FACULTAD DE DERECHO

RÉGIMEN JURÍDICO APLICABLE A LA INTELIGENCIA ARTIFICIAL: ANÁLISIS DEL REGLAMENTO (UE) 2024/1689 DE INTELIGENCIA ARTIFICIAL Y SUS CONSECUENCIAS PARA EL DERECHO CIVIL ESPAÑOL

Autor: Tomás Moré Sebastián

4ºE-5 FIPE

DERECHO CIVIL

Tutora: Guillermina Yanguas Montero

MADRID

31 DE MARZO DE 2025

RESUMEN

El TFG tiene por objeto analizar el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de Inteligencia Artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), y los desafíos derivados de la utilización de tecnologías de Inteligencia Artificial. Se analizará cómo afecta esta norma al Derecho español, con especial mención a las obligaciones que impone en el derecho de daños, el derecho de propiedad intelectual y el derecho de contratos, desde la perspectiva de los contratos de seguros.

Palabras clave: Inteligencia Artificial, Reglamento de Inteligencia Artificial, sistemas de alto riesgo, derecho de daños, propiedad intelectual, contratos de seguros

ABSTRACT

This paper aims to analyse Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) No. 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU (EU) 2019/2144. No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), and the challenges arising from the use of artificial intelligence technologies. It will also explore how this regulation affects Spanish law, with special mention to the obligations it imposes regarding damages, intellectual property law, and contract law from the perspective of insurance agreements.

Keywords: Artificial Intelligence, Artificial Intelligence Act, high risk systems, damages, intellectual property law, insurance agreements

TABLA DE CONTENIDOS

IV. IMPACTO DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL SOBRE EL DERECHO CIVIL ESPAÑOL

1. IMPACTO DEL REGLAMENTO DE INTELIGENCIA ARTIFICAL EN EL DERECHO DE DAÑOS ESPAÑOL
2. IMPACTO DEL REGLAMENTO DE INTELIGENCIA ARTIFICAL EN EL DERECHO DE PROPIEDAD INTELECTUAL ESPAÑOL
3. IMPACTO DEL REGLAMENTO DE INTELIGENCIA ARTIFICAL EN EL DERECHO CONTRACTUAL ESPAÑOL DESDE LA PERSPECTIVA DE LOS CONTRATOS DE SEGUROS

V. CONCLUSIONES

VI. BIBLIOGRAFÍA

I. INTRODUCCIÓN

1. OBJETO DE ESTUDIO

El objeto de este Trabajo de Fin de Grado (TFG) es el **análisis del régimen jurídico aplicable a la Inteligencia Artificial (IA)**, en especial del **Reglamento (UE) 2024/1689** del Parlamento Europeo y del Consejo (Reglamento de Inteligencia Artificial). Este Reglamento establece normas armonizadas dentro de la Unión Europea para la regulación de la IA. El presente trabajo examina sus implicaciones específicas para el **Derecho civil español** con el objetivo de evaluar cómo esta normativa encaja en el marco jurídico nacional y su posible impacto para los actores involucrados.

Tras un análisis conceptual sobre los Sistemas de Inteligencia Artificial, sus tipos y sus sectores de aplicación, el trabajo aborda la regulación objeto de estudio desde los **desafíos éticos y jurídicos** que plantea la expansión de la IA, tales como la **privacidad y protección de datos**, la **transparencia**, los **sesgos y la discriminación**, y la **responsabilidad** en la toma de decisiones autónomas.

Se analiza el contenido del Reglamento de forma general para después profundizar en las obligaciones que impone y su impacto en áreas como el derecho de daños, la propiedad intelectual, o los contratos de seguros.

El TFG también incluye un estudio sobre las **propuestas legislativas** en el ámbito europeo, como la **Directiva** relativa a la responsabilidad por daños causados por productos defectuosos. Este estudio permite una comparación de cómo el Reglamento (UE) 2024/1689 se inserta en un marco regulatorio más amplio, dirigido a hacer frente a los riesgos asociados al uso de tecnologías de IA, y puede ser útil para establecer predicciones sobre futuros desarrollos.

2. JUSTIFICACIÓN DEL TEMA

La **Inteligencia Artificial (IA) se ha desarrollado de forma frenética en los últimos años impulsada por la aparición de modelos de lenguaje generativos como Chat GPT o Copilot.** Puede apreciarse un interés entre las grandes empresas tecnológicas en lograr su adaptación a múltiples sectores clave, desde la sanidad hasta el transporte y las finanzas. No se trata de una cuestión meramente teórica. Es un hecho que la

Inteligencia Artificial está transformando profundamente la manera en que las sociedades operan. Sin embargo, su integración plantea **importantes desafíos jurídicos y éticos**, ya que muchos sistemas de IA no solo influyen en la toma de decisiones, sino que también pueden causar **daños directos o indirectos** a las personas o bienes. Esta cuestión abre un campo crucial para el Derecho, que debe adaptarse a la nueva realidad tecnológica y establecer marcos claros para regular la IA, sin por ello ser excesivamente restrictivo ni impedir la innovación tecnológica.

El **Reglamento (UE) 2024/1689**, conocido como "Reglamento de Inteligencia Artificial," es una de las primeras normas a nivel mundial que establece un marco legal comprensivo para regular la IA. La importancia de este Reglamento radica en que se trata de una **regulación pionera**, cuyo objetivo es **armonizar las reglas** sobre IA en todos los Estados miembros de la Unión Europea y garantizar un uso seguro, ético y responsable de esta tecnología. Dada su novedad y su amplio alcance, resulta fundamental analizar sus disposiciones para comprender su **impacto** en los ordenamientos nacionales. En este trabajo, el análisis se centra en el **Derecho civil español**.

3. EXPLICACIÓN DE LA ESTRUCTURA

La estructura seguida para analizar la cuestión descrita consta de cuatro apartados. El primer apartado aborda el concepto de Inteligencia Artificial desde una perspectiva general e incluye una definición y un análisis de los distintos tipos de IA y sus principales aplicaciones en sectores relevantes tales como la sanidad o el transporte. Tras esta definición, se presentan los principales **retos jurídicos y éticos** que se asocian al uso de la IA.

Posteriormente, en el segundo apartado, se lleva a cabo un **análisis exhaustivo** del Reglamento (UE) 2024/1689 y su interrelación con otras normas europeas y propuestas legislativas en el ámbito de la **responsabilidad civil**. El objetivo principal de este apartado es comprender el alcance y las implicaciones de esta nueva regulación para los Estados miembros, así como su papel en la creación de un marco normativo armonizado para la IA dentro de la Unión Europea.

En el tercer apartado, se estudia el **impacto directo** que el **Reglamento (UE) 2024/1689** tiene sobre el **Derecho civil español** desde la perspectiva de las tres áreas ya

mencionadas. El objetivo es analizar cómo la normativa europea influye en el marco jurídico español y qué **adaptaciones** serán necesarias para asegurar una correcta implementación de la regulación.

El trabajo finaliza con una síntesis de las principales **conclusiones** derivadas del análisis del **Reglamento (UE) 2024/1689** y su impacto en el **Derecho civil español**.

4. OBJETIVOS DEL TRABAJO

La **finalidad** de este trabajo de fin de grado (TFG) es analizar en profundidad el **Reglamento (UE) 2024/1689 sobre Inteligencia Artificial** y su impacto en el **Derecho civil español**. Se estudian las implicaciones éticas y jurídicas que surgen de la intersección de la tecnología y el derecho en este ámbito.

En un momento en el que la Inteligencia Artificial o IA se está convirtiendo en una parte integral de nuestra vida cotidiana, resulta esencial examinar no solo cómo se aplican las normas, sino también cómo estas pueden contribuir a aumentar la confianza en la innovación tecnológica sin por ello limitarla. El trabajo identifica y analiza los desafíos que plantea la IA en el ámbito jurídico, así como la atribución de responsabilidad en caso de daños causados por sistemas de alto riesgo. Igualmente, los dilemas éticos asociados a la **privacidad**, la **transparencia** y los **sesgos algorítmicos**. Este enfoque permite una reflexión sobre la necesidad de equilibrar la innovación tecnológica con la salvaguarda de los derechos de los ciudadanos.

5. MÉTODO

Para estudiar la cuestión descrita, se han consultado una pluralidad de fuentes y se ha empleado el análisis jurídico, la investigación bibliográfica y la reflexión crítica. En el primer capítulo, que trata cuestiones relativas a la definición de Inteligencia Artificial y los principales desafíos éticos y jurídicos que plantea, se ha analizado la doctrina especializada que ha abordado esta cuestión. En los capítulos posteriores, se analizan las disposiciones del Reglamento de Inteligencia Artificial y otra legislación europea asociada.

Se estudian los criterios de clasificación de sistemas de IA según su nivel de riesgo que establece, además de las obligaciones impuestas a los operadores y desarrolladores

de IA, así como los mecanismos de responsabilidad establecidos. Este análisis permite identificar las implicaciones directas del Reglamento en el marco jurídico español, y analizar cómo estas normas afectan a la regulación de la responsabilidad civil y a la protección de los derechos de los consumidores y usuarios.

Finalmente, se exponen conclusiones sobre el posible impacto del Reglamento en el marco normativo español una vez entre plenamente en vigor.

II. LA INTELIGENCIA ARTIFICIAL: CONCEPTOS CLAVE

1. CONCEPTO DE INTELIGENCIA ARTIFICIAL, TIPOS Y APLICACIONES

1.1. Concepto de Inteligencia Artificial

La Inteligencia Artificial (IA) se ha convertido en uno de los campos más transformadores de la tecnología en las últimas décadas, lo que ha causado un impacto significativo en múltiples sectores de la sociedad. En términos generales, podemos decir que la IA hace referencia a la capacidad de máquinas o sistemas informáticos para realizar tareas que tradicionalmente requieren "inteligencia humana". Desde un punto de vista más técnico, el High-Level Expert Group on Artificial Intelligence (HLEG) la define como "sistemas de software (y posiblemente también de hardware) diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital percibiendo su entorno mediante la adquisición de datos, interpretando los datos estructurados o no estructurados recogidos, razonando, o procesando la información, derivada de estos datos y decidiendo la(s) mejor(es) acción(es) a tomar para alcanzar el objetivo dado. Los sistemas de IA pueden utilizar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento analizando cómo se ve afectado el entorno por sus acciones anteriores."[1].

La definición del HLEG es especialmente relevante, además, porque ha sido utilizada como base por el Joint Research Centre (JRC)[2], que es el principal asesor en cuestiones científicas para la Comisión Europea, lo que puede ayudar a entender la perspectiva del legislador europeo en esta materia.

Russell y Norwig[3] clasifican las principales definiciones doctrinales sobre el concepto de IA y realizan una división entre el pensamiento/acción humana, basado en hipótesis y confirmaciones mediante experimentos; y el pensamiento/acción racional, combinación de matemáticas e ingeniería, pero cabe resaltar que según va progresando la

[1] HLEG. (2019). *Una Definición de la Inteligencia Artificial: Principales Capacidades y disciplinas Científicas*. Comisión Europea. Pág. 8.
[2] Samoili, S., Cobo, M. L., Gómez, E., De Prato, G., Martínez-Plumed, F., & Delipetrev, B. (2020). AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence. JRC Technical Reports. Pág. 15.
[3] Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Tercera Edición. Pearson. Pág. 30.

tecnología, esta división va dejando paso a sistemas de IA cada vez más capaces de ofrecer tanto un enfoque humano como uno racional.

1.2. Tipos de Inteligencia Artificial

En términos generales, los sistemas de Inteligencia Artificial se dividen en dos grandes categorías diferenciadas por su funcionamiento: IA débil e IA fuerte.

La principal diferencia entre ambos tipos reside en su funcionamiento. La IA débil se limita a simular la inteligencia humana en un rango limitado y definido previamente para lograr un fin concreto.[4] Un ejemplo de IA débil es Siri, el asistente virtual de Apple que simula precisamente a un asistente humano y ayuda al usuario en sus tareas diarias, pero no es capaz de tomar decisiones autónomas y su eficacia disminuye cuando se le pregunta algo fuera de sus funciones predeterminadas.

La IA fuerte, en cambio, es capaz de replicar la toma de decisiones a través del "machine learning" o aprendizaje automático para aprender de experiencias pasadas y tomar decisiones autónomas.[5] Un ejemplo de IA fuerte son los prototipos de vehículos autónomos como los de Waymo, cuya IA ha demostrado ser capaz de predecir trayectorias de vehículos en escenarios complejos y las interacciones entre ellos en la carretera.[6]

La distinción es relevante precisamente porque esa autonomía que caracteriza a la IA fuerte puede justificar que se le aplique un marco legal más restrictivo que a la IA débil.[7] De hecho, así parece ser, ya que el Reglamento de Inteligencia Artificial establece una clasificación de riesgos asociados a usos específicos de la IA de la que parece intuirse una mayor preocupación del legislador europeo por la IA fuerte. Un gran número de usos asociados a los sistemas de IA fuerte son considerados como de alto riesgo (conducción autónoma), o riesgo inaceptable (actuación policial predictiva), mientras que otros usos más propios de la IA débil son considerados como de riesgo mínimo o nulo (videojuegos).

