

INTELIGENCIA ARTIFICIAL Y DERECHO: DESAFÍOS JURÍDICOS DE UNA TRANSFORMACIÓN TECNOLÓGICA

Miriam Judit Gómez Romero

Leticia Latorre Luna

Carlos Teruel Fernández

José Torres Remírez

Alejandro Zornoza Somolinos

FORO JURÍDICO

**INTELIGENCIA ARTIFICIAL
Y DERECHO: DESAFÍOS JURÍDICOS
DE UNA TRANSFORMACIÓN
TECNOLÓGICA**

CONSEJO EDITORIAL

MIGUEL ÁNGEL COLLADO YURRITA

JOAN EGEA FERNÁNDEZ

ISABEL FERNÁNDEZ TORRES

JOSÉ IGNACIO GARCÍA NINET

JAVIER LÓPEZ GARCÍA DE LA SERRANA

BELÉN NOGUERA DE LA MUELA

LUIS PRIETO SANCHÍS

FRANCISCO RAMOS MÉNDEZ

RICARDO ROBLES PLANAS

SIXTO SÁNCHEZ LORENZO

JESÚS-MARÍA SILVA SÁNCHEZ

JOAN MANUEL TRAYTER JIMÉNEZ

JUAN JOSÉ TRIGÁS RODRÍGUEZ

Director de publicaciones

INTELIGENCIA ARTIFICIAL Y DERECHO: DESAFÍOS JURÍDICOS DE UNA TRANSFORMACIÓN TECNOLÓGICA

Miriam Judit Gómez Romero

Leticia Latorre Luna

Carlos Teruel Fernández

José Torres Remírez

Alejandro Zornoza Somolinos

La presente obra colectiva se realiza con financiación procedente del Proyecto de Innovación Docente PID 2024-2025 "IA Jurídica: aprendizaje colaborativo y crítico del Derecho a través de la inteligencia artificial generativa", concedido por la Universidad Católica San Antonio de Murcia (UCAM).

Los costes de publicación en acceso abierto serán sufragados con cargo a la financiación otorgada al citado proyecto, dentro de las actuaciones de difusión y transferencia de resultados previstas en el mismo.

Reservados todos los derechos. De conformidad con lo dispuesto en los arts. 270, 271 y 272 del Código Penal vigente, podrá ser castigado con pena de multa y privación de libertad quien reproducire, plagiar, distribuyere o comunicare públicamente, en todo o en parte, una obra literaria, artística o científica, fijada en cualquier tipo de soporte, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

Este libro ha sido sometido a un riguroso proceso de revisión por pares.

© 2026 Los autores

© 2026 Atelier

Santa Dorotea 8, 08004 Barcelona
e-mail: editorial@ateliereditorial.com
<https://atelieropenaccess.com/>
Tel.: 93 295 45 61

I.S.B.N.: 979-13-88510-22-9

Depósito legal: B 20891-2026

Composición: Grafime, Av. Meridiana, 310-312, 08027 Barcelona
www.grafime.com

Impresión: Safekat

SUMARIO

ABREVIATURAS Y ACRÓNIMOS	11
------------------------------------	----

CAPÍTULO I. INTELIGENCIA ARTIFICIAL Y EJERCICIO PROFESIONAL DEL DERECHO: OPORTUNIDADES, RIESGOS Y LÍMITES EN LA PRESTACIÓN DE SERVICIOS JURÍDICOS	13
<i>Carlos Teruel Fernández</i>	

1. La irrupción de la inteligencia artificial en el ejercicio de las profesiones jurídicas.	13
2. Aplicaciones de la inteligencia artificial en la prestación de servicios jurídicos	15
2.1. Investigación jurídica y análisis de jurisprudencia	16
2.2. Redacción de escritos y elaboración documental.	18
2.3. Predicción de resultados y apoyo a la toma de decisiones	21
3. Riesgos jurídicos y deontológicos asociados al uso de la inteligencia artificial	23
3. 1. Fiabilidad, sesgos y alucinaciones	24
3. 2. Protección de datos y confidencialidad profesional	25
3.3. Transparencia, supervisión humana y responsabilidad profesional	27
4. ¿Puede la inteligencia artificial sustituir al jurista?	31
4.1. Límites técnicos y jurídicos de la automatización.	32
4.2. El valor añadido del razonamiento jurídico humano	33
4.3. Nuevos perfiles y competencias profesionales	34
5. Conclusiones	37
6. Bibliografía	40

CAPÍTULO II. LA DIGITALIZACIÓN DEL TRABAJO: INTELIGENCIA ARTIFICIAL, VIGILANCIA COGNITIVA Y NUEVOS DERECHOS LABORALES		43
<i>Miriam Judit Gómez Romero</i>		
1.	Introducción	43
2.	De la automatización del trabajo a la extracción de datos mentales	46
3.	La respuesta regulatoria europea ante la gestión algorítmica: la directiva sobre trabajo en plataformas y el reglamento de IA	49
4.	La expansión de la vigilancia algorítmica en el entorno laboral	56
5.	Neurotecnologías e inteligencia artificial en el trabajo	58
6.	Los neuroderechos ¿una nueva generación de derechos laborales?	61
7.	Conclusiones	65
8.	Bibliografía	68
CAPÍTULO III. RESPONSABILIDAD CIVIL Y DILIGENCIA EN LA CADENA DE VALOR DE LA INTELIGENCIA ARTIFICIAL		71
<i>Alejandro Zornoza Somolinos</i>		
1.	El marco fragmentado de la responsabilidad civil.	71
2.	La fatiga ante los dilemas de la responsabilidad civil por daños causados por sistemas inteligentes	76
3.	La arquitectura preventiva del riesgo y la relevancia civil de la cadena de valor	79
4.	Del deber regulatorio a la culpa y al defecto	89
5.	Protección del consumidor y diligencia reforzada en el uso de IA	92
6.	Conclusiones	94
7.	Bibliografía	99
CAPÍTULO IV. LA INTELIGENCIA ARTIFICIAL COMO HERRAMIENTA EFICAZ PARA LA PREVENCIÓN DE INSOLVENCIA Y LA REESTRUCTURACIÓN DE DEUDAS		103
<i>Leticia Latorre Luna</i>		
1.	Introducción.	103

2.	La inteligencia artificial como herramienta avanzada para la detección proactiva de riesgos financieros	105
2.1.	Evaluación y análisis de activos mediante el uso de la inteligencia artificial	105
2.2.	La optimización de las labores legales y administrativas en los procedimientos de insolvencia mediante el uso de la inteligencia artificial.	108
3.	La implementación de soluciones basadas en inteligencia artificial dentro del proceso de reestructuración de deudas	118
3.1.	La negociación y la toma de decisiones en los procesos de reestructuración de deudas mediante la aplicación de inteligencia artificial	119
3.2.	La aplicación de la inteligencia artificial como herramienta para optimizar el monitoreo y la ejecución de acuerdos y planes de reestructuración	120
4.	Límites y riesgos de la aplicación de la inteligencia artificial en los procedimientos de insolvencia	121
5.	Conclusiones	123
6.	Bibliografía	125

CAPÍTULO V. INTELIGENCIA ARTIFICIAL, ECONOMÍA Y DERECHO: IMPLICACIONES ECONÓMICAS DE LA TOMA DE DECISIONES AUTOMATIZADAS

José Torres Remírez

1.	Introducción.	129
2.	El impacto económico de la digitalización en la economía española (1980-2010)	132
2.1.	La incorporación de las tecnologías de la información y la comunicación	133
2.2.	Productividad y crecimiento económico	134
2.3.	La transformación del mercado de trabajo.	135
2.4.	Competitividad empresarial y apertura internacional.	136
2.5.	El sector público y la administración electrónica.	137
2.6.	La brecha digital como limitación al crecimiento.	138
3.	La incidencia de la digitalización en el Derecho.	138
3.1.	La adaptación del Derecho a la sociedad de la información	139
3.2.	La contratación electrónica y la economía digital	140
3.3.	La protección de datos personales: de la privacidad al activo económico	143

3.3. La protección de datos personales: de la privacidad al activo económico	141
3.4. La administración electrónica y la transformación del sector público.	143
3.5. La digitalización como presupuesto jurídico de la inteligencia artificial	144
4. El impacto económico de la Inteligencia Artificial	144
4.1. La inteligencia artificial como tecnología de propósito general.	145
4.2. Productividad y crecimiento económico	146
4.3. Inteligencia artificial y mercado de trabajo	147
4.4. Competencia, concentración empresarial y poder de mercado	148
4.5. Desigualdad y distribución de la renta	149
5. Conclusiones	150
6. Bibliografía.	154

ABREVIATURAS Y ACRÓNIMOS

BEPS:	Base Erosion and Profit Shifting (Plan BEPS)
BOE:	Boletín Oficial del Estado
CDFUE:	Carta de los Derechos Fundamentales de la Unión Europea
CDI:	Comisión de Derecho Internacional
CE:	Comunidad Europea
CEDH:	Convenio Europeo de Derechos Humanos
CFC:	<i>Controlled Foreign Corporation</i> (sociedades extranjeras controladas)
CIADI:	Centro Internacional de Arreglo de Diferencias Relativas a Inversiones
CIJ:	Corte Internacional de Justicia
CNUDMI:	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
CPJI:	Corte Permanente de Justicia Internacional
CVDT:	Convención de Viena sobre el Derecho de los Tratados
DOUE:	Diario Oficial de la Unión Europea
ECLI:	<i>European Case Law Identifier</i> (identificador europeo de jurisprudencia)

GATT:	Acuerdo General sobre Aranceles Aduaneros y Comercio
ICCA:	<i>International Council for Commercial Arbitration</i> (Consejo Internacional de Arbitraje Comercial)
IFA:	<i>International Fiscal Association</i>
ILA:	<i>International Law Association</i>
IRPF:	Impuesto sobre la Renta de las Personas Físicas
IVA:	Impuesto sobre el Valor Añadido
OCDE:	Organización para la Cooperación y el Desarrollo Económicos
OMC:	Organización Mundial del Comercio
PESC:	Política Exterior y de Seguridad Común
TC:	Tribunal Constitucional
TEDH:	Tribunal Europeo de Derechos Humanos
TFUE:	Tratado de Funcionamiento de la Unión Europea
TGUE:	Tribunal General de la Unión Europea
TJUE:	Tribunal de Justicia de la Unión Europea
TUE:	Tratado de la Unión Europea
UE:	Unión Europea

CAPÍTULO I

INTELIGENCIA ARTIFICIAL Y EJERCICIO PROFESIONAL DEL DERECHO: OPORTUNIDADES, RIESGOS Y LÍMITES EN LA PRESTACIÓN DE SERVICIOS JURÍDICOS

Carlos Teruel Fernández

1. LA IRRUPCIÓN DE LA INTELIGENCIA ARTIFICIAL EN EL EJERCICIO DE LAS PROFESIONES JURÍDICAS

La incorporación de la inteligencia artificial (en adelante, IA) al ámbito jurídico constituye, probablemente, una de las transformaciones más relevantes que han experimentado las profesiones jurídicas desde la generalización del uso de Internet y de las bases de datos documentales. Durante las últimas décadas, la digitalización permitió modernizar la gestión de los despachos profesionales, agilizar el acceso a la legislación y a la jurisprudencia y facilitar las comunicaciones entre los distintos operadores jurídicos. Todas esas innovaciones actuaban como instrumentos de apoyo al trabajo del jurista, pero no intervenían directamente en la construcción del razonamiento jurídico.

La aparición de los sistemas de inteligencia artificial generativa (en adelante, IAG) ha alterado sustancialmente esta realidad. Por primera vez, una herramienta tecnológica no se limita a almacenar o recuperar información, sino que puede generar textos complejos, resumir documentos, elaborar argumentos jurídicos, comparar resoluciones judiciales o proponer distintas alternativas ante un conflicto. Nos encontramos ante una tecno-

logía que empieza a intervenir en actividades tradicionalmente vinculadas al trabajo intelectual del profesional del Derecho, circunstancia que explica el interés que ha despertado tanto en la doctrina como en la práctica profesional (SUSSKIND, *Tomorrow's Lawyers*, 3.^a ed., 2023).

No estamos, por tanto, únicamente ante la incorporación de una nueva herramienta informática al ejercicio profesional. La IA está modificando la forma de prestar los servicios jurídicos. Hasta hace pocos años, una parte importante del trabajo de cualquier abogado, graduado social, asesor jurídico o juez consistía en localizar la información relevante para resolver un determinado asunto. El tiempo dedicado a consultar legislación, jurisprudencia y doctrina era más que considerable. Sin embargo, con las nuevas herramientas de IA, estas tareas pueden realizarse con mucha mayor rapidez ya que tales herramientas son capaces de identificar normas, resumir resoluciones o sugerir líneas iniciales de análisis.

La aparición de la IA en el ámbito jurídico está desplazando progresivamente el centro de gravedad del ejercicio profesional ya que ahora la función del jurista no reside exclusivamente en utilizar sus capacidades para acceder a la información jurídica, sino en saber seleccionarla de forma efectiva, comprobar su fiabilidad, interpretarla correctamente y aplicarla a las circunstancias concretas de cada caso. Por tanto, pese a que el conocimiento del Derecho sigue siendo fundamental, adquiere una importancia creciente la calidad del juicio profesional que se construye a partir de esa información.

Esta transformación o evolución tecnológica alcanza al conjunto de las profesiones jurídicas ya que la IA ya se está utilizando tanto en la elaboración de escritos procesales, como en la revisión de contratos, la investigación jurídica, la gestión documental, el análisis de riesgos normativos o la preparación de estrategias procesales. Incluso las propias administraciones públicas y la Administración de Justicia están incorporando de forma progresiva sistemas destinados a mejorar la gestión de los procedimientos administrativos y judiciales y facilitar tareas de apoyo. Así, como indica un sector de la doctrina, estamos

ante un fenómeno transversal que afecta a buena parte de los operadores encargados de interpretar y aplicar el Derecho (BARRIO ANDRÉS, Legal Tech. La transformación digital de la abogacía, 2ª Ed., 2023).

Las herramientas de IA están agilizando y facilitando la labor de los operadores jurídicos y, por tanto, cambiando el planteamiento del trabajo jurídico. Si determinadas tareas de búsqueda, clasificación o elaboración inicial de documentos pueden ejecutarse de forma cada vez más rápida, resulta razonable pensar que el profesional dedicará una parte creciente de su actividad a aquellas funciones que requieren análisis, interpretación, estrategia, negociación y valoración de las circunstancias concretas del caso.

Más que anticipar la desaparición de las profesiones jurídicas, parece adecuado hablar de una transformación profunda de su ejercicio. Algunas tareas podrán automatizarse o desarrollarse con una eficiencia muy superior, mientras que otras seguirán dependiendo esencialmente del criterio del profesional. Sobre las posibilidades reales que ofrece actualmente la IA en la prestación de servicios jurídicos se centran los apartados siguientes.

2. APLICACIONES DE LA INTELIGENCIA ARTIFICIAL EN LA PRESTACIÓN DE SERVICIOS JURÍDICOS

La incorporación de la IA al ejercicio profesional del Derecho ha dejado de constituir una posibilidad futura para convertirse en una realidad cotidiana. Despachos de abogados, asesorías jurídicas, administraciones públicas e incluso órganos judiciales recurren ya a estas herramientas para agilizar tareas como la investigación jurídica, la elaboración de documentos, el análisis de información o el apoyo a la toma de decisiones. Como pone de manifiesto la doctrina, la verdadera transformación de los servicios jurídicos no reside únicamente en la aparición de nuevas tecnologías, sino en la forma en que estas están modificando la organización y la prestación del trabajo jurídico

(SUSSKIND, *Tomorrow's Lawyers. An Introduction to Your Future*, 3.^a ed., Oxford University Press, Oxford, 2023).

Ahora bien, no todas las aplicaciones presentan la misma utilidad ni ofrecen el mismo grado de fiabilidad. Mientras que algunas resultan especialmente eficaces para optimizar tareas repetitivas o de apoyo, otras continúan requiriendo necesariamente la intervención y el criterio del profesional. En los apartados siguientes se analizan tres de las aplicaciones que presentan una mayor utilidad práctica en el ejercicio cotidiano de las profesiones jurídicas: la investigación jurídica y el análisis de jurisprudencia, la redacción de escritos y elaboración documental, y el apoyo a la toma de decisiones.

2.1. Investigación jurídica y análisis de jurisprudencia

La investigación jurídica es el ámbito en el que la IA ha demostrado hasta el momento una mayor utilidad práctica. Hasta ahora, esta labor ha exigido la consulta de forma sucesiva de la legislación aplicable, la jurisprudencia más reciente y la doctrina científica. Esto suponía dedicar un tiempo más que considerable al tratamiento de la información antes incluso de comenzar el análisis jurídico del caso. La aparición de herramientas de IAG ha modificado esta dinámica de manera considerable ya que éstas permiten localizar normas, resumir resoluciones judiciales, identificar líneas jurisprudenciales o sugerir argumentos jurídicos en cuestión de segundos. Como señala cierto sector de la doctrina, una de las principales aportaciones de estas tecnologías consiste precisamente en facilitar el tratamiento de grandes volúmenes de información jurídica mediante técnicas de aprendizaje automático y procesamiento del lenguaje natural, sin que ello implique un verdadero razonamiento jurídico por parte del sistema (SURDEN, *Artificial Intelligence and Law: An Overview*, 2019).

En la práctica profesional, estas herramientas permiten obtener una primera aproximación al problema jurídico planteado con rapidez sorprendente que hasta hace poco apenas se podía

imaginar. A día de hoy, es posible solicitar a un sistema de IA que identifique la normativa aplicable a un caso concreto, resuma la doctrina jurisprudencial existente sobre una determinada cuestión o incluso se le puede pedir que sugiera distintos enfoques jurídicos desde los que abordar un procedimiento judicial. Todas estas aplicaciones prácticas suponen un importante ahorro de tiempo y facilitan que el profesional pueda concentrar sus esfuerzos en el análisis crítico de la información obtenida y en la construcción de la estrategia jurídica más adecuada.

Sin perjuicio de lo anterior, la utilización de estas herramientas exige una importante cautela, y es que una herramienta de IA generativa de propósito general no garantiza por sí misma que una resolución citada sea auténtica ni que las referencias normativas o jurisprudenciales ofrecidas sean correctas y se encuentren actualizadas. Los sistemas de IA generan respuestas a partir de patrones estadísticos presentes en los datos con los que han sido entrenados, pero no comprenden el verdadero significado de las normas jurídicas ni verifican por sí mismos la exactitud de la información que proporcionan. No saben derecho, pero saben disimularlo perfectamente. Por ello, cualquier cita jurisprudencial o normativa obtenida mediante una herramienta de IA debe ser debidamente contrastada en fuentes oficiales o en bases de datos jurídicas especializadas, como CENDOJ o en cualquier fuente jurídica fidedigna.

Pongamos un ejemplo sobre la utilidad práctica de estas herramientas. Imaginemos una trabajadora que solicita asesoramiento porque desea presentarse a un examen oficial y plantea si puede acogerse al permiso previsto en el artículo 23.1.a) del Estatuto de los Trabajadores. La trabajadora puede consultar a la IA y en cuestión de segundos obtendrá una primera explicación del contenido del precepto, localizará resoluciones judiciales relacionadas con su interpretación e incluso identificará posibles argumentos favorables o contrarios a la pretensión de la trabajadora. Sin embargo, podríamos considerar que esa información es el «punto de partida». Debe ser el profesional quien realmente compruebe la existencia y vigencia de esas resoluciones citadas, analice si resultan real-

mente aplicables al supuesto concreto y valore si existen pronunciamientos más recientes que puedan modificar el criterio inicialmente ofrecido por la herramienta, pues la herramienta puede y suele ofrecer información desactualizada y, en muchas ocasiones, desacertada.

Ante este panorama, parece evidente que la IA no puede sustituir la investigación jurídica, pero sí ha transformado la forma de desarrollarla. Como se ha comentado, ahora las tareas de búsqueda y localización de información se realizan con mayor rapidez, pero la selección de las fuentes relevantes, la interpretación de la jurisprudencia y la construcción de la argumentación jurídica siguen dependiendo del conocimiento y del criterio de los profesionales. Por tanto, el verdadero valor de estas herramientas no reside en ofrecer respuestas definitivas, sino en facilitar a los profesionales una investigación más ágil y eficiente que les permita dedicar más tiempo a aquello que ninguna IA puede hacer por ellos: interpretar el Derecho y aplicarlo correctamente a las circunstancias específicas de cada asunto.

2.2. Redacción de escritos y elaboración documental

La redacción de escritos constituye otra de las aplicaciones en las que la IA ha experimentado un desarrollo especialmente significativo. Actualmente, estas herramientas permiten elaborar en pocos segundos borradores de demandas, recursos, contratos, informes jurídicos o escritos de trámite a partir de unas instrucciones básicas proporcionadas por el usuario. Como destaca determinado sector doctrinal, la automatización de determinadas tareas documentales está transformando la forma en que los profesionales del Derecho organizan su trabajo, al reducir considerablemente el tiempo dedicado a la elaboración material de documentos y permitir concentrar los esfuerzos en aquellas actividades que requieren un mayor valor añadido (SUSSKIND, *Tomorrow's Lawyers. An Introduction to Your Future*, 3.^a ed., Oxford University Press, Oxford, 2023).

En el ámbito jurídico, la utilidad de estas herramientas a la hora de comenzar a redactar desde cero cualquier tipo de escrito jurídico es más que evidente ya que pueden elaborar un borrador que sirva como aceptable punto de partida. Cualquier tipo de demanda, recurso o informe puede ser estructurado con gran rapidez mediante IA, incorporando incluso referencias normativas, argumentos jurídicos o propuestas de redacción que posteriormente deberán ser revisadas y adaptadas por el profesional. Si se utilizan de esta manera, estas aplicaciones permiten reducir el tiempo dedicado a tareas mecánicas y facilitan que el jurista concentre su atención en los aspectos verdaderamente relevantes del asunto.

Ahora bien, debe tenerse en cuenta que un escrito procesal no es una mera sucesión de fundamentos de Derecho correctamente redactados, sino que su eficacia depende de múltiples factores, como la selección de los hechos jurídicamente relevantes, la elección de la acción más adecuada, la valoración de la prueba disponible, la anticipación de los argumentos de la parte contraria o la determinación del momento procesal más oportuno para formular determinadas alegaciones. Hasta el día de hoy, las herramientas actuales de IA no permiten valorar de forma plenamente fiable y contextualizada todos estos factores y ofrecer una respuesta completamente sólida, debiendo ostentar el profesional las competencias necesarias para finalizar con éxito la redacción del escrito.

Otra utilidad práctica y cada vez más utilizada por los profesionales consiste en emplear la IA para revisar los escritos y documentos jurídicos previamente elaborados. En efecto, estos sistemas sirven de gran ayuda para detectar incoherencias argumentales u omisiones, mejorar la claridad y la estructura expositiva, reforzar determinados fundamentos jurídicos o adaptar un mismo escrito a distintos destinatarios, como un cliente, un órgano jurisdiccional o una administración pública. Si se utiliza con esta finalidad, la IA puede actuar como un instrumento complementario muy útil de revisión y control de calidad documental, debiendo en todo caso el profesional realizar la revisión final y aplicar el criterio jurídico más adecuado, adaptando el documento según el caso.

Cabe destacar que la utilización de estas herramientas de IA exige una revisión necesariamente rigurosa. No debe olvidarse que el profesional es el responsable del contenido del documento que firma y presenta. Por ello, debe incidirse en la importancia de comprobar la exactitud de las referencias normativas y jurisprudenciales, verificar la vigencia de las disposiciones citadas y adaptar el texto a las particularidades del asunto concreto. Los sistemas actuales de IA generan respuestas que pueden parecer admisibles y razonables, pero carecen de la capacidad para valorar por sí mismos la corrección jurídica de los resultados que ofrecen (SURDEN, «Artificial Intelligence and Law: An Overview», *Georgia State University Law Review*, vol. 35, núm. 4, 2019). Esta exigencia resulta coherente con el modelo de supervisión humana previsto por el Reglamento (UE) 2024/1689, de Inteligencia Artificial (en adelante, RIA), que, en relación con los sistemas de IA de alto riesgo, exige que puedan ser vigilados de manera efectiva por personas físicas durante su utilización. Aunque esta previsión no resulta directamente aplicable a toda herramienta de IA utilizada en la práctica jurídica, pone de manifiesto la importancia que el legislador europeo atribuye al mantenimiento de un control humano efectivo sobre aquellos sistemas susceptibles de generar riesgos relevantes (art. 14 RIA).

Por tanto, con respecto a la redacción de escritos y documentos, parece innegable que la IA contribuye significativamente a mejorar la eficiencia de la labor de redacción del jurista, pero en ningún caso puede sustituir esta función, pues como se ha comentado, el profesional debe adaptar cada documento al caso concreto. El escrito o documento definitivo seguirá requiriendo conocimiento jurídico, capacidad de argumentación y criterio profesional, disminuyendo únicamente el tiempo dedicado a su elaboración.

2.3. Predicción de resultados y apoyo a la toma de decisiones

La posibilidad de utilizar herramientas de IA para anticipar el resultado de un litigio constituye una de las aplicaciones que mayor interés ha despertado en los últimos años. Gracias al análisis automatizado de grandes volúmenes de resoluciones judiciales, estas herramientas pueden identificar patrones de decisión, localizar precedentes relevantes o detectar determinadas tendencias jurisprudenciales. No obstante, estos sistemas no realizan un verdadero razonamiento jurídico, sino que identifican regularidades estadísticas a partir de los datos con los que han sido entrenados (SURDEN, Artificial Intelligence and Law: An Overview, 2019).

Estas herramientas resultan muy prácticas durante la fase inicial de estudio de un asunto ya que permiten localizar resoluciones jurídicas y/o administrativas relevantes, explorar distintas líneas argumentales, identificar posibles riesgos procesales o analizar la viabilidad de una determinada pretensión. En este sentido, la doctrina ha puesto de relieve que la IA está modificando la forma en que los profesionales prestan sus servicios jurídicos, permitiéndoles dedicar menos tiempo a tareas mecánicas y concentrar sus esfuerzos en aquellas actividades que verdaderamente requieren conocimiento, estrategia y capacidad de decisión (SUSSKIND, Tomorrow's Lawyers. An Introduction to Your Future, 3.^a ed., Oxford University Press, Oxford, 2023).

Desde la práctica profesional, una de las aplicaciones más interesantes y útiles consiste en utilizar la IA como una especie de «abogado del diablo», esto es, una vez el jurista tiene definida la estrategia inicial del asunto, puede solicitarle a la IA que adopte la posición procesal de la parte contraria, identificando posibles debilidades de la demanda o proponiendo argumentos alternativos que permitan poner a prueba la solidez del planteamiento inicialmente diseñado, tanto en el escrito procesal, documento, o incluso a la hora de preparar la instrucción para un juicio. Del mismo modo, la IA puede sugerir medios de prueba

adicionales con lo que no habíamos contado o interpretaciones diferentes de la normativa aplicable, favoreciendo una reflexión jurídica más completa antes de adoptar una decisión definitiva.

Por tanto, la utilización de la IA no se limita al ahorro de tiempo (algo que parece evidente), sino que, empleada como instrumento de contraste, también puede contribuir a mejorar la calidad del asesoramiento jurídico, al obligar al profesional a reconsiderar su propia posición y argumentos, explorar interpretaciones alternativas o anticipar objeciones que han podido pasar inadvertidas. En este sentido, y en este ámbito, la utilidad de la IA no reside únicamente en proporcionar respuestas, sino también en plantear nuevas cuestiones que permitan corroborar si la estrategia jurídica diseñada es la más adecuada para el asunto concreto. Esto ayudará al jurista a adoptar una decisión definitiva ante cualquier planteamiento. Así, la IA puede actuar como un mecanismo complementario de reflexión que amplía las posibilidades de análisis del profesional, pero no desplaza en ningún caso la responsabilidad profesional en la elección definitiva de su estrategia.

Como se ha indicado, conviene evitar interpretaciones excesivamente optimistas acerca de las capacidades predictivas de estas herramientas toda vez que el resultado de un procedimiento judicial depende de multitud de elementos que difícilmente pueden ser reproducidos mediante un algoritmo, como la valoración de las pruebas practicadas por las partes, la credibilidad de las propias partes y de los testigos, las circunstancias específicas del procedimiento o la propia interpretación que pueda realizar el órgano jurisdiccional. Como advierte la doctrina especializada, pese a que las aplicaciones de IA ofrecen mejores resultados cuando procesan grandes cantidades de información, debe tenerse en cuenta que presentan importantes limitaciones en aquellas tareas que exigen razonamiento, interpretación o valoración contextual (KAPOOR/HENDERSON/ NARAYANAN, *Promises and Pitfalls of Artificial Intelligence for Legal Applications*, 2024).

Por todo lo anterior, resultaría correcto señalar que la IA no puede predecir el resultado de un procedimiento judicial, pero

sí puede contribuir a mejorar el proceso de toma de decisiones del profesional. Sin ninguna duda, estas herramientas serán útiles para ordenar información, identificar riesgos, ofrecer distintas perspectivas de análisis y facilitar una visión más completa del problema jurídico. Sin embargo, la elección final de la estrategia procesal corresponderá en todo caso al jurista. El profesional debe valorar críticamente toda la información de la que dispone y asumir la responsabilidad que exige la toma de decisiones en este ámbito.

3. RIESGOS JURÍDICOS Y DEONTOLÓGICOS ASOCIADOS AL USO DE LA INTELIGENCIA ARTIFICIAL

Pese a que, como se ha indicado, la progresiva incorporación de herramientas de IA al ejercicio de las profesiones jurídicas ofrece importantes ventajas en términos de eficiencia y productividad, su utilización también está planteando desafíos significativos desde la perspectiva jurídica y deontológica. El peligro de generar respuestas incorrectas o desactualizadas, el tratamiento de información confidencial y la opacidad de estos sistemas obligan a extremar la diligencia en su uso ya que pueden derivar en una exigencia de responsabilidad hacia el profesional. Los abogados, graduados sociales, asesores jurídicos y demás operadores jurídicos responden profesionalmente de los escritos y documentos que elaboran, de las decisiones que adoptan y del asesoramiento que prestan a sus clientes. En consecuencia, el aprovechamiento de las ventajas que ofrece la IA exige conocer también sus principales limitaciones y actuar siempre con criterio crítico y supervisión humana.

Partiendo de estas premisas, en los apartados siguientes se analizarán tres de los principales riesgos asociados a la utilización de la IA en el ámbito jurídico: la fiabilidad de las respuestas generadas por estos sistemas y el fenómeno de las denominadas «alucinaciones», la protección de los datos personales y la confidencialidad de la información utilizada y, finalmente, las

exigencias de transparencia, supervisión humana y responsabilidad profesional que deben presidir el empleo de estas herramientas.

3.1. Fiabilidad, sesgos y alucinaciones

La principal limitación que presenta actualmente la IA en el ámbito jurídico no radica en su capacidad para generar respuestas, sino en la fiabilidad de dichas respuestas. Los modelos de IAG producen textos con un elevado grado de coherencia lingüística, lo que puede transmitir al usuario una apariencia de seguridad y precisión que, en ocasiones, no se corresponde con la realidad. Estos sistemas generan respuestas a partir de patrones estadísticos presentes en los datos con los que han sido entrenados, pero no verifican la veracidad de la información ni comprenden el significado jurídico de las normas o resoluciones que citan (SURDEN, *Artificial Intelligence and Law: An Overview*, 2019).

A esta circunstancia se une otro de los fenómenos más conocidos de la IAG, las denominadas alucinaciones. Bajo esta expresión se hace referencia a aquellas situaciones en las que el sistema ofrece información objetivamente falsa (como citas jurisprudenciales inexistentes, referencias normativas incorrectas o afirmaciones carentes de respaldo jurídico) presentándola con absoluta naturalidad y sin advertir al usuario de su posible inexactitud. Como señala LUNA ÁLVAREZ, este problema constituye uno de los principales desafíos para la utilización responsable de la IA en el ámbito jurídico, ya que la apariencia de corrección formal puede inducir al profesional a confiar en respuestas que carecen de fundamento jurídico (LUNA ÁLVAREZ, «Anatomía jurídica del sesgo algorítmico en el uso de la inteligencia artificial», *Revista de Derecho y Proceso Penal*, n.º 79, 2025).

En los últimos años ya se han producido casos en los que profesionales del Derecho han incorporado a sus escritos resoluciones judiciales inexistentes o referencias jurisprudenciales

inventadas por herramientas de IA, dando lugar incluso a pronunciamientos judiciales y expedientes disciplinarios. Estos supuestos ponen de manifiesto que el principal riesgo para el profesional es la falta de verificación crítica y efectiva del resultado obtenido, pudiendo llegar a ser sancionado por una infracción deontológica, sin perjuicio de los daños y perjuicios ocasionados. Como se ha señalado, la IA puede equivocarse y ofrecer información incorrecta y/o desactualizada, por lo que toda referencia normativa, jurisprudencial o doctrinal obtenida mediante IA debe contrastarse posteriormente en fuentes oficiales o en bases de datos jurídicas especializadas. Como recuerda determinado sector doctrinal, la incorporación de la IA al razonamiento jurídico sólo resulta compatible con un ejercicio responsable de la profesión cuando el profesional conserva el control sobre el proceso de interpretación y verifica de forma crítica la información suministrada por la herramienta (MARCILLA CÓRDOBA, «Inteligencia artificial y razonamiento jurídico: una aproximación a su alcance y límites», *Anales de la Cátedra Francisco Suárez*, n.º 60, 2026).

