde la perspectiva aseguradora, la normativa de ordenación también detalla, pormenorizadamente, la protección de datos de carácter personal de tomadores, asegurados, beneficiarios o terceros perjudicados (art. 99 LOSSEAR).

Igualmente, resulta relevante la propuesta formulada por EIOPA en su informe de 2019 (“Report on best practices ...”, cit., p. 31) alentado a las autoridades nacionales de supervisión a exigir una información clara y precisa a las plataformas P2P. En concreto, se demanda a los proveedores de estas plataformas que informes a los consumidores que no son entidades sujetas a supervisión y, por tanto, su nivel de protección es mucho menor al de las entidades que sí lo están.

57 Sobre esta función de los big data, v. MUÑOZ PAREDES, M. L.: “El ‘big data’ y la transformación del contrato de seguro”, en AA. VV.: *Dimensiones y desafíos del seguro de responsabilidad civil* (dir. por A. B. VEIGA COPO), Civitas, Madrid, 2021, pp. 1017 ss. ALARCÓN FIDALGO, J.: “Big data, blockchain y algoritmos y su repercusión en la contratación de seguros”, en AA. VV.: *Transparencia y competitividad*, cit., pp. 33 ss.

58 Sobre este punto, v. el informe elaborado por la BEUC “The use of big data and artificial intelligence in insurance” (ref: BEUC-X-2020-039), de fecha 19 de marzo de 2020. En dicho informe, se pone de manifiesto los nuevos riesgos -especialmente de discriminación- que puede generar el empleo de la “big data” por la industria aseguradora en los consumidores y usuarios.

y que sus elecciones son las que determinan su verdadero potencial. Por otro lado, el marco regulador de la Unión Europea para la IA ha de ser adecuado y proporcionado y debe ser objeto de una minuciosa evaluación. Esta evaluación requiere, además, un análisis específico de los riesgos y obstáculos que puede suscitar en las innovaciones y en las pymes. Como se ha apuntado con anterioridad, la solución no puede ser única, sino que dependerá de cada riesgo afectado. Igualmente, el marco regulador debe evitar la fragmentación del mercado y fomentar las actividades de inversión e investigación. Ello explica la necesidad de contar con obligaciones jurídicas comunes y principios éticos, como se pretende en las propuestas comunitarias examinadas en los epígrafes precedentes.

De esto modo, el legislador comunitario propone un control de riesgos en la digitalización del sector asegurador. La IA, la robótica y las tecnologías conexas deben considerarse de alto riesgo y, por lo tanto, estar sujetas al obligado cumplimiento de las obligaciones jurídicas y los principios éticos tal como se establecen en el marco regulador para la IA, es necesario basarse siempre en una evaluación *ex ante* imparcial, regulada y externa apoyada en criterios concretos y definidos. El resultado permite poner de manifiesto la interconexión entre dos aspectos claves: la transparencia en el proceso contractual y la controvertible independencia de los algoritmos⁵⁹.

4. Nuevos riesgos ligados a la aplicación de la IA.

Finalmente, no podemos concluir el trabajo sin recordar, en primer lugar, las múltiples aplicaciones de la IA en sectores muy relevantes del seguro (marítimo, transporte, automóvil, industria, salud, ...) o en otros nuevos (por ej., el aseguramiento de los robots⁶⁰). En estos ámbitos, se ha manifestado la existencia de diversos proyectos de innovación ligados a la IA, como por ejemplo el promovido por UNESPA en la declaración de accidentes en el seguro de automóviles, mediante el empleo de las nuevas tecnologías, IA y digitalización⁶¹. Y también los llamados "open insurance", nueva modelo de negocio que se postula como un instrumento tecnológico avanzado en el que los operadores económicos y otras entidades intercambian una gran cantidad de información y datos⁶². Ello

59 Sobre este punto, y desde la perspectiva del Derecho de sociedades, cabe atender al trabajo del prof. N. Abriani, "La corporate governance nell'era dell'algoritmo Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla corporate governance" (*Il nuovo Diritto delle Società*, núm. 3, 2020, pp. 261 ss.) en el que se pone de manifiesto los riesgos inherentes a la incorporación de los sistemas de IA en la adopción de decisiones en el órgano de administración y, en especial, las situaciones de conflicto de intereses.