[4]Martinez, R. (2018). *Artificial intelligence: Distinguishing between types & definitions*. Nevada Law Journal, 19(3), Págs. 1016-1037.
[5]Martinez, R. (2018). *Artificial intelligence: Distinguishing between types & definitions*. Nevada Law Journal, 19(3), Págs . 1016-1037.
[6]Waymo. VectorNet: *Predicting behaviour to help the Waymo Driver make better decisions*. (s.f.). Recuperado el 17 de Octubre de 2024 de https://waymo.com/blog/2020/05/vectornet/
[7]Martinez, R. (2018). *Artificial intelligence: Distinguishing between types & definitions*. Nevada Law Journal, 19(3), Págs. 1016-1037.

1.3. Principales Sectores de Aplicación

El legislador también tiene en cuenta los sectores de aplicación de los Sistemas de Inteligencia Artificial para determinar su riesgo. Si bien es muy probable que la Inteligencia Artificial se acabe extendiendo a prácticamente todas las áreas de trabajo, los sectores más sensibles actualmente son: medicina, transporte, finanzas y defensa.

En la medicina, se prevé el uso de Inteligencia Artificial para, entre otras funciones, realizar diagnósticos, sugerir tratamientos, predecir enfermedades o monitorizar pacientes. Los beneficios de su implementación incluyen el avance de los tratamientos actuales, la disminución de sus costes, y el aumento de la seguridad de los hospitales.[8] Por otro lado, la sensibilidad de este sector radica tanto en el gran impacto que tienen las decisiones médicas sobre la vida de los pacientes y a que los sistemas de IA dedicados a este sector, necesariamente operan con grandes bases de datos médicos personales; lo que necesariamente genera dudas desde el punto de vista de salvaguardar la privacidad del paciente. Por ello, desde los Comités de ética asistencial y clínica (CEA) y los Comités de investigación (CEI) se aboga por el uso de sistemas que anonimicen los datos a los que tengan acceso y que tengan salvaguardias para evitar su reidentificación posterior. También se recomienda mantener en todo momento la supervisión humana de las decisiones y diagnósticos realizados por los sistemas de Inteligencia Artificial, incluso si su nivel de fiabilidad es alto.[9]

En el ámbito del transporte, ya hemos mencionado como distintas plataformas como Waymo están logrando grandes avances a la hora de diseñar vehículos capaces de conducción autónoma. La prioridad en este campo siempre ha de ser la seguridad del conductor del vehículo autónomo, la del resto de vehículos en la vía y la de los peatones. Por ello, la aplicación de la IA en este sector plantea importantes dilemas con respecto a su seguridad y la atribución de responsabilidad por los daños derivados de decisiones tomadas por sistemas de Inteligencia Artificial; dilemas que las instituciones de la Unión Europea tienen especialmente presentes.

[8] Haleem, Abid. Javaid, Mohd (2019). Current status and applications of Artificial Intelligence (AI) in the medical field: An overview. *Current Medicine Research and Practice Journal*, 9 (6), Págs. 231-237. https://www.sciencedirect.com/science/article/abs/pii/S235208171930193X

[9] Ruiz, F. J. B. (2022). Aplicaciones de la inteligencia artificial al ámbito biosanitario: Protección de datos y privacidad. Implicaciones éticas y legales. En *Anales de la Cátedra Francisco Suárez*, 56, Págs. 245-268.

En las finanzas, la implementación de sistemas de IA se está llevando a cabo especialmente en áreas como la concesión de préstamos; la prevención del fraude; predicción de variables económicas y financieras; la gestión de carteras y valoración de activos, y la gestión y trato con los clientes bancarios. El principal beneficio de la aplicación de la IA en este sector es su precisión a la hora de identificar sucesos con base en las directrices dadas con el apoyo de grandes bases de datos. Por otro lado, se pueden exponer consideraciones similares a las expuestas respecto de la privacidad en el uso de la IA en el campo de la medicina, y además, la dificultad a la hora de interpretar los resultados en ciertos supuestos puede reducir su efectividad.[10] Estos problemas de interpretación se derivan de que muchas veces estos sistemas operan como "algoritmos de caja negra", es decir, aquellos sistemas cuya toma de decisiones es tan compleja que ni sus programadores son capaces de predecir la respuesta concreta que va a dar el sistema ante determinadas preguntas, incluso si son modelos altamente fiables.[11]

Por último, el uso de sistemas de Inteligencia Artificial en el ámbito de la defensa plantea especiales consideraciones éticas en el caso de Sistemas de Armas Autónomos (SAA) capaces de planificar ataques y llevarlos a cabo sin necesidad de un operador humano. Por un lado, estos sistemas disminuyen la sobreexposición de soldados a riesgos en operaciones militares y disminuyen el tiempo de respuesta ante un posible ataque, pero también puede llevar a la desensibilización de la comunidad internacional ante conflictos armados al sustituir a los combatientes humanos por robots, y relegar la toma de decisiones estratégicas a sistemas de IA que, como hemos visto, funcionan como cajas negras y no son siempre predecibles incluso para sus propios creadores.[12]

2. DESAFÍOS JURÍDICOS Y ÉTICOS

A medida que la tecnología avanza y la Inteligencia Artificial se integra en sectores clave, como la salud o la seguridad, surgen preguntas fundamentales sobre cómo regular su uso, quién es responsable de sus decisiones y cómo se puede evitar que su

[10]Banco de España. (2022). *Inteligencia artificial y finanzas: una alianza estratégica*. https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/22/Fich/do2222.pdf

[11] Gràcia, X. G. & Sancho-Gil, J. M. (2021). Artificial intelligence in education: Big data, black boxes, and technological solutionism. *International journal of media, technology and lifelong learning*, 17 (2). https://doi.org/10.7577/seminar.4281

[12] Moliner Juan. (2021). Desafíos éticos en la aplicación de la inteligencia artificial a los sistemas de defensa. *Revista DIECISIETE*, Pág 4. DOI: 10.36852/2695-4427_2021_04.06

implementación infrinja derechos fundamentales. Este apartado del trabajo aborda las principales preocupaciones legales y éticas asociadas a la IA, centrándose en cuestiones como la privacidad de los datos, la transparencia de los algoritmos, los sesgos y la discriminación en las decisiones automatizadas.

2.1. Privacidad y Protección de Datos

La cantidad de datos personales recopilados y procesados por los sistemas de Inteligencia Artificial ha incrementado especialmente desde la introducción de modelos de lenguaje generativos como Chat GPT. Estos modelos requieren de acceso continuo a grandes cantidades de datos tanto externos como derivados de sus interacciones con usuarios para su constante entrenamiento. Esto genera preocupaciones sobre cómo se gestionan, almacenan y utilizan dichos datos, y si se están respetando los derechos de los individuos en materia de privacidad.

Estas cuestiones han llevado a los principales investigadores a abogar por la integración de pausas éticas que ayuden a mitigar estos riesgos y del aprendizaje federado en el desarrollo de sistemas de Inteligencia Artificial, lo que permitiría descentralizar su proceso de aprendizaje y evitar riesgos a la vez que se aumenta la colaboración en el proceso de desarrollo de estos sistemas.[13]

Además, el uso de privacidad diferencial ha probado ser eficaz a la hora de limitar la información revelada de sujetos individuales durante el análisis de datos grupales recopilados[14]. Este método se basa en la adición de "ruido estadístico" en las computaciones para mantener la privacidad de individuos cuyos datos personales forman parte del conjunto de datos sin afectar a la utilidad del conjunto.[15]

En el espacio europeo la normativa de protección de datos recogida en el Reglamento General de Protección de Datos (RGPD) incluye disposiciones relevantes

[13]Kumar Anil. (2023). Advances in Data Protection and Artificial Intelligence: Trends and Challenges. *International Journal of Advanced Engineering Technologies and Innovations*, 1(01), Págs. 294-319. https://ijaeti.com/index.php/Journal/article/view/392
[14]Dwork, C. (2008). Differential Privacy: A Survey of Results. En Agrawal, M., Du, D., Duan, Z., Li, A. (eds) *Theory and Applications of Models of Computation*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-79228-4_1
[15]Dwork, C. (2008). Differential Privacy: A Survey of Results. En Agrawal, M., Du, D., Duan, Z., Li, A. (eds) *Theory and Applications of Models of Computation*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-79228-4_1

para proteger los datos personales de los ciudadanos de la UE. Sin embargo, todas estas sugerencias propuestas por la doctrina se mantienen como algo optativo para las empresas desarrolladoras de sistemas de Inteligencia Artificial. Por eso, múltiples investigadores han urgido a la comunidad internacional a colaborar y armonizar los mecanismos regulatorios empleados para salvaguardar la privacidad ante la implantación de la Inteligencia Artificial, y fomentar el desarrollo de las tecnologías mencionadas.[16]

2.2. Transparencia

En relación con el punto anterior, la falta de transparencia en la forma de operar de sistemas de Inteligencia Artificial, especialmente en cuanto al uso y toma de decisiones automatizadas que impactan directamente en los individuos y en la sociedad, es otra de las principales barreras que pueden generar rechazo a su adopción a gran escala. No en vano, la transparencia es una herramienta que actúa como garantía de múltiples derechos fundamentales y principios democráticos y además nos permite evaluar el buen funcionamiento de los sistemas de Inteligencia Artificial.

Por tanto, la transparencia algorítmica ha de ser mayor en proporción al riesgo, opacidad y tipo asociado a la IA en cuestión.[17] Esta transparencia algorítmica puede interpretarse como un principio de notificación al usuario de distintos factores como pueden ser el hecho de que está interactuando con una IA; de la adopción de decisiones por un sistema de IA y la opción de no usarlas o aportarles información de quienes son los proveedores de las IA y su finalidad.[18]

El artículo 13 RGPD obliga cuando se obtengan de un interesado datos personales relativos a él, a facilitar información sobre "a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de

[16]Kumar Anil. (2023). Advances in Data Protection and Artificial Intelligence: Trends and Challenges. *International Journal of Advanced Engineering Technologies and Innovations*, 1(01), Págs. 294-319. https://ijaeti.com/index.php/Journal/article/view/392

[17]Cotino, L. (2022). Transparencia y explicabilidad de la inteligencia artificial y "compañía" (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad…). Para qué, para quién y cuánta. *Transparencia y explicabilidad de la inteligencia artificial*, Págs. 29-70. https://dialnet.unirioja.es/servlet/articulo?codigo=8709893

[18]Cotino, L. (2023). Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida. *Revista española de la transparencia*, (16), Págs. 17-63.

protección de datos, en su caso;" Y, también, "e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso."

Es especialmente sensible la ausencia en los marcos regulatorios actuales de una obligación de transparencia al sector público que establezca un registro de qué sistemas de IA existen y su impacto en las Administraciones Públicas.

Por último, en todo supuesto en el que intervengan decisiones automatizadas, la doctrina distingue distintos principios éticos y mejores prácticas relacionadas con la notificación sobre los datos personales utilizados y los procesos lógico-técnicos que utiliza el sistema para tomar dichas decisiones.[19] Dichos principios han sido recogidos en normas como el art. 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Según este artículo "Todo interesado tendrá 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." Otro ejemplo podría ser el art. 64.4.d) del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (Estatuto de los Trabajadores), según el cual los Comités de Empresa tienen derecho a "Ser informados por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de Inteligencia Artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles."

Ambos ejemplos muestran que tanto el legislador europeo como el nacional se muestran receptivos a la codificación de estos principios éticos y mejores prácticas, especialmente en supuestos particularmente sensibles como los relativos al empleo.

[19]Cotino, L. (2023). Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida. *Revista española de la transparencia*, (16), Págs. 17-63.

2.2. Sesgos y Discriminación

La última preocupación ética que se analiza en este apartado reside en la preocupación de que los sistemas de IA, aunque desarrollados con el objetivo de mejorar la eficiencia y la precisión en la toma de decisiones, puedan perpetuar o incluso amplificar los sesgos existentes en los datos que utilizan. Esto puede dar lugar a decisiones discriminatorias que afecten de manera injusta a determinados grupos o individuos, especialmente en los sectores claves discutidos como el acceso a servicios financieros o la atención médica.