Es cierto que la IA puede cometer errores con una apariencia de autoridad que puede generar una confianza injustificada, pero la fiabilidad de la respuesta nunca debe presumirse, sino que debe comprobarse.

3.2. Protección de datos y confidencialidad profesional

La utilización de herramientas de IA en el ejercicio de las profesiones jurídicas plantea importantes interrogantes en materia de protección de datos personales y confidencialidad profesional. A diferencia de otras aplicaciones tecnológicas utilizadas habitualmente en los despachos, los sistemas de IAG requieren que el usuario introduzca información para generar una respuesta adaptada a sus necesidades. Cuando esa información procede de un expediente profesional, contiene datos personales de clientes o incorpora estrategias procesales, el tratamiento de dichos datos debe realizarse con pleno respeto a la

normativa vigente y a los deberes de secreto profesional que caracterizan el ejercicio de la abogacía.

Los asuntos jurídicos que se encomiendan a los profesionales del Derecho contienen todo tipo de datos personales e información que en ocasiones es especialmente sensible por su carácter económico, empresarial o familiar, a veces afectando incluso a menores de edad. La introducción de estos datos en una plataforma de IA cuyo funcionamiento o condiciones de tratamiento no resultan suficientemente conocidos puede comprometer la confidencialidad de la información y generar riesgos importantes tanto para el cliente, que podría ver filtrada esa información, como para el propio profesional, que podría responder profesionalmente por este hecho. La doctrina ha afirmado que la incorporación de la IA a la práctica jurídica obliga a reinterpretar los tradicionales deberes de confidencialidad y secreto profesional a la luz de las nuevas formas de tratamiento automatizado de la información (BELDARRAIN GONZÁLEZ, I., «La inteligencia artificial y el futuro ético de la abogacía», 2025).

Desde una perspectiva normativa, el tratamiento de los datos personales mediante herramientas de IA está sometido a las exigencias del Reglamento (UE) 2016/679 (RGPD), de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, así como, en el ámbito profesional, a la reciente Ley Orgánica 5/2024, de 11 de noviembre, del Derecho de Defensa. Esta Ley Orgánica, principalmente en su artículo 16, refuerza la garantía de confidencialidad de las comunicaciones entre abogado y cliente y la protección del secreto profesional como elementos esenciales del derecho de defensa.

Los profesionales deben ser muy cautelosos antes de incorporar información de un cliente a una herramienta de IA, sobre todo, en aquellas que no son estrictamente jurídicas y que nutren de información a la propia herramienta. En todo caso, resulta aconsejable anonimizar previamente los documentos, eliminar cualquier dato o información que permita reconocer directa o indirectamente a alguna de las partes integrada en el procedimiento administrativo o judicial. Del mismo modo, siempre conviene utilizar herramientas de IA que ofrezcan sufi-

cientes garantías sobre el tratamiento de la información, preferiblemente que sean específicas del sector jurídico o al menos de entornos corporativos en los que el proveedor garantice que los datos no serán utilizados para el entrenamiento de modelos ni cedidos a terceros.

Cabe destacar que el deber de confidencialidad constituye una obligación deontológica que no desaparece por el hecho de que el profesional utilice una aplicación de IA. El jurista sigue siendo responsable de preservar el secreto profesional y de adoptar las medidas necesarias para impedir accesos no autorizados o tratamientos incompatibles con la finalidad para la que obtuvo la información de su cliente. En este sentido, la doctrina viene confirmando que la IA no modifica el contenido del deber de secreto profesional, sino que simplemente obliga a extremar las precauciones para garantizar su cumplimiento dentro de un entorno tecnológico mucho más complejo (FEBLES POZO y NIETO ROJAS, dirs., *Inteligencia artificial y protección de datos: desafíos en la era digital*, 2025).

En virtud de lo anterior, sería conveniente que los profesionales del Derecho incorporaran protocolos internos de actuación que permitan compatibilizar las ventajas de las herramientas de IA con el pleno respeto a la privacidad, a la protección de datos y a la confidencialidad profesional. La confianza del profesional con su cliente es uno de los pilares básicos sobre los que se asienta el ejercicio de las profesiones jurídicas y, por tanto, ninguna mejora en términos de eficiencia puede justificar que la utilización de la IA pueda vulnerar el deber esencial de confidencialidad que se les exige.

3.3. Transparencia, supervisión humana y responsabilidad profesional

El progresivo uso de herramientas de IA en el ámbito jurídico sitúa en el centro del debate tres aspectos estrechamente vinculados: la transparencia, la supervisión humana y la responsabilidad profesional. Su importancia es evidente toda vez

que estas tecnologías intervienen en actividades vinculadas con la interpretación y aplicación del Derecho, en las que el resultado obtenido puede influir en decisiones que afectan directamente a los derechos e intereses de las personas.

Uno de los principales problemas que presentan los actuales modelos de IA es la dificultad para conocer cómo alcanzan determinadas conclusiones. Normalmente, los usuarios reciben respuestas aparentemente correctas, pero sin disponer de la información suficiente sobre las fuentes que se han utilizado para llegar a la misma, el proceso que se ha seguido para generarla o las razones que han justificado el resultado obtenido. Esta falta de transparencia, conocida habitualmente como el «problema de la caja negra» (o «black box»), dificulta que los profesionales puedan confiar plenamente en la información recibida y constituye uno de los principales retos para la incorporación de la IA al ámbito jurídico (PERICH SEÑÉ y SÁNCHEZ PÉREZ, *Inteligencia artificial, justicia y Estado de Derecho*, 2026).

Como es lógico, un profesional del Derecho no puede otorgar el mismo valor a una respuesta cuyo fundamento puede identificar y comprobar que a otra respecto de la cual desconoce las fuentes o el proceso que ha conducido al resultado. Esta circunstancia obliga a extremar la cautela cuando los resultados de la herramienta pretenden incorporarse a un dictamen, una demanda, un recurso o cualquier otro documento o escrito procesal susceptible de producir consecuencias jurídicas en el seno de un procedimiento. Por muy sofisticada que parezca la respuesta, esta debe comprobarse en todo caso sin que pueda convertirse, por sí sola, en una garantía de corrección jurídica.

Para hacer frente a estos riesgos y garantizar su adecuada utilización, el RIA atribuye una especial importancia a la supervisión humana. En particular, su artículo 14 establece que los sistemas de IA de alto riesgo deberán diseñarse y desarrollarse de manera que puedan ser vigilados de forma efectiva por personas físicas durante el período en el que estén siendo utilizados. Con este precepto, el RIA pretende que quienes intervienen en el funcionamiento de estos sistemas de IA puedan comprender adecuadamente sus capacidades y limitaciones,

interpretar sus resultados, detectar posibles anomalías y, cuando resulte necesario, decidir no utilizarlos o apartarse de las respuestas proporcionadas. En este sentido, la doctrina destaca que la supervisión debe ser real y efectiva y no convertirse en una mera intervención formal del profesional (LAZCOZ MORATINOS, *La vigilancia o supervisión humana en el artículo 14 del Reglamento de inteligencia artificial: ¿Un mero requisito obligatorio para los sistemas de alto riesgo?*, 2024).

La exigencia de intervención humana no puede consistir simplemente en validar el resultado ofrecido por la herramienta, pues ello convertiría la supervisión en un trámite carente de contenido material. El abogado, graduado social o asesor jurídico debe encontrarse en condiciones de cuestionar la respuesta, identificar sus posibles deficiencias y apartarse de ella cuando su conocimiento del Derecho o las circunstancias específicas del asunto así lo aconsejen. Por tanto, este control humano exige que el profesional conserve el dominio sobre el proceso de decisión y que la utilización de la IA no reduzca su capacidad para formar un juicio jurídico propio.

Cabe destacar en este punto el denominado sesgo de automatización, esto es, la tendencia a confiar de forma automática o excesiva en los resultados proporcionados por un sistema. El propio artículo 14.4.b) RIA contempla expresamente este riesgo al regular la supervisión de los sistemas de IA de alto riesgo. En el ámbito jurídico, este sesgo puede resultar bastante problemático, puesto que cuando se obtiene una respuesta bien estructurada, formulada con un lenguaje técnico y aparentemente respaldada por referencias normativas o jurisprudenciales puede generar una confianza superior a la que realmente merece. La supervisión humana debe servir precisamente para evitar que esa apariencia de autoridad reduzca el juicio crítico del profesional, quien debe cuestionarse y revisar en todo momento las respuestas facilitadas por estas herramientas.

La cuestión de la supervisión conduce directa e inevitablemente a la responsabilidad profesional. La utilización de herramientas de IA no modifica el régimen de responsabilidad propio del ejercicio de las profesiones jurídicas, por lo que todo profe-

sional que firme una demanda, interponga un recurso, elabore un contrato o emita un informe jurídico será responsable de su contenido, con independencia de que se haya apoyado o no en estas herramientas para su preparación. Como se ha señalado anteriormente, la aplicación puede participar activamente en la búsqueda de información, en la elaboración de un borrador de documento o escrito, o en el análisis de posibles alternativas, pero no puede asumir la posición jurídica del profesional ni responde frente al cliente, los tribunales o terceros por las consecuencias derivadas de la información suministrada.

Por ello, la incorporación de la IA obliga a reinterpretar los tradicionales deberes de diligencia y competencia profesional de los juristas. La diligencia profesional se extiende ahora también a la forma en que se seleccionan y utilizan las herramientas de IA empleadas en la prestación del servicio jurídico, debiendo conocerse sus limitaciones, comprobar la información obtenida y determinar en qué tareas pueden apoyarse en estas aplicaciones y en cuáles se requiere una intervención exclusivamente profesional. Como ha puesto de relieve la doctrina, la incorporación de herramientas de IA en el ámbito jurídico no elimina los deberes tradicionales de diligencia, independencia y competencia profesional, sino que exige reinterpretarlos ante la creciente utilización de sistemas algorítmicos en la prestación de servicios jurídicos (MEDINA CASCALES, *Responsabilidad algorítmica y deontología profesional en la abogacía: opacidad epistémica, imputación jurídica y redistribución del riesgo en entornos de IA*, 2026).

Como se ha señalado, ante esta nueva realidad tecnológica, sería aconsejable que tanto despachos como asesorías y organizaciones jurídicas desarrollasen protocolos internos para fomentar y garantizar un uso responsable de la IA. Estos protocolos podrían incorporar medidas que redujeran considerablemente los riesgos asociados al uso de la IA, como la selección de las herramientas específicas autorizadas, la determinación de qué información puede introducirse en ellas, la verificación de las fuentes utilizadas, la revisión íntegra de los documentos generados o la identificación de aquellos supuestos en los que resulte

aconsejable prescindir de estos sistemas. Así, se establecerían unas pautas mínimas que permitirían aprovechar sus ventajas sin rebajar los estándares de diligencia propios de la profesión.

4. ¿PUEDE LA INTELIGENCIA ARTIFICIAL SUSTITUIR AL JURISTA?

La creciente incorporación de la IA al ejercicio de las profesiones jurídicas ha reabierto un debate que, hasta hace pocos años, pertenecía más al ámbito de la prospectiva tecnológica que al de la realidad profesional: ¿es posible que estas herramientas lleguen a sustituir al jurista? El extraordinario desarrollo experimentado por los modelos de IAG, unido a su capacidad para redactar documentos, analizar información jurídica o proponer soluciones a problemas complejos, ha alimentado la idea de que determinadas funciones tradicionalmente desempeñadas por abogados, jueces, asesores jurídicos o graduados sociales podrían llegar a ser completamente automatizadas.

Sin embargo, la respuesta a esta cuestión dista mucho de ser sencilla. La IA ha demostrado un enorme potencial para asistir al profesional en numerosas tareas, pero ello no implica necesariamente que pueda reemplazar el conjunto de conocimientos, habilidades y responsabilidades que caracterizan el ejercicio de las profesiones jurídicas. Como sostiene un sector de la doctrina, el futuro de los servicios jurídicos pasará previsiblemente por una profunda transformación tecnológica, aunque ello no significa la desaparición del jurista, sino una redefinición de su papel dentro de un entorno cada vez más digitalizado (SUSSKIND, *Tomorrow's Lawyers. An Introduction to Your Future*, 3.^a ed., Oxford University Press, Oxford, 2023).

Desde esta perspectiva, más que preguntarse si la IA sustituirá al jurista, parece más acertado analizar cuáles son los límites técnicos y jurídicos de la automatización, qué funciones continúan requiriendo necesariamente la intervención humana y cuáles serán las nuevas competencias que deberán adquirir los profesionales del Derecho para desenvolverse en un entor-

no en el que la IA formará parte de su actividad cotidiana. Estos son, precisamente, los aspectos que se examinan en los apartados siguientes.

4.1. Límites técnicos y jurídicos de la automatización

Los avances experimentados por la IA durante los últimos años han alimentado la idea de que determinadas funciones propias de las profesiones jurídicas podrían llegar a automatizarse. La capacidad de estas herramientas para analizar grandes volúmenes de información, localizar jurisprudencia o redactar documentos jurídicos ha llevado a cuestionar si, en un futuro próximo, podrán sustituir total o parcialmente al profesional del Derecho. Sin embargo, esta conclusión resulta, por el momento, difícilmente sostenible.

Desde un punto de vista técnico, los actuales sistemas de IA presentan limitaciones que impiden atribuirles una verdadera capacidad de decisión jurídica. Como explica la doctrina, estos modelos generan respuestas a partir del reconocimiento de patrones estadísticos presentes en los datos con los que han sido entrenados, pero no comprenden el significado de las normas ni desarrollan un auténtico razonamiento jurídico (SURDEN, *Artificial Intelligence and Law: An Overview*, 2019). La evolución de la IA aplicada al Derecho muestra, además, un progresivo desplazamiento desde los sistemas tradicionales de razonamiento basado en casos hacia técnicas de aprendizaje automático capaces de identificar patrones en grandes volúmenes de información jurídica, lo que amplía considerablemente sus posibilidades de análisis sin equiparar necesariamente estas capacidades al razonamiento jurídico humano (ROTOLO/SARTOR, «Artificial Intelligence and Law: Case-Based Reasoning and Machine Learning», 2023).

A estas limitaciones técnicas se añaden otras de naturaleza estrictamente jurídica. La aplicación del Derecho no consiste únicamente en identificar la norma aplicable, sino en interpretar conceptos jurídicos indeterminados, ponderar derechos e

intereses en conflicto, valorar pruebas o apreciar circunstancias específicas del caso. Se trata de operaciones que exigen juicio, prudencia y una valoración contextual difícilmente reducible a un proceso automatizado.

Esta preocupación por preservar la intervención humana se refleja también en el marco regulador europeo. En particular, para los sistemas de IA de alto riesgo, el artículo 14 RIA exige que puedan ser supervisados de forma efectiva por personas físicas y que quienes ejerzan esa supervisión estén en condiciones de interpretar adecuadamente sus resultados y, cuando resulte necesario, decidir no utilizarlos o apartarse de ellos.

A ello se suma una cuestión difícilmente automatizable: la responsabilidad. Quien asesora a un cliente, firma una demanda o emite un informe jurídico responde personal y profesionalmente de su actuación. Esa responsabilidad constituye uno de los pilares del ejercicio de las profesiones jurídicas y no puede trasladarse a un sistema de IA.

Por todo ello, parece más acertado afirmar que la IA automatizará determinadas tareas, pero no el ejercicio profesional del Derecho. Las actividades repetitivas o basadas en el tratamiento masivo de información serán cada vez más eficientes gracias a estas herramientas; sin embargo, aquellas que exigen interpretación, ponderación, estrategia y asunción de responsabilidades continuarán dependiendo del criterio del jurista.

4.2. El valor añadido del razonamiento jurídico humano

El ejercicio de las profesiones jurídicas no consiste únicamente en conocer el contenido de las normas o localizar la jurisprudencia aplicable, sino que su verdadera complejidad reside en interpretar el Derecho, ponderar intereses en conflicto y ofrecer soluciones adaptadas a las circunstancias particulares de cada asunto. Estas tareas constituyen el principal valor añadido del profesional del Derecho y exigen una capacidad de razonamiento que va más allá del mero tratamiento automatizado de la información.

Como manifiesta la doctrina, el razonamiento jurídico no puede reducirse a la aplicación mecánica de reglas previamente establecidas, sino que implica interpretar conceptos jurídicos indeterminados, resolver conflictos entre principios y justificar racionalmente la decisión adoptada. Igualmente, destaca que las herramientas de IA pueden contribuir a identificar precedentes o construir argumentos jurídicos, pero la valoración crítica de esos argumentos y su adecuación al caso concreto siguen dependiendo del jurista (ASHLEY, *Artificial Intelligence and Legal Analytics. New Tools for Law Practice in the Digital Age*, Cambridge University Press, Cambridge, 2017).

La preparación de un procedimiento judicial exige mucho más que elaborar un escrito que sea técnicamente correcto. Es necesario decidir los hechos que deben destacarse, la estrategia procesal que resulta más conveniente, las pruebas que conviene proponer o incluso cuándo resulta preferible llegar a un acuerdo antes que acudir a los tribunales. Este tipo de decisiones requieren experiencia, conocimiento del funcionamiento de la práctica jurídica y capacidad para valorar circunstancias que difícilmente pueden ser reproducidas mediante un algoritmo.

A ello se añade una dimensión esencial de la profesión jurídica como es la relación con el cliente ya que los juristas asesoran, generan confianza, gestionan expectativas y ayudan a adoptar decisiones que, en muchas ocasiones, tienen una importante carga personal, económica o incluso emocional. Esa relación de confianza abogado-cliente no puede ser sustituida por ninguna IA.

Por ello, y como se ha indicado, el verdadero impacto de la IA no consiste en desplazar al jurista, sino en permitirle dedicar menos tiempo a tareas repetitivas y más a aquellas funciones en las que aporta un valor diferencial.

4.3. Nuevos perfiles y competencias profesionales

Tal como se ha señalado, la incorporación de la IA al ejercicio de las profesiones jurídicas está transformando de manera

evidente el perfil competencial que deberán reunir los profesionales del Derecho durante los próximos años. Pese a que el conocimiento técnico del ordenamiento jurídico continúa siendo un requisito indispensable, ante este nuevo panorama, ya no sería suficiente. Ahora, la práctica profesional exige incorporar nuevas habilidades que permitan utilizar estas nuevas herramientas de forma eficaz, crítica y jurídicamente responsable.

Así, las competencias digitales adquieren un protagonismo fundamental toda vez que el profesional del Derecho debe familiarizarse con el funcionamiento básico de las herramientas de IA, conocer sus posibilidades y limitaciones y ser capaz de integrarlas en su trabajo cotidiano sin renunciar al rigor jurídico. Ello no implica que abogados, jueces o asesores jurídicos deban convertirse en expertos en programación o en ingeniería informática, sino que comprendan suficientemente estas tecnologías para ser capaces de utilizarlas de manera segura y eficiente en sus despachos y/o asesorías. Como pone de manifiesto la doctrina, el jurista del futuro no será necesariamente quien más conocimientos tecnológicos posea, sino quien mejor sepa combinar la IA con el razonamiento jurídico y la atención personalizada al cliente (SUSSKIND, *Tomorrow's Lawyers. An Introduction to Your Future*, 3.^a ed., Oxford University Press, Oxford, 2023).

De forma inherente a estas competencias tecnológicas, para optimizar las capacidades de las herramientas de IA, los profesionales deberán tener capacidad para formular correctamente las consultas dirigidas a los sistemas de IA, esto es, deben ser buenos preguntadores para obtener buenas respuestas ya que la calidad de las respuestas depende, en gran medida, de la precisión con la que el jurista describa el problema jurídico, proporcione el contexto necesario y delimite el alcance de la consulta. Así, la formulación de *prompts* adecuados se perfila como una nueva y significativa habilidad profesional, estrechamente vinculada al conocimiento jurídico del usuario porque cuanto mayor sea la preparación técnica del profesional, mayor será también su capacidad para realizar mejores *prompts* y, en consecuencia, obtener resultados más útiles y precisos y, por

supuesto, detectar posibles errores en las respuestas generadas por la herramienta.

Sin perjuicio de lo anterior, la que probablemente continúe siendo la competencia más importante será la capacidad de pensamiento crítico ya que la abundancia de información que genera la herramienta IA obliga al profesional a desarrollar una actitud especialmente rigurosa frente a las respuestas que obtiene de la misma. Saber verificar una resolución judicial, identificar una interpretación errónea, detectar un sesgo o cuestionar una conclusión aparentemente correcta será tan importante como conocer el contenido de una determinada institución jurídica. Como advierte cierto sector doctrinal, la utilización responsable de la IA exige reforzar, y no sustituir, la capacidad crítica del jurista frente a la información proporcionada por estas herramientas (TODOLÍ SIGNES/BELTRÁN DE HEREDIA RUIZ, dirs., *La regulación de la inteligencia artificial y el Derecho del Trabajo. Retos en materia de dirección algorítmica del trabajo*, 2025).

A estas competencias deben añadirse otras habilidades tradicionalmente vinculadas al ejercicio profesional y que, lejos de perder importancia, probablemente adquirirán un mayor protagonismo en los próximos años. La capacidad de negociación, la comunicación con el cliente, el juicio ético, la creatividad en la construcción de soluciones jurídicas o la toma de decisiones en contextos de incertidumbre son competencias difícilmente automatizables y seguirán constituyendo algunos de los principales elementos diferenciadores del profesional del Derecho.

Todo ello obliga también a replantear la formación de los futuros juristas. Las Facultades de Derecho y los programas de formación especializada deberán incorporar progresivamente contenidos relacionados con la IA, la protección de datos, la ética digital y el uso responsable de las nuevas tecnologías aplicadas al ámbito jurídico. No se trata de sustituir la formación jurídica tradicional, sino de complementarla con nuevas competencias que permitan a los futuros profesionales desenvolverse con solvencia en un entorno profundamente digitalizado. La formación continua en IA dejará de ser una opción para convertirse en una exigencia inherente al ejercicio de la profesión.

Dicho lo anterior, podemos afirmar que la IA está contribuyendo a redefinir el perfil del jurista, pero en ningún caso a sustituirlo. El profesional del futuro deberá combinar un sólido conocimiento del Derecho con competencias tecnológicas, pensamiento crítico, sensibilidad ética y capacidad para tomar decisiones responsables. Paradójicamente, cuanto mayor sea el desarrollo de la IA, mayor será también la necesidad de contar con juristas capaces de supervisarla, interpretarla y ponerla al servicio de los principios que inspiran el Estado de Derecho. Esa será, probablemente, la principal competencia del jurista del siglo XXI.

5. CONCLUSIONES

La irrupción de la IA constituye uno de los mayores desafíos a los que se han enfrentado las profesiones jurídicas en las últimas décadas. Más allá del evidente desarrollo tecnológico que suponen estas herramientas, el verdadero alcance de esta evolución debe valorarse por la forma en que está afectando directamente al ejercicio cotidiano del Derecho. La IA es ya una realidad presente que forma parte del trabajo diario de abogados, graduados sociales, asesores jurídicos, jueces y del resto de operadores jurídicos toda vez que existen no sólo multitud de herramientas generales de IA, sino que gran parte de las editoriales jurídicas ya han desarrollado sus propias herramientas de IA, alimentadas con contenidos jurídicos especializados, aunque tampoco sean infalibles.

Parece indiscutible que la IA ofrece importantes oportunidades para que los profesionales presten sus servicios jurídicos de forma más efectiva toda vez que facilita labores esenciales como la investigación jurídica, la elaboración documental o el análisis preliminar de estrategias procesales. Estas funciones pueden desarrollarse actualmente con una rapidez y una eficiencia que hace apenas unos años era difícil de imaginar. Gracias a estas herramientas, el profesional puede ahorrar un tiempo considerable en determinadas tareas repetitivas y dedicarse

mucho más a aquellas funciones que verdaderamente aportan valor al cliente y al sistema de justicia.

Sin perjuicio de lo anterior, no deben ignorarse los riesgos que estas herramientas suponen como las alucinaciones de los modelos generativos, los sesgos presentes en los datos de entrenamiento o la protección de la información confidencial. Ello pone de manifiesto la necesidad de garantizar una supervisión humana efectiva y una actitud especialmente prudente por parte de los profesionales del Derecho. La eficiencia en la gestión de un asunto nunca puede alcanzarse a costa de sacrificar la seguridad jurídica, el secreto profesional o la calidad del asesoramiento prestado.

Con la introducción de estas herramientas, el debate no debería centrarse exclusivamente en determinar si la IA llegará a sustituir a los juristas, una posibilidad que, atendiendo a las capacidades actuales de estos sistemas, no parece plausible en relación con el conjunto de funciones propias de las profesiones jurídicas. La verdadera cuestión ahora es identificar qué funciones van a seguir correspondiendo a los profesionales del Derecho ante un entorno que cada vez más automatizado.

Como se ha comentado, la IA no desplaza en ningún caso el valor del jurista, sino que lo redefine. Tradicionalmente, una parte importante del trabajo jurídico ha estado vinculada a la localización de información, consulta de jurisprudencia o elaboración de documentos y escritos jurídicos. A día de hoy, estas tareas pueden realizarse con ayuda de herramientas de IA en apenas unos segundos, por lo que esa labor ya no constituye por sí sola un valor añadido para el profesional. El verdadero valor añadido del jurista consiste en recopilar la información obtenida, interpretarla críticamente, contextualizarla y convertirla en una estrategia jurídica coherente. Por supuesto, asumirá toda la responsabilidad de las decisiones que adopte, sin que pueda derivarse a la herramienta de IA, al no ser una fuente de información plenamente fiable.

Por tanto, debe concluirse que el futuro de las profesiones jurídicas no depende del grado de desarrollo de la IA, sino de la capacidad de adaptación de quienes las ejercen,

pues el jurista del siglo XXI debe combinar un sólido conocimiento del Derecho con altas competencias tecnológicas, pensamiento crítico, sensibilidad ética y una formación continua que le permita aprovechar las ventajas de estas herramientas sin renunciar a los principios que inspiran el Estado de Derecho.

Debe tenerse en cuenta que en un Estado de Derecho como el actual, y a día de hoy, la IA no puede suponer en ningún caso el final de las profesiones jurídicas, sino el final de una determinada forma de ejercerlas. Los profesionales no van a desaparecer, pero sí deben evolucionar. Las tareas repetitivas se están automatizando, pero tareas como la interpretación del Derecho, la ponderación de intereses en conflicto, la negociación, la creatividad jurídica o el juicio crítico no pueden ser automatizadas en la actualidad, al menos no de forma efectiva. Por ello, el mejor jurista será aquel que sepa integrar la IA en su trabajo como una herramienta al servicio del conocimiento jurídico y no como un sustituto del mismo ya que el Derecho continúa siendo una actividad profundamente humana. La IA puede aplicar normas, redactar documentos u obtener información en segundos, pero las decisiones jurídicas siguen exigiendo prudencia, responsabilidad, capacidad de interpretación y compromiso con la justicia. Mientras esos valores continúen siendo la esencia del Derecho, el jurista seguirá ocupando un lugar insustituible en la prestación de los servicios jurídicos.

La IA no ha venido a sustituir al jurista, sino a exigirle ser mejor jurista. Cuando el acceso a la información deja de ser un elemento diferencial, el verdadero valor del profesional reside en aquello que ninguna tecnología puede automatizar plenamente: el juicio crítico, la responsabilidad y el compromiso con una aplicación justa del Derecho.

6. BIBLIOGRAFÍA

- ASHLEY, K. D., *Artificial Intelligence and Legal Analytics. New Tools for Law Practice in the Digital Age*, Cambridge University Press, Cambridge, 2017.
- BARRIO ANDRÉS, M., *Legal ech. La transformación digital de la abogacía*, 2ª ed. Wolters kluwer, madrid, 2023.
- BELDARRAIN GONZÁLEZ, I., «La inteligencia artificial y el futuro ético de la abogacía», *Derecho Digital e Innovación. Digital law and innovation review*, n.º 26, 2025.
- FEBLES POZO, J. L./NIETO ROJAS, P. (Dirs.), *Inteligencia artificial y protección de datos: desafíos en la era digital*, *Colex, a Coruña*, 2025.
- KAPOOR, S./HENDERSON, P./NARAYANAN, A., «Promises and Pitfalls of Artificial Intelligence for Legal Applications», *Journal of Cross-disciplinary Research in Computational Law*, vol. 2, N.º 2, 2024.
- LAZCOZ MORATINOS, G., «La vigilancia o supervisión humana en el artículo 14 del Reglamento de inteligencia artificial: ¿Un mero requisito obligatorio para los sistemas de alto riesgo?», En COTINO HUESO, L./SIMÓN CASTELLANO, P. (Dirs.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi, 2024, pp. 681-699.
- LUNA ALVAREZ, E. R., «Anatomía jurídica del sesgo algorítmico en el uso de la inteligencia artificial», *Revista de Derecho y Proceso Penal*, nº 79, 2025.
- MARCILLA CÓRDOBA, G. M., «Inteligencia artificial y razonamiento jurídico: una aproximación a su alcance y límites», *Anales de la Cátedra Francisco Suárez*, 60, 2026, pp. 325-353.
- MEDINA CASCALES, J.Á., «Responsabilidad algorítmica y deontología profesional en la abogacía: opacidad epistémica, imputación jurídica y redistribución del riesgo en entornos de IA», *ius et Scientia. Revista electrónica de Derecho y Ciencia*, vol. 12, N.º 1, 2026, pp. 143-153.
- PERICH SEÑÉ, G./SÁNCHEZ PÉREZ, P., «Inteligencia artificial, justicia y Estado de Derecho», *Esade Law Review: De lege ferenda*, n.º 7, 2026, pp. 205-230.

- ROTOLO, A./SARTOR, G., «Artificial Intelligence and Law: Case-Based Reasoning and Machine Learning», en SELLERS, M./KIRSTE, S. (Eds.), *Encyclopedia of the Philosophy of Law and Social Philosophy*, Springer, Dordrecht, 2023, pp. 145-152.
- SURDEN, H., «Artificial Intelligence and Law: An Overview», *Georgia State University Law Review*, vol. 35, N.º 4, 2019, pp. 1305 y ss.
- SUSSKIND, R., *Tomorrow's Lawyers. An Introduction to Your Future*, 3.ª ed., Oxford University Press, Oxford, 2023.
- TODOLÍ SIGNES, A./BELTRÁN DE HEREDIA RUIZ, I. (Dirs.), *La regulación de la inteligencia artificial y el Derecho del Trabajo. Retos en materia de dirección algorítmica del trabajo*, Aranzadi la Ley, Madrid, 2025.

CAPÍTULO II

LA DIGITALIZACIÓN DEL TRABAJO: INTELIGENCIA ARTIFICIAL, VIGILANCIA COGNITIVA Y NUEVOS DERECHOS LABORALES

Miriam Judit Gómez Romero

Profesora Ayudante Doctora Derecho del Trabajo
y de la Seguridad Social
Universidad de Cantabria

1. INTRODUCCIÓN

En la actualidad, los sistemas automatizados de toma de decisiones se aplican a la organización y gestión del trabajo en prácticamente todos los entornos laborales. Los datos personales de las personas trabajadoras se utilizan para optimizar los sistemas algorítmicos de organización y control del trabajo, lo que la doctrina ha denominado gestión algorítmica,¹ así como para asignar tareas y jornadas, determinar la remuneración y evaluar el rendimiento laboral. En consecuencia, la toma de decisiones automatizada constituye hoy un elemento omnipresente en las relaciones de trabajo.

Este proceso de «ratificación» del trabajo ha sido caracterizado por parte de la doctrina como una modalidad de control

1. BAIOTTO S./FERNÁNDEZ MACÍAS E. *The algorithmic management of work: A basic compass, European Commission*. 2022 <https://publications.jrc.ec.europa.eu/repository/handle/JRC129819>

«tecno-normativa»², frecuentemente sustentada en procesos de gamificación del trabajo en plataformas³, entendida esta gamificación como el utilizzo de técnicas y elementos propios de los videojuegos aplicados a la gestión de tareas a desarrollar por personas que trabajan en un entorno digital tales como puntos, niveles o tablas de clasificación con el objetivo principal de impulsar la productividad, esta automatización de la gestión del trabajo descansa sobre un auténtico ciclo de datos de las personas trabajadoras.

En un primer estadio se procede a la recopilación y análisis en tiempo real de la información generada en el entorno laboral por quienes prestan servicios, con el fin de construir representaciones digitales de la actividad desarrollada y seguidamente, esa información se evalúa conforme a objetivos previamente definidos y a determinados estándares de rendimiento, una vez recopilada esta información, se adoptan intervenciones dirigidas a modificar la conducta de las personas trabajadoras para garantizar el cumplimiento de dichos estándares.

