
This is the **published version** of the bachelor thesis:

Fernández Morales, Marc. *El reparto de responsabilidades por daños derivados del uso de sistemas de inteligencia artificial en el comercio electrónico : la diligencia del administrador y la regulación del contrato con proveedores tecnológicos*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2026 (Dret). 47 pàg.

This version is available at <https://ddd.uab.cat/record/331915>

under the terms of the  license.

UAB

Universitat Autònoma de Barcelona

El reparto de responsabilidades por daños derivados del uso de sistemas de inteligencia artificial en el comercio electrónico: la diligencia del administrador y la regulación del contrato con proveedores tecnológicos

Autor: Marc Fernández Morales

Directora: Dra. Concepción Blázquez Giménez

Trabajo de Final de Grado

Área de Derecho Mercantil

Grado en Derecho

Curso 2025/2026

Índice

OBJETIVOS	4
RESUMEN.....	5
ABSTRACT	6
ABREVIATURAS	7
INTRODUCCIÓN	9
1. LA INTELIGENCIA ARTIFICIAL EN EL E-COMMERCE: DELIMITACIÓN CONCEPTUAL, USOS Y RIESGO	12
1.1. El Concepto de Inteligencia Artificial y su aplicación al <i>e-commerce</i>	12
1.2. Los Principales casos de uso de Inteligencia Artificial en tiendas online y <i>marketplaces</i>	13
1.3. El Mapa de actores	14
2. EL MARCO JURÍDICO APLICABLE A LA RESPONSABILIDAD POR IA EN E- COMMERCE: LA NORMATIVA DE LA UNIÓN EUROPEA PARA EL USO DE LA IA EN EL MERCADO DIGITAL Y SU TRANSPOSICIÓN A ESPAÑA.....	16
2.1. El marco general de la regulación de la IA en la Unión Europea y en los Organismos Internacionales.....	16
2.2. La regulación específica sobre la responsabilidad en caso de fallo o error de una Inteligencia Artificial	17
2.3. La transposición de la Directiva (UE) 2024/2853	20
3. LA DILIGENCIA DEL ADMINISTRADOR Y EL GOBIERNO DEL RIESGO POR IA: LA FIGURA DEL ADMINISTRADOR, SUS DEBERES Y EL ESTÁNDAR DE DILIGENCIA.....	23
3.1. La figura del administrador.....	23
3.2. Los deberes del administrador	24
3.3. El estándar de diligencia	25
4. MODELO DE GOBIERNO DEL RIESGO POR IA EN EL E-COMMERCE: LA DILIGENCIA DEL ADMINISTRADOR Y LA IMPLANTACIÓN DE CONTROLES INTERNOS A LOS SISTEMAS DE IA.....	26
4.1. Análisis y explicación de los posibles controles y su viabilidad	26
4.2. La evaluación de riesgos y la documentación mínima	28
4.3. La revisión humana, la monitorización y las métricas.....	29
4.4. El registro de decisiones, la auditoría y la gestión de incidentes	30
4.5. Las medidas frente a sesgos, los errores y el <i>drift</i> del modelo	32

5. EL MODELO DE GOBIERNO DEL RIESGO POR IA EN EL E-COMMERCE: EL REPARTO CONTRACTUAL DE RIESGOS CON PROVEEDORES TECNOLÓGICOS	35
5.1. La función del contrato como instrumento de gobierno del riesgo.....	35
5.2. La definición del objeto contratado y el nivel de servicio.....	35
5.3. La cooperación técnica y probatoria	36
5.4. La distribución de la responsabilidad y las indemnidades	37
5.5. La terminación, la reversibilidad y la continuidad del servicio	38
CONCLUSIONES.....	40

OBJETIVOS

1. Delimitar el concepto de inteligencia artificial a efectos jurídicos en el contexto del *e-commerce*, identificando los principales usos y sus riesgos asociados.
2. Identificar y clasificar los tipos de daños y escenarios de conflicto que puede generar la IA en el comercio electrónico
3. Examinar el marco normativo europeo aplicable hoy en día a la responsabilidad derivada del uso de IA en *e-commerce*
4. Determinar los criterios jurídicos de imputación de responsabilidad entre los distintos actores
5. Analizar el deber de diligencia del administrador y de los responsables de sector en la adopción, supervisión y gobierno de sistemas de IA, concretando qué medidas mínimas se les puede exigir
6. Estudiar el papel de la prueba y de la documentación técnica como elemento clave para acreditar diligencia y asignar responsabilidades.
7. Proponer un esquema de contratación y reparto de riesgos con proveedores tecnológicos que contemple cláusulas esenciales para la determinación de responsabilidades

RESUMEN

En el comercio electrónico contemporáneo, muchas decisiones que antes eran humanas se externalizan a sistemas de inteligencia artificial. Esta automatización incrementa la eficiencia, pero también genera riesgos jurídicos cuando el sistema produce daños o resultados ilícitos. En estos escenarios, la imputación de responsabilidad tiende a diluirse entre la empresa operadora que implanta el sistema y los proveedores tecnológicos que lo instalan

Este Trabajo de Fin de Grado analiza quién debe responder por los daños vinculados al uso de IA en *e-commerce* y cuál es el estándar exigible de diligencia del administrador en la selección, supervisión y gobierno de estos sistemas. Para ello, se examina el marco normativo europeo y español relevante junto con doctrina y manualística seleccionadas.