Estos sesgos pueden ser producto del mero análisis de datos por el sistema sin establecer relaciones causa-efecto entre ellos o identificar circunstancias subyacentes a problemas sociales complejos. Así, por ejemplo, se podría incluso llegar a considerar a personas de distinta raza como simplemente más propensas a la delincuencia[20], o disminuir las probabilidades de ascenso laboral de las mujeres si en la empresa en la que se implementa el sistema había un patrón en el que los hombres eran ascendidos desproporcionadamente por encima de sus compañeras de trabajo.[21]

La eliminación de estos sesgos puede conseguirse si evitamos que la Inteligencia Artificial pueda tomar decisiones con base en características protegidas (sexo, raza…), pero esto puede llevar a una pérdida de eficacia del sistema. Por ello, también se propone introducir barreras en su programación y entrenamiento que establezcan consideraciones técnicas, sociales, legales y éticas que permitan al sistema reconocer la discriminación y ser consciente de ella.[22]

Podemos conectar esta cuestión con las preocupaciones expresadas respecto a la transparencia, puesto que si somos capaces de entender como la Inteligencia Artificial ha tomado una decisión discriminatoria, es más probable que podamos corregir esos problemas en su código o entrenamiento. Este marco facilitará la conversión de

[20]Belloso Martín, N. (2022). La problemática de los sesgos algorítimicos (con especial referencia a los de género). ¿Hacia un derecho a la protección a los sesgos? En F. H. (Coordinador), *Inteligencia Artificial y filosofía del Derecho,* Págs. 45-69. Murcia: Ediciones Laborum S.L.

[21]Aránguez Sánchez, T. (2022). Sesgos sexistas de los algoritmos e Inteligencia Artificial. En T. A. Sánchez, & O. Olariu, *Algoritmo, teletrabajo y otros grandes temas del feminismo digital*, Págs. 71-86. Madrid: Dykinson S.L.

[22]Ferrer, X., Van Nuenen, T., Such, J. M., Coté, M., & Criado, N. (2021). Bias and discrimination in AI: a cross-disciplinary perspective. *IEEE Technology and Society Magazine*, 40(2), Págs. 72-80. https://arxiv.org/abs/2008.07309

algoritmos discriminatorios en no discriminatorios. Por otro lado, tampoco podemos ignorar que, a veces, los elementos discriminatorios pueden ser introducidos por el propio usuario.

III. ANÁLISIS DE LA REGULACIÓN DE LA UNIÓN EUROPEA SOBRE INTELIGENCIA ARTIFICIAL

1. EL REGLAMENTO (UE) 2024/1689 (REGLAMENTO DE INTELIGENCIA ARTIFICIAL)

1.1. Antecedentes y proceso de elaboración del Reglamento de Inteligencia Artificial

El Reglamento de Inteligencia Artificial es, sobre todo, una regulación sobre riesgos. Por ello, se enmarca en un proceso de intervención pública progresiva en sectores altamente tecnificados como es la digitalización. Regulaciones como el RGPD constituyen un claro antecedente para el Reglamento de Inteligencia Artificial al anticipar la necesidad "de minimizar los riesgos que produce una actividad con riesgo inherente a la que no se puede o quiere renunciar."[23]

Su proceso de elaboración ha sido particularmente largo, con múltiples debates sobre su texto antes de su aprobación. A continuación, se describen los principales hitos en este proceso:

En 2018, la Comisión Europea publicó dos Comunicaciones relacionadas con la IA ("Inteligencia Artificial Para Europa"[24] y "Plan Coordinado Sobre Inteligencia Artificial"[25]) y en 2020 el "Libro Blanco sobre la Inteligencia Artificial"[26]. Todos estos documentos nos revelan los principios que guían la estrategia europea en materia de Inteligencia Artificial. Estos principios son:

[23]Miranzo-Diaz, J. (2024). El Reglamento de Inteligencia Artificial de la Unión Europea: regulación de riesgos y sistemas deestandarización. A&C - Revista de Direito Administrativo & Constitucional, 24(96), Págs. 43-78 https://doi.org/10.21056/aec.v24i96.1932

[24]Comisión Europea. (2018) *Inteligencia artificial para Europa.* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0237

[25]Comisión Europea. (2018) *Plan coordinado sobre la inteligencia artificial.* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0795

[26]Comisión Europea. (2020) *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0065

1. Crear un ecosistema de confianza y excelencia.
2. Fomentar un enfoque ético, transparente y centrado en el ser humano.
3. Implementar un marco regulador para garantizar la seguridad y los derechos fundamentales.
4. Promover la colaboración público-privada y aumentar inversiones en IA.
5. Promover alianzas estratégicas entre los Estados miembros y el sector privado.

En Abril de 2021, la Comisión Europea presentó una propuesta de un marco regulador sobre Inteligencia Artificial que recogiese los principios fundamentales para abordar las implicaciones humanas y éticas de esta tecnología. En 2022, la Comisión Europea introdujo, a su vez, dos propuestas de Directivas sobre responsabilidad por daños causados por productos defectuosos, y en materia de IA, ambas aplicables a la Inteligencia Artificial. La primera de estas propuestas ya ha sido aprobada, mientras que la segunda fue retirada el 11 de febrero de 2025 porque la Comisión no consideraba previsible que se alcanzase un acuerdo respecto de su texto. La Comisión considerará si se debe introducir otra propuesta o realizar un cambio de enfoque en esta cuestión.[27]

Dentro del proceso de enmiendas y propuestas destacan las planteadas por el Consejo y el Parlamento en junio de 2023, tras las cuales se logró un acuerdo en el Consejo en diciembre de 2023. En febrero de 2024, se creó la Oficina Europea de Inteligencia Artificial. Por último, el Parlamento aprobó el Reglamento de Inteligencia Artificial en 2024, que entró en vigor el 1 de agosto de ese año.[28]

Estos antecedentes reflejan la complejidad de regular los riesgos de una tecnología en constante evolución, con implicaciones profundas para la sociedad, la economía y los derechos fundamentales. La elaboración de este reglamento no solo evidencia el compromiso de la Unión Europea por liderar la regulación ética y responsable de la inteligencia artificial, sino que también sienta un precedente global al abordar por primera vez de manera proactiva los riesgos de la IA mientras se impulsa su desarrollo sostenible, posicionando a Europa como referente en la gobernanza de tecnologías emergentes.

[27]Comisión Europea. (2025) *Moving forward together: A Bolder, Simpler, Faster Union.* Anexo III. https://commission.europa.eu/document/download/7617998c-86e6-4a74-b33c249e8a7938cd_en?filename=COM_2025_45_1_annexes_EN.pdf#page=23.12

[28]Historic timeline. EU Artificial Intelligence Act. (2024). Recuperado el 16 de Diciembre de 2024 de https://artificialintelligenceact.eu/developments/

1.2. Análisis del Contenido del Reglamento de Inteligencia Artificial

Dada su concepción como una regulación sobre riesgos, es lógico que uno de los pilares centrales del Reglamento de Inteligencia Artificial (RIA) sea su enfoque basado en la clasificación de riesgos. Este modelo jerarquiza los riesgos en diferentes categorías y permite distinguir entre sistemas de IA, y establece obligaciones específicas según la naturaleza y el impacto de cada categoría.

1.2.1. Clasificación de Riesgos en el Reglamento de Inteligencia Artificial

Dentro de esta clasificación de riesgos encontramos los **sistemas de IA prohibidos** por constituir un riesgo no permitido. Estos sistemas son definidos en el Capítulo II del Reglamento de IA e incluyen aquellos que explotan vulnerabilidades de una persona física o un determinado colectivo de personas, y emplean manipulación subliminal o engañosa para alterar sustancialmente el comportamiento de las personas (art. 5 RIA a y b RIA). También incluyen sistemas que tengan como finalidad el "social scoring" (art. 5c RIA), la predicción de delitos (art. 5d RIA), la creación o ampliación de bases de datos de reconocimiento facial (art. 5e RIA), y la inferencia de emociones en lugares de trabajo o educativos, salvo en casos médicos o de seguridad (art. 5f RIA). Por último, se prohíben también aquellos sistemas dedicados a la categorización biométrica con la finalidad de inferir o deducir categorías especiales de datos, y aquellos sistemas dedicados a la identificación biométrica remota en tiempo real y en espacios de acceso público (art. 5g y h RIA) salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar objetivos como la prevención de amenazas graves o la búsqueda de víctimas de delitos específicos, siempre bajo estrictas condiciones legales y de proporcionalidad.

También encontramos los **sistemas de IA de alto riesgo,** definidos en el Capítulo III del Reglamento de IA. Un sistema de IA se considerará de alto riesgo si está destinado a ser utilizado como componente de seguridad de un producto regulado por los actos legislativos de armonización de la Unión (Anexo I RIA) o es uno de dichos productos, y dicho producto o sistema debe someterse a una evaluación de conformidad por terceros antes de ser introducido en el mercado. Además de lo anterior, los sistemas enumerados en el Anexo III se clasifican automáticamente como de alto riesgo, salvo excepciones. (art. 6.1 RIA)

Los sistemas clasificados como de alto riesgo en el Anexo III están agrupados según sus ámbitos de uso (art. 6.2 RIA):

En biometría, aquellos dedicados a la identificación biométrica remota (excepto para simplemente verificar la identidad de una persona), la categorización biométrica según atributos sensibles y el reconocimiento de emociones. (Anexo III.1 RIA)

En infraestructuras críticas, aquellos sistemas utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas, del tráfico rodado, o cadenas de suministros. (Anexo III.2 RIA)

En educación y formación profesional, aquellos sistemas utilizados para la determinación de acceso o admisión a instituciones educativas, la evaluación de resultados de aprendizaje para orientar procesos educativos y la supervisión de comportamientos prohibidos en exámenes (Anexo III.3 RIA).

En cuestiones de empleo, aquellos sistemas utilizados para la contratación, promoción, rescisión o selección de personas y asignación de tareas (Anexo III.4 RIA).

En cuestiones relativas al acceso a servicios esenciales, aquellos sistemas dedicados a la evaluación de elegibilidad para asistencia pública o sanitaria, la calificación crediticia (salvo para la detección de fraudes), la evaluación de riesgos en seguros de vida y salud (Anexo III. 5 RIA).

En cuestiones relativas al cumplimiento del Derecho, aquellos sistemas dedicados a la evaluación del riesgo de que una persona sea víctima de un crimen por las autoridades competentes o la elaboración de perfiles durante la detección, la investigación o el enjuiciamiento de delitos (Anexo III. 6 RIA).

En cuestiones relacionadas con la migración, aquellos sistemas diseñados para la evaluación de riesgos (seguridad, salud, migración irregular), el análisis de solicitudes de asilo, visado o residencia y la detección e identificación de personas (Anexo III. 7 RIA).

En cuestiones relacionadas con la administración de justicia, aquellos sistemas dedicados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una

autoridad judicial en la investigación e interpretación de hechos y de la ley (Anexo III. 8 RIA).

Existen excepciones a esta clasificación automática para aquellos sistemas que no plantean riesgos significativos para la salud, seguridad o derechos fundamentales, y cumplen cualquiera de las siguientes condiciones: realizan tareas procedimentales limitadas; mejoran una actividad humana sin reemplazar el juicio humano; detectan patrones o desviaciones sin sustituir decisiones humanas previas ni influir sustancialmente en ellas; o realizan tareas preparatorias para decisiones humanas en ámbitos del anexo III. No obstante, siempre se considerarán de alto riesgo cuando impliquen elaboración de perfiles de personas físicas (Art. 6.3 RIA).

Los **sistemas de riesgo limitado**, entre los que se incluyen "chatbots" o Inteligencias Artificiales generadoras de contenido como "Chat GPT", deben cumplir con ciertas obligaciones de transparencia ante sus usuarios y el público general.

Los sistemas de IA deben informar a las personas físicas de que están interactuando con una IA, salvo que esto sea evidente para un usuario razonablemente informado y considerando el contexto. Existe una excepción para sistemas de IA autorizados por ley para detectar, prevenir, investigar o enjuiciar delitos, con sujeción a las garantías adecuadas para los derechos y libertades de terceros, salvo que estos sistemas estén a disposición del público para denunciar un delito (art. 50.1 RIA).

Los sistemas de IA que generen contenido (audio, video, texto, imágenes) deben etiquetar los resultados como generados o manipulados artificialmente, en un formato legible por máquina. Existen también excepciones para sistemas que actúen como apoyo a la edición estándar sin alterar significativamente los datos de entrada, o sistemas autorizados para fines legales como la prevención o investigación de delitos en los mismos términos que en el caso anterior (art. 50.2 RIA).

Los sistemas de IA dedicados al reconocimiento de emociones o a la categorización biométrica deben informar a las personas expuestas al sistema sobre su funcionamiento y tratarán sus datos personales de conformidad con la legislación aplicable. También está prevista una excepción para sistemas autorizados con fines legales en los mismos términos que los anteriores supuestos (art. 50.3 RIA).