Uno de los ámbitos en los que la gestión algorítmica ha alcanzado una mayor implantación es el trabajo en plataformas digitales, especialmente en los sectores del transporte y la logística⁴. En este sentido, la plataformización del trabajo y la gestión algorítmica constituyen fenómenos estrechamente interrelacionados. Resulta igualmente significativo que el trabajo en plataformas, no solo esté sometido a sistemas de gestión algorítmica, sino que también sirva como fuente de datos para el

2. Griesbach K./ REICH A./ ELLIOTT-NEGRI L. /MILKMAN R. *Algorithmic control in platform food delivery work*, *Socius*, 2019

3. DUBAL V. *The house always wins: The algorithmic gamblification of work*, LPE Project. <https://lpeproject.org/blog/the-house-always-wins-the-algorithmic-gamblification-ofwork>, 2023

4. HASSEL A./ ÖZKIZILTAN D. *Governing the work-related risk of AI: Implications for the German government and trade unions*, *Transfer*, 29 (1), 71-86., 2023

entrenamiento y perfeccionamiento de sistemas de inteligencia artificial⁵.

Así, como hemos observado en la última década, las tecnologías basadas en algoritmos, incluidos los sistemas automatizados de supervisión y de toma de decisiones, han hecho posible la aparición y expansión de las plataformas digitales de trabajo, en este punto, no podemos perder de vista el desequilibrio que supone esta nueva forma de trabajo en relación con el poder y opacidad en los procesos de adopción de decisiones y en la alta posibilidad de que la vigilancia tecnológica agrave las prácticas discriminatorias aumentando considerablemente el riesgo para la privacidad, la seguridad, la salud de las personas trabajadoras y el respeto de su dignidad humana.

Desde esta perspectiva, la cuestión jurídica no se agota en la ya clásica discusión sobre la naturaleza laboral o autónoma del vínculo, sin restar importancia a ese debate que sigue siendo central, la mutación más profunda quizá se encuentre en la emergencia de formas de subordinación algorítmica capaces no solo de ordenar la prestación, sino de anticipar conductas, clasificar riesgos, puntuar rendimientos, modular incentivos e inferir estados emocionales, patrones cognitivos o niveles de disponibilidad de la persona trabajadora.

El capítulo aborda la articulación entre el derecho a la privacidad y a la protección de los datos personales, por un lado, y los objetivos de tutela laboral, protección social y seguridad y salud en el trabajo, por otro. Desde esta doble perspectiva, sostiene que la Directiva de Plataformas Digitales⁶ debe garantizar mecanismos efectivos de supervisión, control y tutela frente a

5. GUGLIELMETTI, M. *Automated work and workers' rights: Platform work and AI work management systems*. En L. Hondrich & A. Mollen (Eds.), *Artificial Intelligence, Labour and Society* pp. 127–140. European Trade Union Institute (ETUI), 2024

6. Directiva (UE) 2024/2831 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativa a la mejora de las condiciones laborales en el trabajo en plataformas

las decisiones automatizadas que afecten a las personas trabajadoras.

Del mismo modo, se analiza la regulación de los sistemas de gestión del trabajo basados en inteligencia artificial contenida en el Reglamento de Inteligencia Artificial ⁷, a la luz de las enmiendas de compromiso aprobadas por el Parlamento Europeo.

A partir de dicho análisis, se identifican determinadas lagunas en la protección de las personas trabajadoras y se formulan posibles soluciones destinadas, al menos parcialmente, a corregir tales deficiencias.

2. DE LA AUTOMATIZACIÓN DEL TRABAJO A LA EXTRACCIÓN DE DATOS MENTALES

La transformación tecnológica a la que asistimos presenta rasgos distintos a las anteriores revoluciones industriales, mientras que la mecanización de tareas y automatización de las mismas permitieron sustituir al humano por máquinas en la realización de tareas repetitivas, la aparición y desarrollo de la Inteligencia Artificial afectan a la esfera más íntima ligada al trabajo intelectual y por tanto a la mente humana, por lo que nos acercamos a la sustitución del humano en su esfera más íntima, la mente, así, en el ámbito laboral, los sistemas de Inteligencia Artificial generan inferencias, formulan recomendaciones y participan, con un grado creciente de autonomía, en procesos de decisión que afectan directamente a la organización del trabajo y al ejercicio de las facultades empresariales.

7. 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).

Durante décadas, el debate jurídico se centró, principalmente, en el impacto de la automatización sobre el empleo y la sustitución de mano de obra, sin embargo, el verdadero desafío que plantea la inteligencia artificial no radica únicamente en cuántos puestos de trabajo podrán desaparecer o transformarse, sino en cómo la delegación progresiva de funciones cognitivas en sistemas automatizados altera la propia configuración de la prestación laboral. La cuestión adquiere especial relevancia cuando la organización empresarial desplaza de forma sistemática la deliberación humana hacia sistemas algorítmicos, el riesgo no se limita a una eventual sustitución de la persona trabajadora, sino que alcanza también a la progresiva erosión de aquellas competencias que tradicionalmente justificaban su intervención. Desde esta perspectiva, la gestión algorítmica deja de plantear exclusivamente problemas de transparencia o de protección de datos para proyectarse sobre una dimensión menos explorada: la preservación de la autonomía profesional de la persona trabajadora.

En este punto resulta imprescindible destacar la creciente preocupación del legislador europeo por los riesgos que la gestión algorítmica plantea para los derechos fundamentales de las personas trabajadoras. Dicha preocupación se manifiesta de forma especialmente intensa tanto en la Directiva relativa a la mejora de las condiciones laborales en el trabajo en plataformas, como en el Reglamento de Inteligencia Artificial, ambas normas comparten que la utilización de sistemas algorítmicos en el ámbito laboral no puede traducirse en una sustitución de la decisión humana cuando estén en juego derechos o intereses esenciales de las personas trabajadoras.

La inteligencia artificial ya no pretende únicamente conocer qué hace el trabajador, cuánto produce o cómo ejecuta sus funciones, sino también anticipar cómo se siente, cuál puede ser su nivel de estrés, la probabilidad de desarrollar ansiedad o incluso el riesgo de padecer un síndrome de agotamiento profesional⁸.

8. BELTRÁN DE HEREDIA RUIZ, I. *Inteligencia artificial y neuroderechos: La protección del yo inconsciente de la persona*. Aranzadi, 2023

En este contexto resulta ilustrativo el caso de la empresa española *Healthy Minds*, la cual, ha desarrollado un sistema de inteligencia artificial destinado a predecir la aparición de riesgos psicosociales a partir de los resultados agregados de las evaluaciones obligatorias de riesgos laborales. Según sus promotores, el algoritmo es capaz de estimar con un elevado nivel de precisión la probabilidad de que en una determinada organización aparezcan situaciones de estrés, ansiedad o depresión sin recurrir, al menos formalmente, a la evaluación individualizada de cada trabajador. La herramienta se completa con sistemas automatizados de entrevistas mediante avatares digitales o «metahumanos», que permiten ampliar la obtención de información cualitativa sobre el clima psicosocial de la organización en plazos muy inferiores a los de las metodologías preventivas tradicionales.⁹ El dato relevante ya no es únicamente el facilitado de manera consciente por la persona trabajadora, sino aquel que el sistema es capaz de deducir mediante técnicas de inteligencia artificial a partir de múltiples variables, generando perfiles predictivos sobre su bienestar psicológico o su vulnerabilidad frente a determinados riesgos. No se trata, sin embargo, de una iniciativa aislada, ya que otras empresas¹⁰, han desarrollado plataformas que emplean inteligencia artificial y analítica predictiva para identificar patrones organizativos asociados al estrés, el burnout, la ansiedad o el deterioro del bienestar laboral.

Este fenómeno conecta directamente con la noción de «datos mentales», entendidos estos como aquella información que permite inferir procesos cognitivos, estados emocionales, rasgos

9. CARVAJAL, R. *Healthy Minds: la IA que anticipa problemas mentales en el trabajo*, La Razón, 18 de mayo de 2025, disponible en: https://www.larazon.es/economia/healthy-minds-que-anticipa-problemas-mentales-trabajo_202505186825b5c6f7f20a10d03e30af.html (última consulta: 3 de agosto de 2026).

10. Como por ejemplo Saalg Geomean, Culture Amp, Peakon o Limeade, creadoras de herramientas que comparten la finalidad de anticipar la aparición de riesgos psicosociales mediante el tratamiento automatizado de datos colectivos u organizativos, aunque difieren en las fuentes de información empleadas y en el grado de individualización de los análisis

de personalidad, niveles de atención, fatiga o estabilidad psicológica. Aunque tales datos no siempre proceden de una manifestación explícita del trabajador, pueden obtenerse mediante el análisis combinado de cuestionarios, patrones de comportamiento, interacciones digitales o cualquier otra información susceptible de tratamiento algorítmico. La creciente capacidad de estos sistemas para elaborar inferencias sobre dimensiones internas de la persona plantea interrogantes de gran relevancia constitucional, especialmente en relación con los derechos a la intimidad, a la protección de datos personales, a la dignidad, a la no discriminación y al libre desarrollo de la personalidad.

Desde la óptica preventiva, resulta indudable que herramientas de esta naturaleza pueden contribuir a mejorar la identificación temprana de riesgos psicosociales y facilitar el cumplimiento de las obligaciones empresariales derivadas de la Ley de Prevención de Riesgos Laborales¹¹, pero no debemos perder de vista que la finalidad preventiva no puede convertirse en una vía para legitimar mecanismos permanentes de monitorización psicológica ni para construir perfiles que condicionen decisiones empresariales relativas al acceso al empleo, la promoción profesional, la evaluación del desempeño o el mantenimiento de la relación laboral.

3. LA RESPUESTA REGULATORIA EUROPEA ANTE LA GESTIÓN ALGORÍTMICA: LA DIRECTIVA SOBRE TRABAJO EN PLATAFORMAS Y EL REGLAMENTO DE IA

La Directiva sobre trabajo en plataformas¹² dedica su Capítulo III a la gestión algorítmica, imponiendo obligaciones de

11. Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, BOE núm. 269, de 10 de noviembre de 1995

12. Directiva (UE) 2024/2831 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativa a la mejora de las condiciones laborales en el trabajo

transparencia respecto de los sistemas automatizados de seguimiento y de toma de decisiones, limitando el tratamiento de determinadas categorías de datos personales, entre ellos, los relativos al estado emocional o psicológico de la persona trabajadora y, especialmente, exigiendo que las decisiones con efectos relevantes sobre la relación laboral sean objeto de supervisión humana efectiva, así como del correspondiente derecho a obtener una explicación y solicitar su revisión. Esta misma línea observamos en el Reglamento de Inteligencia Artificial que califica como sistemas de alto riesgo aquellos utilizados en materia de empleo, acceso al trabajo, gestión de la relación laboral y evaluación del rendimiento, sometiénolos a estrictas exigencias de gobernanza, transparencia, supervisión humana y gestión de riesgos.

En el ámbito nacional, España llega a la transposición de la Directiva 2024/2831 con una posición normativa singularmente avanzada en el contexto europeo, pero no por ello suficiente. La Ley 12/2021, de 28 de septiembre¹³, introdujo novedades de gran calado como incorporación de una presunción de laboralidad para las personas que prestan servicios retribuidos de reparto o distribución a través de plataformas digitales cuando la empresa ejerce facultades de organización, dirección y control, directa, indirecta o implícitamente, mediante la gestión algorítmica del servicio o de las condiciones de trabajo. Esta tendencia encuentra reflejo en el art. 64.4.d) del ET¹⁴, que reconoce el derecho de la representación legal de las personas trabajadoras

en plataformas

13. Ley 12/2021, de 28 de septiembre, por la que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales, BOE núm. 233, de 29 de septiembre de 2021.

14. 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 (Ref. BOE-A-2015-11430), texto consolidado, última actualización de 4 de diciembre de 2025

a ser informada de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que inciden en la toma de decisiones susceptibles de afectar a las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles. Asimismo, esta regulación debe interpretarse de forma sistemática con el artículo 22 del Reglamento UE de Protección de datos personales (RGPD¹⁵), y la Ley Orgánica de Protección de Datos (LOPD)¹⁶ que reconoce el derecho de toda persona a no ser objeto de una decisión basada únicamente en un tratamiento automatizado cuando produzca efectos jurídicos o le afecte significativamente de modo similar, salvo las excepciones legalmente previstas. Una de las principales insuficiencias del marco regulador radica en que, pese a introducir importantes limitaciones respecto al uso y acceso de datos personales, no consagra un principio general de indisponibilidad de la esfera mental de las personas trabajadoras.

El Reglamento de Inteligencia Artificial¹⁷ introduce límites relevantes respecto de determinados sistemas considerados especialmente intrusivos, ejemplo de ello es su artículo 5 «... *Quedan prohibidas las siguientes prácticas de IA: a) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas delibera-*

15. 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), DOUE L 119, de 4 de mayo de 2016,

16. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE núm. 294, de 6 de diciembre de 2018

17. 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).

damente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas...» prohibiendo así ciertos sistemas que emplean técnicas subliminales, manipuladoras o explotadoras susceptibles de distorsionar de manera significativa el comportamiento de las personas cuando ello pueda ocasionar un perjuicio relevante.

Asimismo, restringe el empleo de sistemas de reconocimiento de emociones en el ámbito laboral, si bien esta prohibición presenta un alcance limitado al circunscribirse a supuestos concretos y admitir determinadas excepciones, particularmente por razones médicas o de seguridad. El Reglamento estructura los sistemas de inteligencia artificial usando la escala del riesgo imponiendo obligaciones de evaluación, transparencia, supervisión humana, sin embargo, estas previsiones no equivalen a una prohibición de la extracción y utilización ordinaria de datos relativos a la actividad mental de las personas trabajadoras.

Esta ausencia resulta particularmente significativa cuando se examina desde la perspectiva de los neuroderechos, pues si la libertad de pensamiento, la autonomía cognitiva y la integridad mental constituyen bienes jurídicos merecedores de protección autónoma, parece insuficiente que el acceso empresarial a la información relativa a los procesos mentales quede sometido únicamente a los tradicionales juicios de proporcionalidad, necesidad o licitud propios de protección de datos, pues estas categorías fueron concebidas para disciplinar el tratamiento de datos personales, pero no para responder a los riesgos distintos derivados de tecnologías capaces de inferir estados cognitivos, emociones, niveles de atención, fatiga o predisposiciones conductuales a partir de la monitorización de la actividad.

Mientras la legislación en materia de protección de datos, el RGPD y la LOPD, responden esencialmente a la pregunta acerca de cómo pueden tratarse los datos obtenidos, la teoría de los neuroderechos se plantea si existen determinadas categorías de información mental cuya captación o explotación debería considerarse incompatible con la dignidad de la persona y con la preservación de su autonomía cognitiva, es decir, si determinadas categorías de información mental o neuronal, por su especial vinculación con la identidad, la libertad de pensamiento y la autonomía cognitiva del individuo, deberían quedar excluidas de toda captación o explotación, con independencia de que su tratamiento pudiera cumplir formalmente la normativa de protección de datos.

Esta reflexión adquiere especial relevancia si se conecta con el paradigma del extractivismo de datos, la cual fija su interés en la lógica económica que impulsa la captación permanente de información personal como recurso generador de valor. Trasladado al ámbito laboral, este fenómeno implica que variables tradicionalmente ajenas al poder de dirección empresarial, como son los estados emocionales, los niveles de atención, la carga cognitiva, los indicadores de fatiga o determinadas respuestas neurofisiológicas, pueden convertirse en nuevos activos susceptibles de extracción, tratamiento e inferencia mediante sistemas de inteligencia artificial o mediante sistemas neuro tecnológicos.

Desde esta perspectiva, la principal laguna legal reside en la inexistencia de un límite material que excluya, con carácter general, la mercantilización de la esfera mental de las personas trabajadoras. El Reglamento de IA restringe determinados usos particularmente graves, pero no impide que la actividad mental pueda incorporarse al circuito ordinario de extracción y explotación de datos siempre que concurran las condiciones generales de licitud del tratamiento.

Precisamente por ello, la construcción doctrinal de los neuroderechos aporta un elemento distinto al ordenamiento vigente, al propugnar que ciertos aspectos de la vida mental constituyen un espacio jurídicamente indisponible cuya protección

no puede quedar supeditada exclusivamente a criterios de proporcionalidad o de gestión del riesgo, sino que exige reconocer límites materiales derivados directamente de la dignidad humana, de la libertad de pensamiento y de la integridad mental de la persona trabajadora.

Llegados a este punto, cabría preguntarnos si realmente necesitamos crear una nueva categoría de derechos o si estos derechos se corresponden con los recogidos en el Título I de nuestra Constitución¹⁸.

En el plano Internacional, la aprobación del Convenio de la OIT sobre el trabajo decente en la economía de plataformas, el 12 de junio de 2026 por la 114.^a Conferencia Internacional del Trabajo¹⁹, evidencia que la preocupación por el impacto de los sistemas automatizados sobre las condiciones de trabajo ha adquirido una dimensión global. contribuyendo a la configuración de un estándar universal de protección frente a la gestión algorítmica, así la adopción, del Convenio sobre el trabajo decente en la economía de plataformas introduce un elemento normativo de extraordinaria relevancia, no solo por la extensión geográfica potencial de sus efectos, sino también por la forma en que articula la tutela del trabajo en plataformas como un espacio en el que deben hacerse efectivos los principios y derechos fundamentales en el trabajo, la seguridad y salud, la no discriminación, la protección de datos, el acceso a la seguridad social y las garantías frente a los sistemas automatizados.

El art. 13 del Convenio dispone que *«Todo Miembro exigirá a las plataformas digitales de trabajo que informen a los trabajadores de plataformas digitales, antes de su empleo o contratación, y a sus representantes o a las organizaciones representativas de trabajadores y, cuando existan, a las organizaciones*

18. CONSTITUCIÓN ESPAÑOLA, Título I («De los derechos y deberes fundamentales»), *BOE* núm. 311, de 29 de diciembre de 1978.

19. ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (OIT), Convenio sobre el trabajo decente en la economía de plataformas, 2026 (núm. 193), adoptado en Ginebra por la 114.^a Conferencia Internacional del Trabajo, el 12 de junio de 2026

que representen a los trabajadores de plataformas digitales, sobre: a) el uso de sistemas automatizados, basados en algoritmos o en métodos similares, con fines de seguimiento o evaluación del trabajo o de generación de decisiones relativas al trabajo; b) la medida en que el uso de tales sistemas automatizados tiene un impacto en las condiciones de trabajo de los trabajadores de plataformas digitales o en el acceso al trabajo», mientras el art. 14 exige que tales sistemas sean utilizados de manera responsable y conforme a las obligaciones de los Estados y el art. 15, reconoce a los trabajadores de plataformas digitales, el derecho a obtener: *«cuando las decisiones sean generadas por un sistema automatizado de toma de decisiones, todo Miembro adoptará medidas apropiadas para exigir a las plataformas digitales de trabajo que se aseguren de que los trabajadores de plataformas digitales tengan acceso, previa solicitud y sin demora injustificada, teniendo en cuenta la clasificación de la situación en el empleo, a:*

a) una explicación por escrito de las decisiones significativas que afecten negativamente a sus modalidades de trabajo y su acceso al trabajo;

b) una revisión de las decisiones, cuando proceda, que tengan como consecuencia el no abono de todo monto adeudado a los trabajadores de plataformas digitales, o la suspensión o desactivación de sus cuentas, o la terminación de su empleo o contratación con una plataforma digital de trabajo.

2. Al dar efecto al párrafo 1, todo Miembro se asegurará de que las plataformas digitales de trabajo cuenten con una intervención humana apropiada».

En la misma línea, el art. 16 impone a los Estados el deber de establecer garantías efectivas y apropiadas respecto de los datos personales de los trabajadores de plataformas y de asegurar su tratamiento para fines legítimos, así como el derecho de acceso, rectificación y supresión de tales datos.

Debe advertirse, no obstante, que el Convenio no regula expresamente el tratamiento de datos neuronales o de información mental inferida. pero ofrece un armazón normativo apto para una interpretación evolutiva del Derecho del Trabajo en

clave de privacidad mental, integridad cognitiva y autonomía decisional.

4. LA EXPANSIÓN DE LA VIGILANCIA ALGORÍTMICA EN EL ENTORNO LABORAL

La expansión de la gestión algorítmica plantea un problema adicional que el Derecho del Trabajo apenas ha comenzado a tematizar: la posibilidad de que la organización digital del trabajo se aproxime a la esfera mental de la persona trabajadora, tradicionalmente, el poder de dirección se proyectaba sobre el tiempo, la presencia y el comportamiento observable de la persona trabajadora mientras que hoy comienza a proyectarse también sobre dimensiones más íntimas: la disponibilidad cognitiva, la concentración, el estado anímico, la reactividad emocional o la fatiga. La empresa no se limita a vigilar qué hace el trabajador; sino que pretende saber cómo se encuentra, cómo responde, cuándo decae su atención, qué grado de estrés presenta o qué patrones conductuales permiten predecir su rendimiento futuro. Se abre así la posibilidad de una forma de vigilancia que ya no se dirige solo al cuerpo o a la conducta, sino a la interioridad psíquica.

Es en este punto donde el debate sobre los neuroderechos adquiere relevancia laboral. bajo esta expresión se agrupan propuestas de protección de la privacidad mental, la identidad personal, la integridad psicológica, la libertad cognitiva o la autonomía frente a tecnologías capaces de registrar, inferir, manipular o explotar la actividad mental o sus correlatos. Puede discutirse si estamos ante derechos verdaderamente nuevos o ante una intensificación de derechos fundamentales ya existentes, como se ha apuntado anteriormente en este capítulo, haciendo referencia a los derechos fundamentales de intimidad, protección de datos, integridad física y moral, libertad ideológica, dignidad, o salud, lo decisivo es reconocer que el desarrollo tecnológico obliga a ensanchar el contenido protector de los derechos fundamentales de la persona trabajadora frente a un

poder de dirección cada vez más capaz de penetrar en su esfera cognitiva y emocional.

España no dispone todavía de una regulación específica de neuroderechos en el trabajo. Existen, sí, referencias relevantes en la Carta de Derechos Digitales, que contempla la necesidad de regular legalmente las condiciones, límites y garantías de implantación y uso de neurotecnologías con respecto a la dignidad, la autonomía y la no discriminación; resulta además de interés la Recomendación de la UNESCO sobre la Ética de la Neurotecnología, adoptada el 11 de noviembre de 2025²⁰. Sin embargo, el marco positivo español sigue siendo fragmentario y descansa, en esencia, sobre la combinación entre RGPD, LOPD, el ET, la normativa de prevención de riesgos laborales y régimen antidiscriminatorio, sin embargo, estos instrumentos presentan límites relevantes cuando se proyectan sobre la problemática específica de la esfera mental en el trabajo.

Una primera dificultad reside en que la información mental o cuasi mental puede no proceder de una neurotecnología invasiva ni de un dato de salud formalmente identificado como tal. Un sistema puede inferir fatiga, vulnerabilidad emocional, estrés, distracción o impulsividad a partir de patrones de teclado, tiempos de reacción, voz, micro expresiones, interacción con la aplicación o datos de localización. Nos encontramos así ante una categoría de datos inferidos cuya sensibilidad material puede ser altísima, aunque su estatuto jurídico no siempre resulte claro bajo las categorías tradicionales de datos especiales.

En la práctica, muchas decisiones empresariales descansan en sistemas que generan una recomendación o un resultado que luego un operador humano valida de forma casi automática. Una intervención humana meramente ritual no neutraliza ni la opacidad, ni el sesgo, ni la dependencia de la decisión res-

20. UNESCO, Recomendación sobre la Ética de la Neurotecnología, adoptada por la Conferencia General en su 43.^a reunión, Samarcanda, 2025

pecto del sistema automatizado. Por eso, la exigencia de «intervención humana apropiada» presente tanto en la Directiva 2024/2831 como en el Convenio OIT 2026 debería traducirse, en sede de transposición, en un estándar material de supervisión real, competente, informada y con capacidad efectiva de modificar o revocar la decisión.

La tercera carencia es más profunda: el ordenamiento no prohíbe con la claridad deseable la utilización, con fines ordinarios de gestión empresarial, de tecnologías o sistemas dirigidos a medir, inferir o explotar variables emocionales, cognitivas o neurofisiológicas de la persona trabajadora. La licitud de estas prácticas se desplaza hacia el terreno, siempre inestable, de la proporcionalidad, la minimización o la base jurídica del tratamiento. Pero quizá el problema exija un salto cualitativo: afirmar que determinadas formas de penetración en la esfera mental son *prima facie* incompatibles con la dignidad y con el estatuto de ciudadanía laboral, salvo supuestos excepcionadísimos y con garantías reforzadas.

5. NEUROTECNOLOGÍAS E INTELIGENCIA ARTIFICIAL EN EL TRABAJO

Se entiende por tecnologías de mente digital aquellas capaces de explorar, analizar o influir en datos mentales, entendiendo por datos mentales toda información que puede organizarse y procesarse para inferir estados cognitivos, afectivos o volitivos de una persona. Estos datos pueden derivarse tanto de fuentes neuronales como, por ejemplo, los registros de actividad cerebral, como de fuentes no neuronales; entre ellas la voz, expresiones faciales, hábitos de consumo, patrones de comportamiento o interacción social. El despliegue disruptivo de la neurotecnología y la neurociencia han planteado un cúmulo de escenarios, este tipo de tecnologías poseen la capacidad de alterar características esenciales del ser humano mediante la modificación de pensamientos o sentimientos; recuerdos o aspectos de la personalidad; capacidades psicológicas o físicas; se ha llegado a sostener que

algunos dispositivos incluso podrían llegar a revelar y exponer aspectos privados que se albergan en la mente humana²¹.

En este contexto, la neuroética surge como un esfuerzo por enfrentar dilemas filosóficos relevantes y anticipar cambios sociales disruptivos vinculados al uso de la neurotecnología, es decir, la neuroética surge de la necesidad de revisar los procesos y procedimientos para observar si la neurociencia puede ser utilizada para influir en las personas y qué consecuencias puede tener esto en los derechos individuales. Sin embargo, aún existe mucha desconexión y poco diálogo entre las diferentes disciplinas implicadas, pero lo que parece estar claro es que en todos los campos preocupan los desafíos que presenta el uso de las neurotecnologías.

Rafael Yuste y la *NeuroRights Foundation* ²² distinguen cinco categorías de neuroderechos:

1. Privacidad mental
2. Identidad personal
3. Libre albedrío
4. Acceso equitativo al aumento mental
5. Protección frente al sesgo²³.

Ahora bien, ¿qué significa cada uno de estos neuroderechos?

- a) El derecho a la privacidad mental tutela la información obtenida a partir de la actividad cerebral, reconociéndola como una manifestación especialmente sensible de la es-

21. OBSERVATORIO DE DERECHOS DIGITALES, «Sobre el epígrafe XXIV: Derechos digitales en el empleo de las neurotecnologías», Gobierno de España, disponible en: <https://www.derechosdigitales.gob.es/es/novedades/sobre-el-epigrafe-xxiv-derechos-digitales-en-el-empleo-de-las-neurotecnologias> (último acceso: 4 de agosto de 2026).

22. YUSTE ROJAS, R. *Neuroderechos: Un viaje hacia la protección de lo que nos hace humanos.*, 2025.

23. ARELLANO TOLEDO, W. *Los neuroderechos y su regulación*. INTELETICA. Revista de Inteligencia Artificial, Ética y Sociedad, 1(1), 4–13, 2024

fera íntima del individuo y como consecuencia de esto, la captación, almacenamiento o tratamiento de dichos datos solo puede realizarse con el consentimiento libre e informado de su titular.

- b) Atendiendo al derecho a la identidad personal, este busca preservar la integridad de la personalidad, la memoria, las emociones y aquellos elementos que configuran la individualidad de cada ser humano, impidiendo que las intervenciones tecnológicas alteren la esencia de la persona sin su consentimiento.
- c) El derecho al libre albedrío supone una garantía indispensable de la autonomía individual que protege la capacidad de adoptar decisiones libres de manipulaciones o influencias indebidas ejercidas mediante tecnologías capaces de incidir sobre los procesos cognitivos.
- d) El derecho al acceso equitativo al aumento mental responde a la necesidad de evitar que los beneficios derivados de los avances científicos queden reservados exclusivamente a determinados sectores sociales, promoviendo una distribución justa de las tecnologías destinadas a potenciar las capacidades cognitivas.
- e) La protección frente al sesgo persigue asegurar que los sistemas de inteligencia artificial y las neurotecnologías operen conforme a criterios de objetividad, transparencia y no discriminación, evitando que decisiones basadas en datos neuronales reproduzcan prejuicios o generen tratamientos desiguales.

Siendo un campo relativamente nuevo, todavía no existe consenso en la definición del concepto de neuroderechos, algunos la han relacionado con el ámbito del derecho destinado a salvaguardar aspectos fundamentales de la identidad mental ²⁴. Dicho de otra manera, son un conjunto emergente de derechos

24. YUSTE ROJAS, R.. *Neuroderechos: Un viaje hacia la protección de lo que nos hace humanos*. Ediciones Paidós, 2025

destinados a proteger la mente humana frente al uso de neurotecnologías capaces de registrar, interpretar o incluso influir en la actividad cerebral.

6. LOS NEURODERECHOS ¿UNA NUEVA GENERACIÓN DE DERECHOS LABORALES?

A pesar de que una parte de la doctrina sostiene que el marco vigente de derechos fundamentales permite responder adecuadamente a los desafíos derivados de las neurotecnologías, como se ha observado en estas líneas, también se han impulsado iniciativas orientadas al reconocimiento expreso de los denominados neuroderechos.

En el ámbito normativo, destaca la reforma constitucional chilena²⁵, cuyo artículo 19, apartado primero, incorpora una referencia expresa a la protección de la actividad cerebral y de la información obtenida de ella: *«El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella»*

En España, aunque no existe un reconocimiento legal específico sobre los neuroderechos, la Carta de Derechos Digitales²⁶, aprobada en el marco del Plan España Digital 2025 y de la Estrategia Nacional de Inteligencia Artificial, muestra una dedicación a las neurotecnologías. En dicho instrumento se proclama la ne-

25. CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE CHILE, art. 19.1, tras la reforma introducida por la Ley n.º 21383, publicada en el Diario Oficial de 25 de octubre de 2021.

26. Gobierno de España «Carta de Derechos Digitales», 2021«https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/ficheros/Carta_Derechos_Digitales_RedEs.pdf

cesidad de que la implantación y utilización de estas tecnologías quede sometida a una regulación legal que establezca las condiciones, los límites y las garantías necesarias para la protección de los derechos fundamentales de las personas.

La UNESCO²⁷, por su parte, ha apuntado a la importancia de establecer un marco normativo que regule el uso de las neurotecnologías y la IA considerando que la neurotecnología puede acceder directamente, manipular y emular la estructura del cerebro, y con ello producir información sobre las identidades, emociones y miedos convirtiéndose en una amenaza para las nociones de identidad humana, dignidad humana, libertad de pensamiento, autonomía, privacidad mental y bienestar; sin embargo no establece una definición cerrada del marco de neuroderechos²⁸.

Por su parte, la OIT y otros instrumentos internacionales buscan que los Estados miembros establezcan políticas para regular la neurotecnología en el lugar de trabajo, adaptando las normativas existentes sin establecer tampoco un concepto cerrado del marco de neuroderechos. Es decir, más allá del debate acerca del reconocimiento de nuevos derechos, existe un amplio consenso respecto de la necesidad de reforzar la protección jurídica de los datos obtenidos mediante interfaces cerebro-computador.

La estrecha relación entre el funcionamiento de las neurotecnologías y la recopilación de información relativa a la actividad cerebral convierte a los denominados neurodatos en uno de los principales focos de preocupación desde la perspectiva de la protección de datos personales, en este sentido, la Organización para la Cooperación y el Desarrollo Económicos (OC-

27. UNESCO. *Ética de la neurotecnología: la UNESCO adopta la primera norma mundial para esta tecnología de vanguardia*. <https://www.unesco.org/es/articles/etica-de-la-neurotecnologia-la-unesco-adopta-la-primera-norma-mundial-para-esta-tecnologia-de>, 2025

28. BOTERO URQUIJO, D. A./ HOYOS CONTRERAS, S. A./ VILLAMIZAR ACEVEDO, D. C. *Desafíos ético-jurídicos de los neuroderechos: Aportes y dilemas desde su desarrollo normativo en Chile*, 2024

DE), en su Recomendación sobre Innovación Responsable en Neurotecnología, define los neurodatos como la información relativa al funcionamiento o a la estructura del cerebro de una persona identificada o identificable, susceptible de revelar aspectos especialmente sensibles de su fisiología, su estado de salud o sus procesos mentales²⁹.