60 BADILLO ARIAS, J. A.: "La responsabilidad civil y el aseguramiento obligatorio de los robots" en AA. VV., *Retos y desafíos*, cit., pp. 913 ss.

61 ALARCÓN, J.: "El futuro", cit., p. 374.

62 Este modelo de negocio está basado en la existencia de una gran cantidad de datos con los que cuentan sus partícipes y las funciones esenciales que desempeñan son comunes al de cualquier empresa de datos: consumir, compartir y colaborar.

se pretende crear nuevos productos de seguros, mejorar la cadena de valor y su eficiencia, ofreciendo un producto más personalizado y ajustado a sus clientes⁶³. No obstante, cabe considerar los riesgos de que tal intercambio de información entre entidades pueda ser calificado, en cierto modo, como un acuerdo anticompetitivo y, por tanto, prohibido⁶⁴. Ello requiere una atención especial por el legislador español y comunitario para diferenciar entre la mera circulación de datos y lo que es propiamente un acuerdo anticompetitivo entre empresas de seguros⁶⁵.

Y, en segundo lugar, cabe destacar que la actividad desarrollada por los sistemas de IA suscita -y genera- nuevos riesgos necesitados de cobertura. Ello implica la necesidad de contratar nuevas coberturas para los llamados “riesgos cibernéticos”⁶⁶, que representan uno de los más frecuentes peligros existentes en la innovación y entraña una dificultad evidente en su configuración contractual por las entidades aseguradoras⁶⁷.

Claro ejemplo de la dificultad de tales “coberturas cibernéticas” (pérdida de datos, interrupción del negocio, responsabilidad, ...) se refleja en su habitual concurrencia como una pluralidad de riesgos en un mismo siniestro. O la existencia de nuevos riesgos generados por el “cloud computing”, en cuanto que las TIC ofrecen un “ambiente” más vulnerable y problemático. Junto a ello, cabe también poner de manifiesto la problemática de la materialización de tal riesgo en un daño. El recurso a la compensación de daños no parece la solución más eficaz, pues concurre no sólo la dificultad de delimitarlo sino también una cadena interminable de pérdidas sufridas (“an interminable chain of losses and events prejudicial”)⁶⁸.

63 Al respecto, puede ser interesante la consulta del “discussion paper” elaborado por EIOPA sobre el tema, v. en <https://www.eiopa.europa.eu/content/open-insurance-accessing-and-sharing-insurance-related-data>. Sobre el mismo, con carácter crítico, v. LANDINI, S.: “Insurtech”, cit., pp. 16 ss. Por otro lado, y con carácter explicativo del significado y funcionamiento del “open insurance”, v. el blog de la empresa Accenture: <https://insuranceblog.accenture.com/the-ultimate-guide-to-open-insurance>.

64 Al respecto, y desde la perspectiva italiana, la prof. S. LANDINI (“Insurtech”, cit., p. 18) llama la atención sobre los riesgos a la competencia y la postura de las autoridades italianas de mercado.

65 *Ibidem*.

66 Téngase en cuenta el crecimiento exponencial de los seguros cibernéticos. Según el último informe de Global Data (“Cyber Insurance, 2021 Update – Thematic Research”), las primas brutas suscritas en 2021 alcanzaron un valor de 7.000 millones de dólares -que representaba un crecimiento del 33,5% respecto del año anterior- y se prevé que en 2025 alcance los 20.600 millones de dólares.

67 Sobre el tema, v. recientemente, desde la perspectiva contractual, ILLESCAS, R.: “Ciberriesgos y su aseguramiento: lineamientos contractuales”, en AA. VV.: *Transparencia y competitividad*, cit., pp. 20 ss., quien, ante su escasa regulación, propone el establecimiento del “ciberriesgo” como un nuevo ramo de seguro vinculado a la electrónica (*ibidem*, p. 27). Igualmente, v. ALARCÓN FIDALGO, J.: “Big data, blockchain y algoritmos y su repercusión en la contratación de seguros”, en AA. VV.: *Transparencia y competitividad*, cit., pp. 29 ss.