Los sistemas de IA que generen o manipulen imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación ("deepfakes" en inglés) deben informar públicamente que el contenido ha sido generado o manipulado por IA. Existen excepciones para casos de sistemas autorizados con fines legales y aquellos sistemas dedicados a la creación de contenidos creativos (arte, sátira, ficción), donde basta con una notificación adecuada que no interfiera en el disfrute de la obra. Si un texto generado por IA se publica para informar sobre asuntos de interés público, se debe divulgar su origen artificial, salvo que haya sido revisado o controlado editorialmente y exista una responsabilidad editorial asumida por una persona física o jurídica (art. 50.4 RIA).

Por último, encontramos los **sistemas de IA de riesgo mínimo o nulo**, que son todos aquellos sistemas que no puedan encuadrarse en ninguna de las categorías anteriores (filtros de correo o videojuegos, por ejemplo). Estos sistemas no están regulados por el reglamento, y por lo tanto, pueden usarse sin restricciones.

1.2.2. Modelos de IA de Uso General

Aparte de la clasificación de sistemas de IA en función de su riesgo, el Reglamento de Inteligencia Artificial contiene también una regulación especifica para los **modelos de IA de uso general y modelos de IA de uso general y riesgo sistémico**. Estos modelos son aquellos que no tienen una finalidad concreta, sino que se le pueden dar múltiples usos sin estar limitados a una función específica.

El Considerando 110 del Reglamento determina como de riesgo sistémico aquellos modelos que puedan producir efectos negativos reales o razonablemente previsibles en relación con accidentes graves, perturbaciones de sectores críticos, salud y seguridad públicas; efectos negativos reales o razonablemente previsibles sobre los procesos democráticos; y la difusión de contenidos ilegales, falsos o discriminatorios. Un modelo es de riesgo sistémico cuando tenga capacidades de alto impacto, lo que se presume siempre que la potencia de cálculo empleada en su preparación supere los 10^25 FLOPS (cálculos matemáticos que puede hacer por segundo una CPU y GPU).

Los proveedores de estos modelos deben mantener actualizada la documentación técnica a fin de facilitarla a la Oficina de IA y a las autoridades pertinentes. (art. 53.1a RIA). Esta documentación deberá contener, como mínimo, una descripción general del

modelo; las tareas que vaya a realizar, políticas de uso razonable, fecha de lanzamiento y distribución, arquitectura y número de parámetros, modalidad, y licencia. También deberán incluir una descripción de los elementos técnicos del modelo que incluya, como mínimo, las herramientas e infraestructura necesarias para su integración, las especificaciones del diseño y proceso de entrenamiento, los datos de entrenamiento, prueba y validación, el consumo de energía y los recursos computacionales utilizados. Por último, los modelos con riesgo sistémico deben incluir también una descripción detallada de las estrategias de evaluación; sus métodos, criterios y resultados, incluyendo las limitaciones de estos. También deben incluir una descripción de pruebas adversas internas o externas y ajustes realizados al modelo, además de una explicación de como los componentes del software interactúan y se integran en el procesamiento general (Anexo XI RIA).

Asimismo, deben compartir información clave sobre el sistema con los proveedores de sistemas de IA que tengan la intención de integrar el modelo de IA de uso general en sus sistemas (art. 53.1b RIA). Esta información incluirá como mínimo los elementos del Anexo XI más la manera en que el modelo interactúa o puede utilizarse para interactuar con el hardware o el software que no formen parte del propio modelo, y sin tener que incluir el consumo de energía del modelo. Estas obligaciones deben compaginarse con el respeto a la propiedad intelectual y secretos comerciales, y no se exigirán a los proveedores de modelos de IA que se divulguen con arreglo a una licencia libre y de código abierto.

Además de estas obligaciones, los modelos de IA de uso general con riesgo sistémico deben cumplir una serie de medidas de seguridad adicionales relacionadas con la evaluación y mitigación de riesgos; la monitorización y notificación de incidentes graves y medidas correctivas a la Oficina de IA y la autoridad pertinente; y el mantenimiento de un nivel adecuado de protección en ciberseguridad. Los proveedores pueden usar códigos de buenas prácticas o normas armonizadas para demostrar conformidad. Si no las utilizan, deberán demostrar el cumplimiento por otros medios de prueba alternativa. La confidencialidad de la información y documentación, incluidos secretos comerciales, se protegerán conforme al artículo 78 (arts. 55 y 92 RIA).

1.2.3. Vigilancia y Poscomercialización

Los proveedores deben establecer un sistema de **vigilancia poscomercialización** para Sistemas de IA de alto riesgo. Dicho sistema deberá compilar los datos que puedan recopilarse sobre el funcionamiento del sistema durante su vida útil y su interacción con otros sistemas a fin de evaluar el cumplimiento de los requisitos establecidos en el Reglamento (art. 72 RIA). También deberán notificar a las autoridades de vigilancia del mercado de los Estados miembros cualquier incidente grave vinculado al sistema de IA en un plazo máximo de 15 días, 10 días si el incidente está vinculado al fallecimiento de una persona, o 48h si se trata de un incidente generalizado. Posteriormente, el proveedor deberá cooperar con las autoridades y realizar una evaluación de riesgos del incidente e integrar medidas correctoras (art. 73 RIA).

Si una autoridad de vigilancia del mercado recibe información sobre un incidente grave durante una prueba en condiciones reales podrá, en su territorio, suspenderla o requerir al proveedor o responsable del despliegue que realicen modificaciones a dichas pruebas (art. 76.3 RIA). Asimismo, si considera que un Sistema de IA presenta riesgos, la autoridad de vigilancia del mercado realizará una evaluación para verificar su cumplimiento del Reglamento, prestando especial atención a riesgos para colectivos vulnerables y derechos fundamentales. En caso de incumplimiento, requerirá al operador tomar medidas correctoras, retirar o recuperar el sistema en un plazo máximo de 15 días hábiles; y si el operador no cumple este requerimiento, podrá tomar todas las medidas provisionales adecuadas para prohibir o restringir la comercialización o puesta en servicio del Sistema de IA.

Estas medidas provisionales se considerarán justificadas si ninguna otra autoridad de vigilancia del mercado ha planteado objeciones tras 3 meses. En caso contrario, la Comisión consultará a la autoridad de vigilancia del mercado del Estado miembro y a los operadores involucrados para evaluar la medida nacional. En un plazo de seis meses, o de 60 días si se trata de prácticas de IA prohibidas según el artículo 5, decidirá si la medida está justificada y notificará su decisión tanto a la autoridad correspondiente como a las demás autoridades de vigilancia del mercado (art. 81 RIA).

La autoridad informará y cooperará con organismos nacionales pertinentes, y los operadores deberán colaborar con las autoridades. El operador se asegurará de que se

adopten todas las medidas correctoras adecuadas en relación a todos los sistemas de IA afectados que haya comercializado en la Unión (art. 79.2 y 79.4-5 RIA).

Por último, el Reglamento contempla medidas específicas para abordar incumplimientos mediante **sanciones** que deben ser efectivas, proporcionadas y disuasorias.

Toda persona física o jurídica que tenga motivos para considerar que se ha infringido lo dispuesto en el Reglamento de Inteligencia Artificial podrá presentar reclamaciones ante la autoridad de vigilancia del mercado pertinente (art. 85 RIA).

En el caso de incumplimientos del art. 5 (Prácticas Prohibidas), las sanciones previstas serán multas administrativas de hasta 35.000.000 EUR o, si el infractor es una empresa, de hasta el 7 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior (o inferior si es una PYME) (art. 99.3 RIA).

El incumplimiento de las obligaciones establecidas en los arts. 16, 22-24, 26, 31, 33.1, 33.3, 33.4, 34 y 50 estará sancionado con multas administrativas de hasta 15.000.000 EUR o, si el infractor es una empresa, de hasta el 3 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior (o inferior si la empresa es una PYME) (art. 99.4 RIA).

Por otro lado, la presentación de información falsa o incompleta a las autoridades competentes, que implica un incumplimiento de las obligaciones de transparencia estudiadas, está sancionada con multas administrativas de hasta 7 500 000 EUR o, si el infractor es una empresa, de hasta el 1 % del volumen de negocios (o inferior si la empresa es una PYME) (99.5 RIA).

La cuantía en cada caso concreto se fijará, con sujeción a los anteriores limites, tras valorar la naturaleza de la infracción, su gravedad, duración, consecuencias, e impacto. También el tamaño y volumen de negocios del infractor, su cuota de mercado, la existencia de sanciones previas. Por último, se consideran elementos agravantes o atenuantes como los beneficios obtenidos por el infractor, su cooperación, las medidas adoptadas por este para mitigar daños, el grado de responsabilidad, su intencionalidad y sus acciones tomadas para minimizar los perjuicios causados (99.7 RIA).

En el caso de infracciones por instituciones, órganos u organismos de la UE, el incumplimiento de las prohibiciones del art. 5 conlleva multas de hasta 1.500.000 EUR. Otras infracciones conllevarán multas de hasta 750.000 EUR. Tras permitir a la institución infractora ser oída, la cuantía en concreto se fijará tras valorar la gravedad de la infracción, su duración, consecuencias, y el impacto en las personas afectadas, además del grado de responsabilidad de la institución, sus acciones tomadas para mitigar daños, la cooperación con el Supervisor Europeo de Protección de Datos, antecedentes de infracciones similares, la notificación de la infracción y el presupuesto anual del organismo involucrado (art. 100 RIA).

Si el incumplimiento es meramente formal (falta de registro en la base de datos de la UE, documentación técnica…) la autoridad de vigilancia del mercado podrá requerir su subsanación, y si esta no se produce, restringir o prohibir la comercialización del Sistema de IA de alto riesgo (art. 83 RIA).

La Comisión también podrá imponer multas a proveedores de modelos de IA de uso general si estos han incumplido una medida de la Comisión, han infringido las disposiciones del Reglamento, no han respondido a una solicitud de información o han facilitado información incompleta o falsa, o no dieron acceso a la Comisión al modelo de IA de uso general o al modelo de IA de uso general con riesgo sistémico para que se lleve a cabo una evaluación. Dichas multas no superarán el 3 % de su volumen de negocios mundial total anual correspondiente al ejercicio financiero anterior o de 15.000.000 EUR, si esta cifra es superior. El TJUE podrá anular, reducir o aumentar la cuantía fijada por la Comisión. Antes de adoptar una decisión, la Comisión comunicará sus conclusiones preliminares al Consejo de IA y al proveedor del modelo de IA de uso general o del modelo de IA y le dará la oportunidad de ser oído (art. 101 RIA).

2. LA DIRECTIVA SOBRE RESPONSABILIDAD POR LOS DAÑOS CAUSADOS POR PRODUCTOS DEFECTUOSOS

Si bien el Reglamento de Inteligencia Artificial es el principal objeto de estudio en este trabajo, el análisis breve de otras propuestas legislativas dentro de la UE puede facilitar la interpretación de su contenido y de posibles evoluciones legislativas en materia de Inteligencia Artificial.

Tanto el Reglamento de Inteligencia Artificial como la Directiva sobre responsabilidad por los daños causados por productos defectuosos encajan dentro de la Estrategia Europea de IA, cuyo propósito es consolidar a la Unión Europea como líder mundial en el desarrollo y uso ético de la Inteligencia Artificial.

Dado que este trabajo se centra en el Reglamento de Inteligencia Artificial y su impacto en el Derecho civil español, el propósito de esta sección no es realizar un análisis exhaustivo de esta norma, sino exponer aquellos aspectos de su articulado que mayor interacción van a tener con el Reglamento y con el Derecho civil español.

2.1. La Directiva del Parlamento Europeo y del Consejo Sobre Responsabilidad por los Daños Causados por Productos Defectuosos

La Directiva del Parlamento Europeo y del Consejo sobre Responsabilidad por los Daños Causados por Productos Defectuosos, se propuso el 18 de septiembre de 2022 y fue aprobada el 18 de noviembre de 2024. En ella, se propuso garantizar que los derechos de los consumidores estén adecuadamente protegidos frente a los riesgos inherentes a productos defectuosos, incluyendo aquellos que integran Inteligencia Artificial. Su texto legal es de aplicación a sistemas de Inteligencia Artificial sin importar su nivel de riesgo al incluir programas informáticos en la definición de productos, aunque sean productos inmateriales.

La definición de producto defectuoso como producto que no ofrece la seguridad que el público general tiene derecho a esperar es continuista con anteriores normas dictadas en este ámbito. Para la determinación de esta expectativa de seguridad, la Directiva incluye en su Artículo 6 una serie de criterios, de los cuales destacan los siguientes por su relación con la IA.[29]

El art. 6.1b) contempla tanto el uso razonablemente previsible como el indebido, por lo que los proveedores de Sistemas de IA deberán de suministrar instrucciones de uso para no correr el riesgo de que se les impute responsabilidad por no haber suministrado esta información.