Los riesgos asociados al tratamiento de neurodatos han sido igualmente destacados por el Supervisor Europeo de Protección de Datos y por la Agencia Española de Protección de Datos en el informe conjunto *TechDispatch. Neurodata*³⁰. Ambas instituciones advierten que las neurotecnologías permiten la obtención continua y masiva de información cerebral, circunstancia que puede comprometer principios esenciales del RGPD, como la minimización de datos, la proporcionalidad o la exactitud. Asimismo, alertan de la posibilidad de generar nuevas formas de discriminación derivadas del tratamiento automatizado de información neuronal y de los riesgos inherentes a la creación de grandes bases de datos cerebrales

En consecuencia, el desarrollo de las neurotecnologías plantea la conveniencia de valorar si los neurodatos deben recibir un tratamiento jurídico diferenciado respecto de otras categorías especiales de datos personales y, al mismo tiempo, exige encontrar un equilibrio entre el impulso a la innovación tecnológica y la preservación efectiva de los derechos fundamentales, particularmente en ámbitos especialmente sensibles como el laboral. Por su parte, el Grupo Asesor del Consejo de Derechos Humanos prioriza el fortalecimiento de los derechos humanos ya reconocidos y la adopción de principios de

29. Organización para la Cooperación y el Desarrollo Económicos (OCDE), Recommendation of the Council on Responsible Innovation in Neurotechnology, OECD/LEGAL/0457, París, 2019. OECD Legal Instruments

30. European DATA PROTECTION SUPERVISOR (EDPS)/AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), *TechDispatch. Neurodata*, 2024 <https://www.aepd.es/guias/neurodatos-aepd-edps.pdf>

carácter interpretativo, en lugar de promover la creación de nuevos³¹

Asimismo, diversos estudios elaborados por el Consejo de Europa y por el Parlamento Europeo, este último, específicamente en materia de privacidad, sostienen que el marco vigente de Derechos Humanos resulta suficiente para afrontar los desafíos jurídicos planteados por las neurotecnologías, sin que sea necesaria la consagración de nuevos derechos fundamentales³².

Por otro lado, y como se señala con anterioridad se han propuesto cinco categorías de Neuroderechos, formulación que ha abierto un intenso debate doctrinal acerca de su verdadera naturaleza jurídica.

La cuestión central no reside únicamente en determinar la conveniencia de reconocer un nuevo catálogo de derechos específicamente adaptado a los desafíos planteados por las neurotecnologías, sino, sobre todo, en dilucidar si tales facultades constituyen auténticos derechos de nueva generación o si, por el contrario, encuentran ya suficiente cobertura en el contenido esencial de los derechos fundamentales tradicionalmente reconocidos por los ordenamientos constitucionales e internacionales, singularmente en los derechos a la dignidad, a la integridad física y moral, a la intimidad, a la protección de datos personales, a la libertad ideológica, al libre desarrollo de la personalidad y a la igualdad³³.

Desde esta perspectiva, el verdadero interés jurídico de los neuroderechos no radica tanto en la creación de un nuevo catálogo autónomo de derechos fundamentales como en su capacidad para evidenciar las insuficiencias que puede presentar la

31. COUNCIL OF EUROPE / OECD. *Neurotechnologies and Human Rights Framework: Do We Need New Rights? – Rapporteurs' Report of the Round Table*. Strasbourg: CoE & OECD, 2021

32. EUROPEAN PARLIAMENTARY RESEARCH SERVICE [EPRS]. *The protection of mental privacy in the area of neuroscience*. Brussels: European Parliament, 2024

33. GOERING S / YUSTE R. *On the Necessity of Ethical Guidelines for Novel Neurotechnologies*. Cell 167(4):882-885, 2016

aplicación de las categorías tradicionales frente a tecnologías capaces de acceder, inferir o influir sobre la actividad cerebral. En otras palabras, más que proclamar derechos inéditos, los neuroderechos cumplen una función interpretativa y sistematizadora, al reforzar el contenido y alcance de derechos ya consolidados en el constitucionalismo contemporáneo. Ello no excluye, sin embargo, la necesidad de adaptar el marco regulatorio vigente mediante garantías específicas que respondan a las particularidades de los neurodatos y de las tecnologías que los generan.

Esta exigencia adquiere una especial intensidad en el ámbito de las relaciones laborales, donde el desequilibrio estructural entre las partes puede favorecer la utilización de herramientas neurotecnológicas con fines de vigilancia, evaluación o gestión algorítmica de la fuerza de trabajo. En consecuencia, el debate sobre los neuroderechos debe entenderse menos como una discusión terminológica acerca de la aparición de nuevos derechos fundamentales y más como una oportunidad para fortalecer la tutela efectiva de la dignidad, la autonomía y la libertad de la persona trabajadora frente a los riesgos derivados de la progresiva digitalización de la mente humana.

7. CONCLUSIONES

Las consideraciones expuestas a lo largo de este capítulo permiten afirmar que el desarrollo de las neurotecnologías constituye uno de los mayores desafíos contemporáneos para el Derecho del Trabajo y, en términos más amplios, para el sistema de garantías de los derechos fundamentales.

Los avances experimentados durante la última década en inteligencia artificial, neurociencia computacional y análisis masivo de datos han ampliado de forma extraordinaria la capacidad de registrar, interpretar e incluso influir sobre la actividad cerebral, inaugurando un escenario inédito en el que la mente humana deja de ser un ámbito exclusivamente interior para convertirse en una fuente potencial de datos susceptibles de

tratamiento económico, organizativo y algorítmico. El verdadero problema jurídico no reside únicamente en la posibilidad técnica de acceder a la actividad cerebral, sino en la progresiva conversión de los procesos cognitivos, emocionales y conductuales en información explotable, capaz de ser utilizada para predecir comportamientos, condicionar decisiones o intensificar mecanismos de vigilancia y control. Esta transformación, que parte de la doctrina identifica ya como la configuración de una auténtica mente digital, obliga a replantear las categorías tradicionales de protección de la persona trabajadora, pues los instrumentos normativos construidos para garantizar la intimidad o la protección de datos personales resultan insuficientes cuando aquello que se encuentra en riesgo es la propia esfera cognitiva y la libertad de autodeterminación del individuo.

No resulta casual, por ello, que la comunidad internacional haya comenzado a construir un marco normativo específico destinado a responder a estos desafíos. La adopción por la UNESCO, en 2025, de la Recomendación sobre la Ética de la Neurotecnología constituye un primer hito regulatorio al reconocer la necesidad de preservar la integridad mental mediante principios como el consentimiento libre e informado, la voluntariedad en el uso de neurodispositivos, la prohibición de prácticas coercitivas y la protección reforzada de los neurodatos. Sin embargo, estos avances internacionales únicamente alcanzarán una eficacia real si se proyectan sobre los ordenamientos internos mediante reformas normativas capaces de anticiparse a los riesgos derivados de la utilización de estas tecnologías en el ámbito laboral.

En este sentido, la transposición al ordenamiento español de la Directiva (UE) 2024/2831, interpretada a la luz de las exigencias contenidas en el Convenio núm. 193 de la OIT sobre el trabajo decente en la economía de plataformas, representa una oportunidad que el legislador no debería desaprovechar. No basta con una adaptación meramente formal del texto europeo, sino que resulta necesaria una reforma de mayor alcance que incorpore una categoría de protección reforzada para los datos inferidos de alta sensibilidad relativos a estados mentales, emocionales o cognitivos, sometiéndolos a un régimen especial-

mente estricto de necesidad, proporcionalidad, finalidad y control. Del mismo modo, cualquier sistema algorítmico utilizado en procesos de selección, asignación de tareas, evaluación del rendimiento, fijación de la remuneración, promoción profesional, suspensión o extinción de la relación laboral debería quedar sujeto a una evaluación de impacto ex ante que integrase no solo las exigencias derivadas de la protección de datos personales, sino también las relativas a la seguridad y salud en el trabajo, la igualdad de trato y la prohibición de discriminación, prestando especial atención a los sesgos de género y a las discriminaciones de carácter interseccional.

Igualmente, la exigencia de supervisión humana prevista en la Directiva sobre trabajo en plataformas, en el Reglamento de Inteligencia Artificial y en el citado Convenio de la OIT no puede reducirse a una intervención meramente formal. La revisión humana únicamente satisface las exigencias de tutela efectiva cuando es realizada por una persona suficientemente cualificada, con acceso a la lógica de funcionamiento del sistema automatizado, capacidad real para modificar la decisión adoptada por el algoritmo y obligación de motivar jurídicamente el resultado alcanzado. A ello deben añadirse procedimientos ágiles de revisión e impugnación, tanto en sede administrativa como inspectora y judicial, que garanticen una protección efectiva frente a decisiones automatizadas que puedan afectar a derechos fundamentales de las personas trabajadoras.

El poder de dirección empresarial, aun cuando se ejerza mediante herramientas digitales o sistemas de inteligencia artificial, encuentra un límite infranqueable en la dignidad de la persona trabajadora, por lo que la organización de la actividad productiva no puede legitimar la apropiación empresarial de la interioridad psíquica, ni justificar la mercantilización de la actividad mental mediante técnicas de vigilancia cognitiva, perfilado emocional o predicción conductual. Precisamente porque las neurotecnologías permiten inferir información extremadamente sensible relativa a la salud mental, la estabilidad emocional, la maternidad, situaciones de violencia de género, estados de vulnerabilidad psicológica o aspectos íntimos de la persona-

lidad, los riesgos de lesión de los derechos fundamentales trascienden ampliamente el ámbito de la privacidad tradicional para proyectarse sobre la autonomía decisional, la igualdad, la libertad y el libre desarrollo de la personalidad.

En definitiva, la tutela jurídica del trabajo en la economía digital exige ampliar el contenido de los derechos fundamentales tradicionalmente reconocidos para incorporar una protección específica de la privacidad mental, la integridad cognitiva y la autonomía decisional frente a nuevas formas de vigilancia, perfilado y control algorítmico. Si la futura reforma española aspira verdaderamente a situarse a la altura del cambio tecnológico que ya se está produciendo, no debería limitarse a regular las condiciones de funcionamiento de las plataformas digitales, sino aprovechar esta oportunidad para establecer, con claridad y vocación de permanencia, los límites jurídicos que deben impedir la colonización algorítmica del trabajo y la progresiva mercantilización de la mente de las personas trabajadoras.

8. BIBLIOGRAFÍA

- ARELLANO TOLEDO, W. «Los neuroderechos y su regulación». *INTELETICA. Revista de Inteligencia Artificial, Ética y Sociedad*, 1(1), pp.4–13, 2024
- BAIOCCO S./ FERNÁNDEZ MACÍAS E. «*The algorithmic management of work: A basic compass*». European Commission,, 2022 <https://publications.jrc.ec.europa.eu/repository/handle/JRC129819>
- BELTRÁN DE HEREDIA RUIZ, I. «*Inteligencia artificial y neuroderechos: La protección del yo inconsciente de la persona*». Aranzadi, 2023
- BOTERO URQUIJO, D. A./ HOYOS CONTRERAS, S. A./ VILLAMIZAR ACEVEDO, D. C. «*Desafíos ético-jurídicos de los neuroderechos: Aportes y dilemas desde su desarrollo normativo*» *Revista Academia & Derecho*, Año 16, No. 30, 2025, pp. 1-33

- CARVAJAL, R. «Healthy Minds: *la IA que anticipa problemas mentales en el trabajo*», La Razón, 18 de mayo de 2025, https://www.larazon.es/economia/healthy-minds-que-anticipa-problemas-mentales-trabajo_202505186825b5c6f7f20a10d03e30af.html
- COUNCIL OF EUROPE & OECD. «*Neurotechnologies and human rights framework: Do we need new rights? Rapporteurs' report of the round table*». Council of Europe, 2021 <https://rm.coe.int/round-table-report-en/1680a969ed>
- DUBAL V. «The house always wins: *The algorithmic gambification of work*», LPE Project., 2023 <https://lpeproject.org/blog/the-house-always-wins-the-algorithmic-gambification-of-work>
- GRIESBACH K./ REICH A./ ELLIOTT-NEGRI L / MILKMAN R. «*Algorithmic control in platform food delivery work*», Socius, Sociological Research for a Dynamic World 5, 2019
- GOERING S, YUSTE R. «*On the Necessity of Ethical Guidelines for Novel Neurotechnologies*». Cell 167(4): pp. 882-885, 2016 <https://blogs.cuit.columbia.edu/rmy5/files/2018/02/ethicalguidelines.pdf>
- GUGLIEMMETTI, M. «*Automated work and workers' rights: Platform work and AI work management systems.*» En L. Hon-drich & A. Mollen (Eds.), «*Artificial Intelligence, Labour and Society*», pp. 127-140. European Trade Union Institute (ETUI), 2024
- HASSEL A./ ÖZKIZILTAN D. «*Governing the work-related risk of AI: Implications for the German government and trade unions*», Transfer, Transfer: European Review of Labour and Research 29 (1), 71-86, 2023
- European Data Protection Supervisor (EDPS)/ Agencia Española de Protección de Datos (AEPD), «TechDispatch. Neurodata», 2024 <https://www.aepd.es/guias/neurodatos-aepd-edps.pdf>
- EUROPEAN PARLIAMENTARY RESEARCH SERVICE. «*The protection of mental privacy in the area of neuroscience*». European Parliament, 2024
- OBSERVATORIO DE DERECHOS DIGITALES, *Sobre el epígrafe XXIV: «Derechos digitales en el empleo de las neurotecnologías»*, disponible en: <https://www.derechosdigitales.gob.es/es/no>

vedades/sobre-el-epigrafe-xxiv-derechos-digitales-en-el-empleo-de-las-neurotecnologias (acceso: 4 de agosto de 2026).

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (OCDE), «*Recommendation of the Council on Responsible Innovation in Neurotechnology*», París, 2019.

UNESCO, «*Recomendación sobre la Ética de la Neurotecnología, adoptada por la Conferencia General en su 43.^a reunión*», Samarcanda, 11 de noviembre de 2025 <https://www.unesco.org/es/legal-affairs/recommendation-ethics-neurotechnology>

YUSTE ROJAS, R. «*Neuroderechos: Un viaje hacia la protección de lo que nos hace humanos*». Ediciones Paidós, 2025

CAPÍTULO III

RESPONSABILIDAD CIVIL Y DILIGENCIA EN LA CADENA DE VALOR DE LA INTELIGENCIA ARTIFICIAL

Alejandro Zornoza Somolinos

Universidad Nacional de Educación a Distancia

1. EL MARCO FRAGMENTADO DE LA RESPONSABILIDAD CIVIL

Tradicionalmente, la responsabilidad civil por los daños causados por las cosas que se encuentran bajo nuestro control ha encontrado su fundamento en dos causas: bien en la negligencia de quien debía desplegar una conducta responsable para controlarlas y no lo hizo (esto es, la llamada responsabilidad subjetiva o por culpa), bien en el riesgo que genera la mera tenencia de las cosas por quien las posee (por contra, la responsabilidad objetiva o por riesgo). La aparición de las primeras máquinas con autonomía (a las que entonces nos referíamos, simplemente, como robots) hizo que debiera considerarse si un producto capaz de tomar decisiones por sí mismo era susceptible de estar bajo los esquemas clásicos de la responsabilidad civil o si debían explorarse nuevos ámbitos para el Derecho.

Así, el Parlamento Europeo abrió el debate sobre una reformulación de los principios que debían regir los sistemas de responsabilidad civil de los daños causados por robots (Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL), DOUE C 252, de 18 de julio de 2018), planteando fórmulas como el reconocimiento de una personalidad jurídica electrónica para los siste-

mas más sofisticados y autónomos, que supondría hacerles responsables de sus propios actos.

Afortunadamente, esta senda se abandonó en aras de soluciones más prudentes por considerar que los ordenamientos jurídicos disponían, por aquel momento, de instrumentos adecuados para afrontar los retos de los sistemas autónomos, sin perjuicio de que hubieran de realizarse las actualizaciones necesarias.

Desde entonces, y tras un caudal de publicaciones y trabajos previos³⁴, la Unión Europea ha afrontado la regulación de la IA por la vía de la seguridad de los productos y la gestión del riesgo. Si bien es un área en la que se goza de vasta experiencia normativa, doctrinal y jurisprudencial, lo cierto es que ello no garantiza que la regulación de la IA, sin resultar una tarea sencilla, vaya a ser también una tarea de éxito temprano.³⁵

34. A modo de ejemplo: Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Bruselas, 21.4.2021, COM(2021) 206 final; comunicación de la Comisión Inteligencia artificial para Europa, Bruselas, 25.4.2018, COM(2018) 237 final; Plan coordinado sobre la inteligencia artificial (Bruselas, 7.12.2018, COM(2018) 795 final); Comunicación de la Comisión Generar confianza en la inteligencia artificial centrada en el ser humano (Bruselas, 8.4.2019, COM(2019) 168 final); Directrices éticas para una IA fiable (Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, Directrices éticas para una IA fiable, Oficina de Publicaciones, 2019; Libro Blanco sobre la inteligencia artificial, publicado en febrero de 2020 (Comisión Europea, Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza, Bruselas 19.02.2020, COM(2020) 65 final); Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)).

35. El calendario originario de aplicación del Reglamento (UE) 2024/1689 se encontraba establecido en su artículo 113: aplicación general desde el 2 de agosto de 2026; aplicación de los capítulos I y II desde el 2 de febrero de 2025; aplicación del capítulo III, sección 4, de los capítulos V, VII y XII y del artículo 78 desde el 2 de agosto de 2025 (con excepción del artículo 101); y aplicación del artículo 6.1 y de las obligaciones correspondientes a los sistemas de IA de alto riesgo vinculados a productos incluidos en el anexo I desde el 2 de agosto de 2027. Sólo dos años después de su publicación, este calendario ha sido

La Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)) (DOUE C 404, de 6 de octubre de 2021) propuso la creación de un régimen autónomo y único de responsabilidad para los daños causados por sistemas de IA. De un modo similar a cómo gestionan los ordenamientos del *common law* los supuestos de daños causados por animales, en

modificado por el Reglamento (UE) 2026/1744 del Parlamento Europeo y del Consejo, de 8 de julio de 2026, por el que se modifican los Reglamentos (UE) 2024/1689, (UE) 2018/1139 y (UE) 2023/1230 en lo que respecta a la simplificación de la aplicación de las normas armonizadas en materia de inteligencia artificial (DOUE L 2026/1744, de 24 de julio de 2026), en vigor desde el 27 de julio de 2026. Conforme a la nueva redacción del artículo 113 RIA, las secciones 1, 2 y 3 del capítulo III (clasificación, requisitos y obligaciones de los operadores de sistemas de alto riesgo), salvo el artículo 6.5, serán aplicables desde el 2 de diciembre de 2027 respecto de los sistemas clasificados como de alto riesgo con arreglo al artículo 6.2 y al anexo III, y desde el 2 de agosto de 2028 respecto de los sistemas vinculados a productos clasificados conforme al artículo 6.1 y al anexo I. El Reglamento (UE) 2026/1744 introduce asimismo un régimen transitorio para los proveedores de sistemas de IA que generen contenido sintético de audio, imagen, vídeo o texto y hayan sido introducidos en el mercado antes del 2 de agosto de 2026, debiendo cumplir la obligación de marcado prevista en el artículo 50.2 a más tardar el 2 de diciembre de 2026. Para los sistemas introducidos en el mercado desde el 2 de agosto de 2026, dicha obligación resulta aplicable desde su introducción, de acuerdo con la fecha general de aplicación del artículo 50. Entre las restantes modificaciones relevantes se encuentran: la habilitación conferida a la Comisión para limitar, mediante actos delegados, la aplicación de los requisitos de los artículos 9 a 15 y 17 a 25 a determinados sistemas del artículo 6.1 cuando la legislación sectorial de armonización garantice una protección equivalente o superior; la precisión del concepto de «componente de seguridad» del artículo 3.14; la reformulación del artículo 4, que obliga a adoptar medidas de apoyo a la alfabetización en IA sin exigir que se garantice un nivel específico para cada persona; la introducción del artículo 4 bis, que amplía, bajo condiciones de estricta necesidad y con garantías específicas, la posibilidad de tratar categorías especiales de datos para detectar y corregir sesgos a otros proveedores y responsables del despliegue de sistemas y modelos de IA; y la extensión a las pequeñas empresas de mediana capitalización de diversas medidas de simplificación, proporcionalidad y apoyo anteriormente dirigidas principalmente a las pymes y empresas emergentes.

los que el tipo de responsabilidad que se exige del propietario del animal se hace depender de la peligrosidad del animal, el texto establecía un régimen de responsabilidad objetiva para sistemas de IA de alto riesgo y un sistema de responsabilidad subjetiva para el resto de los sistemas. No obstante, se terminó abandonando esta idea bajo la premisa de que la seguridad en los productos y la responsabilidad por los daños causados por los productos son momentos distintos de un mismo hecho, por lo que merecen regulaciones diferentes.

En lo que parece un claro intento del legislador europeo de ofrecer una respuesta coordinada a ambas cuestiones, se aprobaron el Reglamento (UE) 2024/1689, de 13 de junio, por el que se establecen normas armonizadas en materia de inteligencia artificial (DOUE L 1689, de 12 de julio de 2024, en adelante, RIA) y la Directiva (UE) 2024/2853, de 23 de octubre, sobre responsabilidad por los daños causados por productos defectuosos (DOUE L 2853, de 18 de noviembre de 2024, en adelante, DPD).

Ahora bien, el RIA no regula acciones indemnizatorias por los daños ocasionados mediante sistemas de IA, sino que establece un marco preventivo basado en el riesgo en el que distribuye un amplio conjunto de obligaciones entre los operadores implicados en la cadena de valor, y siempre en relación con la introducción y permanencia de los sistemas en el mercado.

Por su parte, la DPD incorpora al tradicional régimen de responsabilidad objetiva de los productos defectuosos los programas informáticos. Sólo a través de un ejemplo dado en el Considerando 13 de la Directiva, en el que se mencionan los sistemas de IA como parte integrada en la expresión «programas informáticos», se da por sentada la relación entre la DPD y el RIA, pero lo cierto es que la DPD no realiza ningún esfuerzo para hacer ver que los sistemas de IA forman parte de su ámbito de aplicación, por lo que es lícito preguntarse si hay un auténtico interés por integrar la IA en el marco de responsabilidad por daños causados por productos defectuosos (MARTÍN FABA, *Cesco*, 2025-53, 14-19).

En la medida en que el análisis exhaustivo de la DPD no es el objeto de estas líneas, para su lectura recomiendo los traba-

jos de (CARRASCO PERERA, Cesco, 2024, 1-7), (EVANGELIO LLORCA, *Causalidad*, 2024, 549-619), (MARTÍN CASALS, *Líneas generales*, 2024, 35-76) y (PÉREZ GARCÍA, *Indret*, 3-2025, 206-239).

Para lo que aquí interesa, debe tenerse en cuenta que la DPD sólo cubre determinados daños (muerte o lesiones corporales, daños a bienes con determinadas exclusiones y destrucción o corrupción de datos no profesionales -art. 6 DPD- quedando fuera, entre otros, los daños patrimoniales puros, los daños profesionales y ciertas lesiones de derechos de la personalidad) y siempre que exista una relación de causalidad entre el defecto y el daño. Además, siguen sin resolverse de manera satisfactoria cuestiones tradicionales como los riesgos asociados al desarrollo, tan estudiados por nuestra doctrina (SALVADOR CODERCH, RUBÍ PUIG, *Tratado*, 2008, 585-646; PARRA LUCÁN, *La protección*, 2011, 180-185).

Debió haber también un tercer instrumento: la Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, COM(2022) 496 final (en adelante, Propuesta de DRC), a la que le habría correspondido aliviar las dificultades probatorias de las reclamaciones fundadas en la culpa cuando se viesan involucrados sistemas de IA, pero el texto no superó el trámite de aprobación y fue retirado del Programa de Trabajo de la Comisión en octubre de 2025.

Ante este panorama, en que los regímenes de responsabilidad de los daños causados por sistemas de IA deben examinarse a la luz de las categorías generales del Derecho de daños, del Derecho contractual y del Derecho de consumo, resulta más conveniente resolver qué conducta es exigible a quien diseñó, introdujo en el mercado, integró o desplegó un sistema de IA que causó un daño, para determinar después si ese estándar fue infringido y si dicha infracción guarda relación con el daño causado, pudiendo señalar, con posterioridad, quién debe responder del daño.

De ahí que, personalmente, considere que las obligaciones establecidas por el RIA pueden contribuir a concretar un estándar civil de diligencia, que sin embargo no transforman automáticamente su incumplimiento en culpa, defecto o causalidad. A la

hora de determinar la responsabilidad, estas obligaciones sólo pueden adquirir relevancia si se toma en consideración su aplicabilidad material y subjetiva del deber, su pertenencia a la esfera de control del demandado, la correspondencia entre el fin de protección de la norma y el riesgo materializado, el carácter sustantivo de la infracción y su conexión causal con el daño.

2. LA FATIGA ANTE LOS DILEMAS DE LA RESPONSABILIDAD CIVIL POR DAÑOS CAUSADOS POR SISTEMAS INTELIGENTES

La responsabilidad civil por los daños causados mediante sistemas de IA se ha convertido en uno de los caminos más transitados del Derecho privado. No en vano, la complejidad de estos sistemas, la opacidad de sus procesos internos y la pluralidad de sujetos que participan en su desarrollo, comercialización e integración, han alimentado durante años un debate centrado, sobre todo, en las dificultades de imputación de responsabilidades. Así, los procesos para la identificación del responsable, la conveniencia o no de invertir la carga de la prueba, la reconstrucción del nexo causal y la dificultad del perjudicado para acceder a la información necesaria con el objetivo de fundamentar su pretensión cuando el empresario se escuda en figuras propias de la propiedad industrial han ocupado, con razón, una posición central en la producción científica.

Desde la perspectiva de nuestro CC, y al igual que sucede en otros ordenamientos de corte romanista, la responsabilidad extracontractual basada en la culpa del artículo 1902 impone al demandante la identificación de una conducta humana antijurídica como causa del daño cuyo resarcimiento se pretende.

En muchos casos, los daños ocasionados por sistemas de IA difícilmente podrán atribuirse a un único origen, sino que serán el resultado de una acumulación de datos, instrucciones, decisiones de diseño y condiciones concretas de uso.

En este contexto, prodigar un régimen subjetivo de responsabilidad plantea serias dificultades para garantizar la tutela

efectiva de las personas perjudicadas, especialmente cuando los sistemas objetivos de responsabilidad han demostrado ser más adecuados para hacer frente a la complejidad causal y probatoria de estos sistemas, pues la persona que puede ejercer alguna influencia o control sobre la causalidad se encuentra en mejor situación para prevenir los daños, internalizar sus costes o trasladarlos mediante mecanismos de aseguramiento.

En la medida en que el reproche no siempre puede descansar sobre una imputación individual, resulta oportuno dar a los sistemas de IA el mismo tratamiento objetivo que se da a otras actividades cotidianas que, sin embargo, generan un riesgo anormal para las personas y sus bienes. Además, resulta complejo seguir defendiendo un sistema basado en la culpa cuando la complejidad de los sistemas (o, si se prefiere, su opacidad incluso para el experto) dificultan la previsibilidad de cualesquiera daños, lo que lleva de nuevo a valorar un sistema de responsabilidad objetiva como la mejor de las fórmulas posibles. Pero Incluso bajo un régimen objetivo será necesario delimitar el riesgo cubierto, el defecto, la causalidad y las causas de exoneración, y, bajo el régimen general por culpa, habrá que reconstruir la conducta exigible.

Ante el riesgo de que los Estados Miembro elaborasen, separadamente, normativa específica para tratar las cuestiones relativas a los daños causados por sistemas de IA, la UE quiso garantizar que las víctimas de daños causados por la IA obtuvieran una protección equivalente a la de las víctimas de daños causados por los demás productos, evitando además la aparición de normativas nacionales específicas en materia de responsabilidad adaptadas a la IA, lo que habría generado incertidumbre para los operadores económicos al encontrar dificultades para anticipar cuándo podrían ser considerados responsables, especialmente si el daño se producía en un contexto transfronterizo.

La Propuesta de DRC fue planteada para solventar, precisamente, los problemas de acceso a la prueba y a la distribución de la carga probatoria, que tradicionalmente han constituido uno de los principales obstáculos para la efectividad del régi-

men de los productos defectuosos, pues la determinación del defecto y, sobre todo, del nexo causal, puede resultar extraordinariamente complejo y costoso para la persona perjudicada, sobre todo cuando el funcionamiento del sistema es opaco, como sucede con los sistemas de IA.

Así, el artículo 3 de la Propuesta de DRC preveía que un órgano jurisdiccional pudiera ordenar la exhibición de pruebas pertinentes relativas a sistemas de IA de alto riesgo específicos de los que se sospechase que habían causado daños, y el artículo 4 establecía una presunción refutable de causalidad entre la culpa y la información de salida del sistema, siempre que concurrieran determinadas condiciones, a saber: que el demandante hubiera demostrado o el órgano jurisdiccional hubiera supuesto la culpa del demandado o de una persona de cuyo comportamiento fuese responsable el demandado, consistente en el incumplimiento de un deber de diligencia establecido normativamente; que pudiera considerarse razonablemente probable, basándose en las circunstancias del caso, que la culpa había influido en los resultados producidos por el sistema de IA o en la no producción de resultados por parte del sistema de IA; y que el demandante hubiera demostrado que la información de salida producida por el sistema de IA o la no producción de una información de salida por parte del sistema de IA causó los daños.

La culpa, por tanto, debía consistir en una acción u omisión contraria a un deber de diligencia, ya fuera derivado del Derecho nacional o europeo, directamente destinado a proteger frente al daño producido, y debía influir necesaria y relevantemente en el resultado perjudicial causado. Sin embargo, la Propuesta de DRC estaba lejos de ser el instrumento normativo que se necesitaba: no determinaba cuál era la diligencia exigible, no identificaba el tipo de daños cubiertos ni los sujetos a los que se podía considerar responsables.

3. LA ARQUITECTURA PREVENTIVA DEL RIA Y LA RELEVANCIA CIVIL DE LA CADENA DE VALOR

El enfoque basado en el riesgo adoptado por el legislador europeo permite presentar el RIA como una intervención normativa proporcionada, orientada a prevenir los peligros más relevantes que los sistemas de IA puedan generar para la salud, la seguridad, los derechos fundamentales, la democracia, el Estado de Derecho y el medio ambiente. Por eso, no es de extrañar que se hayan concentrado las restricciones más intensas (incluida la prohibición de determinados sistemas de IA -art. 5 RIA-) en aquellos casos de uso que entrañan mayores riesgos, al tiempo que se preserva un amplio espacio para el desarrollo, la comercialización y la utilización de sistemas que no presenten ese nivel de peligrosidad.

El Reglamento articula, así, distintos bloques de requisitos y obligaciones cuya intensidad varía según el riesgo asociado a cada sistema, atendiendo, entre otros factores, a sus capacidades, su finalidad prevista y el contexto en el que vaya a utilizarse (PEGUERA, *Perspectiva*, 2024, 925 y ss).

El artículo 25.1 del RIA identifica a una serie de sujetos de la cadena de valor de un sistema de IA, para los que establece una regla de reasignación de la condición regulatoria de proveedor. Para determinar quién debe formar parte de dicha cadena, el legislador europeo asocia deberes concretos a posiciones de control concretas relativas al ámbito de información, decisión e intervención efectivamente atribuible a cada operador, estableciendo que el importador³⁶, el distri-

36. El importador es «una persona física o jurídica ubicada o establecida en la Unión que introduzca en el mercado un sistema de IA que lleve el nombre o la marca de una persona física o jurídica establecida en un tercer país» (art. 3.6 RIA). El importador no ejerce una función de control directa sobre el sistema, pero sí ocupa una posición de control sobre el acceso al mercado del sistema, debiendo comprobar la evaluación de conformidad, la existencia de documentación técnica, el marcado CE, la declaración de conformidad, las instrucciones de uso y, cuando corresponda, la designación de representante autorizado. En caso de

buidor³⁷, el responsable del despliegue³⁸ o un tercero, serán considerados proveedores³⁹ a los efectos de exigir responsabilidades si colocan su nombre o marca sobre el sistema, realizan una modificación sustancial o alteran la finalidad prevista del sistema de tal manera que el sistema pase a ser considerado como un sistema de alto riesgo.

La identificación de estos sujetos a través de sus atribuciones facilita delimitar el ámbito de la responsabilidad extracontractual. Así, se verá que la infracción del artículo 9 puede revelar una prevención deficiente; la del artículo 10, una gobernanza inadecuada de datos; la de los artículos 13 y 14, información o supervisión insuficientes; la del artículo 26, un despliegue negligente; y la de los artículos 20, 72 y 73, una respuesta tardía a riesgos conocidos.

A pesar de la equiparación, la posición de estos operadores no es equivalente: mientras el proveedor controla el diseño, el desarrollo y la conformidad del sistema, el responsable del despliegue decide sobre su utilización concreta, y el importador y el distribuidor ejercen funciones de control sobre su acceso al mercado y su posterior comercialización.

considerar que el sistema no es conforme, está falsificado o va acompañado de documentación falsificada, debe abstenerse de introducirlo en el mercado.

37. El distribuidor es «la persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión» (art. 3.7 RIA). De un modo similar al importador, el distribuidor ejerce un control sobre la permanencia del sistema de IA en el mercado.

38. El responsable del despliegue es «una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional» (art. 3.4 RIA).

39. Se considera proveedor a «una persona física o jurídica, autoridad pública órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente» (art. 3.3 RIA).

Ahora bien, el artículo 25 no determina que los sujetos que forman parte de la cadena de valor sean civilmente responsables por una atribución sobrevenida de la condición de proveedor sobre su persona, sino sólo que dichos sujetos quedarán, en caso de cumplir con alguno de los supuestos previstos para ser considerados proveedores, sometidos a las obligaciones del artículo 16 del RIA⁴⁰.