68 Así, S. LANDINI: “Insurtech”, cit., p. 11. No obstante, el mercado de los seguros cibernéticos está, actualmente, experimentando una creciente expansión -v. las cifras indicadas en la nota 64- con altos límites de cobertura y tarifa plana, que, progresivamente, van a ir reduciéndose y aumenta la prima al compás de la cadena interminable de daños mencionada por la autora. Sin embargo, se prevé un fuerte crecimiento de las primas suscritas a partir de los próximos años por el crecimiento de estos fenómenos, que se han visto incrementados a raíz de la pandemia.

Por ello, se considera más adecuada actuar en la búsqueda de medidas preventivas a fin de evitar los efectos tan perjudiciales que causa la realización del daño⁶⁹.

Igualmente, la utilización de información genética en determinados seguros implica la necesidad de contar con un tratamiento jurídico específico que determine el derecho o no de la aseguradora de acceder y utilizar los datos genéticos de los asegurados, incluso en los casos de concurrencia de un riesgo de discriminación⁷⁰.

También cabe indicar como la piratería informática tiene consecuencias muy graves en diferentes sectores de la actividad económica y paraliza el funcionamiento de los sistemas tecnológicos más avanzados⁷¹. Igualmente, el secreto empresarial es uno de los puntos más afectados por estas prácticas en las empresas y ponen en riesgo su gestión y crecimiento, especialmente en las pequeñas y medianas empresas y en el buen funcionamiento del mercado.

En definitiva, todo este complejo entramado de riesgos cibernéticos demanda de la propuesta de reglamento comunitario la adopción de medidas preventivas -especialmente ante los ciberataques- y la configuración de un seguro adecuado a las nuevas necesidades y a la complejidad creciente generada por la IA y su empleo por las empresas y otros operadores económicos del tráfico.

69 *Ibidem*.

70 En este sentido, cabe considerar las críticas recibidas por la BEUC a la Propuesta de Reglamento antes analizada e importante considerar también las cuestiones éticas relevantes a la luz de los seguros abiertos. Además de lo que dijo la EIOPA en su documento, vemos un problema particular de discriminación. El análisis de Big Data por parte de las compañías de seguros podría conducir a evaluaciones de riesgo hiperpersonalizadas, dejando a ciertos y posiblemente segmentos más amplios de consumidores "no asegurables". Es importante encontrar formas de coberturas para esas personas. En seguros de salud podría ser importante promover formas de mutualidad (Ver informe BEUC sobre "El uso de big data e inteligencia artificial en seguros", MAYO 2020). Sobre este tema, v. recientemente, MUÑOZ PAREDES, M. L.: "La discriminación de los asegurados en el precio del contrato fijado con uso del *Big Data*" en AA. VV.: *Transparencia y competitividad*, cit., pp. 224 ss.

71 Sin entrar en otro tipo de actividades, de carácter delictivo, como la llamada "agresión electrónica", que se concreta en los supuestos de robo de identidad o acoso.

BIBLIOGRAFÍA

AA. VV.: *El contrato de seguro y su distribución en la encrucijada* (dir. por P. GIRGADO PERANDONES), Aranzadi, Cizur Menor, 2018.

AA. VV.: *La distribución de los seguros privados* (dir. por J. BATALLER GRAU y M. R. QUINTÁNS EIRAS), Marcial Pons, Madrid, 2019.

AA. VV.: *Un Derecho del seguro más social y transparente* (dir. por J. BATALLER GRAU y M. J. PEÑAS MOYANO), Aranzadi, Cizur Menor, 2017.

ALARCÓN FIDALGO, J.: "Big data, blockchain y algoritmos y su repercusión en la contratación de seguros", en AA. VV.: *Transparencia y competitividad en el mercado asegurador* (coord. por GIRGADO PERANDONES, P./ GONZALES BUSTOS, J. P), Comares, Granada, 2021, pp. 28 ss.

ALARCÓN FIDALGO, J.: "El futuro Libro Blanco de las insurtech", *Revista Española de Seguros (RES)*, núm. 180, 2019, pp. 373-395.

ATIENZA NAVARRO, M. L.: "La responsabilidad civil por daños causados por sistemas de inteligencia artificial" en AA. VV., *Retos y desafíos del contrato de seguro: del necesario aggiornamento a la metamorfosis del contrato. Libro Homenaje al profesor Rubén Stiglitz* (dir. por A. B. VEIGA COPO), Civitas, Madrid, 2020, pp. 1093-1104.