[29]Garea, C. (2023). La Propuesta de Directiva sobre responsabilidad por daños ocasionados por productos defectuosos y su aplicación a la inteligencia artificial. En Santos, F.C.S (et al.), *Estudos en homenagem ao Profesor Doutor Antonio Pinto Monteiro. Volume 1: Direito Civil*. Boletim da Facultade de Direito, Págs. 179-206.

La evaluación de seguridad también deberá tener en cuenta la capacidad de autoaprendizaje del modelo de IA concreto, lo que puede generar dudas sobre si los errores producidos tras la evaluación y su entrenamiento pueden redundar en su calificación como producto defectuoso. Por ello, también debe prestarse atención a en qué momento comienza a funcionar el sistema de forma autónoma y su productor deja de ejercer control sobre el mismo, lo que puede ser posterior a su introducción en el mercado o no producirse. Ello no implica que, si un sistema requiere de una actualización posterior a su salida al mercado, este fuese defectuoso antes de recibir esta actualización.

En consonancia con el Reglamento de Inteligencia Artificial, la Directiva también requiere en sus arts. 7.1f) y 7.1g) que los proveedores y productores de sistemas de IA cumplan las exigencias de seguridad y transparencia con los organismos reguladores que allí se establecen. Ello se extiende también a cuestiones de ciberseguridad, ya que la vulnerabilidad de un sistema ante un ataque informático puede resultar en su calificación como producto defectuoso.

Más allá de estos criterios, la responsabilidad prevista en esta norma se ve limitada por la extensión del daño indemnizable cubierto por ella. Por ejemplo, no será indemnizable el daño puramente económico que deriva en daños de una persona distinta del demandante. Tampoco serán indemnizables los daños morales distintos de daños para la salud psicológica, salvo que estén previstos en el derecho nacional del Estado miembro en concreto.[30] En este caso es especialmente relevante que solo son resarcibles las pérdidas económicas derivadas del borrado o corrupción de datos informáticos, no el hecho en si.

Con respecto al régimen de responsabilidad que establece esta Directiva, el demandante debe probar el carácter defectuoso del producto, los daños padecidos y el nexo causal ante ambos. Por tanto, el fundamento básico de la imputación de responsabilidad en este caso es el defecto del producto en cuestión, ya que sin él los daños no serán indemnizables. Dicho defecto es independiente de la actuación negligente o no

[30]Garea, C. (2023). La Propuesta de Directiva sobre responsabilidad por daños ocasionados por productos defectuosos y su aplicación a la inteligencia artificial. En Santos, F.C.S (et al.), *Estudos en homenagem ao Profesor Doutor Antonio Pinto Monteiro. Volume 1: Direito Civil*. Boletim da Facultade de Direito, Pág. 179-206.

del operador. Parece, por tanto, que se ha optado por un régimen de imputación de responsabilidad objetiva limitada[31].

En relación con la imputación de responsabilidad, el art. 10.2 establece una presunción de que el producto es defectuoso cuando el demandado incumpla la obligación de exhibir pruebas establecida en el art. 9.1. Se trata de una presunción refutable diseñada para facilitar la prueba del defecto para el demandante. Esta presunción operará también en aquellos supuestos en los que el demandante pruebe que el Sistema de IA causó un daño por un mal funcionamiento manifiesto; o no cumple con las obligaciones de seguridad del Derecho de la UE, lo que incluye evidentemente el Reglamento de Inteligencia Artificial.

Por último, y como contraparte para fomentar la innovación tecnológica, el art. 11 de la Directiva incluye supuestos de exención de responsabilidad por los daños causados por un producto defectuoso.

Según esto, los fabricantes e importadores quedarán exentos de responsabilidad si no introdujeron el producto en el mercado ni lo pusieron en servicio; el defecto no era detectable con los conocimientos disponibles en el momento o responde al cumplimiento de otros requisitos legales.

Los distribuidores podrán eximirse de responsabilidad si demuestran no haber participado en la comercialización del producto, o si el defecto no existía en el momento de su comercialización.

Un operador que modifica productos quedará exento de responsabilidad si el defecto no está relacionado con su modificación.

En conclusión, la Directiva del Parlamento Europeo y del Consejo sobre Responsabilidad por los Daños Causados por Productos Defectuosos refuerza la protección de los consumidores frente a los riesgos asociados a productos inseguros, adaptando el marco normativo existente a los desafíos tecnológicos actuales. Al abordar los daños derivados de productos complejos, como los que integran sistemas de

[31]Garea, C. (2023). La Propuesta de Directiva sobre responsabilidad por daños ocasionados por productos defectuosos y su aplicación a la inteligencia artificial. En Santos, F.C.S (et al.), *Estudos en homenagem ao Profesor Doutor Antonio Pinto Monteiro. Volume 1: Direito Civil*. Boletim da Facultade de Direito, Pág. 179-206.

inteligencia artificial, la propuesta favorece una mayor claridad y equidad en la asignación de responsabilidades. Esto no solo beneficia a las víctimas al facilitar la compensación por daños, sino que también incentiva a los fabricantes y operadores a mantener altos estándares de calidad y seguridad en el diseño y desarrollo de sus productos.

IV. IMPACTO DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL SOBRE EL DERECHO CIVIL ESPAÑOL

Si bien el Reglamento de IA es una norma de Derecho público de la Unión Europea, su implementación implica cambios significativos en múltiples áreas del Derecho civil español tales como el derecho de daños, el derecho de propiedad intelectual o el derecho de contratos, que en este apartado se analiza desde la perspectiva de los contratos de seguros. Por ello, su adecuada implementación requiere de iniciativa, proactividad y dinamismo por parte de nuestras instituciones, ya que como recuerda José Ramón Chaves, en esta materia "la actividad judicial no debe ser ni indiferente, ni insuficiente ni deferente."[32]

1. IMPACTO DEL REGLAMENTO DE INTELIGENCIA ARTIFICAL EN EL DERECHO DE DAÑOS ESPAÑOL

En esta área la interacción entre el Reglamento de Inteligencia Artificial y la Directiva sobre responsabilidad por los daños causados por productos defectuosos va a ser fundamental, tal y como resulta del análisis del art. 10.2b) del segundo texto legal mencionado. El incumplimiento de los requisitos obligatorios de seguridad del producto establecidos en el Derecho de la Unión o nacional, lo que incluye las disposiciones del Reglamento, conllevará la presunción iuris tantum de que el producto en cuestión es defectuoso, con las consecuencias que ello implica para el derecho de daños.

Sobre esta cuestión, A.R. Puig se pronuncia y afirma que "las potenciales reclamaciones privadas por daños derivados del funcionamiento y uso de modelos y sistemas de inteligencia artificial de alto riesgo exigirán en muchos casos identificar infracciones de deberes de seguridad establecidos en el propio Reglamento de IA y valorar si estas pueden servir por si solas para acreditar la negligencia de los demandados en el pleito."[33]

[32]Chaves, J. (24 de febrero de 2025). *Reglamento de inteligencia artificial, buena administración y control judicial: un nudo gordiano - delajusticia.com - El rincón jurídico de José Ramón Chaves*. Recuperado el 10 de marzo de 2025 en delaJusticia.com. https://delajusticia.com/2025/02/20/reglamento-de-inteligencia-artificial-buena-administracion-y-control-judicial-un-nudo-gordiano/

[33] Puig, A. R. (2024). Una lectura del reglamento de inteligencia artificial desde el derecho privado. *InDret*, (4), Págs. 1-8.

Esto no quiere decir que el mero cumplimiento de las obligaciones establecidas en el Reglamento pueda usarse como argumento por parte de los demandados para evitar la imputación de responsabilidad civil, especialmente en el caso de sistemas de alto riesgo. A.R Puig se pronuncia categóricamente al respecto: "El éxito de alegaciones en este sentido es poco probable. El Reglamento de IA ha de considerarse una normativa de mínimos en materia de deberes de seguridad para los sistemas de IA de alto riesgo, especialmente, en un campo tan dinámico y con altos niveles de innovación en estos momentos como la inteligencia artificial"[34]

Otro problema con respecto a la atribución de responsabilidad civil en Inteligencia Artificial es la pluralidad de sujetos que intervienen en su desarrollo, entrenamiento y comercialización. Por ello, se prevé que las diferentes obligaciones que el Reglamento de Inteligencia Artificial impone a cada operador, y el sistema de vigilancia poscomercialización que establece podrían simplificar este proceso de atribución de la responsabilidad civil. Ahora bien, existen todavía importantes dudas en supuestos de responsabilidad múltiple.

Los únicos casos en los que hay una respuesta legal explícita a esta cuestión son aquellos en los que intervenga la Directiva sobre productos defectuosos, puesto que su art. 12.1 introduce una regla de responsabilidad solidaria para los operadores económicos involucrados.

Dado que no existe una previsión legal similar aplicable al resto de supuestos de responsabilidad múltiple respecto de daños causados por sistemas de IA, parece que entraría en juego el Código Civil español, cuyo art. 1137 rechazaría la responsabilidad solidaría puesto que "sólo habrá lugar a esto cuando la obligación expresamente lo determine, constituyéndose con el carácter de solidaria."

Sin embargo, sería deseable desde el punto de vista del principio "favor creditoris" otorgar un tratamiento idéntico a los supuestos de responsabilidad múltiple por daños cubiertos por el Reglamento de IA y aquellos cubiertos por la Directiva sobre productos defectuosos, estableciendo en ambos casos un régimen de responsabilidad solidaria. Esto es así porque ahorraría tiempo y recursos al demandante a la hora de

[34] Puig, A. R. (2024). Una lectura del reglamento de inteligencia artificial desde el derecho privado. *InDret*, (4), Págs. 1-8.

interponer una demanda de responsabilidad civil por daños al permitirle reclamar la totalidad de la indemnización a cualquiera de los responsables. Además, en todas las normas analizadas se aprecia que la estrategia de la Unión es facilitar al demandante fundamentar su demanda como respuesta a la complejidad asociada a la toma de decisiones por sistemas de IA. Aplicar un régimen de responsabilidad mancomunada en aquellos supuestos no cubiertos por la Directiva sobre productos defectuosos sería contrario a esta estrategia, y puede llevar a resultados dispares y a obstaculizar la eficacia de las normas europeas.

Una forma de solventar este problema y optar en ambos casos por un régimen de responsabilidad solidaria sería mediante la figura de la solidaridad impropia. La solidaridad impropia es una construcción jurisprudencial diseñada para abordar situaciones en las que varias personas son responsables de un daño o de una obligación, pero sin que exista un vínculo jurídico expreso que establezca la solidaridad entre ellas. La jurisprudencia ha justificado esta calificación como impropia o bien porque no deriva de pacto ni norma legal[35], porque se crea en la propia sentencia condenatoria,[36] o porque se produce una disociación entre las relaciones externas e internas.[37]

Esta doctrina encuentra su razón de ser, tal y como expone el Fundamento jurídico segundo de la Sentencia del Tribunal Supremo de 12 de Diciembre de 1998, Sala de lo Civil (rec. 2104/1994), en la "necesidad de salvaguardar el interés social y proteger a los perjudicados en los casos de responsabilidad extracontractual, entre los sujetos a quienes alcanza la responsabilidad por ilícito culposo, con pluralidad de agentes y posibilidad de que el perjudicado pueda dirigirse contra ellos, como deudor por entero de la obligación de reparar en su integridad el daño causado"

La mencionada sentencia pertenece a un conjunto de resoluciones jurisprudenciales del Tribunal Supremo que aplican la solidaridad impropia en supuestos en los que "no sea posible determinar el porcentaje en que cada uno de (los causantes del daño) ha contribuido al daño final"[38] aunque no es necesario que actúen conjuntamente o

[35]Sentencia del Tribunal Supremo núm. 793/2004, de 10 de febrero de 2004, Sala de lo Civil, (rec. 1105/1999).
[36]Sentencia del Tribunal Supremo núm. 4410/2002, de 17 de junio de 2002, Sala de lo Civil (rec. 34/1997).
[37] Sentencia del Tribunal Supremo núm. 13461/1992, de 22 de abril de 1992, Sala de lo Civil (rec. s.n.)
[38]López, J. A. (2006) *La llamada solidaridad impropia en la jurisprudencia del Tribunal Supremo*. Comunicación presentada en el 6º Congreso de la Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguro.

de común acuerdo. De acuerdo con esta doctrina, la mera contribución a un daño mediante acción u omisión por parte de un operador económico en el contexto de daños causados por sistemas de IA podrá resultar en su responsabilidad solidaria, sin ser necesario que exista previsión legal o contractual al respecto, ni que la conducta de cada uno de ellos sea de la suficiente entidad como para causar por si misma el daño final.[39]

La aplicación de esta construcción jurisprudencial conlleva una serie de consecuencias que influirán en las demandas por daños derivados de sistemas de IA en las que intervengan múltiples responsables.