Si bien el catálogo de conductas más relevantes lo encontramos en el Capítulo III del RIA, respecto de los sistemas de alto riesgo, también encontramos otras medidas que pueden ayudar a valorar la relevancia de una conducta cuando el daño se vincula al riesgo que se pretende controlar: el artículo 4 impone medidas de alfabetización en materia de IA a proveedores y responsables del despliegue, el artículo 50 establece obligaciones de transparencia para ciertos sistemas que interactúan con personas o generan contenido sintético, y el Capítulo V (artículos 51 a 56) regula los modelos de IA de uso general.

El artículo 9 del RIA es el artículo central de la prevención de riesgos en relación con los sistemas de IA de alto riesgo, cuya gestión, documentación y mantenimiento durante todo el ciclo de vida del sistema se atribuye al proveedor de estos sistemas. Una referencia temporal («durante todo el ciclo de vida de un sistema») que permite afirmar que la diligencia del proveedor no

40. El artículo 16 RIA impone al proveedor de un sistema de IA de alto riesgo las obligaciones de garantizar el cumplimiento de los requisitos sustantivos previstos en los artículos 8 a 15 (gestión de riesgos, gobernanza de datos, documentación técnica, conservación de registros, transparencia, supervisión humana, precisión, solidez y ciberseguridad); identificarse en el sistema o en la documentación que lo acompañe; establecer un sistema de gestión de la calidad; conservar la documentación y, cuando estén bajo su control, los archivos de registro; someter el sistema a la correspondiente evaluación de conformidad antes de su introducción en el mercado o puesta en servicio; elaborar la declaración UE de conformidad, colocar el marcado CE y efectuar el registro exigido; adoptar las medidas correctoras y facilitar la información previstas para los sistemas no conformes; demostrar la conformidad ante la autoridad competente; y garantizar el cumplimiento de los requisitos de accesibilidad aplicables.

concluye cuando el sistema es introducido en el mercado o cuando intervienen el resto de sujetos de la cadena de valor. No en vano, los artículos 20, 72 y 73 articulan medidas correctoras, vigilancia poscomercialización y notificación de incidentes graves, respectivamente, debiendo el proveedor adoptar medidas para corregirlo, retirarlo, desactivarlo o recuperarlo. Y, del mismo modo, debe el responsable del despliegue vigilar el funcionamiento del sistema, informar de riesgos e incidentes y suspender el uso cuando existan motivos para considerar que el sistema puede presentar un riesgo. (art. 26.5 RIA).

Los riesgos a los que se refiere el artículo 9 son aquellos que pueden mitigarse o eliminarse razonablemente mediante el desarrollo o el diseño del sistema de IA de alto riesgo o el suministro de información técnica adecuada, por lo que deben ser riesgos conocibles, determinables y evaluables. De este modo, se produce una acotación o concreción de la diligencia preventiva.

El legislador parte de la premisa de que el riesgo cero no existe y admite, por ello, la subsistencia de riesgos residuales, siempre que hayan sido previamente identificados, evaluados y sometidos a medidas adecuadas y específicas de gestión. Conforme al artículo 9.5 del RIA, dichos riesgos sólo podrán considerarse aceptables cuando se hayan adoptado todas las medidas razonablemente exigibles para eliminarlos o reducirlos, atendiendo a su naturaleza, gravedad y previsibilidad.

Desde la perspectiva civil, lo relevante no es la mera existencia o ausencia formal de la documentación que integra el sistema de gestión de riesgos, sino la calidad real del proceso seguido. Podrá ser indicativa de negligencia una evaluación incompleta, la falta de actualización, la omisión de riesgos razonablemente detectables o la aceptación injustificada de un riesgo residual. A la inversa, la existencia de documentación no acredita por sí sola una actuación diligente cuando el procedimiento se haya limitado a un cumplimiento meramente formal o haya ignorado información técnica disponible.

En lo referente a la gobernanza y la calidad de los datos, el artículo 10 del RIA exige que los conjuntos de datos de entre-

namiento, validación y prueba de los sistemas de alto riesgo sean objeto de prácticas de gobernanza y gestión adecuadas atendiendo al destino del sistema de IA de alto riesgo. El precepto presta atención al origen y recogida de los datos, las operaciones de preparación, los supuestos de diseño, la disponibilidad y adecuación, los sesgos, las lagunas y las deficiencias. Los datos deben ser pertinentes, suficientemente representativos y, en la medida de lo posible, completos y carentes de errores, atendiendo a la finalidad prevista y al entorno geográfico, contextual, conductual o funcional.

Esta obligación no está orientada a garantizar resultados fiables, sino tan sólo a exigir del proveedor un proceso razonable para conocer y mitigar limitaciones que puedan afectar a derechos especialmente protegidos, por lo que la evaluación de la responsabilidad deberá considerarse si el error deriva de una deficiencia que un proveedor diligente habría podido detectar y corregir según la finalidad y contexto de uso del sistema de IA.

Conforme al artículo 26 del RIA, apartados cuarto y quinto, la expuesta obligación del artículo 10 es exigible tanto para el proveedor del sistema como para el responsable del despliegue, quien debe asegurarse de que los datos de entrada sean pertinentes y suficientemente representativos atendiendo a la finalidad prevista del sistema de IA de alto riesgo, en la medida en que ejerza el control sobre ellos. Es decir: el proveedor responde del diseño y de los conjuntos utilizados para desarrollar y validar el sistema, mientras que el responsable del despliegue puede responder de la calidad de los que introduce en el caso concreto, pues un sistema adecuado puede producir un resultado perjudicial por datos de entrada impropios y, a la inversa, datos correctos no compensan un modelo deficientemente entrenado.

Sin embargo, esta respuesta no debe resultarnos satisfactoria, pues como se ha apuntado, muchas veces será imposible explicar el porqué de la conducta del sistema, pudiendo sólo observar la correlación de datos de entrada y salida (QUESADA PÁEZ, *InDret*, 2026-I, 200).

Esta obligación de crear sistemas de IA seguros no impide que haya sistemas que puedan ser defectuosos y que, por razón

de ese defecto, se genere un daño. En este sentido, con base en el artículo 7.1 de la DPD, para considerar defectuoso un sistema de IA, comercializado bien como software bien como elemento integrado en un producto, éste debe presentar una falta de la seguridad que una persona tiene derecho a esperar y que se exige en virtud del Derecho de la Unión o del Derecho nacional.

Para determinar si una vez producido el daño existe dicha falta de seguridad, en su valoración deben atenderse todas las circunstancias, incluyendo la presentación del producto, las instrucciones, el uso previsible, la capacidad de aprendizaje, la interconexión, el control del fabricante, la ciberseguridad, las retiradas y las necesidades del grupo de usuarios finales a los que va dirigido el producto (art. 7.2 DPD), considerando además que los deberes de riesgo, datos, transparencia, supervisión o ciberseguridad impuestos por el RIA forman parte de las circunstancias relevantes para determinar la seguridad esperable.

Sin perjuicio de lo anterior, la propia DPD permite establecer presunciones de defectuosidad si, en un proceso judicial de reclamación de daños por producto defectuoso, el demandante demuestra que el producto incumple requisitos obligatorios de seguridad destinados a proteger frente al riesgo del daño sufrido (art. 10.2.b DPD). De este modo, el legislador conecta la DPD con los requisitos obligatorios de seguridad que impone el RIA.

La DPD mantiene el espíritu del RIA de garantizar que la seguridad de un sistema persista después de su introducción en el mercado y durante todo el ciclo de vida del producto. De ahí, que la responsabilidad por producto defectuoso quepa exigirla, no sólo al fabricante del producto o al fabricante del componente defectuoso, sino también al importador y al representante autorizado en el caso de un fabricante de un producto o componente establecido fuera de la Unión (art. 8 DPD). También a la persona que modifica sustancialmente un producto fuera del control del fabricante y lo comercializa o lo pone en servicio, a quien se considera a los efectos, fabricante.

Pero la responsabilidad objetiva de la DPD no es una responsabilidad objetiva pura, sino que admite causas de exoneración, de modo que el operador (por quien se entiende todo fabricante de un producto o componente, prestador de un servicio conexo, representante autorizado, importador, prestador de servicios logísticos o distribuidor) no resultará responsable si concurren alguna de las causas previstas⁴¹. A este respecto, me merecen especial atención tres causas de exoneración íntimamente relacionadas entre sí: las causas de inexistencia de la vulnerabilidad en el momento de la introducción en el mercado o puesta en servicio del producto (art. 11.1.c) DPD), los riesgos del desarrollo (art. 11.1.e) DPD), y las vulnerabilidades y actualizaciones de seguridad (art. 11.2 DPD).

En materia de ciberseguridad, la exoneración por riesgos del desarrollo del artículo 11.1.e) DPD sólo resultaría admisible cuando la vulnerabilidad existente en el momento de la introducción del producto en el mercado no pudiera ser detectada

41. Art. 11.1. DPD «Los operadores económicos (...) no serán responsables de los daños causados por un producto defectuoso si demuestran que: a) en el caso de un fabricante o importador, que no ha introducido el producto en el mercado ni lo ha puesto en servicio; b) en el caso de un distribuidor, que no ha comercializado el producto; c) que es probable que el carácter defectuoso que haya causado el daño no existiera en el momento en que el producto fue introducido en el mercado, puesto en servicio o, en el caso de un distribuidor, comercializado, o que ese carácter defectuoso se originase después de ese momento; d) que el carácter defectuoso que haya causado el daño se debe a que el producto cumple requisitos legales; e) que el estado objetivo de los conocimientos científicos y técnicos en el momento en que el producto fue introducido en el mercado, puesto en servicio o durante el período en el que el producto estaba bajo el control del fabricante no permitía detectar el carácter defectuoso; f) en el caso de un fabricante de un componente defectuoso, a que se refiere el artículo 8, apartado 1, párrafo primero, letra b), que el carácter defectuoso del producto en el que se ha incorporado dicho componente sea imputable al diseño de ese producto o a las instrucciones dadas por el fabricante de tal producto al fabricante de dicho componente; g) en el caso de una persona que modifica un producto según lo dispuesto en el artículo 8, apartado 2, que el carácter defectuoso que haya causado el daño esté relacionado con una parte del producto no afectada por la modificación».

conforme al nivel más avanzado del conocimiento científico y técnico objetivamente accesible. Por el contrario, la exoneración no operaría respecto de vulnerabilidades conocidas o publicadas en las bases de datos correspondientes, ni cuando la vulnerabilidad fuera descubierta durante el período de soporte y pudiera ser corregida mediante una actualización de seguridad, supuesto en el que el fabricante estaría obligado a comunicarla y subsanarla. La explotación de la vulnerabilidad por un tercero podría dar lugar a una concurrencia de responsabilidades, mientras que la negativa del usuario a instalar una actualización disponible podría incidir en la imputación del daño. Como vemos, el ámbito de esta causa de exoneración parece quedar reducido a vulnerabilidades verdaderamente desconocidas, no reportadas y técnicamente indetectables en el momento relevante (IZQUIERDO GRAU, InDret, 2025-IV, 115 y ss.).

El RIA establece también obligaciones de documentación, registros y trazabilidad: los artículos 11 y 12 obligan a elaborar documentación técnica y a permitir el registro automático de acontecimientos durante el ciclo de vida del sistema. Los artículos 18 y 19 regulan la conservación de documentación y archivos de registro por el proveedor. El artículo 26.6 impone al responsable del despliegue conservar los registros que estén bajo su control durante un período adecuado, en principio no inferior a seis meses, salvo que otra norma disponga lo contrario.

Si bien todas estas obligaciones permiten evaluar la conformidad, la vigilancia del mercado y la detección de riesgos, también revelan la finalidad prevista del sistema, las limitaciones conocidas, los parámetros de rendimiento, los cambios introducidos y las medidas de supervisión. Gracias a los registros, se puede determinar cuándo se utilizó el sistema, qué entradas recibió, qué salidas produjo y cuál fue la intervención humana en el proceso.

Todas estas obligaciones quedan registradas documentalmente. Ahora bien, en línea con lo que señalaba la Propuesta de DRC, la ausencia de un documento no puede ser suficiente para sostener una presunción de causalidad si la infracción formal no puede influir en la salida dada por el sistema, aunque sí

puede impedir reconstruir los hechos y justificar consecuencias probatorias cuando el operador está legalmente obligado a generar o conservar documentación.

Dado que el demandante puede observar el resultado, pero es el demandado quien tiene acceso a los datos y registros del modelo, la asimetría probatoria cuando hay involucrado un sistema de IA en la causación del daño, aumenta. Por ello, el artículo 9 de la DPD permite exigir al demandado la exhibición de pruebas pertinentes cuando el perjudicado haya aportado pruebas suficientes para respaldar la verosimilitud de su reclamación y, por tanto, la exhibición de la información sea proporcional.

Corresponde al órgano jurisdiccional ponderar y proteger los intereses legítimos de todas las personas afectadas, incluidos terceros, en relación con la protección de la información confidencial y los secretos comerciales, debiendo adoptar las medidas específicas necesarias tanto para preservar la confidencialidad de esa información cuando se utilice o se mencione en el transcurso del procedimiento judicial o después de este, como para exigir que dichas pruebas se aporten de manera fácilmente accesible y comprensible, si dicha aportación es proporcionada en términos de costes y esfuerzo para la parte requerida. Con ello, se pretende evitar que el demandado se esconda en la protección de su propiedad industrial para no poner a disposición de la persona perjudicada aquello que necesita, precisamente, para probar la causalidad del daño, y convierta su control sobre la información en inmunidad.

Lo anterior viene reforzado por un incentivo perverso: si el demandado incumple la orden de exhibición, el órgano judicial puede presumir la existencia del defecto (art. 10 DPD). Se presume también el defecto cuando se demuestra la infracción de requisitos obligatorios de seguridad destinados a proteger frente al riesgo sufrido o cuando el daño procede de un mal funcionamiento manifiesto en uso razonablemente previsible. Además, permite presumir defecto, causalidad o ambos cuando la complejidad técnica o científica provoca dificultades excesivas y el demandante demuestra su probabilidad.

Estas presunciones no eximen de toda actividad probatoria, pues en un estadio previo es la víctima quien debe construir una narración verosímil, identificar el producto y el daño, y aportar elementos que justifiquen la exhibición o la probabilidad causal.

Por su parte, el artículo 13 del RIA exige que los sistemas de alto riesgo tengan un nivel de transparencia suficiente para que los responsables del despliegue puedan interpretar y utilizar correctamente los resultados, mediante instrucciones de uso precisas, concisas, completas, correctas, claras, pertinentes, accesibles y comprensibles, con el fin de garantizar un uso seguro y correcto del sistema. Deben informar, entre otras cuestiones, de la finalidad prevista, los niveles de precisión, solidez y ciberseguridad, las circunstancias conocidas o previsibles que puedan generar riesgos, las limitaciones, los datos de entrada y las medidas de supervisión humana.

De este modo, si el proveedor conoce una limitación del sistema y no la comunica, o no la comunica debidamente, el responsable del despliegue no puede adoptar las medidas de prevención necesarias, pudiendo incurrir el proveedor en responsabilidad por negligencia a causa de una información defectuosa que puede ser apreciable tanto en la presentación del sistema (publicidad) como en las instrucciones.

El diseño y desarrollo de los sistemas de IA de alto riesgo requieren de un nivel adecuado de precisión, solidez y ciberseguridad durante todo su ciclo de vida (art. 15 RIA), por lo que deben resistir errores, fallos e incoherencias derivados de su interacción con personas u otros sistemas, debiendo incorporar medidas frente a ataques específicos, como el envenenamiento de datos o modelos, ejemplos adversarios y ataques a la confidencialidad.

Ahora bien, el artículo emplea conceptos abiertos (nivel adecuado, resistencia posibles, medidas apropiadas) que aportan poca seguridad jurídica a los responsables y que, en el mejor de los casos, son dependientes de desarrollos normativos posteriores de especificaciones comunes o de documentación técnica, etc.

En la medida en que del daño debe responder una persona, el artículo 14 del RIA configura la supervisión humana también como una medida de reducción del riesgo. El sistema debe diseñarse para ser vigilado por personas durante su uso, por lo que deben ser capaces de entender las capacidades y limitaciones del sistema, detectar anomalías, evitar el sesgo de automatización, interpretar las salidas, decidir no utilizar el sistema, descartar resultados e intervenir o detenerlo. El artículo 26.2 del RIA exige al responsable del despliegue encomendar esa función a personas con competencia, formación y autoridad suficientes.

Ahora bien, que exista la obligación de que haya supervisión humana no significa que la falta de supervisión sea la causa del error del sistema y, por tanto, la causación del daño, pero sí puede justificar que el error no sea detectado, que no se haya evitado o que sus efectos se hayan prolongado.

4. DEL DEBER REGULATORIO A LA CULPA Y AL DEFECTO

Con base en todo lo anterior, ya debiera ser posible intuir que hay una suerte de diligencia ante sistemas de IA que cabe exigir a quien diseña, desarrolla, comercializa, integra o utiliza profesionalmente un sistema de IA, y que designa el conjunto de medidas técnicas, organizativas e informativas que, atendiendo a la finalidad del sistema, sus usos razonablemente previsibles, el estado de la técnica, la gravedad y probabilidad de los riesgos, las características de las personas afectadas y la posición de control del operador, resultan razonablemente exigibles para identificar, evaluar, prevenir, reducir, documentar, comunicar y supervisar los riesgos asociados a su diseño y utilización.

Dicha diligencia debe estar orientada a identificar, prevenir, mitigar, documentar, supervisar y comunicar razonablemente los riesgos asociados al sistema, atendiendo a la finalidad prevista para la que están destinados, el uso indebido previsi-

ble, el estado del arte, la posición de control del sujeto y las características de las personas afectadas.

Esta diligencia no constituye, en ningún caso, un régimen autónomo de responsabilidad, sino un criterio para concretar los deberes de conducta dentro de los regímenes civiles aplicables, pero dada la pluralidad de sujetos intervinientes en la cadena de valor, el RIA indica qué riesgos deben ser considerados, qué procesos deben existir y qué información debe circular. Así, el proveedor del sistema responderá por las cuestiones relacionadas con el diseño, desarrollo, evaluación y comunicación de limitaciones. Al responsable del despliegue cabe exigirle un uso conforme a las instrucciones, datos de entrada adecuados, supervisión y seguimiento. Al fabricante, por su parte, se le atribuyen obligaciones cuando integra el sistema bajo su nombre o marca. Pero para que la falta de diligencia exigida por el RIA pueda generar responsabilidad, no es suficiente con su mera infracción, sino que se requiere daño, criterio de imputación y relación causal.

La Propuesta de DRC estrechaba el cerco sobre las obligaciones, los riesgos e intereses que se debían proteger al referirse a un deber directamente destinado a proteger frente al daño producido, exigiendo que fuera razonablemente probable que la culpa hubiera influido en la salida del sistema. De este modo, debía ponderarse la intensidad del indicio en función de la obligación incumplida: la falta de gestión de un riesgo que termina materializándose, la utilización de datos manifiestamente inadecuados o la ausencia de supervisión exigida mantienen una relación sustantiva con el daño, mientras que la omisión de un trámite registral, que es algo administrativamente sancionable, carecería de relevancia causal, casi con seguridad. En un ámbito intermedio se encontraría la falta de documentación que, si bien no causaría el daño, sí impediría demostrar cómo se produjo.

Tampoco debe aceptarse la proposición inversa, según la cual el cumplimiento formal excluye la culpa: la evaluación de conformidad, el marcado CE o la aplicación de normas armonizadas acreditan conformidad regulatoria, pero no sustituyen el

juicio sobre el caso concreto. El artículo 40 RIA establece una presunción de conformidad con los requisitos cubiertos por normas armonizadas; esa presunción opera dentro del sistema regulatorio y en la medida en que la norma contemple los requisitos pertinentes, pero no hace que el operador quede blindado frente a daños derivados de riesgos no evaluados, usos previsibles o información insuficiente. Así, no es descabellado considerar que cabe exigir una conducta adicional, por encima de lo contemplado en la regulación general, cuando las circunstancias concretas revelan un riesgo que el legislador no ha considerado suficientemente.

En otras palabras: el cumplimiento normativo es la diligencia mínima exigible, no el límite superior de ésta.

Que la conformidad regulatoria constituye una circunstancia relevante para valorar el carácter defectuoso del producto, pero no excluye por sí sola la responsabilidad, es un principio clásico de la responsabilidad por productos defectuosos. El artículo 7 de la DPD exige atender al conjunto de circunstancias del caso, entre ellas la presentación y el diseño del producto, su uso razonablemente previsible, su capacidad de aprendizaje, la interconexión con otros productos, el control posterior del fabricante y los requisitos de seguridad y ciberseguridad aplicables. Por ello, la superación de una evaluación de conformidad, la colocación del marcado CE o la observancia de determinados estándares no impiden necesariamente apreciar que el producto no ofrecía la seguridad legítimamente esperable.

Distinto es el supuesto contemplado en el artículo 11.1.d, que exonera al operador cuando demuestre que el carácter defectuoso causante del daño se debe precisamente a que el producto cumple requisitos legales. No se trata de un puerto seguro general basado en el cumplimiento normativo, sino de una exoneración causal más restringida: el defecto ha de ser consecuencia de una exigencia legal vinculante cuya observancia se impusiera al fabricante. En cambio, cuando la regulación se limite a establecer mínimos de seguridad o deje margen para adoptar medidas adicionales, su cumplimiento no impide valorar si, atendiendo a los riesgos conocidos y a las circunstancias

del producto, resultaban exigibles otras medidas de prevención.

5. PROTECCIÓN DEL CONSUMIDOR Y DILIGENCIA REFORZADA EN EL USO DE IA

Por último, debe abordarse la posición de los usuarios finales de los sistemas de IA, pues las normas destinadas a su protección imponen también a los distintos sujetos de la cadena de valor deberes de conducta susceptibles de integrar el estándar de diligencia exigible.

Sea como fuere, cuando el sistema de IA se suministra como contenido o servicio digital, adquiere especial relevancia el régimen de conformidad previsto en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (BOE núm. 287, de 30 de noviembre; en adelante, TRLGDCU). Este régimen impone al empresario obligaciones relativas, entre otros extremos, a la funcionalidad, compatibilidad, seguridad, actualización e información del contenido o servicio digital, cuyo incumplimiento puede proyectarse sobre la valoración de su conducta desde la perspectiva civil.

Ahora bien, coincidiendo con (GÓMEZ LIGÜERRE, *La Ley Europea*, 2025, 4), la DPD debe ser considerada, ante todo, una norma de Derecho de daños. Desde esta perspectiva, la sistemática del TRLGDCU presenta una cierta anomalía, al ubicar la responsabilidad por productos defectuosos dentro de la legislación de consumo pese a que sus normas no protegen exclusivamente al consumidor contractual del producto, sino también a cualquier persona perjudicada que reúna los requisitos establecidos por el régimen, con independencia de que haya adquirido o utilizado el producto como consumidora. Quizás se deba al hecho de que el Derecho de consumo, a pesar de su denominación, es un sistema heterogéneo en el que confluyen tanto normas de Derecho público como de Derecho privado y que no

encaja en ninguna de las ramas conocidas del Derecho (LASARTE ÁLVAREZ, *Manual*, 2018, 15).

Se trata, por tanto, de una disciplina de responsabilidad civil con vocación protectora general, aunque formalmente integrada en el texto refundido de consumidores y usuarios.

Sin perjuicio de ello, los artículos 114 y siguientes del TRLGDCU se aplican a la compraventa de bienes y al suministro de contenidos o servicios digitales. Los artículos 115 bis y 115 ter exigen que el bien o servicio se ajuste a la descripción, posea la funcionalidad, compatibilidad e interoperabilidad pactadas, sea apto para los fines normales y específicos aceptados, se entregue con las instrucciones esperables y reciba las actualizaciones necesarias.

Las características anunciadas del sistema, sus niveles de precisión, la existencia de supervisión humana o la aptitud para una finalidad determinada pueden integrarse en el contrato de prestación de servicios: mientras que el artículo 60 del TRLGDCU obliga al empresario a facilitar información clara, comprensible, accesible, relevante, veraz y suficiente sobre las características principales del producto o servicio, el artículo 61 hace exigible el contenido de la oferta, promoción y publicidad, aunque no figure expresamente en el documento contractual.

A este respecto, el RIA puede concretar qué información resulta relevante cuando el empresario utiliza un sistema regulado, pues no toda obligación dirigida por el artículo 13 al responsable del despliegue se traduce automáticamente en información debida al consumidor. Ahora bien, en la medida en que el empresario conoce las limitaciones capaces de afectar a la prestación no puede ocultarlas cuando sean determinantes para la decisión contractual o el uso seguro. La obligación civil se apoya entonces en la buena fe, la información precontractual, la conformidad y la normativa de consumo, mientras que el RIA ayuda a identificar el contenido técnicamente relevante.

Podría considerarse que el usuario de sistemas de IA es un usuario más vulnerable, si cabe, que el usuario convencional en la medida en que desconoce el funcionamiento y las limita-

ciones del sistema, no sabe qué datos, proveedor o criterios intervienen y carece de acceso a registros y documentación.

Así, el artículo 3 del TRLGDCU reconoce la figura de la persona consumidora vulnerable en relaciones concretas cuando circunstancias personales, económicas, educativas o sociales generan subordinación, indefensión o desprotección. Es decir, que un consumidor puede llegar a ser vulnerable en un momento determinado de su vida y sólo respecto de un ámbito concreto del consumo, lo que puede llevar a considerar que el consumidor de sistemas de IA requiere de un estatuto reforzado de protección o, desde otro punto de vista, que cabe exigir del proveedor una diligencia mayor que a proveedores de otro tipo de productos.

Como se sabe, en el ámbito del consumo la transparencia debe ser funcional, adaptada al destinatario y al medio, no bastando una mención genérica de la información relevante oculta entre términos y condiciones extensos.

Sin embargo, la narrativa de la vulnerabilidad requiere ser matizada: el Derecho de consumo se construye sobre la premisa de que la información adecuada permite al consumidor tomar decisiones autónomas y racionales. La exigencia de información previa, clara, inteligible y veraz sigue siendo la piedra angular del sistema y lo cierto es que hoy el consumidor dispone de un arsenal de recursos: acceso instantáneo a comparadores y opiniones, portales institucionales, o asociaciones de consumidores y organismos de supervisión que canalizan reclamaciones impiden que no toda vulnerabilidad sea inevitable ni absoluta.

6. CONCLUSIONES

Primera. La responsabilidad civil por los daños relacionados con sistemas de IA no exige atribuir personalidad ni capacidad de obrar al sistema, ni tampoco construir necesariamente un régimen íntegramente autónomo. Los resultados dañosos que se presentan como «decisiones de la IA» remiten, en reali-

dad, a una sucesión de decisiones humanas y organizativas relativas al diseño, los datos, la finalidad prevista, la integración, la comercialización, la configuración, la supervisión y el mantenimiento del sistema. La función del Derecho de daños consiste en reconstruir esa secuencia, determinar qué sujeto controlaba cada decisión relevante y comprobar si el riesgo que finalmente se materializó pertenecía a su esfera de actuación.

Segunda. El RIA no establece un sistema de indemnización ni resuelve por sí mismo la atribución de responsabilidad civil. Su naturaleza es predominantemente preventiva y regulatoria: clasifica determinados usos, distribuye obligaciones entre operadores y organiza mecanismos de conformidad, vigilancia y corrección. Sin embargo, esa circunstancia no priva a sus normas de relevancia civil. Los deberes de gestión de riesgos, gobernanza de datos, documentación, trazabilidad, transparencia, supervisión humana, precisión, solidez, ciberseguridad y vigilancia poscomercialización proporcionan un catálogo normativo especialmente útil para concretar qué conducta podía exigirse a cada operador antes y después de la introducción del sistema en el mercado.

Sobre esta base, puede definirse la diligencia ante sistemas de IA como el conjunto de medidas técnicas, organizativas e informativas que, atendiendo a la finalidad del sistema, sus usos razonablemente previsibles, el estado de la técnica, la gravedad y probabilidad de los riesgos, las características de las personas afectadas y la posición de control del operador, resultan razonablemente exigibles para identificar, evaluar, prevenir, reducir, documentar, comunicar y supervisar los riesgos asociados a su diseño y utilización. Esta diligencia no constituye una categoría de responsabilidad independiente, sino un criterio de concreción de los deberes de conducta aplicables dentro de los distintos regímenes contractuales y extracontractuales.

La infracción del RIA no debe equipararse automáticamente a la culpa civil. Para que un incumplimiento regulatorio pueda fundamentar un reproche indemnizatorio deben concurrir, al menos, cinco comprobaciones: i) la obligación ha de resultar temporal, material y subjetivamente aplicable al demandado; ii)

debe referirse a una decisión o información situada dentro de su esfera efectiva de control; iii) el fin de protección de la norma infringida ha de comprender el interés lesionado y el tipo de riesgo que se materializó; iv) debe tratarse de un incumplimiento sustantivo y no de una irregularidad meramente formal carente de incidencia sobre la seguridad o el resultado y v) ha de existir una conexión causal jurídicamente suficiente entre la infracción y el daño, sin perjuicio de las presunciones y reglas de facilidad probatoria que puedan resultar aplicables.

Tercera. La distribución de obligaciones a lo largo de la cadena de valor resulta fundamental para identificar quién asumió decisiones capaces de modificar el perfil de riesgo y qué obligaciones regulatorias pasaron a corresponderle. El proveedor concentra normalmente el control sobre el diseño, el desarrollo, los datos empleados para el entrenamiento y la validación, la evaluación de conformidad y la comunicación de las limitaciones del sistema. El responsable del despliegue controla el contexto concreto de utilización, los datos de entrada que se encuentren bajo su autoridad, la organización de la supervisión humana y la reacción ante resultados anómalos o riesgos sobrevenidos. Importadores y distribuidores ejercen, por su parte, funciones de verificación, acceso y permanencia en el mercado.

El sistema de gestión de riesgos del artículo 9 RIA constituye una de las manifestaciones más claras de esta diligencia. El Reglamento no exige eliminar cualquier posibilidad de daño, porque el riesgo cero no existe, sino implantar un proceso continuo de identificación, evaluación, mitigación, prueba, información y revisión. Del mismo modo, la materialización de un daño no demuestra automáticamente que la gestión haya sido negligente: deberá comprobarse si el riesgo era razonablemente cognoscible y si existían medidas proporcionadas que habrían permitido evitarlo o reducirlo.

La gobernanza de los datos confirma que la diligencia es relacional y se distribuye según el control efectivo. El proveedor debe aplicar prácticas adecuadas a los conjuntos de entrenamiento, validación y prueba; el responsable del despliegue de-

be velar por la pertinencia y representatividad de los datos de entrada que controle.

Las obligaciones de documentación, conservación de registros y trazabilidad cumplen una doble función. En el plano regulatorio permiten evaluar la conformidad y vigilar el comportamiento del sistema. En el plano civil, constituyen una infraestructura probatoria capaz de revelar la finalidad prevista, las limitaciones conocidas, las versiones utilizadas, los datos de entrada, los resultados de salida, las intervenciones humanas y las medidas correctoras.

La transparencia y la supervisión humana deben interpretarse también conforme a su función preventiva. La información exigible no consiste en una explicación exhaustiva de cada operación matemática del modelo, sino en la comunicación funcional de aquello que permita comprender la finalidad, las capacidades, las limitaciones, las condiciones de uso y los riesgos relevantes. La supervisión humana, por su parte, no se establece para fabricar artificialmente un responsable, sino para mantener capacidades reales de interpretación, intervención, corrección o detención.

El cumplimiento normativo tampoco opera como un puerto seguro: la evaluación de conformidad, el marcado CE, la observancia de normas armonizadas o la elaboración de documentación constituyen indicios cualificados de diligencia, pero no sustituyen el juicio civil sobre el caso concreto. Cuando el operador conoce un riesgo específico no cubierto suficientemente por el estándar regulatorio y dispone de medidas adicionales razonables y proporcionadas, el cumplimiento formal de los mínimos no debería excluir el reproche. A la inversa, la desviación respecto de una norma técnica tampoco implica necesariamente negligencia si se acredita que se adoptó una solución alternativa con un nivel de protección equivalente o superior.

Cuarta. La DPD ofrece una segunda vía cuando el sistema de IA constituye un programa informático o se integra en un producto. Se trata de una responsabilidad objetiva, porque la persona perjudicada no ha de probar la culpa del fabricante, aunque sí el daño, el carácter defectuoso y la relación causal,

con las modulaciones probatorias establecidas por la propia Directiva. Los requisitos del RIA pueden contribuir a determinar la seguridad que legítimamente cabía esperar y, en determinados supuestos, su incumplimiento puede activar una presunción de defectuosidad. No obstante, la responsabilidad objetiva no equivale a responsabilidad automática: subsisten los límites relativos a los daños resarcibles, las causas de exoneración y la necesidad de conectar el defecto con el perjuicio.