BADILLO ARIAS, J. A.: "La responsabilidad civil y el aseguramiento obligatorio de los robots" en AA. VV., *Retos y desafíos*, cit., 913-954.

BENITO OSMA, F.: "El mercado digital de seguros", en AA. VV.: *Transparencia y competitividad*, cit., pp. 42 ss.

BENITO OSMA, F.: "Vehículos y sistemas inteligentes en la circulación: responsabilidad civil y seguro", *RES*, núm. 173, 2018, pp. 43-61.

BENITO OSMA, F.: *La transparencia en el mercado asegurador*, Comares, Granada, 2021.

EIOPA ("European Authority on Insurance and Pensions Funds"), *Report on best practices on licencing requirements, peer-to-peer insurance and the principle of proportionality in an insurtech context*, EIOPA, Luxembourg, 2019.

EIOPA, "Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the european insurance sector. A report

from EIOPA's Consultative Expert Group on Digital Ethics in insurance", EIOPA, Luxembourg, 2021.

FELIU REY, J.: "Tecnología y seguro: la automatización (*smart contracts*)", *RES*, núm. 117, 2019, pp. 53-80.

FERNÁNDEZ DE LIS, S./URBIOLA ORTÚN, P.: "Transformación digital y competencia en el sector financiero", *Información Comercial Española (ICE)*, núm. 905, 2018, pp. 73-82.

FERNÁNDEZ MANZANO, L. A.: "Insurtech: ¿revolución o evolución? una aproximación a los desafíos regulatorios y contractuales que plantea la aplicación de la tecnología en el sector asegurador" en AA. VV., *Retos y desafíos*, cit., pp. 955-986.

ILLESCAS, R.: "Ciberriesgos y su aseguramiento: lineamientos contractuales", en AA. VV.: *Transparencia y competitividad*, cit., pp. 20 ss.

LANDINI, S.: "Insurtech: Innovation in production, distribution, governance and supervision in the insurance market", en AA. VV.: *Transparencia y competitividad*, cit., pp. 9 ss.

LÓPEZ ONETO, M.: *Fundamentos para un Derecho de la inteligencia artificial*, Tirant lo Blanch, Valencia, 2020.

MARTÍNEZ-GIJÓN MACHUCA, P.: "Diseño, aprobación, control y distribución de productos de seguro", *RES*, núm. 185-186, 2021, pp. 217-238.

MARTÍNEZ-GIJÓN MACHUCA, P.: "Requisitos en el diseño, aprobación y control de productos de seguro y en materia de gobernanza (a propósito del artículo 185 del Real Decreto-Ley 3/2020, de 4 de febrero)", en AA. VV.: *Transparencia y competitividad*, cit., pp. 86 ss.

MUÑOZ PAREDES, M. L.: "El 'big data' y la transformación del contrato de seguro" en AA. VV., *Dimensiones y desafíos del seguro de responsabilidad civil* (dir. por A. B. VEIGA COPO), Aranzadi, Pamplona, 2021, pp. 1017-1052.

PASTOR SEMPERE, M. C.: *Economía digital sostenible*, Pamplona, ed. Aranzadi, 2020.

TAPIA HERMIDA, A. J.: "Insurtech" en AA. VV., *Revolución digital, derecho mercantil y Token economía* (dir. por A. F. MUÑOZ PÉREZ), ed. Tecnos, Madrid, 2019, pp. 545-559.

TAPIA HERMIDA, A.J.: "Anteproyecto de Ley de medidas para la transformación digital del sistema financiero", *Revista de Derecho Bancario y Bursátil (RDBB)*, núm. 152, 2018, págs. 355-360.

URÍA FERNÁNDEZ, F./ REQUEIJO TORCAL, Á.: "Insurtech. Retos y desafíos de cara a la nueva distribución y contratación de seguros", *RES*, núm. 169, 2017, pp. 3-94.

VEIGA COPO, A. B.: *Seguro y Tecnología. El impacto de la digitalización en el contrato de seguro*, Civitas, Madrid, 2020.

ZURITA MARTÍN, I.: "Las propuestas de reforma legislativa del Libro Blanco Europeo sobre inteligencia artificial en materia de seguridad y responsabilidad civil", *Actualidad Jurídica Iberoamericana (AJI)*, núm. 14, 2021, pp. 438 ss.