Procesalmente, resulta relevante mencionar que, al aplicar la solidaridad impropia, el Tribunal Supremo parece exigir el litisconsorcio pasivo necesario a fin de evitar sentencias materialmente contradictorias que afecten a la ratio decidendi[40]. Esto puede plantear problemas en el caso de demandas conjuntas a un proveedor de un sistema de IA y a un organismo público de evaluación de conformidad, lo que ”obligará a acudir a la jurisdicción contencioso-administrativa y a la regulación de la responsabilidad patrimonial."[41]

Otra consideración a tener en cuenta es la interrupción de la prescripción, ya que el art. 1974.1 del Código Civil establece la propagación de la solidaridad, por la que la interrupción extiende sus efectos a todos los acreedores. Sin embargo, jurisprudencia del Tribunal Supremo ha negado la aplicación de este artículo en supuestos de solidaridad impropia basándose en que no existía antes de la sentencia que la instaura.[42]

https://www.asociacionabogadosrcs.org/congreso/6congreso/ponencias/Ponencia%20Joaquin%20Ataz%20.pdf

[39]Gómez Calle (2006). Los sujetos de la responsabilidad civil. La responsabilidad civil por hecho ajeno, en Tratado de responsabilidad civil dirigido por REGLERO, 3ª edición. Pág. 486.

[40]Sentencia del Tribunal Supremo núm. 6323/1993, de 28 de septiembre de 1993, Sala de lo Civil, (rec. 360/1991)

[41] Puig, A. R. (2024). Una lectura del reglamento de inteligencia artificial desde el derecho privado. *InDret*, (4), Págs. 1-8.

[42]Sentencia del Tribunal Supremo núm. 223/2003, Sala de lo Civil, de 14 de marzo de 2003, Sala de lo Civil, (rec. 2235/1997).

2. IMPACTO DEL REGLAMENTO DE INTELIGENCIA ARTIFICAL EN EL DERECHO DE PROPIEDAD INTELECTUAL ESPAÑOL

La implementación del Reglamento de Inteligencia Artificial también tendrá consecuencias para el derecho de propiedad intelectual español.

Una de las principales cuestiones que han generado controversia en este ámbito es la protección que merecen los datos y contenidos que sean utilizados para diseñar y entrenar a los sistemas de Inteligencia Artificial. El análisis de esta cuestión toma como base el considerando 105 del Reglamento de IA, según el cual "Todo uso de contenidos protegidos por derechos de autor requiere la autorización del titular de los derechos de que se trate, salvo que se apliquen las excepciones y limitaciones pertinentes en materia de derechos de autor." José Manuel Muñoz Vela se expresa en términos similares al considerar que estos contenidos "pueden estar protegidos legal y/o contractualmente, (…) de modo que únicamente deberían ser utilizados por los sistemas inteligentes cuando exista expresa autorización del titular, o se halle expresamente excepcionado de la misma y, consecuentemente legitimado, en virtud de una exención o limitación prevista por el ordenamiento jurídico que resulte de aplicación".[43]

Pues bien, el Reglamento de Inteligencia Artificial impone en su art. 53.1 a los proveedores de modelos de IA de uso general el deber de elaborar "directrices para cumplir el Derecho de la Unión en materia de derechos de autor y derechos afines y en particular, para detectar y cumplir, por ejemplo, a través de tecnologías punta, una reserva de derechos expresada de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790", y poner "a disposición del público un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo de IA de uso general, con arreglo al modelo facilitado por la Oficina de IA". En conexión con este Artículo, el considerando 106 del Reglamento busca evitar que los proveedores de sistemas de IA eviten esta obligación al afirmar que "Todo proveedor que introduzca un modelo de IA de uso general en el mercado de la Unión debe cumplir esta obligación, independientemente de la jurisdicción en la que tengan lugar los actos pertinentes en

[43]Vela, J. M. M. (2024). Inteligencia artificial generativa. Desafíos para la propiedad intelectual. *Revista de Derecho de la UNED (RDUNED),* (33), Págs. 17-75. https://doi.org/10.5944/rduned.33.2024.41924

materia de derechos de autor que sustentan el entrenamiento de dichos modelos de IA de uso general."

El art. 4 de la Directiva a la que se hace mención en el anterior artículo, es decir, la Directiva (UE) 2019/790, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital, fue transpuesto al derecho español en el art. 67 del Real Decreto-ley 24/2021, de 2 de noviembre, de transposición de directivas de la Unión Europea en las materias de bonos garantizados, distribución transfronteriza de organismos de inversión colectiva, datos abiertos y reutilización de la información del sector público, ejercicio de derechos de autor y derechos afines aplicables a determinadas transmisiones en línea y a las retransmisiones de programas de radio y televisión, exenciones temporales a determinadas importaciones y suministros, de personas consumidoras y para la promoción de vehículos de transporte por carretera limpios y energéticamente eficientes.

Este texto legal estableció una excepción a la aplicación de derechos de autor y afines que cubre "todas aquellas reproducciones y extracciones de obras y otras prestaciones accesibles de forma legítima para actividades de minería de textos y datos con finalidades distintas a la investigación científica y, por tanto, incluyendo, por ejemplo, aquellas actividades con fines comerciales"[44].

Esto podría dar a entender que las reproducciones de obras para la extracción de datos que sirvan para entrenar un modelo de IA para su posterior comercialización son viables, pero el mencionado Artículo 67 del Real Decreto-ley 24/2021 incluye en su tercer apartado una reserva por la que dicha excepción "no será aplicable cuando los titulares de derechos hayan reservado expresamente el uso de las obras a medios de lectura mecánica u otros medios que resulten adecuados"[45]. Esta reserva implica la existencia de un mecanismo de "opt out" a la excepción prevista en el Artículo 53.1 del Reglamento de Inteligencia Artificial.

Por último, cabe matizar que las obligaciones impuestas por el Reglamento en este artículo se aplicarán en nuestro país con mayor o menor flexibilidad en función del

[44]Puig, A. R. (2024). Una lectura del reglamento de inteligencia artificial desde el derecho privado. *InDret*, (4), Págs. 1-8.

tamaño del proveedor, a fin de no limitar la innovación tecnológica. Esto se deriva del considerando 109 del Reglamento según el cual, "sin perjuicio del Derecho de la Unión en materia de derechos de autor, el cumplimiento de esas obligaciones debe tener debidamente en cuenta el tamaño del proveedor y permitir formas simplificadas de cumplimiento para las pymes, incluidas las empresas emergentes, que no deben suponer un coste excesivo ni desincentivar el uso de dichos modelos."

Más allá de esta excepción y el mecanismo de opt out asociado a ella, lo cierto es que la regulación actual, aunque proporciona cierta seguridad jurídica, o no se pronuncia expresamente, o deja sin resolver numerosas cuestiones fundamentales en materia de propiedad intelectual como la posible protección de las respuestas del sistema de IA y las secuencias de "prompts" proporcionadas a este.

Con respecto a la posible protección de los resultados ofrecidos por sistemas de IA, si bien el Reglamento de IA no se pronuncia expresamente, de el considerando 108 parece entenderse que entrará en juego la legislación aplicable en el derecho nacional, contenida en el caso español en el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Puesto que nuestra legislación considera autor a la persona natural que crea alguna obra literaria, artística o científica, (Art. 5 Real Decreto Legislativo 1/1996) la respuesta a esta incógnita dependerá de la intensidad de la intervención humana en el proceso de obtención de esta respuesta. "Si el sistema generativo constituye una mera herramienta o medio para la creación por parte del autor humano, quedarán protegidas (sus respuestas) como creación de éste (…). Sin embargo, si por las características del sistema y, supuesta autonomía, las creaciones son llevadas a cabo por el propio sistema inteligente generativo sin intervención humana o con su intervención, pero no siendo ésta significativa o no relevante para el resultado específico, las mismas no podrían ser protegidas como obra intelectual conforme a los marcos jurídicos vigentes, reguladores del derecho de autor, por no concurrir los requisitos de autoría humana y originalidad."

Con respecto a si las propias instrucciones suministradas al sistema de IA pueden ser protegidas a través de derechos de autor, algunos autores consideran que si la secuencia evidencia complejidad y esfuerzo propios de la autoría humana podrían ser

protegibles incluso como obras literarias o técnicas, pero la cuestión todavía resulta controvertida para la doctrina.[46]

La legislación actual y las contribuciones del Reglamento de IA en esta materia son insuficientes, pero servirán como referencia para futuros desarrollos legislativos que ayuden a diseñar un marco jurídico que fomente la innovación tecnológica sin generar incertidumbre legal.

3. IMPACTO DEL REGLAMENTO DE INTELIGENCIA ARTIFICAL EN EL DERECHO CONTRACTUAL ESPAÑOL DESDE EL PUNTO DE VISTA DE LOS CONTRATOS DE SEGUROS

En el ámbito contractual, la creciente autonomía de estos sistemas plantea desafíos respecto a la formación, validez y cumplimiento de los contratos celebrados total o parcialmente por inteligencia artificial. Por otro lado, en el sector asegurador, la utilización de la IA en la evaluación de riesgos, la fijación de primas y la gestión de siniestros puede dar lugar a cuestiones sobre equidad, transparencia y posible discriminación algorítmica. La necesidad de compaginar el derecho español con estos cambios será crucial para garantizar la seguridad jurídica y la protección de los consumidores en un entorno digital cada vez más automatizado.

El legislador europeo considera el derecho contractual, particularmente en sectores esenciales como los contratos financieros o los contratos de seguros, como un área sensible. Esto se ve en el hecho de que en el Anexo III del Reglamento se consideran como de alto riesgo los sistemas de IA "destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud". La misma consideración se da a los sistemas de IA "usados para evaluar la calificación crediticia o solvencia de las personas físicas". Esto, en primer lugar, implica que las compañías bancarias y aseguradoras en España que quieran incorporar sistemas de Inteligencia Artificial en sus operaciones estarán sometidos a las obligaciones más exigentes del Reglamento en términos de seguridad, calidad y transparencia, siendo particularmente relevante la obligación de llevar a cabo una

[46]Vela, J. M. M. (2024). Inteligencia artificial generativa. Desafíos para la propiedad intelectual. *Revista de Derecho de la UNED (RDUNED),* (33), Págs. 17-75. https://doi.org/10.5944/rduned.33.2024.41924

evaluación de impacto relativa a los derechos fundamentales, y notificar su resultado a la autoridad de vigilancia del mercado antes de su puesta en funcionamiento.

Dicha evaluación de impacto se encuentra regulada en el art. 27 del Reglamento de Inteligencia Artificial, y consistirá en: una descripción de los procesos en los que se utilizará el sistema; el período y la frecuencia de su uso; las categorías de personas y colectivos que podrían verse afectados; la identificación de los riesgos específicos para dichos grupos, basándose en la información proporcionada por el proveedor; una descripción de las medidas de supervisión humana aplicadas; y las medidas y mecanismos de gobernanza interna y reclamación que se adoptarán en caso de que los riesgos se materialicen.

A fin de facilitar el cumplimiento de esta obligación, la Oficina de IA elaborará un modelo de cuestionario y una herramienta automatizada. (Art. 27.5 RIA)

Por lo tanto, es conveniente analizar las repercusiones que tendrá la adopción de sistemas de IA en los procesos de contratación dentro de estos sectores de alto riesgo tomando como ejemplo los contratos de seguros de vida y de salud.

El Reglamento de Inteligencia Artificial impactará el derecho de contratos y seguros en España a lo largo de tres fases clave (precontractual, contractual y poscontractual)[47] en función de que uso se de al sistema de Inteligencia Artificial.

En la fase precontractual, el asegurador puede emplear sistemas de inteligencia artificial que interactúen directamente con posibles clientes en la forma de "chatbots" por lo que será de aplicación la obligación de transparencia contenida en el art. 50.1 del Reglamento, que exige que dichos posibles clientes sean informados de que están interactuando con una IA. También pueden usarse estos sistemas en esta fase para determinar el riesgo a cubrir con base en el cuestionario de riesgo que se debe presentar al tomador de acuerdo con el art. 10 de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro (LCS). Puesto que un sistema de IA con esta finalidad ayudaría a la toma de decisiones relacionadas con una persona física, deberá cumplirse la obligación de transparencia prevista en el art. 26.11 del Reglamento. Esta obligación implica informar

[47]Tapia, A (6 de Junio de 2024) *Inteligencia artificial y pólizas de seguro*. Recuperado el 1 de febrero de 2025 de https://ajtapia.com/2024/06/inteligencia-artificial-y-polizas-de-seguro/

al tomador previamente de que si decide continuar con el proceso, estará expuesto al uso de sistemas de IA de alto riesgo.