La DPD no cubre, sin embargo, todos los perjuicios vinculados a sistemas de IA. Quedan fuera, según los casos, pérdidas económicas puras, daños a bienes de uso exclusivamente profesional y lesiones de derechos fundamentales o de la personalidad que no se traduzcan en alguna de las categorías indemnizables previstas. Estos supuestos deben reconducirse a las reglas generales de responsabilidad contractual o extracontractual, al régimen de protección de datos, a la normativa antidiscriminatoria, a la competencia desleal o a la legislación de consumo. La diligencia ante sistemas de IA cumple aquí una función transversal: ayuda a concretar la conducta exigible, pero no sustituye los presupuestos ni los remedios propios de cada régimen.

Quinta. En las relaciones con consumidores, conviene diferenciar la responsabilidad por daños del régimen contractual de conformidad. Cuando un sistema se suministra como bien, contenido o servicio digital, la falta de funcionalidad, compatibilidad, interoperabilidad, seguridad, información o actualización puede activar los remedios del TRLGDCU sin necesidad de acreditar un daño indemnizable. Reparación, puesta en conformidad, reducción del precio o resolución responden a una lógica distinta de la responsabilidad extracontractual y pueden ofrecer una respuesta más eficaz frente a fallos funcionales que no causan lesiones personales ni daños a otros bienes. El RIA puede contribuir a identificar qué información técnica era relevante, pero la obligación frente al consumidor se funda en la buena fe, la información precontractual, la publicidad vinculante y los requisitos subjetivos y objetivos de conformidad.

Tampoco debe afirmarse que toda persona que utiliza un sistema de IA sea, por esa sola circunstancia, consumidora vul-

nerable. La vulnerabilidad debe apreciarse en la relación concreta, atendiendo a las características personales, económicas, educativas o sociales del destinatario, a la finalidad del sistema, a la intensidad de sus efectos, a la asimetría informativa y a la posibilidad real de comprender, impugnar y corregir el resultado. La transparencia ha de ser funcional: no basta con acumular advertencias en condiciones generales extensas, sino que debe facilitarse en el momento, formato y lenguaje adecuados la información capaz de influir en la decisión contractual o en el uso seguro. Cuanto más significativa sea la consecuencia automatizada, mayor deberá ser la posibilidad efectiva de reclamación y revisión.

En definitiva, la principal aportación del RIA al Derecho privado no consiste en crear un nuevo responsable ni en convertir cualquier incumplimiento administrativo en responsabilidad civil. Consiste en hacer visible una arquitectura de decisiones, controles, información y riesgos que antes permanecía técnicamente opaca. Esa arquitectura permite concretar el estándar de conducta, distribuir deberes conforme a las esferas de control, identificar la información que debería existir y valorar de manera más rigurosa el defecto, la culpa y la causalidad. La responsabilidad civil derivada del uso de sistemas de IA deberá construirse, por ello, mediante una lectura coordinada del RIA, la normativa de productos defectuosos, el Derecho contractual, el Derecho de consumo y los restantes regímenes sectoriales, evitando tanto la inmunidad derivada de la complejidad técnica como una responsabilidad automática basada en la mera intervención de la inteligencia artificial. El criterio decisivo será siempre si el operador adoptó las medidas razonablemente exigibles para el riesgo que controlaba y si su omisión guarda una relación jurídicamente suficiente con el daño.

7. BIBLIOGRAFÍA

CARRASCO PERERA, Ángel F., «Análisis de la nueva Directiva de responsabilidad por daños causados por productos defectuo-

sos. Síntesis y crítica de la regulación más contenida en la Directiva 2024/2853», Estudios Jurídicos. Centro de estudios de consumo, 2024.

EVANGELIO LLORCA, Raquel, «Causalidad y responsabilidad civil por daños ocasionados por sistemas de inteligencia artificial», en: ÁLVAREZ LATA, Natalia (Coord.), Derecho de contratos, responsabilidad extracontractual e inteligencia artificial, Asociación de Profesoras y Profesores de Derecho Civil, Aranzadi, Madrid, 2024, 549-619.

GÓMEZ LIGÜERRE, Carlos, «La nueva Directiva de responsabilidad por daños causados por productos defectuosos», La Ley Unión Europea, núm. 133, febrero 2025.

IZQUIERDO GRAU, Guillem, «Vulnerabilidades de ciberseguridad en productos con elementos digitales y su incidencia en la responsabilidad del fabricante», InDret, IV, 2025 97-125.

LASARTE ÁLVAREZ, Carlos «Manual sobre protección de consumidores y usuarios», Tirant LoBlanch, Valencia, 2018.

MARTÍN CASALS, Miquel, «Líneas generales de la nueva Directiva europea de responsabilidad por los daños causados por productos defectuosos», Revista de Derecho de la Universidad del Desarrollo, 50, 2024, 35-76.

MARTÍN FABA, José María, «La inteligencia artificial en la nueva directiva de Responsabilidad por los daños causados por Productos defectuosos ¿realidad o expectativa» Revista Cesco de Derecho de consumo, 53, 2025, 14-19.

PARRA LUCÁN, M^a Ángeles, La protección del consumidor frente a los daños. Responsabilidad civil del fabricante y del prestador de servicios, Reus, Madrid, 2011.

PEGUERA, Miquel, «Perspectiva y categorización del riesgo en el Reglamento de Inteligencia Artificial» en: Moreno Martínez, Juan Antonio/ Femenía López, Pedro José (Coords.), Inteligencia artificial y derecho de daños: Cuestiones actuales: Acorde al Reglamento (UE) 2024/1689, Dykinson, 2024.

PÉREZ GARCÍA, Juan Máximo, «La responsabilidad por los daños causados por productos defectuosos: análisis de la Directiva (UE) 2024/2853 y una propuesta de *lege ferenda* de incorporación al Ordenamiento español», Indret, III, 2025, 206-239.

QUESADA PÁEZ, Abigail, «La atribución de responsabilidad civil por actos de sistemas autónomos de inteligencia artificial: desafíos para el derecho privado», *InDret*, I, 2026, 193-226.

SALVADOR CODERCH, Pablo/RUBÍ PUIG, Antoni, «Causas de exoneración de la responsabilidad. Excepción por riesgos de desarrollo», en: Salvador Coderch, Pablo/Gómez Pomar, Fernando (Dirs.), *Tratado de responsabilidad civil del fabricante*, Aranzadi, Pamplona, 2008.

Capítulo IV

LA INTELIGENCIA ARTIFICIAL COMO HERRAMIENTA EFICAZ PARA LA PREVENCIÓN DE INSOLVENCIA Y LA REESTRUCTURACIÓN DE DEUDAS

Leticia Latorre Luna

1. INTRODUCCIÓN

En los procedimientos de insolvencia, con la finalidad de proteger tanto a los deudores como a los acreedores a través de una distribución equitativa de los activos y atender al pago de las deudas pendientes, tradicionalmente algunas de las herramientas que se han aplicado y, continúan aplicándose para la prevención y reestructuración empresarial – reguladas la mayoría en la Directiva (UE) 2019/1023 – son:

Por un lado, el uso obligatorio de estados financieros normalizados conforme al Plan General Contable o normativa sectorial aplicable, los sistemas automatizados de detección de incoherencias o inconsistencias en libros contables, facturación y declaraciones tributarias, así como la necesidad de una valoración periódica de activos, incluyendo intangibles, y flujos de caja proyectados, todo ello con la finalidad de garantizar una calidad documental con incentivos legales.

Por otro lado, a fin de asegurar una reestructuración fiable y preventiva únicamente en aquellos deudores viables, se aplican diversos criterios predictivos tales como: la proyección en los próximos cinco años de ingresos y EBITDA bajo escenarios conservadores, la valoración de la unidad productiva como activo transferible, el análisis de dependencia de clientes o proveedores clave y, la evaluación del capital humano y tecnológico,

entro otros, en los que se ha de sumar la valoración de la buena fe del deudor, con indicadores como: ausencia de sanciones tributarias o penales por fraude económico, colaboración con el juzgado y la administración concursal, no ocultación de bienes, ingresos o documentación relevante y, solicitud del concurso en plazo legal. En este sentido, se ha de tener presente que dichas herramientas predictivas deben ser capaces de identificar el tipo de insolvencia (actual, inminente o probable) según umbrales objetivos⁴² a fin de distinguir si la empresa se encuentra ante una situación transitoria que se puede solucionar a través de un proceso de reestructuración o ante una insolvencia estructural sin viabilidad (ARROYO, AC, 2025).

Sin embargo, a pesar de la aplicación de las anteriores herramientas, todas ellas eficaces a pesar de que «los procesos de insolvencia tradicionales frecuentemente sufren de ineficiencias, demoras y falta de transparencia» (LORENTE, *RJUSA*, 2024, 3) en los últimos años estamos apreciando cómo la inteligencia artificial (IA) y el aprendizaje automático (ML) están redefiniendo el modelo operativo empresarial, teniendo un impacto significativo en el ámbito de los procedimientos de insolvencia desde una perspectiva jurídico-económica, cuestión que se abordará en el presente trabajo donde se analizarán algunas de las formas esenciales de la aplicación práctica de la IA para la prevención de insolvencia y la reestructuración de deudas. Ahora bien, la consecuencia de este objeto requiere tener en cuenta que no se trata únicamente de habilitar automatización, sino más bien de asentar las bases de una infraestructura cognitiva, que sea capaz de operar bajo nuevas condiciones de mercado y escalar sin reiterar problemas anteriores (GARCÍA, OT, 2025).

42. Al respecto, algunos de los umbrales objetivos a tener en consideración son: las ratios de liquidez inmediata y endeudamiento operativo; análisis de margen bruto recurrente y servicio de la deuda y; detección de deterioro patrimonial (perdidas continuadas, capital social erosionado, impagos a empleados o Hacienda).

2. LA INTELIGENCIA ARTIFICIAL COMO HERRAMIENTA AVANZADA PARA LA DETECCIÓN PROACTIVA DE RIESGOS FINANCIEROS

Es indudable que la utilización de la IA está teniendo un impacto significativo en la detección anticipada de riesgos financieros, dado que a través del análisis de grandes volúmenes de datos financieros y no financieros se identifican patrones y sistemas de alarma de posibles problemas de solvencia de una empresa. Por otro lado, a través de la IA se analizan factores de ingresos, deudas, flujos de efectivo y ratios financieros lo que permite acceder a algoritmos de aprendizaje automático, a un análisis predictivo sobre la probabilidad de incumplimiento de pagos de deudore, así como un análisis de los informes financieros y comunicaciones empresariales a fin de detectar otros problemas económicos.

En el ámbito de la práctica financiera, se ha podido apreciar como a través de la utilización de algoritmos de IA en el análisis de factores como la liquidez, insolvencia, la rentabilidad y el flujo de efectivo de una empresa, se identifican varios riesgos financieros y situaciones problemáticas, permitiendo a los directivos y profesiones implicados tomar a tiempo decisiones y medidas proactivas para abordar dichos problemas, lo que implica una mejora de la situación financiera de la empresa y a su vez evitar la insolvencia.

2.1. Evaluación y análisis de activos mediante el uso de la inteligencia artificial

En concreto, la IA permite que la fase de liquidación o venta de activos dentro del procedimiento de insolvencia sea más concisa y realista dado que a través de su aplicación se puede acceder a información en tiempo real sobre el valor de los activos y las condiciones de mercado, lo que permite una toma de decisiones más eficiente al mitigar considerablemente los riesgos, así como una protección de los intereses de las partes del

proceso de insolvencia garantizando a su vez una equidad en el mismo. De hecho, «los algoritmos de IA pueden proporcionar valoraciones de activos más precisas y confiables, lo que permite a los profesionales de la insolvencia tomar decisiones informadas sobre el precio de los activos y los compradores potenciales» (LORENTE, *RJUSA*, 2024, 15).

Así pues, con la IA podemos acceder a una valoración de los activos (incluidos inventarios, bienes inmuebles y cuentas a cobrar) real y actualizada al mercado, lo que en la práctica puede cooperar significativamente en el proceso de liquidación de una empresa en quiebra, siendo capaz la IA de precisar el valor de los activos e incluso facilitar estrategias de liquidación a fin de maximizar la recuperación de los acreedores en comparación de lo que se habría logrado a través de métodos tradicionales.

Entre las técnicas y desarrollos más innovadores que potencian la aplicación de la IA en el ámbito de la predicción de la insolvencia empresarial, se encuentran los Sistemas Expertos (SE), las Redes Neuronales Artificiales, la Teoría de Conjuntos Aproximados y los Sistemas Híbridos. En concreto, uno de los más aplicados son los SE que, incorporan el conocimiento de expertos en materias determinadas dialogando con los usuarios justificando sus respuestas y proporcionando información que ayuda a la toma de decisiones. La aplicación de esta técnica de IA proporciona que las tareas rutinarias se realicen con menos fallos, un análisis de los datos a gran velocidad, captación clara de las conclusiones complejas y difíciles, así como que las conclusiones son más fiables dado que son el resultado de conocimientos de varios expertos, entre otras. No obstante, no hemos de obviar algunas de sus limitaciones, como la inexistencia de estándares de software de infraestructura y de tareas que integren, relacionen y coordinen distintas bases de datos. Al respecto, en el contexto de la predicción de la insolvencia empresarial se encuentran los Sistemas de Expertos que clasifican empresas a través de datos financieros y medidas de entropía, que analizan la solvencia de la empresa para concesión de préstamos, así como para evaluar solicitudes de conce-

sión de créditos en entidades financieras, entre otros (RODRÍGUEZ, *AECA*, 2002, 37-38).

En la esfera financiera vinculada a la prevención de insolvencia y reestructuración de deudas, el uso de la IA, por un lado, contribuye a un control más eficaz y eficiente de la evaluación y seguimiento de la solvencia y probabilidad de impago o predicción de los flujos de caja, como reducción de posibles pérdidas, optimización del capital, automatización de la toma de decisiones o la expansión de la cifra de negocio a través de una ampliación de la base de solicitantes de crédito cuyas peticiones son aprobadas. Por otro lado, la IA en el sector de la banca incrementa la capacidad analítica y predictiva en relación con eventos del mercado al objeto de maximizar el rendimiento de las inversiones en entornos de volatilidad incierta reforzando mecanismos de descubrimiento de precios o reducir las barreras de entrada a mercados de activos menos líquidos, como los de deuda cooperativa o los emergentes (BALSATEGUI/GORJÓN/MARQUÉS, *REF*, 2024, 11-12).

Especialmente, los sistemas de alerta temprana son herramientas basadas en la aplicación de IA a fin de detectar a través de datos en tiempo real posibles riesgos financieros. Por ejemplo, dentro del Derecho Concursal, como más adelante se expone, a través del análisis de la propia información generada dentro de la empresa a través de datos financieros, operativos y comerciales permiten identificar de manera temprana situaciones de desequilibrio financiero en las empresas (retrasos en los pagos de clientes, desviaciones en los flujos de caja o el incremento del endeudamiento) a fin de que se adopten medidas de reestructuración antes de dar lugar a una situación de insolvencia indeseable.

En suma, como se puede apreciar, los beneficios de la IA en el sector financiero de una empresa vienen marcados fundamentalmente: por un lado, al potenciar actuaciones orientadas a controlar la solidez, la solvencia y el comportamiento de las entidades cuya finalidad sea la de salvaguardar la estabilidad de todo el sistema, por otro lado, detectar de manera temprana los posibles riesgos a través de los errores que puedan darse en

los datos reportados, así como generar de manera más precisa los posibles escenarios que pudieran darse identificando las consecuencias de cada uno de ellos.

2.2. La optimización de las labores legales y administrativas en los procedimientos de insolvencia mediante el uso de la inteligencia artificial

Se puede observar también que, los sistemas de IA permiten que los procesos legales y administrativos dimanantes de los procesos de insolvencia se simplifiquen y agilicen además de incrementar su transparencia y reducir los riesgos de errores humanos.

En este sentido la IA, permite una automatización de estos procesos adaptada a las exigencias legales, reduciendo a su vez la carga de trabajo tanto de las Administraciones públicas, abogados, administradores concursales, economista y otros profesionales del sector, al facilitar documentos relevantes como pueden ser, entre otros, contratos, acuerdos de reestructuración, escritos judiciales e informes económico-jurídicos, así como una investigación de antecedentes más completa y detallada.

En síntesis, la IA permite reducir errores humanos, automatizar tareas repetitivas y optimizar la generación de reportes financieros (LINO, *DFFACIL*, 2025, 11). Este acontecimiento facilita a su vez que los profesionales que intervienen en el procedimiento de insolvencia gocen de un tiempo *adicional* para negociar y estudiar estrategias de reestructuración más viables y eficaces, así como para centrarse en tareas de mayor valor, como el análisis estratégico y la supervisión de sistemas automatizados, lo que implica una reducción de los costos y tiempos en los procesos legales (ANGULO, *FR*, 273, 2025).

Uno de los resultados prácticos de la aplicación de la IA en la automatización de procesos legales y administrativos involucrados en el procedimiento de insolvencia es la generación de documentos legales, estrategias de coordinación de reuniones

entre las partes, así como la presentación electrónica de informes y documentos judiciales, simplificando y acelerando así el proceso de insolvencia, facilitando que las partes dispongan de mayor tiempo para la resolución de problemas financieros y operativos. Además, a través de la IA se pueden detectar fraudes durante auditorías (VALLADARES/ORDÓÑEZ, *RMPI*, 2024, 79).

Adicionalmente, otra función práctica de la IA generativa y predictiva es través de los *chatbots* y asistentes virtuales en los procedimientos de liquidación proporcionando respuestas instantáneas a las partes involucradas mejorando su experiencia y garantizando a su vez una continua difusión de la información (LORENTE, *RJUSA*, 2024, 16).

Además, otros de los usos prácticos de la IA y ML es la creación y ejecución de contratos inteligentes en plataformas *Blockchain*, donde a través de la automatización de procesos legales se verifica con mayor eficiencia y seguridad el cumplimiento de las condiciones contractuales sin intervención humana. En este sentido, la tecnología *Blockchain*, en los procedimientos de insolvencia «puede proporcionar un registro auditable, seguro e inmutable de transacciones, transferencias de activos y reclamaciones de acreedores» (LORENTE, *RJUSA*, 2024, 11), lo que implica una distribución de los activos de manera más equitativa y eficiente entre las partes interesadas.

En concreto, las plataformas *Blockchain*, facilitan dos herramientas relevantes en los procedimientos de insolvencia. Por un lado, los *tokens*, que tienen la capacidad de representar la propiedad fraccionada de los activos, facilitando así las ventas complejas y agilizando los procesos de liquidación.

Por otro lado, los *smart contracts*, que son contratos ejecutables de manera automática, rápida y segura a través de acciones predefinidas previamente en un acuerdo manifestado, siempre y cuando se cumplan ciertas condiciones específicas (LORENTE, *RJUSA*, 2024, 11-12).

En lo que respecta a los procedimientos judiciales dimanantes de las situaciones de insolvencia, tras el análisis de grandes volúmenes de datos y jurisprudenciales, los algoritmos de IA y ML identifican patrones y tendencias en litigios y resoluciones

judiciales, lo que permite tener acceso a predicciones futuras de posibles resultados y riesgos del caso concreto, facilitando así que los profesionales del derecho puedan tomar decisiones basadas en estrategias más viables.

En este sentido, el legislador europeo regula el uso de la IA en la Administración de Justicia por parte de la autoridad judicial en el Reglamento (UE) 2024/1689, de 13 de junio de 2024 (RIA)⁴³, optando por un sistema de IA fiable y centrado en el ser humano basado en los valores y principios de la Unión Europea a fin de garantizar «un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de la IA en la Unión, así como prestar apoyo a la innovación» (art. 1.1. RIA).

Sin embargo, la Unión Europea también es consciente de que un «mal uso» o un «uso indebido» de la IA en el sector de la Administración de Justicia puede suponer una amenaza para el ejercicio de los derechos y libertades de los ciudadanos contemplando así distintos niveles de riesgos, estableciendo a su vez diferentes obligaciones a cumplir por los sujetos implicados en todo el proceso, todo ello con la finalidad de garantizar una utilización legal, ético y responsable de los sistemas de IA en el ejercicio de la actividad jurisdiccional.

En concreto, el anexo III RIA establece los sistemas de IA de alto riesgo por sectores y, en lo referente a la Administración de Justicia, el apartado 8 a), especifica que los «Sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial en la investiga-

43. 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.º 300/2008, (UE) n.º 167/2013, (UE) n.º 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).

ción e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos, o a ser utilizados de forma similar en una resolución alternativa de litigios», teniéndose en cuenta a su vez que el apartado 6 del citado anexo incluye el uso de sistemas de IA que también pueden incidir en el ámbito de la actuación de los órganos jurisdiccionales empleados como garantía del cumplimiento del Derecho⁴⁴ (VALLESPÍN, *La utilización*, 2026, 275).

Resta aclarar que la finalidad del RIA es garantizar un marco jurídico sólido de aplicación de la IA de manera uniforme de acuerdo con la normativa vigente, integrada por el propio RIA, el Reglamento General de Protección de Datos y la legislación interna en desarrollo o complementaria de las citadas normas, así como las normas internas específicas en el ámbito judicial.

En este escenario, a nivel interno, contamos, por un lado, con el Real Decreto-Ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, en el que se desarrolla un marco normativo destinado a la digitalización de la justicia, donde en el art. 35 regula la aplicación de las herramientas de IA en la interoperatividad de los sistemas informáticos a disposición de la Administración de Justicia (FONTESTAD, *Derechos y deberes*, 2025, 33-54).

Por otro lado, el Real Decreto 729/2023, de 22 de agosto, que aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial (AESIA), que define los fines, la estructura y las funciones del primer organismo de supervisión de IA creado en Europa, donde en su art. 27 regula la colabora-

44. En concreto, el apartado recoge los sistemas destinados a evaluar el riesgo de que una persona física sea víctima de delitos, cuando se usen polígrafos o herramientas similares, para evaluar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos, para evaluar la posibilidad de delinquir o la reincidencia o elaborar perfiles de personas físicas durante la detección, la investigación o el enjuiciamiento de delitos.

ción de la AESIA a través de su Secretaría General con la Administración de Justicia.

Igualmente a nivel nacional, se ha de destacar el documento sobre *Política de uso de la inteligencia artificial en la Administración de Justicia*, aprobado en junio 2024 por el Pleno del Comité Técnico Estatal de la Administración Judicial Electrónica (CTEAJE), que contempla en el punto cuarto entre los principios básicos del uso de los sistemas de IA en la toma de decisiones judiciales, el principio de control humano real de los procesos en los que ha intervenido la IA, a fin de garantizar que la última palabra corresponda al juez, jueza, magistrado o magistrada en lo referente a la resolución judicial, a la valoración de los hechos o de las pruebas, así como la interpretación y aplicación del Derecho, sin que sea posible sustituir su decisión final por las indicaciones del algoritmo.

Por último, se ha de hacer especial mención a la Instrucción 2/2026, de 28 de enero, del Pleno del Consejo General del Poder Judicial, sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional, que arroja un poco de luz a los jueces, juezas, magistrados y magistradas que deseen utilizar sistemas IA incluidas las herramientas de IA generativa en el ejercicio de la actividad jurisdiccional al establecer algunos criterios, pautas y principios para su correcto uso en consonancia con los principios establecidos en el Reglamento (UE) 2024/1689, de 13 de junio de 2024 (RIA) que regula la aplicación de la IA en la Administración de Justicia por parte de la autoridad judicial.

Así pues, de conformidad con lo previsto en el artículo 5.1. de la citada Instrucción, los jueces únicamente podrán utilizar los sistemas IA que les sean facilitados por las Administraciones competentes en materia de justicia o por el Consejo General del Poder Judicial. No obstante, podrán utilizar los sistemas de IA no proporcionados por Administraciones o CGPJ siempre y cuando sea para finalidades de preparación o estudio (elaboración de resúmenes o traducciones o el análisis de fuentes jurídicas, doctrinales o técnicas), a lo que habría que añadir que la información utilizada a tal fin debe proceder única y exclusi-

vamente de fuentes abiertas (art. 3 g) y, que no se podrán en ningún caso incorporar datos judiciales a los sistemas de IA (DELGADO, CGA, 2026)

Ahora bien, los sistemas IA permitidos se podrán usar únicamente como instrumentos de apoyo o asistencia (art. 6.1.) y en ningún concepto se podrá sustituir al juez por una decisión automatizada, tal y como establecen el art. 8 a) y el art. 4 b) de la citada Instrucción.

En concreto, el art. 6.3 de la Instrucción señala que los sistemas IA podrán usarse para: (1) Búsqueda y localización de información jurídica, incluida la identificación de normativa, jurisprudencia y doctrina relevante, así como la recuperación de antecedentes procesales o documentales; (2) Análisis, clasificación y estructuración de información, documentos o datos contenidos en actuaciones judiciales, con fines de organización, comprensión o apoyo al estudio del asunto; (3) Elaboración de esquemas, resúmenes o borradores de trabajo interno, siempre que no tengan carácter decisorio ni sustituyan la redacción personal de resoluciones judiciales y; (4) Apoyo a tareas organizativas o auxiliares, relacionadas con la gestión del conocimiento jurídico o con la preparación del trabajo jurisdiccional.

Asimismo, se ha de tener en consideración que para la elaboración de borradores de resoluciones judiciales únicamente podrá realizarse con los límites establecidos en el art. 7 de la Instrucción, esto es: en primer lugar, con una revisión y validación personal, completa y crítica por parte del juez, jueza, magistrado o magistrada, quienes mantendrán en todo momento su exclusiva responsabilidad sobre la resolución correspondiente; en segundo lugar, estos borradores no tendrán en ningún caso la consideración de decisiones automatizadas y; por último, los sistemas de IA deberán asegurar que el borrador documental sólo se genere a voluntad del juez, y pueda ser libre y enteramente modificado por éste antes de su validación como resolución judicial o procesal.

Sin embargo, de conformidad con el art. 8 de la Instrucción, los sistemas IA no podrán utilizarse en los siguientes supuestos: (1) La sustitución, automatización o delegación de la toma

de decisiones judiciales, de la valoración de los hechos o de las pruebas, o de la interpretación y aplicación del Derecho; (2) La utilización de resultados generados por los sistemas de IA que condicionen de manera directa o indirecta la independencia judicial o la libertad de criterio de los jueces; (3) La incorporación a resoluciones judiciales de contenidos generados por sistemas de IA sin una validación crítica, completa o personal por parte de los jueces; (4) Para el tratamiento de datos personales especialmente protegidos o de información sujeta a deberes reforzados de confidencialidad, fuera de los supuestos expresamente autorizados por la normativa vigente; (5) Con fines de perfilado de personas, predicción de comportamientos, evaluación de riesgos o clasificación de sujetos, fuera de los supuestos expresamente autorizados por la normativa vigente y; (6) Cualesquiera otros usos contrarios a los criterios, pautas de uso y principios establecidos en la referenciada Instrucción.

Finalmente, para un correcto uso de los sistemas IA permitidos, la Instrucción establece en el art. 4 una serie de principios que han de respetar los jueces, juezas, magistrados y magistradas, a saber:

- 1) *Principio de control humano efectivo.* El uso de los sistemas IA siempre va a estar sometido a un control humano real, consciente y efectivo por parte de los jueces, sin que dichos sistemas puedan operar de forma autónoma para la toma de decisiones judiciales, la valoración de los hechos y o de las pruebas, o la interpretación y aplicación del Derecho.
- 2) *Principio de no sustitución de los jueces.* La utilización de los sistemas de IA no podrá sustituir en ningún caso a los jueces para la toma de decisiones judiciales, la valoración de los hechos o de las pruebas o la interpretación y aplicación del Derecho.
- 3) *Principio de responsabilidad judicial.* Este principio determina que la responsabilidad plena y exclusiva de las resoluciones, decisiones y actuaciones jurisdiccionales corresponde en todo caso a los jueces, con independen-

cia de la utilización de sistemas de IA como instrumento de apoyo o asistencia.

- 4) *Principio de independencia judicial.* La utilización de sistemas de IA debe realizarse de manera compatible con la independencia judicial, sin que los resultados generados por dichos sistemas condicionen, directa o indirectamente, la libertad de criterio del órgano jurisdiccional.
- 5) *Principio de respeto a los derechos fundamentales.* El uso de los sistemas de IA en todo caso debe respetar los derechos fundamentales reconocidos en la Constitución y en el Derecho de la Unión Europea, particularmente, la tutela judicial efectiva, la igualdad, la no discriminación y la protección de datos personales.
- 6) *Principios de confidencialidad y seguridad.* Los sistemas de IA que traten datos judiciales deben garantizar la confidencialidad, integridad y seguridad de la información, evitando accesos no autorizados, usos indebidos o transferencias no permitidas.
- 7) *Principio de prevención de sesgos algorítmicos.* A tenor de este principio, los jueces deben adoptar las cautelas necesarias para identificar y evitar sesgos algorítmicos derivados de la utilización de sistemas de IA.
- 8) *Principio de proporcionalidad y uso limitado.* La utilización de sistemas de IA debe ser proporcionada a la finalidad perseguida y limitada a aquellos supuestos en los que puedan resultar útiles y eficaces como instrumento de apoyo o asistencia a la actividad jurisdiccional.

De los anteriores principios, uno de los principios fundamentales es el de control humano efectivo, que prohíbe que el juez sea sustituido por los sistemas de IA, así como la toma de decisiones, valore pruebas o interprete el Derecho de manera autónoma.

Por último, se ha de tener en consideración el art. 11 de la citada Instrucción donde establece que las consecuencias del incumplimiento de la Instrucción por parte de los jueces, juezas, magistrados y magistradas podrá dar lugar a las responsa-

bilidades reguladas en la Ley Orgánica del Poder Judicial, sin perjuicio de las medidas preventivas o correctoras que puedan adoptarse en el ámbito organizativo o de gobierno del Poder Judicial.

En este contexto, el Consejo General del Poder Judicial, es quien tiene competencia para ejercer las funciones de supervisión y control de la utilización de los sistemas de IA en todo aquello que pudiera afectar a las operaciones de tratamiento de datos personales efectuadas con fines jurisdiccionales (ordinal duodécimo). Asimismo, el CGPJ está obligado a completar la formación y capacitación continua de los jueces, juezas, magistrados y magistradas ofertándoles actividades formativas y de capacitación sobre el uso de sistemas de IA en el ámbito de la Administración de Justicia (ordinal décimo tercero). Así pues, en la nueva Era Digital la formación del juez no únicamente va a ser propiamente jurídica, sino también se le va a requerir que se encuentre familiarizado con los sistemas de IA, a fin de que pueda cumplir satisfactoriamente con su actividad jurisdiccional.

Como se puede apreciar la voluntad del Consejo General del Poder Judicial con la citada Instrucción es adoptar la IA como instrumento beneficioso para la Administración de Justicia garantizando un uso legal y ético que respete los derechos y libertades de los ciudadanos, preservándose a su vez la independencia de los órganos del Poder Judicial ante la generalización del uso de los sistemas de IA, pues si bien es cierto que la actividad jurisdiccional pueda beneficiarse, resulta imprescindible adoptar determinadas cautelas en función del elevado riesgo que representa su uso en la Administración de Justicia para los derechos de los ciudadanos y, en cumplimiento de los principios constitucionales que rigen el ejercicio de la actividad jurisdiccional (VALLESPÍN, *La utilización*, 2026, 286).

En consecuencia, los sistemas de IA pueden ser aplicados dentro de las distintas fases del procedimiento concursal. Así pues, por un lado, en la fase común se puede aplicar a fin de analizar de forma detallada la información almacenada en los sistemas informativos de contabilidad de la empresa en concur-

so, obteniéndose un análisis preciso sobre los motivos y las causas del incumplimiento de las obligaciones y deberes de administración y gestión, como ahorrar tiempo en la búsqueda de información. Por otro lado, en la fase del convenio se pueden aplicar herramientas de IA que permiten analizar jurisprudencia reciente de situaciones similares, facilitando un análisis comparativo y los diversos escenarios jurídicos a fin de planificar una estrategia procesal. En tercer lugar, en la fase de liquidación, la Administración concursal puede hacer uso de la IA para hacer una valoración estimatoria de los activos e incluso el modo más rápido y eficaz de liquidación, lo que ayuda a agilizar el procedimiento concursal y el pago a los acreedores.

En última instancia, en la fase de calificación, el juez puede hacer uso de los sistemas de IA para analizar la documentación aportada por las partes con el objeto de obtener un informe más preciso de los motivos de insolvencia de la empresa concursada a fin de emitir una sentencia más justa y acorde a los motivos reales que dieron lugar a la insolvencia de la concursada. Además, la IA puede detectar movimientos anuales que pudieran ser considerados como indicios de fraude o identificar patrones o anomalías con actividades fraudulentas. Al respecto, teniéndose presente que los sistemas de IA han de utilizarse como un mero instrumento o herramienta por parte del juez, jueza, magistrado o magistrada, este es, ser utilizados de manera accesoria, dado que el su uso es voluntario y, su transcendencia en la decisión judicial carece de relevancia sustancial desde la perspectiva del ejercicio de la justicia, siendo así coherente con la exclusiva responsabilidad del juez, jueza, magistrado o magistrada incluso si han ejercido la jurisdicción con apoyo a la IA (SERRANO, *CEPC*, 2026).