En consonancia con esta obligación de transparencia, se reconoce en el art. 86 del Reglamento un derecho de información por parte de todo sujeto que se vea afectado por una decisión que tenga consecuencias jurídicas y haya sido tomada con base en los resultados de salida proporcionados por un sistema de IA. Este derecho obligará a las empresas aseguradoras a aportar "explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada."

Más allá de estas obligaciones de transparencia, también son relevantes algunas obligaciones relacionadas con la seguridad del sistema, puesto que el Reglamento impone en sus art. 14 y 26 que los sistemas de alto riesgo puedan ser vigilados y sigan el principio de supervisión humana por personas con el apoyo, la competencia, formación y autoridad necesarias para ello. Por eso, las compañías aseguradoras tendrán que prestar especial atención tanto a "las medidas que el proveedor defina y que integre, cuando sea técnicamente viable, en el sistema de IA de alto riesgo antes de su introducción en el mercado o su puesta en servicio", como a "las medidas que el proveedor defina antes de la introducción del sistema de IA de alto riesgo en el mercado o de su puesta en servicio y que sean adecuadas para que las ponga en práctica el responsable del despliegue."

Además, el art. 26.4 del Reglamento obliga a que el implantador garantice que los datos de entrada suministrados al sistema "sean pertinentes y suficientemente representativos a la vista de la finalidad prevista del sistema de IA de alto riesgo." Este requisito puede conectarse con el mencionado cuestionario de riesgo previsto en el art. 10 LCS, en el que el tomador declararía toda información relevante que le fuese preguntada, por lo que parece que este punto no generaría mayores complicaciones siempre que solo se suministren estos datos al sistema.

Por lo tanto, las compañías aseguradoras pueden usar Inteligencia Artificial en la fase precontractual, ya sea como "chatbots" que interactúe directamente con el cliente o como herramienta para analizar el cuestionario de riesgo del art. 10 LCS cumplimentado por el tomador para evaluar el riesgo a cubrir. Sin embargo, ello implica una serie de obligaciones de seguridad y transparencia, y un minucioso seguimiento de las

instrucciones dadas por el proveedor del sistema, que deberán cumplirse para evitar las importantes sanciones administrativas que impone el Reglamento.

En la fase contractual, la LCS en su art. 8 impone unos contenidos mínimos que deben ser incluidos en la póliza:

"1. Nombre y apellidos o denominación social de las partes contratantes y su domicilio, así como la designación del asegurado y beneficiario, en su caso.

2. El concepto en el cual se asegura.

3. Naturaleza del riesgo cubierto, describiendo, de forma clara y comprensible, las garantías y coberturas otorgadas en el contrato, así como respecto a cada una de ellas, las exclusiones y limitaciones que les afecten destacadas tipográficamente.

4. Designación de los objetos asegurados y de su situación.

5. Suma asegurada o alcance de la cobertura.

6. Importe de la prima, recargos e impuestos.

7. Vencimiento de las primas, lugar y forma de pago.

8. Duración del contrato, con expresión del día y la hora en que comienzan y terminan sus efectos.

9. Si interviene un mediador en el contrato, el nombre y tipo de mediador."

Además, la póliza debe ser redactada conforme a los parámetros de claridad, precisión e integridad según el art. 3 de la misma ley. Estos parámetros son interpretados por el Tribunal Supremo de tal forma que "la finalidad del artículo 3º es la de facilitar el conocimiento de las condiciones generales del contrato por parte del tomador del seguro."[48]

[48]Sentencia del Tribunal Supremo núm. 7538/2003, de 27 noviembre de 2003, Sala de lo Civil, (rec. 188/1998).

Esto se traduce en cuatro exigencias para que las cláusulas de la póliza se consideren incorporadas al mismo:

"i) Que se incluyan por el asegurador en la proposición de seguro (si la hubiere) y necesariamente en la póliza del contrato o en un documento complementario.

(ii) Que la póliza y, en su caso, el documento complementario, se suscriba (es decir, se firme) por el asegurado.

(iii) Que se entregue al asegurado copia de tales documentos.

(iv) Que el condicionado de la póliza se redacte de forma clara y precisa."[49]

Por lo tanto, aquellas compañías aseguradoras que quieran integrar sistemas de Inteligencia Artificial generativa en sus procesos de redacción de las pólizas deberán cumplir las obligaciones de seguridad ya detalladas que impone el Reglamento y asegurarse de que el lenguaje, y los contenidos generados por estos sistemas son acordes a los parámetros del art. 3 LCS y se cumplen las 4 exigencias expuestas. También deberán añadir a los contenidos mínimos que incluye el art. 8 LCS la obligación de transparencia del art. 26.11 del Reglamento en los mismos términos que en la fase precontractual. Como particularidad encontramos que también deberán conservar los registros generados por el sistema de Inteligencia Artificial en cuestión durante un periodo mínimo de 6 meses, tal y como se expresa en el art. 26. 6 del Reglamento de Inteligencia Artificial

Por último, en la fase postcontractual, AEFI-UNESPA considera que la IA puede tener 4 usos principales: "i) mejorar el análisis de fraude (puntuación de siniestros, detección de anomalías, análisis de redes sociales y modelización del comportamiento); ii) estimar el valor de las pérdidas, en particular en siniestros de alta frecuencia; iii) evaluar los costes de reparación en seguros de hogar, locales comerciales y automóviles mediante el reconocimiento de imágenes; iv) segmentar de manera automatizada las

[49]Reglero Campos, L. F. (2005). Cláusulas limitativas y cláusulas delimitativas del riesgo en los seguros de responsabilidad civil. *Comentarios a las Sentencias de Unificación de Doctrina (Civil y Mercantil) 2005-2007*, Págs. 179-210.

reclamaciones por tipo y complejidad; y v) automatizar la verificación y el pago de facturas."[50]

Sorprendentemente, el primero de estos usos para la IA estaría exento de la consideración como sistema de alto riesgo, puesto que se trata de un sistema diseñado para "detectar fraudes financieros" y por lo tanto su uso no se encontraría sujeto a las obligaciones del Reglamento mencionadas hasta ahora, salvo que interactúen directamente con el tomador del seguro, en cuyo caso sería de aplicación la obligación de transparencia del art. 50 del Reglamento al estar prevista para sistemas de alto riesgo y riesgo limitado.

En el segundo y el tercero de estos usos para la IA será de aplicación la obligación de transparencia del art. 26.11 del Reglamento en los mismos términos que en la fase precontractual, pero cobrará especial importancia el derecho de información recogido en el art. 86 del Reglamento. Esto tiene su explicación en el hecho de que el sistema de alto riesgo estaría tomando decisiones que afectan directamente a la valoración del siniestro producido y el importe necesario para su reparación, por lo que cualquier decisión tomada por el sistema que perjudique al tomador tendrá efectos jurídicos relevantes que justificarían ejercer este derecho.

El propósito de este derecho es permitir a la parte perjudicada por una decisión de un sistema de IA de alto riesgo conocer qué papel ha tenido el sistema en esa decisión y cómo se ha utilizado. Se puede conectar este derecho de información con otras medidas como las obligaciones de exhibir pruebas en la Directiva analizada en este trabajo, ya que todas ellas encuentran su razón de ser en facilitar la actividad probatoria al demandante en una demanda por daños y contrarrestar la opacidad con la que operan muchos sistemas de IA por el fenómeno "caja negra". En este caso, la particularidad se halla en que el derecho del art. 86 del Reglamento de Inteligencia Artificial no está vinculado a haber ejercido previamente ninguna acción judicial, pero si a la toma de una decisión mediante un sistema de alto riesgo que tiene efectos jurídicos o es significativamente perjudicial.

[50]AEFI-UNESPA (2023) Informe sobre la digitalización de la industria aseguradora. Recuperado de https://www.unespa.es/main-files/uploads/2023/03/Informe-Digitalizacion-Industria-Aseguradora_feb_2023-DEF_V5.pdf. En Paredes, M. L. M. (2024). Digitalización e inteligencia artificial en el seguro: manifestaciones y encaje legal. Teoría & Derecho. *Revista de pensamiento jurídico*, (37), Págs. 90-119.

Por tanto, puede considerarse una actividad previa que permita al tomador evaluar cómo se ha tomado la decisión y si es apropiado ejercer acciones legales al respecto.

En el cuarto y quinto de estos usos para la IA serán de aplicación la obligación del art. 26.6 del Reglamento, que impone conservar los registros del sistema durante al menos 6 meses, y las obligaciones de seguridad relacionadas con la supervisión humana de los arts. 14 y 26 de la misma norma. Sin embargo, puesto que en estos casos el sistema no interactúa directamente con el cliente, ni contribuye a la toma de decisiones, sino que simplemente facilita la clasificación de archivos, no parece que sean de aplicación las obligaciones de transparencia del art. 50.1 o el art. 26. 11 del Reglamento de Inteligencia Artificial.

En conclusión, la introducción de la Inteligencia Artificial y del Reglamento de Inteligencia Artificial en el ámbito del derecho de contratos y seguros en España exige una profunda revisión y adaptación de los instrumentos jurídicos tradicionales a las nuevas realidades tecnológicas. Este nuevo marco no solo introduce importantes modificaciones a las fases precontractual, contractual y postcontractual mediante obligaciones de transparencia, supervisión humana y la adecuada redacción de pólizas; sino que también fortalece la protección del tomador en un entorno cada vez más automatizado.

Cada sector en el que se empleen sistemas de IA de alto riesgo deberá adaptar estas normas a su normativa nacional aplicable y a sus procesos de contratación en consonancia con los avances regulatorios y tecnológicos, lo que se ve reflejado en este caso en el impacto del Reglamento de Inteligencia Artificial en los contratos de seguros de vida y de salud. A.R Puig se pronuncia en este sentido al mencionar que: "Hace ya mucho tiempo que el derecho privado no puede hacerse ni estudiarse de espaldas al derecho regulatorio y al estado de los conocimientos científicos y técnicos de las materias sobre las que se proyecta."[51]

[51]Puig, A. R. (2024). Una lectura del reglamento de inteligencia artificial desde el derecho privado. *InDret*, (4), Págs. 1-8.

V. CONCLUSIONES

La Inteligencia Artificial, especialmente la IA fuerte, plantea importantes desafíos jurídicos relacionados con la transparencia, la privacidad de los datos suministrados a los sistemas y la eliminación de sesgos discriminatorios de sus procesos de toma de decisiones. Estos desafíos derivados de la irrupción de la Inteligencia Artificial en nuestra sociedad requieren una adaptación urgente del derecho privado para hacer frente a las nuevas realidades tecnológicas.

El Reglamento (UE) 2024/1689 de Inteligencia Artificial supone un primer intento de dotar a la Unión Europea de un marco mínimo que garantice la seguridad, transparencia y protección de los derechos fundamentales en el desarrollo y uso de la IA. Esta disposición es, sobre todo, una norma de riesgos que se enmarca en un proceso de intervención pública progresiva en sectores altamente tecnificados.

Este enfoque identifica distintos niveles de riesgo, distinguiendo entre sistemas prohibidos, sistemas de alto riesgo, sistemas de riesgo limitado y sistemas de riesgo mínimo o nulo. El Reglamento asigna a cada uno de estos niveles obligaciones específicas que como es lógico, son menos estrictas según lo bajo que sea el riesgo del sistema por su complejidad, uso previsto o sector de aplicación, y viceversa. Asimismo, el Reglamento también contiene una regulación específica para los modelos de IA de uso general con y sin riesgo sistémico, lo que incluye aquellos sistemas que no tienen una finalidad concreta, sino que se le pueden dar múltiples usos sin estar limitados a una función específica.

Esta regulación de riesgos tiene como objeto compaginar la innovación tecnológica con la protección de los derechos fundamentales. Pese a tratarse de una norma de derecho regulatorio, su impacto en el derecho privado es innegable y el derecho civil español deberá adaptarse a él. En el ámbito del derecho de daños, resulta necesario imponer la solidaridad como régimen de responsabilidad general, ya que el régimen de responsabilidad mancomunada podría dificultar una reparación integral para la víctima, y causar diferencias de trato según la demanda se fundamente en el Reglamento o en la Directiva sobre responsabilidad por productos defectuosos.

Por otro lado, en materia de propiedad intelectual, el Reglamento afronta tangencialmente el debate sobre la protección de los prompts y la generación de contenido por sistemas de IA, pero la regulación en esta materia sigue siendo francamente insuficiente. Es previsible que las disposiciones del Reglamento servirán como referencia para futuros desarrollos legislativos que ayuden a diseñar un marco jurídico que fomente la innovación tecnológica sin generar incertidumbre legal.

Por último, en el campo contractual, y particularmente en los contratos de seguros, el Reglamento de IA mantiene su preocupación ante los sistemas de alto riesgo y constata la necesidad de adaptar las cláusulas a lo largo de todas las fases del proceso para mantener la seguridad y la transparencia. La necesidad de compaginar el derecho español con estos cambios será crucial para garantizar la seguridad jurídica y la protección de los consumidores

Además, si bien el Reglamento de IA es la pieza clave de la estrategia de la Unión Europea en lo que se refiere a esta tecnología, no es la única norma que va a tener efectos sobre ella. La interacción entre el Reglamento de Inteligencia Artificial y la Directiva sobre responsabilidad por daños causados por productos defectuosos será fundamental a la hora de adaptar el derecho de daños español a la visión europea de la Inteligencia Artificial. Si un operador no implementa adecuadamente las medidas incluidas en estas normas y ello ocasiona un daño, dicho incumplimiento puede considerarse una violación de un deber de diligencia que facilitaría la imputación de responsabilidad civil. Sin embargo, esto no implica que el mero cumplimiento de las obligaciones establecidas en el Reglamento pueda usarse como argumento por parte de los demandados para evitar la imputación de responsabilidad.

En definitiva, el reto que impone el Reglamento de IA al Derecho Civil español radica en la urgente necesidad de actualizar y armonizar el ordenamiento jurídico con los avances regulatorios y tecnológicos europeos. Al tratarse de la primera gran norma en materia de inteligencia artificial, su impacto es especialmente significativo, marca un precedente para futuros desarrollos y subraya el rol pionero de Europa en la regulación de esta tecnología disruptiva. Este enfoque exige una participación activa de nuestras instituciones para su adaptación sin el cual será imposible alcanzar un equilibrio adecuado entre la salvaguarda de los derechos fundamentales y el impulso de la competitividad en el entorno digital europeo.

VI. BIBLIOGRAFIA

1) LEGISLACIÓN

[1] Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE (Diario Oficial de la Unión Europea de 17 de mayo de 2019)

[2] Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo (Diario Oficial de la Unión Europea de 18 de noviembre de 2024)

[3] Ley 50/1980, de 8 de octubre, de Contrato de Seguro. (BOE núm. 250, de 17 de octubre de 1980)

[4] Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. (Gaceta de Madrid, de 25 de julio de 1889.)

[5] Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. (BOE núm. 97, de 22 de abril de 1996.)

[6] Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE núm. 255, de 24 de octubre de 2015)

[7] Real Decreto-ley 24/2021, de 2 de noviembre, de transposición de directivas de la Unión Europea en las materias de bonos garantizados, distribución transfronteriza de organismos de inversión colectiva, datos abiertos y reutilización de la información del sector público, ejercicio de derechos de autor y derechos afines aplicables a determinadas transmisiones en línea y a las retransmisiones de programas de radio y televisión, exenciones temporales a determinadas importaciones y suministros, de personas consumidoras y para la promoción de vehículos de transporte por carretera limpios y energéticamente eficientes. (BOE núm. 263, de 03 de noviembre de 2021.)

[8] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Diario Oficial de la Unión Europea de 4 de mayo de 2016)

[9] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de Inteligencia Artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Diario Oficial de la Unión Europea de 12 de julio de 2024)

2) JURISPRUDENCIA

[1] Sentencia del Tribunal Supremo núm. 13461/1992, de 22 de abril de 1992, Sala de lo Civil, (rec. s.n). Fecha de la última consulta: 14 de febrero de 2025.

[2] Sentencia del Tribunal Supremo núm. 6323/1993, de 28 de septiembre de 1993, Sala de lo Civil, (rec. 360/1991). Fecha de la última consulta: 14 de febrero de 2025.

[3] Sentencia del Tribunal Supremo núm. 7518/1998 de 12 de Diciembre de 1998, Sala de lo Civil, (rec. 2104/1994). Fecha de la última consulta: 17 de febrero de 2025

[4] Sentencia del Tribunal Supremo núm. 4410/2002, de 17 de junio de 2002, Sala de lo Civil (rec. 34/1997). Fecha de la última consulta: 14 de febrero de 2025.

[5] Sentencia del Tribunal Supremo núm. 223/2003, Sala de lo Civil, de 14 de marzo de 2003, Sala de lo Civil, (rec. 2235/1997). Fecha de la última consulta: 17 de febrero de 2025

[6] Sentencia del Tribunal Supremo núm. 7538/2003, de 27 noviembre de 2003, Sala de lo Civil, (rec. 188/1998). Fecha de la última consulta: 17 de febrero de 2025

[7] Sentencia del Tribunal Supremo núm. 793/2004, de 10 de febrero de 2004, Sala de lo Civil, (rec. 1105/1999). Fecha de la última consulta: 14 de febrero de 2025.

3) OBRAS DOCTRINALES

[1] HLEG. (2019). *Una Definición de la Inteligencia Artificial: Principales Capacidades y disciplinas Científicas*. Comisión Europea. Pág. 8. https://agatadata.com/wp-content/uploads/2024/11/Una-definicion-de-la-inteligencia-artificial-2019-Comision-Europea.pdf

[2] Samoili, S., Cobo, M. L., Gómez, E., De Prato, G., Martínez-Plumed, F., & Delipetrev, B. (2020). AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence. JRC Technical Reports. https://publications.jrc.ec.europa.eu/repository/handle/JRC118163

[3] Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Tercera Edición. Pearson.

[4] Martinez, R. (2018). Artificial intelligence: Distinguishing between types & definitions. *Nevada Law Journal*, 19(3), Págs. 1016-1037. https://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1799&context=nlj

[5] Haleem, Abid. Javaid, Mohd (2019). Current status and applications of Artificial Intelligence (AI) in the medical field: An overview. *Current Medicine Research and Practice Journal*, 9 (6), Págs. 231-237. https://www.sciencedirect.com/science/article/abs/pii/S235208171930193X

[6] Ruiz, F. J. B. (2022). Aplicaciones de la inteligencia artificial al ámbito biosanitario: Protección de datos y privacidad. Implicaciones éticas y legales. En *Anales de la Cátedra Francisco Suárez*, 56, Págs. 245-268. https://doi.org/10.30827/acfs.v56i.21677

[7] Banco de España. (2022). *Inteligencia artificial y finanzas: una alianza estratégica*. https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/22/Fich/do2222.pdf

[8] Gràcia, X. G. & Sancho-Gil, J. M. (2021). Artificial intelligence in education: Big data, black boxes, and technological solutionism. *International journal of media, technology and lifelong learning*, 17 (2). https://doi.org/10.7577/seminar.4281

[9] Moliner Juan. (2021). Desafíos éticos en la aplicación de la inteligencia artificial a los sistemas de defensa. *Revista DIECISIETE*, Pág. 4. DOI: 10.36852/2695-4427_2021_04.06

[10] Kumar Anil. (2023). Advances in Data Protection and Artificial Intelligence: Trends and Challenges. *International Journal of Advanced Engineering Technologies and Innovations*, 1(01), Págs 294-319. https://ijaeti.com/index.php/Journal/article/view/392

[11] Dwork, C. (2008). Differential Privacy: A Survey of Results. En Agrawal, M., Du, D., Duan, Z., Li, A. (eds) *Theory and Applications of Models of Computation*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-79228-4_1

[12] Cotino, L. (2022). Transparencia y explicabilidad de la inteligencia artificial y "compañía" (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad…). Para qué, para quién y cuánta. *Transparencia y explicabilidad de la inteligencia artificial*, Págs. 29-70. https://dialnet.unirioja.es/servlet/articulo?codigo=8709893

[13] Cotino, L. (2023). Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida. *Revista española de la transparencia*, (16), Págs. 17-63. https://doi.org/10.51915/ret.272

[14] Belloso Martín, N. (2022). La problemática de los sesgos algorítmicos (con especial referencia a los de género). ¿Hacia un derecho a la protección a los sesgos? En F. H. (Coordinador), *Inteligencia Artificial y filosofía del Derecho,* Págs. 45-69. Murcia: Ediciones Laborum S.L.

[15] Aránguez Sánchez, T. (2022). Sesgos sexistas de los algoritmos e Inteligencia Artificial. En T. A. Sánchez, & O. Olariu, *Algoritmo, teletrabajo y otros grandes temas del feminismo digital*, Págs. 71-86. Madrid: Dykinson S.L

[16] Ferrer, X., Van Nuenen, T., Such, J. M., Coté, M., & Criado, N. (2021). Bias and discrimination in AI: a cross-disciplinary perspective. *IEEE Technology and Society Magazine*, 40(2), Págs. 72-80. https://arxiv.org/abs/2008.07309

[17] Miranzo-Diaz, J. (2024). El Reglamento de Inteligencia Artificial de la Unión Europea: regulación de riesgos y sistemas deestandarización. A&C - Revista de Direito Administrativo & Constitucional, 24(96), Págs. 43-78 https://doi.org/10.21056/aec.v24i96.1932

[18] Comisión Europea. (2018) *Inteligencia artificial para Europa.* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0237

[19] Comisión Europea. (2018) *Plan coordinado sobre la inteligencia artificial.* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0795

[20] Comisión Europea. (2020) *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza.* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0065

[21] Comisión Europea. (2025) *Moving forward together: A Bolder, Simpler, Faster Union.* Anexo III. https://commission.europa.eu/document/download/7617998c-86e6-4a74-b33c249e8a7938cd_en?filename=COM_2025_45_1_annexes_EN.pdf#page=23.12

[22] Garea, C. (2023). La Propuesta de Directiva sobre responsabilidad por daños ocasionados por productos defectuosos y su aplicación a la inteligencia artificial. En Santos, F.C.S (et al.), *Estudos en homenagem ao Profesor Doutor Antonio Pinto Monteiro. Volume 1: Direito Civil*. Boletim da Facultade de Direito, Págs. 179-206. http://hdl.handle.net/2183/40214

[23] Puig, A. R. (2024). Una lectura del reglamento de inteligencia artificial desde el derecho privado. *InDret*, (4), Págs. 1-8. https://indret.com/wp-content/uploads/2024/10/1906.pdf

[24] López, J. A. (2006) *La llamada solidaridad impropia en la jurisprudencia del Tribunal Supremo*. Comunicación presentada en el 6º Congreso de la Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguro. https://www.asociacionabogadosrcs.org/congreso/6congreso/ponencias/Ponencia%20Joaquin%20Ataz%20.pdf

[25] Gómez Calle (2006). Los sujetos de la responsabilidad civil. La responsabilidad civil por hecho ajeno, en Tratado de responsabilidad civil dirigido por REGLERO, 3ª edición. Pág. 486.

[26] Vela, J. M. M. (2024). Inteligencia artificial generativa. Desafíos para la propiedad intelectual. *Revista de Derecho de la UNED (RDUNED),* (33), Págs. 17-75. https://doi.org/10.5944/rduned.33.2024.41924

[27] Reglero Campos, L. F. (2005). Cláusulas limitativas y cláusulas delimitativas del riesgo en los seguros de responsabilidad civil. *Comentarios a las Sentencias de Unificación de Doctrina (Civil y Mercantil) 2005-2007*, Págs. 179-210.

[28] AEFI-UNESPA (2023) Informe sobre la digitalización de la industria aseguradora. En Paredes, M. L. M. (2024). Digitalización e inteligencia artificial en el seguro: manifestaciones y encaje legal. Teoría & Derecho. *Revista de pensamiento jurídico*, (37), Págs. 90-119.

4) RECURSOS DE INTERNET

[1] Waymo. VectorNet: Predicting behaviour to help the Waymo Driver make better decisions. (s.f.). Recuperado el 17 de Octubre de 2024 de https://waymo.com/blog/2020/05/vectornet/

[2] Historic timeline. EU Artificial Intelligence Act. (2024). Recuperado el 16 de Diciembre de 2024 de https://artificialintelligenceact.eu/developments/

[3] Tapia, A (6 de Junio de 2024) *Inteligencia artificial y pólizas de seguro.* Recuperado el 1 de febrero de 2025 de https://ajtapia.com/2024/06/inteligencia-artificial-y-polizas-de-seguro/

[4] Chaves, J. (24 de febrero de 2025) Reglamento de inteligencia artificial, buena administración y control judicial: un nudo gordiano - delajusticia.com - El rincón jurídico de José Ramón Chaves. Recuperado el 10 de marzo de 2025 de delaJusticia.com. https://delajusticia.com/2025/02/20/reglamento-de-inteligencia-artificial-buena-administracion-y-control-judicial-un-nudo-gordiano/