3. LA IMPLEMENTACIÓN DE SOLUCIONES BASADAS EN INTELIGENCIA ARTIFICIAL DENTRO DEL PROCESO DE REESTRUCTURACIÓN DE DEUDAS

En líneas generales, la reestructuración de deuda es el proceso mediante el cual una empresa reorganiza sus obligaciones financieras para adaptarlas a su realidad operativa, a su capacidad de generación de caja y a su ciclo de negocio. Así pues, cuando se trata de reestructurar la deuda, se trata de rediseñar de forma integral los plazos de amortización, coste financiero, calendario de pagos, condiciones contractuales, nivel de flexibilidad ante escenarios adversos, entre otros, con la finalidad de poder pagar a los acreedores sin que conlleve grandes dificultades al negocio a fin de que pueda seguir operando con normalidad (DE LA TORRE, *LF*, 2026).

Para ello, los expertos en reestructuración utilizan algunos mecanismos con la finalidad de adaptar las obligaciones financieras a la capacidad de pago del deudor, entre los más destacables se encuentran: la ampliación de plazos; la reducción de intereses; los aplazamientos de pagos; las quitas (condonación parcial); la consolidación/reunificación de deudas y; los planes de reestructuración, que son instrumentos legales formales donde se acuerdan cambios operativos y financieros, a menudo gestionados ante un juez con la finalidad de proteger a la empresa de procedimientos concursales.

Sin embargo, en los últimos años, algunos de estos mecanismos se han visto transformados con la aplicación de la IA, al permitir la automatización de los procesos, mejorar la eficiencia y proporcionar análisis predictivos, siendo su adopción fundamental en el entorno de los procesos de reestructuración dado que se ahorra tiempo, reduce costos y aumenta la productividad. Por ende, como veremos, la aplicación práctica de las herramientas de IA a lo largo del proceso de reestructuración supone una mejora significativa en la eficiencia, la precisión, capacidad de análisis predictivo y la toma de decisiones. A través de tales mecanismos, apreciamos cómo los algoritmos de aprendizaje automático permiten realizar análisis predictivo pa-

ra anticipar quiebras, aumentar la eficiencia operativa y la reducción de errores humanos gracias a la automatización y al análisis avanzado, mejorar la toma de decisiones al proporcionar análisis en tiempo real y predicciones precisas, permitiendo una gestión financiera más informada y estratégica (NÁJERA, *RECIMUNDO*, 2025, 270).

3.1. La negociación y la toma de decisiones en los procesos de reestructuración de deudas mediante la aplicación de inteligencia artificial

Este planteamiento resulta especialmente relevante por lo que se refiera a la mejora de los procesos de negociación y toma de decisiones para la reestructuración de deudas, dado que la IA proporciona información en tiempo real sobre las condiciones de mercado, proporcionando propuestas de reestructuración y negociación más viables al tener en cuenta diversos escenarios como los intereses de los acreedores, perspectivas económicas y capacidad de pago, así como sus consecuencias. Al respecto, se ha de destacar que estas herramientas permiten una gestión financiera más informada y estratégica al proporcionar análisis en tiempo real y predicciones precisas (AHMED, *RIBF*, 2022). Además, la IA ayuda a la sostenibilidad al optimizar el uso de recursos y facilitar decisiones alineadas con los Objetivos de Desarrollo Sostenible (ODS) (PENG, *Sustainability*, 8, 2023).

En la práctica, la IA puede cooperar con las partes interesadas a identificar mejores estrategias de reestructuración de deudas y alcanzar un acuerdo viable, equitativo y aceptable por todas ellas, mejorando así la eficiencia y efectividad del propio proceso de reestructuración y, en el mejor de los casos evitar la insolvencia permitiendo continuar con la actividad empresarial. A su vez, la IA ha mejorado significativamente la transparencia en los procesos de toma de decisiones y auditorías, facilitando la comprensión de los resultados por parte de los usuarios (SHAKDWIPEE, *Artificial Intelligence*, 2023, 169 y WEBER, *Appli-*

cations, 2023, 890). Así pues, en contraste con la auditoría tradicional, la IA permite una capacidad mejorada para prever excepciones y detectar desviaciones inmediatas entre los resultados reales y las predicciones (ANH, *JRFM*, 2024, 273).

3.2. La aplicación de la inteligencia artificial como herramienta para optimizar el monitoreo y la ejecución de acuerdos y planes de reestructuración

Es indudable que, además, la IA permite asegurar un mayor cumplimiento de los acuerdos y planes de reestructuración al identificar situaciones donde es necesario adaptar los mismos a los cambios significativos dimanantes de las condiciones de mercado o de la propia financiación de la empresa, prediciendo a su vez posibles incumplimientos de las obligaciones legales y contractuales de las partes o posibles futuros escenarios a tener en consideración. A su vez, la IA resulta ser una herramienta de gran utilidad en la gestión de riesgos y el cumplimiento normativo, al identificar patrones complejos que favorecen la adecuación a marcos regulatorios (HENTZEN, *IJBM*, 2021, 1.330).

Desde una perspectiva práctica, se puede apreciar que la IA puede llegar a monitorear y garantizar el cumplimiento de los acuerdos del plan de reestructuración tras analizar la situación financiera en tiempo real, comparando los resultados con los propios objetivos y compromisos establecidos en el plan. Así pues, con la identificación de las posibles áreas de incumplimiento las partes pueden adoptar medidas eficientes y concretas que mejoren la probabilidad de éxito del plan de reestructuración.

De manera adicional, en la práctica del ámbito financiero, los *robo-advisors* permiten un asesoramiento automatizado tras la utilización de algoritmos de IA y ML que proporciona consejos de inversión y gestión de carteras adaptadas a las necesidades y objetivos particulares de un determinado inversor, información sumamente relevante al resultar una estrategia a tener en consideración en el propio plan de reestructuración.

Por otro lado, las herramientas de IA también se han aplicado para mejorar el proceso de las cuentas por cobrar, así pues, si se combina la gestión de cuentas por cobrar con la inteligencia artificial y los asistentes digitales, los analistas de cuentas por cobrar pueden evolucionar obteniendo mejores resultados, llevando a una mayor colaboración entre créditos y ventas, una reducción adicional del tiempo de cobro de cuentas por cobrar y una disminución de las pérdidas de ingresos (HAMPTON, SSON, 2020).

Finalmente, otro de los beneficios a destacar de la incorporación de la IA en este sector es el aumento de la eficiencia operativa y la reducción de errores humanos gracias a la automatización y análisis avanzado.

4. LÍMITES Y RIESGOS DE LA APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LOS PROCEDIMIENTOS DE INSOLVENCIA

Si bien es cierto que la IA puede aportar grandes beneficios en los procedimientos de insolvencia ofreciendo perspectivas prometedoras, sin embargo, también se han de tener en consideración algunos de los límites y riesgos desde una perspectiva ético-jurídica que pueden surgir a causa de su aplicación en los procedimientos de insolvencia, que se detallan a continuación:

En primer lugar, desde una perspectiva jurídica, resulta fundamental que paralelamente a la utilización de la IA se cumplan las leyes de privacidad y protección de datos, implementándose medidas de seguridad adecuadas a fin de proteger la información confidencial, dado que la aplicación de estas tecnológicas implica necesariamente acceder a grandes cantidades de datos que, en el contexto que nos concierne, principalmente son datos personales y financieros de las personas involucradas en el procedimiento de insolvencia.

De igual modo, en el ámbito jurídico es necesario establecer las bases de legales en términos de responsabilidad legal, a fin de que regulen de manera clara y concisa quien es el

responsable legal en caso de errores o malas decisiones procedentes de la IA que pudieran afectar al resultado del proceso de insolvencia.

Ahora bien, desde una perspectiva financiera también se han detectado algunas restricciones en la aplicación práctica de estas herramientas, al existir una falta de evidencia empírica, especialmente en estudios aplicados a pequeñas y medianas empresas o en países en vías de desarrollo (CÓRDOBA, *LATAM*, 2024, 1.332). Así pues, uno de los principales riesgos que se puede detectar es la falta de precisión de los modelos de IA al generar textos, imágenes y otros resultados inexactos, incorrectos, engañosos o inapropiados debido a problemas dimanantes a la calidad de los datos, ajustes del propio sistema o por falta de explicabilidad inherente de algunos modelos de IA, lo que puede generar toma de decisiones erróneas. Además, los sistemas IA pueden generar información que aparentemente puede parecer válida, pero que en realidad es inventada y no se basa en la información de los datos de entrenamiento del modelo (BALSATEGUI/GORJÓN/MARQUÉS, *REF*, 2024, 16-17).

Otro de los desafíos que implica la utilización de las herramientas IA es el hecho de que los algoritmos de aprendizaje automático si se pueden basar en datos históricos o incompletos viéndose así afectados por sesgos y discriminación dando como resultado decisiones injustas o desfavorables para las partes involucradas. Así como, garantizar que las decisiones tomadas por la IA sean transparentes y explicables desde los términos legales y financieros, dado que se ha comprado que la IA también genera recomendaciones confusas y de difícil comprensión para los partes incluidos los profesionales involucrados en el procedimiento de solvencia.

A lo anterior habría que añadir una de las grandes preocupaciones de los expertos en los procedimientos de insolvencia es que la IA podría ser utilizada para realizar labores propias de los profesionales del ámbito legal y económico, así como de los empleados en ambos sectores, lo que podría generar un riesgo e impacto negativo en el empleo y la profesión de los expertos en insolvencia y reestructuración. Por ello, se

considera necesario fomentar el uso de esta herramienta como complemento de apoyo en las tareas profesionales y, en ningún caso como sustitución del profesional, cuyo criterio, experiencia y conocimiento será siempre necesario a fin de confirmar y validar que la aplicabilidad en el caso real de los resultados de la IA podría resultar eficaz, viable y exitosa en el procedimiento de insolvencia (LATORRE, *Principales*, 2025, 303-304).

En definitiva, dada la existencia de estos desafíos éticos, técnicos y legales, vinculados con la privacidad de los datos, la calidad de la información utilizada y la falta de estandarización en las técnicas implementadas (SHAKDWIPEE, *ICT*, 2023, 170 y CERNEVICIENE, *AIR*, 19, 2024), es necesario un marco regulatorio y supervisor que garantice el cumplimiento de los derechos de privacidad y protección de datos, la no discriminación, la transparencia y explicabilidad de los modelos de IA, así como un correcto uso de la IA conforme a la ética y la legalidad de la inteligencia artificial a través de marcos legales y normativos desarrollados por legisladores y profesionales expertos en finanzas, derecho, tecnología y ética a fin de establecer salvaguardias y mediadas específicas de protección de dichos derechos y asegurar que los resultados aplicados a la práctica procedimiento de insolvencia sean válidos, eficientes y eficaces.

5. CONCLUSIONES

La aplicación de la IA puede implicar una notoria mejora de los procedimientos de insolvencia, beneficiando a las partes interesadas y contribuyendo a que el propio procedimiento sea más eficiente y efectivo al identificar y resolver problemas de insolvencia.

Así pues, tras un análisis de la aplicación práctica de la IA en los diferentes ámbitos del procedimiento de insolvencia, podemos concluir que la IA resulta una herramienta fundamental a fin de monitorear a tiempo real la situación financiera de una empresa lo que permite prevenir la insolvencia y mitigar riesgos,

valorar activos con el objeto de maximizar la recuperación de los acreedores y facilitar una distribución más equitativa, facilitar la toma de decisiones informadas en procesos de reestructuración de deudas, así como aumentar la probabilidad de éxito y cumplimiento del plan de reestructuración por todas las partes.

En este sentido, no cabe duda de que el uso de la IA resulta determinante para que las entidades financieras, privadas y públicas en, especial, la Administración de Justicia puedan alcanzar objetivos como el aumento de la productividad, la mejora de su eficiencia, el incremento de la calidad o seguridad de sus productos y servicios o la reducción de costes.

El desarrollo de la IA ha facilitado un conjunto de herramientas que aplicables al problema de la predicción de la insolvencia empresarial que proporcionan al usuario una información de fácil comprensión facilitando resultados más efectivos y eficientes.

No obstante, a pesar de los beneficios y el gran potencial de la IA como herramienta eficaz para la prevención de insolvencia y la reestructuración de deudas, en el presente trabajo también se han destacado los posibles desafíos éticos y las limitaciones legales del uso de la IA en este contexto, como la privacidad y protección de datos, el sesgo y discriminación, la responsabilidad legal, la transparencia y el impacto en el empleo y la profesión de las personas involucradas en los procedimientos de insolvencia.

Es la nueva Era Digital, resulta indudable el potencial de la IA en los procedimientos de insolvencia, lo que significa que de manera inevitable en un futuro aumente notoriamente la implementación y utilización de esta herramienta por parte de las partes involucradas en dichos procedimientos, dada su gran utilidad a fin de poner en práctica estrategias financieras y legales más eficientes y efectivas, así como para identificar y resolver de manera temprana problemas de insolvencia. Ahora bien, dicho uso de la IA sería más eficiente, eficaz y viable si en futuro cercano se pudiera disponer de leyes sectoriales específicas y regulaciones actualizadas que abordasen los desafíos éticos y legales del uso de la IA en los procedimientos de insolvencia.

6. BIBLIOGRAFÍA

- AHMED, S./ALSHATER, M./AMMARI, A./HAMMAMI, H., «Artificial Intelligence and Machine Learning in Finance: A Bibliometric Review», *Research in International Business and Finance*, 61, 2022.
- ANGULO BUSTINZA, H. D./TANTALEAN LAM, E., «Análisis de la Inteligencia Artificial en el Entorno Empresarial: Revisión Sistemática (2018-2023)», *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, 29, 2025, 263-304.
- ANH, N. T. M./ HOA, L. T. K./ THAO, L. P., NHI, D. A./LONG, N. T./TRUC, N. T./ NGOC XUAN, V., «The Effect of Technology Readiness on Adopting Artificial Intelligence in Accounting and Auditing in Vietnam», *Journal of Risk and Financial Management*, 17, 1, 2024, 27.
- ARROYO EGIDO, I., «Herramientas gratuitas y eficaces para la prevención y reestructuración empresarial», *Atrium Creditoribus*, 19 de diciembre 2025. Disponible en: <https://atriumc.es/herramientas-insolvencia/>
- BALSATEGUI, I./GORJÓN, S./MARQUÉS, J.M., «La inteligencia artificial en el sistema financiero: implicaciones y avances bajo la perspectiva de un banco central», *Revista de Estabilidad Financiera - Banco de España*, 47, 2024, 5-31.
- ČERNEVIČIENĖ, J./KABAŠINSKAS, A., «Explainable artificial intelligence (XAI) in finance: a systematic literature review», *Artif. Intell. Rev.*, 57, 216, 2024, 1-65.
- CÓRDOVA MORÁN, M., «Los beneficios de la inteligencia artificial en el desarrollo de actividades contables: una revisión de la literatura reciente (últimos 10 años)», *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, 5, 6, 2024, 1326 – 1337.
- DE LA TORRE, J., «¿Qué es la reestructuración de deuda? Señales que saltan en tu empresa cuando la necesita», *Lean Finance*, 14 de enero de 2026. Disponible en: <https://leanfinance.es/blog/reestructuracion-de-deuda/>
- DELGADO MARTÓN, J., «Resumen de la Instrucción 2/2026, sobre la utilización de sistemas de inteligencia artificial en el ejercicio

- de la actividad jurisdiccional», *Consejo General de la Abogacía*, 2026. Disponible en: <https://www.abogacia.es/wp-content/uploads/2026/02/NOTAS-RESUMEN-DE-LA-INSTRUCCION-2-26-IA-EN-LA-FUNCION-JURISDICCIONAL.pdf>
- FONTESTAD PORTALÉS, L., «Derechos y deberes digitales en el ámbito de la Administración de Justicia, A propósito del R.D.L. 6/2023», en David Vallespín (Coord.), *Eficiencia digital, inteligencia artificial y derecho de defensa*, 2025, Oporto, Juruá Editora, 33-53.
- GARCÍA, B., «Más allá de la automatización: cómo la inteligencia artificial está redefiniendo el modelo operativo empresarial», *Omega Talento*, 24 de abril 2025. Disponible en: <https://omegacrmconsulting.com/la-inteligencia-artificial-esta-redefiniendo-el-modelo-operativo-empresarial/>
- HAMPTON, B., «SSON report. Automating Accounts Receivable Optimising Cash & Collections in Uncertain Times. SSON», 2020.
- HASAN, A., «Inteligencia Artificial (IA) en Contabilidad y Auditoría: Una Revisión de la Literatura», *Open Journal of Business and Management*, 10, 2022, 440-465.
- HENTZEN, J./HOFFMANN, A. /DOLAN, R. /PALA, E., «Artificial intelligence in customer-facing financial services: a systematic literature review and agenda for future research», *International Journal of Bank Marketing*, 40, 6, 2021, 1299-1336. Disponible en: <https://www.arvidhoffmann.nl/Hentzen%20et%20al.%202021%20IJBM.pdf>
- IN SOLIDUM ABOGADOS, «El uso de la inteligencia artificial en los procedimientos de insolvencia», 4 de mayo 2023. Disponible en: <https://insolidumabogados.com/el-uso-de-inteligencia-artificial-en-los-procedimientos-de-insolvencia/>
- LATORRE LUNA, L., «Principales utilidades y riesgos del uso de la inteligencia artificial en el sector jurídico» en A. Giménez Morera y A. Ortega Giménez (Dirs.), *Derecho, economía, empresa, nuevas tecnologías, innovación docente y educación: cuestiones prácticas actuales*, Ed. Colex, A Coruña, 2025, 299-306.
- LIANG, P./WU, L., «The Application of Artificial Intelligence in Accounting», 2022, 55-59.

- LINO GAMÍÑO, J. A., «La Inteligencia Artificial y su Impacto en la Contabilidad Pública un Análisis Teórico.: Artificial Intelligence and its Impact on Public Accounting, a Theoretical Analysis», *Diagnóstico fácil Empresarial Finanzas Auditoria Contabilidad Impuestos Legal*, 23, 2025, 9–20.
- LORENTE, J.A., «Aplicación de Inteligencia Artificial en procedimientos concursales: el futuro es hoy», *Revista Jurídica de la Universidad de San Andrés*, 18, 2024, 1-37.
- NÁJERA NÚÑEZ, B. C./BLUM ALCIVAR/H. M., LÓPEZ COLOMA, R. V./VILLEGAS-YAGUAL, F. E., «La inteligencia artificial en contabilidad y finanzas. Una revisión sistemática», *RECIMUNDO*, 9, 2, 2025, 262–277.
- PENG, Y./AHMAD, S./AHMAD, A./SHAIKH, M./DAOUD, M./ALHAMDI, F., «Riding the Waves of Artificial Intelligence in Advancing Accounting and Its Implications for Sustainable Development Goals», *Sustainability*, 15, 19, 2023, 1-12.
- RODRÍGUEZ LÓPEZ, M., «La inteligencia artificial como herramienta de modelización en la predicción de la insolvencia empresarial», *AECA. Asociación Española de Contabilidad y Administración de Empresas*, 61, 2002, 36-40.
- SERRANO PÉREZ, M^a M., «La instrucción del Consejo General del Poder Judicial sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional», *Blog del CEPC*, 18 de febrero de 2026. Disponible en: <https://www.cepc.gob.es/blog/la-instruccion-del-consejo-general-del-poder-judicial-sobre-la-utilizacion-de-sistemas-de>
- SHAKDWIPEE, P./AGARWAL, K./KUNWAR, H./SINGH, S., «Artificial Intelligence in Finance and Accounting: Opportunities and Challenges», *ICT Systems and Sustainability*, 1, 2023, 165-177.
- VALLADARES-ALBARRACÍN, J. J./ORDÓÑEZ-PARRA, Y. L., «La aplicación de inteligencia artificial en la auditoría contable [The application of artificial intelligence in accounting auditing]», *Revista Multidisciplinaria Perspectivas Investigativas*, 4, 2024, 73–85.
- VALLESPÍN PÉREZ, D., «La utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional: especial referencia al acuerdo, de 28 de enero de 2026, del pleno

del cgpj, por el que se aprueba la instrucción 2/2026», en M^a. N. Jimenez López (Dir.), *Nuevas Tecnologías al servicio de la justicia: Inteligencia Artificial, cooperación jurídica y MASC*, Ed. Codex, A Coruña, 2026, 271-291.

WEBER, P., CARL, K./HINZ, O., «Applications of Explainable Artificial Intelligence in Finance—a systematic review of Finance, Information Systems, and Computer Science literature», *Management Review Quarterly*, 74, 2023, 867-907.

CAPÍTULO V

INTELIGENCIA ARTIFICIAL, ECONOMÍA Y DERECHO: IMPLICACIONES ECONÓMICAS DE LA TOMA DE DECISIONES AUTOMATIZADAS

Dr. José Torres Remírez

1. INTRODUCCIÓN

La historia del crecimiento económico puede interpretarse como una sucesión de innovaciones tecnológicas capaces de modificar la productividad de los factores de producción y transformar las instituciones económicas. La máquina de vapor impulsó la Primera Revolución Industrial; la electricidad y la producción en cadena caracterizaron la Segunda; mientras que la informática y las telecomunicaciones marcaron el inicio de la denominada revolución digital. En la actualidad, numerosos autores sostienen que la inteligencia artificial constituye una nueva tecnología de propósito general con capacidad para generar cambios económicos comparables a los producidos por aquellas grandes revoluciones tecnológicas (Acemoglu & Johnson, 2023).

La difusión de la inteligencia artificial está alterando de forma acelerada los procesos de producción, la organización empresarial y la prestación de servicios públicos. Los algoritmos son ya capaces de analizar millones de datos en tiempo real, detectar patrones complejos, elaborar predicciones y ejecutar decisiones con un grado creciente de autonomía. Esta capacidad explica que la IA se haya incorporado rápidamente a sectores tan diversos como la sanidad, el sistema financiero, la industria manufacturera, el comercio electrónico, la educación, la logística o la administración pública.

Desde una perspectiva económica, la inteligencia artificial promete importantes incrementos de productividad, una reducción significativa de los costes de transacción y una mejora en la eficiencia de la asignación de recursos. La automatización de tareas repetitivas permite liberar capital humano para actividades de mayor valor añadido, mientras que el análisis masivo de datos facilita una toma de decisiones más rápida y fundamentada. Sin embargo, estos beneficios potenciales conviven con importantes incertidumbres relacionadas con el empleo, la distribución de la renta, la concentración del poder económico y el aumento de las desigualdades tecnológicas entre empresas, regiones y países (Agrawal et al., 2018).

La dimensión jurídica del fenómeno resulta igualmente trascendental. Tradicionalmente, el Derecho ha partido del presupuesto de que toda decisión relevante era adoptada por una persona física o jurídica plenamente identificable. La aparición de sistemas capaces de generar recomendaciones o incluso resolver procedimientos administrativos de forma automatizada cuestiona algunos de los principios clásicos sobre los que se construye el Estado de Derecho. Conceptos como la responsabilidad, la motivación de los actos administrativos, la transparencia, la tutela judicial efectiva o la igualdad ante la ley adquieren una nueva complejidad cuando las decisiones dependen de algoritmos cuyo funcionamiento puede resultar opaco incluso para sus propios desarrolladores.

La Unión Europea ha respondido a estos desafíos mediante la aprobación de un marco regulatorio pionero a escala internacional, basado en un enfoque de gestión del riesgo. El Reglamento Europeo sobre Inteligencia Artificial establece diferentes obligaciones en función del potencial impacto de cada sistema sobre los derechos fundamentales, configurando un modelo que pretende compatibilizar la innovación tecnológica con elevados estándares de protección jurídica. Esta aproximación contrasta con modelos regulatorios más flexibles, como el estadounidense, o con estrategias centradas en el liderazgo tecnológico, como las desarrolladas por China.

No obstante, la irrupción de la inteligencia artificial no puede comprenderse sin analizar el proceso previo de digitalización. La informatización de las empresas, la expansión de Internet, el desarrollo de las telecomunicaciones y la consolidación de la economía digital transformaron progresivamente las estructuras económicas españolas desde comienzos de la década de 1980. Durante ese periodo se produjeron importantes mejoras en productividad, competitividad e integración internacional, al tiempo que comenzaron a aparecer nuevas formas de contratación electrónica, protección de datos personales y administración digital que obligaron al Derecho a adaptarse a una realidad tecnológica en constante evolución.

En este contexto, el objetivo del presente trabajo es analizar la relación existente entre digitalización, inteligencia artificial y Derecho desde una perspectiva económica. En primer lugar, se estudia el impacto que tuvo la digitalización sobre la economía española entre 1980 y 2010. Posteriormente, se examinan las principales transformaciones jurídicas derivadas de dicho proceso. A continuación, se analizan las consecuencias económicas de la inteligencia artificial, tanto en el sector privado como en la administración pública, prestando especial atención a la productividad, el mercado de trabajo y la eficiencia institucional. Finalmente, se abordan los principales retos regulatorios asociados a la utilización de sistemas automatizados de decisión y se plantean diversas líneas de actuación orientadas a compatibilizar el progreso tecnológico con la protección efectiva de los derechos fundamentales (Frey & Osborne, 2017).

El trabajo adopta una metodología basada en la revisión crítica de la literatura económica y jurídica, complementada con el análisis de informes elaborados por organismos internacionales y de la normativa europea más reciente en materia de inteligencia artificial. En este sentido, se sostiene que la inteligencia artificial no constituye únicamente una innovación tecnológica, sino un cambio estructural que afectará simultáneamente a la organización económica, al funcionamiento de las instituciones públicas y a la configuración futura de los sistemas jurídicos (Acemoglu & Restrepo, 2018).

2. EL IMPACTO ECONÓMICO DE LA DIGITALIZACIÓN EN LA ECONOMÍA ESPAÑOLA (1980-2010)

La digitalización constituye uno de los procesos de transformación económica más relevantes de las últimas décadas. Aunque la actual revolución asociada a la inteligencia artificial concentra gran parte de la atención académica y política, sus fundamentos tecnológicos se encuentran en la progresiva incorporación de las tecnologías de la información y la comunicación (TIC) a la actividad económica desde finales del siglo xx. En el caso español, el período comprendido entre 1980 y 2010 representa una etapa especialmente significativa, pues durante esos treinta años la economía transitó desde un modelo eminentemente industrial hacia una estructura productiva caracterizada por la creciente importancia de los activos intangibles, la información y los servicios digitales (Agrawal et al., 2018).

La incorporación de España a la Comunidad Económica Europea en 1986 aceleró este proceso. La apertura comercial, la llegada de inversión extranjera y la necesidad de competir en un mercado cada vez más integrado incentivaron la modernización tecnológica del tejido empresarial. Paralelamente, la liberalización del sector de las telecomunicaciones, la expansión de Internet y el desarrollo de nuevas infraestructuras digitales favorecieron la aparición de nuevas formas de organización empresarial y de prestación de servicios (David, 1990).

Desde una perspectiva económica, la digitalización puede definirse como el proceso mediante el cual la información, las comunicaciones y los procesos productivos se transforman en formatos digitales susceptibles de ser almacenados, transmitidos y procesados electrónicamente. Esta transformación reduce significativamente los costes de producción y de coordinación, facilita el intercambio de información y aumenta la eficiencia de los mercados. Como señalaron autores como Paul David (1990) o Erik Brynjolfsson y Lorin Hitt (2000), las TIC constituyen una tecnología de propósito general cuyos efectos trascienden a un sector concreto y generan mejoras de productividad en el conjunto de la economía (David, 1990).

Sin embargo, estos efectos no son inmediatos. La denominada «paradoja de la productividad», formulada por Robert Solow en 1987 mediante su célebre afirmación de que «la era de los ordenadores está en todas partes excepto en las estadísticas de productividad», puso de manifiesto que las ganancias derivadas de la informatización requerían importantes cambios organizativos, inversión en capital humano y adaptación institucional antes de reflejarse plenamente en el crecimiento económico (David, 1990).

España constituye un ejemplo ilustrativo de este fenómeno. Durante los años ochenta y buena parte de los noventa la adopción de tecnologías digitales avanzó con relativa lentitud respecto a otras economías desarrolladas. No obstante, a partir de finales de esa década y especialmente durante los primeros años del siglo XXI se produjo una aceleración significativa de la inversión en infraestructuras digitales, software y telecomunicaciones, generando importantes efectos sobre la productividad, el empleo y la competitividad (David, 1990).

2.1. La incorporación de las tecnologías de la información y la comunicación

Durante la década de 1980, el uso empresarial de ordenadores estaba fundamentalmente restringido a grandes compañías financieras, entidades públicas y empresas industriales de mayor tamaño. La informatización se concentraba en tareas administrativas como la contabilidad, la gestión de inventarios o el procesamiento de nóminas. Las pequeñas y medianas empresas, que constituyen la base del tejido productivo español, mostraban todavía bajos niveles de adopción tecnológica debido al elevado coste del hardware, la escasa disponibilidad de personal cualificado y la limitada oferta de software especializado (Acemoglu & Restrepo, 2018).

La situación comenzó a modificarse progresivamente durante los años noventa. La reducción del precio de los equipos informáticos, el desarrollo de aplicaciones empresariales y la expansión de las redes de telecomunicaciones favorecieron una

rápida difusión de las TIC. Paralelamente, la liberalización del mercado de las telecomunicaciones impulsó una mejora significativa de la calidad de los servicios y una reducción de los costes de acceso (Acemoglu & Johnson, 2023).

A finales de la década de 1990 Internet dejó de ser una herramienta exclusiva del ámbito académico para convertirse en un elemento central de la actividad económica. Las empresas comenzaron a utilizar páginas web corporativas, sistemas de comercio electrónico y plataformas digitales de relación con clientes y proveedores. Esta transformación permitió reducir costes de búsqueda de información, mejorar la coordinación logística y ampliar el acceso a mercados internacionales (Acemoglu & Johnson, 2023).

Desde la perspectiva de la teoría económica, estas mejoras pueden interpretarse como una reducción sustancial de los costes de transacción descritos por Ronald Coase (1937) y posteriormente desarrollados por Oliver Williamson (1985). La disponibilidad inmediata de información disminuyó las asimetrías informativas, facilitó la comparación de precios y redujo los costes derivados de la negociación y supervisión de contratos.

2.2. Productividad y crecimiento económico

Uno de los principales debates de la literatura económica ha consistido en determinar hasta qué punto la digitalización contribuye al crecimiento económico. La evidencia internacional muestra que las inversiones en tecnologías digitales generan incrementos significativos de productividad cuando van acompañadas de cambios organizativos, formación del capital humano e innovación empresarial.

En España, el comportamiento de la productividad durante el período analizado presenta una evolución desigual. Durante la década de 1980 los incrementos de productividad estuvieron asociados principalmente a los procesos de reconversión industrial y modernización del aparato productivo. La contribución directa de las tecnologías digitales era todavía limitada.

La situación comenzó a cambiar a finales de los años noventa. Diversos estudios del Banco de España y de la OCDE muestran que la inversión en capital TIC empezó a convertirse en un componente relevante del crecimiento económico. Sectores como las telecomunicaciones, los servicios financieros, la distribución comercial y determinadas industrias manufactureras experimentaron importantes mejoras de eficiencia gracias a la automatización de procesos y a la incorporación de sistemas de gestión informatizados.

No obstante, España mantuvo durante buena parte del período un diferencial negativo de productividad respecto a las economías más avanzadas de Europa occidental y Estados Unidos. Este fenómeno ha sido atribuido a varios factores estructurales: elevada presencia de pequeñas empresas; menor intensidad innovadora; insuficiente inversión en I+D; limitada cualificación digital de parte de la fuerza laboral; especialización productiva en sectores de baja intensidad tecnológica, como la construcción y determinados servicios.

Estos elementos limitaron parcialmente los beneficios potenciales de la digitalización, aunque no impidieron una mejora progresiva de la eficiencia empresarial (Frey & Osborne, 2017).

2.3. La transformación del mercado de trabajo

La digitalización modificó profundamente la estructura ocupacional de la economía española. La automatización permitió sustituir numerosas tareas rutinarias, especialmente aquellas relacionadas con el procesamiento administrativo de información, mientras aumentaba la demanda de trabajadores altamente cualificados (Agrawal et al., 2018)..

Este fenómeno responde al denominado *Skill-Biased Technological Change* (SBTC), según el cual el progreso tecnológico incrementa la productividad relativa del trabajo cualificado frente al trabajo menos especializado. Como consecuencia, aumenta la demanda de profesionales con competencias digitales, analíticas

y de gestión, mientras disminuye la importancia de ocupaciones fácilmente automatizables(Comisión Europea, 2020).

En España este proceso coincidió con una fuerte expansión del sistema universitario y con un notable incremento del número de titulados superiores. Sin embargo, la adaptación del mercado laboral fue desigual. Mientras determinados sectores tecnológicos registraban una creciente escasez de profesionales cualificados, otras actividades experimentaban procesos de sustitución tecnológica y destrucción de empleo administrativo (Frey & Osborne, 2017).

La aparición de nuevas profesiones relacionadas con la informática, las telecomunicaciones, el desarrollo de software o la consultoría tecnológica constituye uno de los principales efectos positivos de la digitalización. Paralelamente, la creciente utilización de herramientas digitales transformó ocupaciones tradicionales en prácticamente todos los sectores económicos (Agrawal et al., 2018).

2.4. Competitividad empresarial y apertura internacional

La digitalización también modificó la capacidad competitiva de las empresas españolas. Internet redujo significativamente las barreras geográficas, facilitando el acceso a clientes internacionales y favoreciendo la internacionalización de numerosas pequeñas y medianas empresas.

La implantación de sistemas ERP (Enterprise Resource Planning), CRM (Customer Relationship Management) y plataformas de comercio electrónico permitió optimizar la gestión empresarial y reducir costes operativos. Asimismo, la utilización de tecnologías digitales facilitó la integración de las empresas españolas en cadenas globales de valor, incrementando su capacidad exportadora.

No obstante, los beneficios de la digitalización fueron muy heterogéneos. Las grandes empresas adoptaron rápidamente tecnologías avanzadas, mientras que numerosas pymes encon-

traron dificultades derivadas de limitaciones financieras, escasez de personal especializado y menores economías de escala (Frey & Osborne, 2017).

Esta denominada «brecha digital empresarial» constituye uno de los principales desafíos identificados por la Comisión Europea y la OCDE durante los primeros años del siglo XXI (Comisión Europea, 2020).

2.5. El sector público y la administración electrónica

La digitalización también produjo importantes transformaciones en el funcionamiento del sector público español. Durante la década de 1990 comenzaron a desarrollarse los primeros proyectos de administración electrónica, orientados inicialmente a informatizar procedimientos internos y mejorar la gestión administrativa.

Posteriormente, la generalización de Internet permitió ofrecer numerosos servicios públicos mediante plataformas electrónicas. La presentación telemática de declaraciones tributarias, la obtención de certificados administrativos y el desarrollo de registros electrónicos redujeron significativamente los costes administrativos tanto para las administraciones públicas como para ciudadanos y empresas (Acemoglu & Restrepo, 2018).

Desde una perspectiva económica, la administración electrónica generó importantes ganancias de eficiencia al disminuir los costes de transacción asociados a la prestación de servicios públicos. La reducción del tiempo necesario para realizar trámites administrativos permitió aumentar la productividad del sector público y mejorar la calidad percibida por los usuarios.

La Agencia Estatal de Administración Tributaria constituye probablemente el ejemplo más representativo de este proceso. La progresiva digitalización de la gestión tributaria facilitó el cumplimiento voluntario de las obligaciones fiscales, mejoró la capacidad de control de la Administración y redujo los costes administrativos del sistema tributario.

Estos avances anticiparon muchas de las aplicaciones actuales de la inteligencia artificial en el ámbito público, especialmente en materia de análisis masivo de datos, detección de fraude y automatización de procedimientos administrativos.

2.6. La brecha digital como limitación al crecimiento

Pese a los importantes avances registrados entre 1980 y 2010, el proceso de digitalización presentó importantes desigualdades territoriales y sociales. Las diferencias de renta, edad, nivel educativo y tamaño empresarial condicionaron significativamente el acceso a las nuevas tecnologías. Las grandes áreas urbanas concentraron la mayor parte de las inversiones digitales, mientras que numerosas zonas rurales experimentaban mayores dificultades para acceder a infraestructuras de banda ancha (Agrawal et al., 2018).

Del mismo modo, la digitalización avanzó con mayor rapidez en determinados sectores intensivos en conocimiento que en actividades tradicionales como la agricultura, determinadas industrias manufactureras o los servicios personales. Estas diferencias contribuyeron a ampliar las desigualdades de productividad entre empresas y territorios, configurando una brecha digital cuyos efectos siguen siendo visibles en la actualidad (Frey & Osborne, 2017).

3. LA INCIDENCIA DE LA DIGITALIZACIÓN EN EL DERECHO

La digitalización no solo ha transformado los procesos productivos y la organización económica, sino que también ha supuesto una profunda modificación del ordenamiento jurídico. A diferencia de anteriores revoluciones tecnológicas, cuya incidencia sobre el Derecho se produjo de manera gradual, la expansión de las tecnologías de la información y las comunicaciones (TIC) ha obligado al legislador a responder con rapidez

ante fenómenos completamente novedosos: el comercio electrónico, la contratación a distancia, la identidad digital, la protección de datos personales, la ciberdelincuencia o la utilización de procedimientos administrativos electrónicos.

Desde una perspectiva institucional, el Derecho cumple una doble función en los procesos de innovación tecnológica. Por una parte, proporciona seguridad jurídica a los agentes económicos, facilitando la inversión y el desarrollo de nuevos mercados. Por otra, establece límites destinados a proteger intereses públicos y derechos fundamentales potencialmente afectados por el uso de las nuevas tecnologías. Como señalan autores vinculados al análisis económico del Derecho, el diseño de las normas debe minimizar los costes de transacción y reducir la incertidumbre sin imponer cargas regulatorias desproporcionadas que puedan obstaculizar la innovación (Agrawal et al., 2018).

La experiencia española entre 1980 y 2010 refleja claramente esta evolución. Durante los primeros años de la digitalización, la regulación jurídica tenía un carácter principalmente reactivo, orientado a adaptar instituciones tradicionales a un entorno tecnológico emergente. Sin embargo, conforme la economía digital fue adquiriendo mayor relevancia, el legislador comenzó a desarrollar un marco normativo específico destinado a regular fenómenos propios de la sociedad de la información. Este proceso culminó con la consolidación de la administración electrónica y con la configuración de un sistema jurídico preparado para afrontar, posteriormente, los retos derivados de la inteligencia artificial.

3.1. La adaptación del Derecho a la sociedad de la información

Los ordenamientos jurídicos occidentales fueron concebidos para regular relaciones desarrolladas en un entorno esencialmente físico. La contratación se realizaba mediante documentos en papel, la identificación de las partes requería su presencia

personal y las actuaciones administrativas descansaban sobre expedientes igualmente físicos. La digitalización alteró profundamente estas premisas (Katz & Shapiro, 1985).

La progresiva incorporación de Internet permitió que un número creciente de relaciones jurídicas se desarrollaran íntegramente por medios electrónicos. Empresas y consumidores comenzaron a celebrar contratos sin contacto presencial, las administraciones públicas ofrecieron servicios en línea y surgieron nuevas formas de intercambio económico basadas exclusivamente en plataformas digitales.

Este fenómeno planteó importantes interrogantes jurídicos. Resultaba necesario determinar cuándo un contrato electrónico debía considerarse válidamente perfeccionado, qué valor probatorio tenían los documentos digitales, cómo podía garantizarse la autenticidad de las comunicaciones electrónicas o qué legislación resultaba aplicable cuando las partes se encontraban en distintos países.

La respuesta del legislador consistió en adaptar los principios generales del Derecho privado y del Derecho administrativo a un entorno tecnológico radicalmente diferente. En lugar de sustituir completamente las instituciones existentes, se optó mayoritariamente por reinterpretarlas conforme al principio de equivalencia funcional, según el cual un documento electrónico puede producir los mismos efectos jurídicos que un documento en papel siempre que garantice idénticos niveles de autenticidad, integridad y conservación.

Este principio ha constituido uno de los pilares fundamentales sobre los que posteriormente se ha construido toda la regulación europea relativa a la transformación digital.

3.2. La contratación electrónica y la economía digital

Uno de los ámbitos donde la digitalización produjo mayores cambios fue el Derecho contractual. La expansión del comercio electrónico durante los años noventa obligó a redefinir numerosos conceptos tradicionales relacionados con la formación del

consentimiento, la información precontractual y la protección del consumidor (Comisión Europea, 2020).

Desde el punto de vista económico, la contratación electrónica redujo significativamente los costes de transacción. Las empresas pudieron ofrecer productos y servicios a escala internacional sin necesidad de disponer de establecimientos físicos, mientras que los consumidores obtuvieron acceso inmediato a una oferta mucho más amplia y competitiva (Comisión Europea, 2020).

Sin embargo, la disminución de los costes económicos vino acompañada de nuevas incertidumbres jurídicas. La contratación entre ausentes exigía garantizar que ambas partes conocieran adecuadamente las condiciones contractuales, que el consentimiento hubiera sido emitido libremente y que existieran mecanismos eficaces para resolver eventuales conflictos.

La legislación europea respondió mediante un conjunto de normas dirigidas a reforzar la transparencia, la información precontractual y los derechos de desistimiento de los consumidores. Este marco jurídico favoreció la expansión del comercio electrónico al incrementar la confianza de los agentes económicos en los nuevos canales digitales (Comisión Europea, 2020).

La confianza constituye precisamente uno de los activos institucionales más importantes para el funcionamiento de la economía digital (Comisión Europea, 2020). Desde la perspectiva del análisis económico del Derecho, una regulación clara y previsible reduce la incertidumbre jurídica, disminuye los costes derivados del incumplimiento contractual y favorece el desarrollo de mercados más eficientes (Agrawal et al., 2018).

3.3. La protección de datos personales: de la privacidad al activo económico

Pocas materias ilustran mejor la transformación jurídica provocada por la digitalización que la protección de los datos personales. Durante buena parte del siglo XX la información personal tenía un alcance relativamente limitado debido al elevado

coste de almacenamiento y tratamiento de los datos. La digitalización modificó completamente esta situación. Empresas y administraciones públicas comenzaron a recopilar cantidades crecientes de información relativa a ciudadanos y consumidores, convirtiendo los datos en uno de los principales activos de la economía digital.

Esta nueva realidad obligó a redefinir el concepto jurídico de privacidad. La protección de datos dejó de entenderse únicamente como una manifestación del derecho a la intimidad para convertirse en un instrumento destinado a garantizar el control efectivo que los individuos ejercen sobre la utilización de su información personal.

Desde una perspectiva económica, los datos presentan características singulares. Constituyen un bien no rival —su utilización por un agente no impide el uso simultáneo por otros— y generan importantes economías de escala y de red. Cuanto mayor es el volumen de información disponible, mayor suele ser el valor económico derivado de su análisis (Acemoglu & Restrepo, 2018)..

Este fenómeno explica el extraordinario crecimiento de las plataformas digitales durante las primeras décadas del siglo XXI. Empresas tecnológicas de dimensión global construyeron modelos de negocio basados en la recopilación masiva de datos y en el desarrollo de algoritmos capaces de transformar dicha información en conocimiento económico (Agrawal et al., 2018).

No obstante, esta concentración de información también incrementó los riesgos asociados al uso indebido de los datos personales, haciendo necesaria una regulación cada vez más exigente en materia de consentimiento, transparencia, seguridad y responsabilidad.

La posterior aprobación del Reglamento General de Protección de Datos (RGPD) consolidó un modelo europeo basado en la protección reforzada de los derechos fundamentales frente al tratamiento automatizado de información personal, estableciendo además importantes obligaciones para las empresas que operan en mercados digitales.

3.4. La administración electrónica y la transformación del sector público

Uno de los cambios jurídicos más profundos derivados de la digitalización tuvo lugar en el ámbito de las administraciones públicas. La tradicional Administración burocrática, caracterizada por procedimientos presenciales y expedientes en soporte papel, fue progresivamente sustituida por modelos organizativos basados en la gestión electrónica de la información.

En España, este proceso culminó con la consolidación de la administración electrónica como principio general de actuación administrativa. La utilización de medios electrónicos dejó de ser una posibilidad excepcional para convertirse en la forma ordinaria de relación entre ciudadanos, empresas y poderes públicos. Desde una perspectiva económica, la administración electrónica permitió reducir considerablemente los costes administrativos. La automatización de numerosos procedimientos disminuyó el tiempo necesario para resolver expedientes, redujo el consumo de recursos materiales y facilitó una asignación más eficiente del personal público. Asimismo, la digitalización incrementó la transparencia institucional mediante la publicación electrónica de información administrativa, mejoró el acceso ciudadano a los servicios públicos y favoreció la interoperabilidad entre distintas administraciones.

No obstante, esta transformación también planteó nuevos problemas jurídicos. La automatización de determinadas actuaciones administrativas obligó a revisar cuestiones relacionadas con la motivación de las resoluciones, la identificación del órgano competente y la posibilidad de impugnar decisiones adoptadas mediante sistemas informáticos.

Estas cuestiones adquieren una importancia aún mayor cuando la automatización evoluciona hacia sistemas dotados de inteligencia artificial capaces de generar recomendaciones o incluso adoptar decisiones con un elevado grado de autonomía.

3.5. La digitalización como presupuesto jurídico de la inteligencia artificial

La regulación actual de la inteligencia artificial no surge en un vacío normativo. Muy al contrario, se apoya sobre un conjunto de instituciones jurídicas desarrolladas durante el proceso de digitalización.

Conceptos como la identidad electrónica, la protección de datos personales, la firma electrónica, la administración digital, la contratación electrónica o la responsabilidad derivada del tratamiento automatizado de información constituyen los cimientos sobre los que posteriormente se ha construido la regulación específica de la IA.

En este sentido, la digitalización puede entenderse como una fase preparatoria que permitió adaptar progresivamente el Derecho a un entorno tecnológico caracterizado por la creciente automatización de las relaciones económicas y administrativas. (Acemoglu & Restrepo, 2018).

La diferencia fundamental radica en que los primeros sistemas digitales ejecutaban instrucciones previamente definidas por el programador, mientras que los actuales modelos de inteligencia artificial poseen capacidad para aprender, inferir patrones y modificar dinámicamente su comportamiento a partir de grandes volúmenes de datos. Esta evolución cualitativa explica por qué muchas de las respuestas jurídicas desarrolladas durante la era digital resultan hoy insuficientes para afrontar los desafíos planteados por la toma de decisiones automatizadas.

4. EL IMPACTO ECONÓMICO DE LA INTELIGENCIA ARTIFICIAL

La inteligencia artificial (IA) representa la etapa más reciente de la transformación digital iniciada durante las últimas décadas del siglo xx. Mientras que la digitalización permitió automatizar procesos previamente definidos mediante reglas

programadas, la IA incorpora una dimensión cualitativamente distinta: la capacidad de aprender a partir de grandes volúmenes de datos, identificar patrones complejos y generar predicciones o decisiones sin necesidad de una programación exhaustiva para cada situación específica. Este avance convierte a la IA en una tecnología de propósito general (*General Purpose Technology*), comparable, por su potencial transformador, a la máquina de vapor, la electricidad o Internet (Agrawal et al., 2018).

Desde una perspectiva económica, la inteligencia artificial constituye uno de los principales motores potenciales del crecimiento durante las próximas décadas. Diversos organismos internacionales estiman que su adopción incrementará la productividad, reducirá los costes de producción, favorecerá la aparición de nuevos modelos de negocio y modificará profundamente la organización de empresas y administraciones públicas. No obstante, estos beneficios potenciales conviven con importantes desafíos relacionados con el empleo, la concentración empresarial, la competencia, la distribución de la renta y la gobernanza de los datos (Brynjolfsson, & Hitt, 2000).

A diferencia de revoluciones tecnológicas anteriores, la IA no se limita a sustituir trabajo físico o tareas rutinarias, sino que comienza a automatizar actividades cognitivas que tradicionalmente se consideraban exclusivas del capital humano altamente cualificado. Ello explica que sus efectos económicos alcancen sectores tan diversos como la sanidad, las finanzas, la educación, la logística, la investigación científica, la industria manufacturera o el asesoramiento jurídico (Agrawal et al., 2018).

4.1. La inteligencia artificial como tecnología de propósito general

La literatura económica define las tecnologías de propósito general como aquellas innovaciones que poseen tres características fundamentales: una amplia aplicabilidad sectorial, capaci-

dad para generar innovaciones complementarias y un impacto persistente sobre la productividad agregada. La máquina de vapor permitió mecanizar la producción industrial; la electricidad transformó prácticamente todos los sectores económicos; Internet revolucionó las comunicaciones y el comercio. La inteligencia artificial parece reunir igualmente estas características.

Su naturaleza transversal permite su incorporación a prácticamente cualquier actividad económica basada en el tratamiento de información. Desde algoritmos capaces de diagnosticar enfermedades hasta sistemas de optimización logística, asistentes virtuales o herramientas de análisis financiero, la IA actúa como una infraestructura tecnológica sobre la que pueden desarrollarse innumerables aplicaciones específicas.

Esta versatilidad explica que numerosos autores consideren que la inteligencia artificial constituye el núcleo de una nueva revolución industrial caracterizada por la automatización inteligente de los procesos productivos (Frey & Osborne, 2017).

Desde el punto de vista macroeconómico, las tecnologías de propósito general presentan una característica común: sus efectos sobre la productividad no son inmediatos. Al igual que ocurrió con la electricidad o las tecnologías digitales, la obtención de ganancias significativas requiere inversiones complementarias en capital físico, capital humano, cambios organizativos e innovación institucional.

4.2. Productividad y crecimiento económico

El principal argumento económico a favor de la inteligencia artificial reside en su capacidad para aumentar la productividad de los factores de producción. La productividad puede mejorar mediante diversos mecanismos. En primer lugar, la automatización de tareas repetitivas reduce el tiempo necesario para realizar numerosas actividades administrativas, industriales y de servicios. En segundo lugar, los algoritmos permiten optimizar procesos complejos mediante el análisis simultáneo de millones de variables que exceden la capacidad de procesamiento

humano. Finalmente, la IA facilita una asignación más eficiente de recursos al mejorar la calidad de las predicciones y reducir la incertidumbre en la toma de decisiones.

En el ámbito empresarial, estas mejoras se traducen en reducciones significativas de costes operativos, menores tiempos de producción y una utilización más eficiente del capital disponible. Los sistemas predictivos permiten anticipar fallos en maquinaria industrial, optimizar inventarios, ajustar cadenas logísticas y personalizar estrategias comerciales con un grado de precisión anteriormente inalcanzable (Acemoglu & Johnson, 2023).

Desde una perspectiva macroeconómica, la adopción generalizada de estas tecnologías podría elevar el crecimiento potencial de las economías desarrolladas. Sin embargo, la magnitud de este efecto dependerá de la velocidad de difusión tecnológica, de la capacidad de adaptación empresarial y del marco institucional que acompañe el proceso de innovación. Al igual que sucedió durante la revolución digital, las ganancias de productividad no dependerán exclusivamente del desarrollo tecnológico, sino también de la capacidad de las organizaciones para rediseñar sus procesos internos y aprovechar las nuevas capacidades ofrecidas por la inteligencia artificial (Acemoglu & Restrepo, 2018).

4.3. Inteligencia artificial y mercado de trabajo

Uno de los debates más intensos en la literatura económica contemporánea gira en torno al impacto de la inteligencia artificial sobre el empleo (Agrawal et al., 2018).

Las primeras investigaciones sobre automatización, desarrolladas durante la pasada década, sostenían que una parte significativa de las ocupaciones existentes podía desaparecer como consecuencia del progreso tecnológico. Sin embargo, trabajos más recientes muestran un panorama considerablemente más complejo (Yeung, 2018).

La evidencia disponible indica que la inteligencia artificial no sustituye profesiones completas, sino tareas específicas den-

tro de cada ocupación. Este fenómeno modifica profundamente la composición del empleo, aumentando la demanda de determinadas competencias mientras reduce la importancia de otras. En términos generales pueden distinguirse tres grandes efectos. En primer lugar, numerosas tareas rutinarias, tanto manuales como cognitivas, presentan un elevado potencial de automatización. Actividades relacionadas con la introducción de datos, determinados procesos contables, la gestión documental o la atención básica al cliente pueden realizarse actualmente mediante sistemas inteligentes con elevados niveles de precisión. En segundo lugar, aumenta considerablemente la productividad de trabajadores altamente cualificados. Médicos, ingenieros, economistas, abogados o investigadores disponen ahora de herramientas capaces de procesar enormes cantidades de información en pocos segundos, permitiéndoles dedicar más tiempo a tareas de análisis, creatividad y supervisión. Finalmente, aparecen nuevas ocupaciones vinculadas al desarrollo, entrenamiento, auditoría y supervisión de algoritmos, así como profesiones especializadas en gobernanza de datos, ética de la inteligencia artificial y ciberseguridad.

Este proceso no implica necesariamente una reducción permanente del empleo agregado, pero sí exige importantes esfuerzos de adaptación educativa y formación continua para evitar desajustes entre oferta y demanda de cualificaciones.

4.4. Competencia, concentración empresarial y poder de mercado

Uno de los aspectos menos analizados por el debate público, aunque de enorme relevancia económica, es el efecto de la inteligencia artificial sobre la competencia.

El desarrollo de modelos avanzados de IA requiere enormes inversiones en infraestructuras computacionales, capacidad de almacenamiento y grandes bases de datos. Estas características generan importantes economías de escala que favorecen la concentración empresarial. Las empresas que disponen de mayores

cantidades de datos poseen ventajas competitivas difíciles de replicar por nuevos competidores. A su vez, el entrenamiento de modelos de gran tamaño exige inversiones que solo pueden afrontar compañías con importantes recursos financieros.

Como consecuencia, existe el riesgo de que la inteligencia artificial contribuya a reforzar posiciones dominantes en determinados mercados digitales, incrementando las barreras de entrada y reduciendo la competencia efectiva. Desde la perspectiva del análisis económico del Derecho, este fenómeno plantea importantes desafíos para las autoridades de competencia. Las herramientas tradicionales diseñadas para analizar mercados industriales pueden resultar insuficientes cuando el principal activo estratégico son los datos y los algoritmos.

En este contexto, la regulación adquiere una función esencial para preservar mercados competitivos sin desincentivar la innovación tecnológica.

4.5. Desigualdad y distribución de la renta

Los efectos distributivos de la inteligencia artificial constituyen uno de los principales focos de preocupación de la literatura económica reciente. Las ganancias de productividad derivadas de la automatización no se distribuyen necesariamente de manera homogénea entre trabajadores, empresas y consumidores. Aquellas empresas capaces de desarrollar o adquirir sistemas avanzados de IA pueden experimentar importantes incrementos de rentabilidad, mientras que otras organizaciones con menor capacidad financiera podrían quedar rezagadas tecnológicamente.

Asimismo, los trabajadores con mayores competencias digitales tienen más probabilidades de beneficiarse de las nuevas oportunidades laborales, mientras que aquellos cuyas tareas resulten fácilmente automatizables afrontan un mayor riesgo de desplazamiento ocupacional.

Este fenómeno puede contribuir a incrementar tanto la desigualdad salarial como las diferencias regionales de productividad (Porter & Heppelmann, 2014).

Por ello, numerosos organismos internacionales insisten en la necesidad de complementar las políticas de innovación con inversiones en educación, formación continua y reciclaje profesional que faciliten la adaptación del capital humano al nuevo entorno tecnológico (Acemoglu & Restrepo, 2018).

5. CONCLUSIONES

La transformación tecnológica experimentada durante las últimas décadas ha modificado profundamente el funcionamiento de las economías modernas y de los sistemas jurídicos que las regulan. La digitalización iniciada a finales del siglo XX constituyó el punto de partida de un proceso de cambio estructural que ha culminado, al menos provisionalmente, con el desarrollo de la inteligencia artificial. Lejos de tratarse de fenómenos independientes, ambos procesos forman parte de una misma evolución tecnológica cuyo denominador común ha sido la creciente automatización del tratamiento de la información y de la toma de decisiones.

El análisis realizado a lo largo de este trabajo pone de manifiesto que la digitalización desempeñó un papel decisivo en la modernización de la economía española entre 1980 y 2010. La incorporación progresiva de las tecnologías de la información y las comunicaciones permitió mejorar la productividad empresarial, facilitar la internacionalización de numerosas compañías, reducir los costes de transacción y favorecer el desarrollo de nuevos modelos de negocio basados en el intercambio digital de información. Asimismo, la implantación de la administración electrónica supuso un importante avance en términos de eficiencia institucional, transparencia y simplificación administrativa, sentando las bases tecnológicas sobre las que posteriormente se desarrollarían las aplicaciones actuales de inteligencia artificial.

Sin embargo, la digitalización también evidenció que el progreso tecnológico no genera automáticamente beneficios económicos homogéneos. La existencia de diferencias en capital

humano, capacidad innovadora, tamaño empresarial e infraestructuras digitales condicionó significativamente el aprovechamiento de las nuevas tecnologías. Las ganancias de productividad fueron mayores allí donde la inversión tecnológica vino acompañada de cambios organizativos, mejoras educativas y un marco institucional favorable a la innovación. Esta experiencia histórica resulta especialmente relevante para comprender los desafíos actuales de la inteligencia artificial.

La IA representa una nueva fase de esta transformación caracterizada por la automatización inteligente de actividades cognitivas. A diferencia de las tecnologías digitales convencionales, los sistemas de inteligencia artificial no solo ejecutan instrucciones previamente programadas, sino que son capaces de aprender, identificar patrones complejos y formular recomendaciones o decisiones basadas en grandes volúmenes de datos. Esta capacidad amplía extraordinariamente el potencial económico de la automatización y explica el creciente interés que despierta entre empresas, administraciones públicas y organismos internacionales.

Desde una perspectiva económica, la inteligencia artificial constituye una tecnología de propósito general con capacidad para incrementar la productividad de prácticamente todos los sectores productivos. La optimización de procesos, la mejora de la asignación de recursos, la reducción de costes administrativos y el impulso a la innovación sitúan a la IA entre los principales motores potenciales del crecimiento económico durante las próximas décadas. No obstante, la magnitud de estos beneficios dependerá en gran medida de la capacidad de las economías para adaptar sus instituciones, formar capital humano especializado y facilitar la difusión tecnológica entre empresas de distinto tamaño.

Paralelamente, la inteligencia artificial plantea importantes desafíos distributivos. La automatización de tareas cognitivas modifica la composición del empleo, incrementa la demanda de trabajadores altamente cualificados y obliga a replantear las políticas educativas y de formación continua. Asimismo, la elevada concentración de datos, capacidad computacional y recur-

Los financieros en un reducido número de grandes empresas tecnológicas puede reforzar posiciones dominantes y aumentar las barreras de entrada en numerosos mercados digitales. La política de competencia y la regulación económica adquieren, por tanto, una relevancia creciente para preservar mercados abiertos e innovadores.

La dimensión jurídica de la inteligencia artificial resulta igualmente trascendental. El análisis desarrollado muestra que las categorías tradicionales del Derecho fueron concebidas para regular actuaciones protagonizadas por personas físicas o jurídicas plenamente identificables. La utilización creciente de algoritmos capaces de influir o incluso adoptar decisiones con efectos jurídicos obliga a reinterpretar conceptos fundamentales como la responsabilidad, la motivación de los actos administrativos, la prueba, la transparencia o la protección de los derechos fundamentales.

Especial relevancia adquieren los problemas derivados de la opacidad algorítmica y de los sesgos incorporados durante el entrenamiento de los modelos de inteligencia artificial. La confianza de ciudadanos y operadores económicos en estas tecnologías dependerá de la existencia de mecanismos eficaces que garanticen la explicabilidad de las decisiones automatizadas, la posibilidad de supervisión humana y la disponibilidad de procedimientos efectivos de impugnación cuando se produzcan errores o discriminaciones. Desde la perspectiva del análisis económico del Derecho, estos mecanismos no constituyen únicamente garantías jurídicas, sino también instrumentos destinados a reducir la incertidumbre, disminuir los costes de transacción y fortalecer la seguridad jurídica de los mercados digitales.

La respuesta regulatoria adoptada por la Unión Europea constituye un intento de compatibilizar innovación y protección de los derechos fundamentales mediante un modelo basado en la evaluación del riesgo. Este enfoque ofrece importantes ventajas al proporcionar seguridad jurídica y criterios homogéneos para el desarrollo de sistemas de inteligencia artificial. Sin embargo, también plantea interrogantes sobre su posible impacto en la competitividad internacional de las empresas euro-

peas si las cargas regulatorias terminan situándolas en una posición de desventaja frente a competidores establecidos en jurisdicciones con marcos normativos menos exigentes. En este sentido, el éxito del modelo europeo dependerá de su capacidad para mantener un equilibrio entre protección e innovación, evitando tanto una regulación excesivamente restrictiva como una ausencia de control incompatible con los valores del Estado de Derecho.

Uno de los principales argumentos defendidos en este trabajo es que la inteligencia artificial no debe contemplarse exclusivamente como un problema tecnológico o jurídico, sino como un fenómeno eminentemente económico e institucional. Las decisiones automatizadas modifican la forma en que se asignan los recursos, se prestan los servicios públicos, se organiza la actividad empresarial y se ejercen los derechos de los ciudadanos. En consecuencia, su regulación exige un enfoque interdisciplinar que combine las aportaciones de la Economía, el Derecho, la Ciencia Política, la Ingeniería y la Ética. Ninguna de estas disciplinas, considerada de forma aislada, resulta suficiente para afrontar la complejidad de los desafíos planteados por la automatización inteligente.

Desde la perspectiva de las políticas públicas, los resultados del análisis permiten identificar varias líneas prioritarias de actuación. En primer lugar, resulta imprescindible reforzar la inversión en educación y formación digital con el fin de facilitar la adaptación del mercado de trabajo a las nuevas demandas tecnológicas. En segundo lugar, debe promoverse la innovación empresarial mediante incentivos que faciliten el acceso de las pequeñas y medianas empresas a herramientas de inteligencia artificial, evitando que la brecha tecnológica amplíe las diferencias de productividad existentes. En tercer lugar, las administraciones públicas deben desarrollar capacidades técnicas que les permitan utilizar la inteligencia artificial para mejorar la eficiencia institucional sin comprometer los principios de legalidad, imparcialidad, transparencia y rendición de cuentas. Finalmente, la cooperación internacional será esencial para afrontar desafíos que trascienden claramente las fronteras nacionales,

como la gobernanza de los datos, la competencia en mercados digitales o la armonización de estándares regulatorios.

En definitiva, la inteligencia artificial constituye una de las transformaciones económicas e institucionales más profundas desde el inicio de la revolución digital. Sus beneficios potenciales en términos de productividad, innovación y bienestar son extraordinarios, pero también lo son los riesgos asociados a una utilización inadecuada o insuficientemente regulada. La experiencia histórica demuestra que el progreso tecnológico genera prosperidad cuando se desarrolla en un entorno institucional capaz de combinar libertad económica, seguridad jurídica y protección efectiva de los derechos fundamentales. La inteligencia artificial no constituye una excepción a esta regla; por el contrario, exige reforzar el papel de las instituciones para garantizar que el extraordinario potencial de esta tecnología se traduzca en un crecimiento económico sostenible, una mejora de la eficiencia pública y una sociedad más próspera, competitiva e inclusiva.

6. BIBLIOGRAFÍA

- ACEMOGLU, D., & JOHNSON, S. (2023). *Power and Progress: Our Thousand-Year Struggle over Technology and Prosperity*. PublicAffairs.
- ACEMOGLU, D., & RESTREPO, P. (2018). Artificial intelligence, automation and work. En A. Agrawal, J. Gans & A. Goldfarb (Eds.), *The Economics of Artificial Intelligence* (pp. 197–236). University of Chicago Press.
- AGRAWAL, A., GANS, J., & GOLDFARB, A. (Eds.). (2018). *The Economics of Artificial Intelligence: An Agenda*. University of Chicago Press.
- BRYNJOLFSSON, E., & HITT, L. M. (2000). Beyond computation: Information technology, organizational transformation and business performance. *Journal of Economic Perspectives*, 14(4), 23–48.
- COASE, R. H. (1937). The nature of the firm. *Economica*, 4(16), 386–405.

- COMISIÓN EUROPEA. (2020). *Libro Blanco sobre la inteligencia artificial: Un enfoque europeo orientado a la excelencia y la confianza*. Oficina de Publicaciones de la Unión Europea.
- DAVID, P. A. (1990). The dynamo and the computer: An historical perspective on the modern productivity paradox. *American Economic Review*, 80(2), 355–361.
- FREY, C. B., & OSBORNE, M. A. (2017). The future of employment: How susceptible are jobs to computerisation? *Technological Forecasting and Social Change*, 114, 254–280.
- KATZ, M. L., & SHAPIRO, C. (1985). Network externalities, competition and compatibility. *American Economic Review*, 75(3), 424–440.
- OECD. (2019). *Artificial Intelligence in Society*. OECD Publishing.
- OECD. (2024). *OECD Digital Economy Outlook 2024*. OECD Publishing.
- PORTER, M. E., & HEPPELMANN, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review*, 92(11), 64–88.
- YEUNG, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523.

La inteligencia artificial ha dejado de ser una tecnología de futuro. Ya forma parte de la actividad de empresas, profesionales y administraciones públicas y está cambiando también la forma de entender y aplicar el Derecho. Este libro analiza algunos de los problemas jurídicos que acompañan a esa transformación, sin perder de vista las posibilidades que ofrecen estas nuevas herramientas.

A lo largo de sus cinco capítulos se estudia el uso de la inteligencia artificial en el ejercicio de las profesiones jurídicas, su incidencia en las relaciones laborales y en las nuevas formas de vigilancia de los trabajadores, la responsabilidad civil por los daños vinculados a sistemas inteligentes, su aplicación en los procedimientos de insolvencia y reestructuración de deudas y las consecuencias económicas de la toma automatizada de decisiones.

La obra combina el análisis de la regulación vigente con cuestiones que ya están surgiendo en la práctica: la fiabilidad de los sistemas de IA, la protección de datos, la supervisión humana, la atribución de responsabilidades o los límites que deben acompañar a su utilización. El propósito es ofrecer al lector una visión jurídica, crítica y cercana a la realidad de una tecnología que avanza con rapidez y que obliga al Derecho a dar respuesta a problemas hasta hace muy poco desconocidos.