A fin de aclarar y regular esta situación que cada vez veremos con más frecuencia por la inevitable evolución de la IA, se propone un modelo práctico de reparto de riesgos con proveedores orientado a garantizar la reparación del daño y a ordenar las acciones de regreso entre los distintos actores.

Palabras clave: inteligencia artificial; comercio electrónico; responsabilidad por daños; diligencia del administrador; ciberseguridad; reparto de riesgos; proveedores tecnológicos.

ABSTRACT

In contemporary *e-commerce*, numerous decisions previously handled by humans are now outsourced to Artificial Intelligence systems. While this automation enhances efficiency, it also introduces significant legal risks when systems cause damages or produce unlawful outcomes. In such scenarios, the attribution of liability tends to become fragmented among the operating company, its board of directors, technology providers, and third-party intervenors.

This Final Degree Project analyzes who should be held liable for damages linked to the use of AI in *e-commerce* and defines the required standard of duty of care for directors regarding the selection, supervision, and governance of these systems. To this end, the study examines the relevant European and Spanish regulatory frameworks alongside selected legal doctrine and case law.

In order to clarify and regulate this increasingly frequent phenomenon driven by the inevitable evolution of AI, this paper proposes a practical risk-sharing model with providers. This model is designed to ensure victim compensation and to streamline recourse actions among the various stakeholders involved.

Keywords: Artificial intelligence; *e-commerce*; liability for damages; directors' duty of care; cybersecurity; risk allocation; technology providers.

ABREVIATURAS

AI Act	Reglamento (UE) 2024/1689 sobre Inteligencia Artificial
AILD	Artificial Intelligence Liability Directive (propuesta de Directiva sobre responsabilidad por IA, retirada)
Art./Arts.	Artículo / Artículos
BCCRT	British Columbia Civil Resolution Tribunal
Cit.	Citado/a (obra ya citada)
Coord./Coords.	Coordinador / Coordinadores
DOI	Digital Object Identifier / Identificador digital de objeto
DPD	Dynamic Parcel Distribution
<i>E-commerce</i>	Comercio electrónico
Ed.	Edición
IA	Inteligencia Artificial
LSC	Ley de Sociedades de Capital (Real Decreto Legislativo 1/2010)
N.º / Núm.	Número
P./Pp.	Página / Páginas
RGPD	Reglamento General de Protección de Datos
SaaS	<i>Software as a Service</i> / Software como servicio
SLA	<i>Service Level Agreement</i> / Acuerdo de nivel de servicio
TFG	Trabajo de Fin de Grado
TRLGDCU	Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios (Real Decreto Legislativo 1/2007)
UAB	Universitat Autònoma de Barcelona

UE	Unión Europea
UNESCO	United Nations Educational, Scientific and Cultural Organization / Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
Vol.	Volumen

INTRODUCCIÓN

El comercio electrónico se ha consolidado en los últimos años como uno de los principales espacios de contratación y prestación de servicios en todo el mundo, hasta el punto de absorber buena parte de la actividad comercial que tradicionalmente se desarrollaba de forma presencial. Este crecimiento ha venido acompañado de un fenómeno que es ya difícil de ignorar, pues hoy en día muchas decisiones que antes dependían de la intervención humana se externalizan a sistemas de inteligencia artificial. Automatizaciones como pueden ser recomendadores de productos, ajustes dinámicos de precio, *chatbots* de atención al cliente o sistemas automatizados de moderación de contenidos son ya elementos cotidianos en cualquier tienda en línea o *marketplace* de cierto tamaño. La automatización de estas decisiones ha incrementado notablemente la eficiencia operativa de las empresas y compañías, pero ha introducido al mismo tiempo nuevos riesgos jurídicos cuyas consecuencias empiezan a ser visibles, especialmente cuando un sistema produce un daño por ofrecer una información incorrecta o adopta una decisión injustificada frente al consumidor.

La cuestión que plantea este fenómeno no es un simple problema tecnológico, sino un dilema jurídico sobre a quién imputar la responsabilidad. Cuando un daño deriva de una decisión automatizada por inteligencia artificial, la atribución de responsabilidad resulta especialmente compleja por tres razones fundamentales. La primera tiene que ver con la fragmentación del ecosistema, ya que la empresa que vende en línea raramente desarrolla por sí misma los sistemas que utiliza, sino que los integra a partir de servicios prestados por terceros, lo que dificulta identificar quién controlaba efectivamente el riesgo en el momento del incidente. La segunda razón tiene que ver con el plano probatorio, pues, en caso de ausencia de una trazabilidad, unos registros y unos deberes de cooperación, reconstruir lo ocurrido y determinar las causas del error se convierte en una tarea casi imposible tanto para el perjudicado como para el propio operador del *e-commerce*. La tercera razón es esencialmente normativa, ya que el marco europeo de responsabilidad por inteligencia artificial se encuentra hoy incompleto; tras la retirada formal por parte de organismos de la Unión Europea de ciertas normativas que se hablarán a lo largo de este trabajo, el régimen normativo que regulaba la responsabilidad de estos sistemas se ha ido diluyendo a lo largo del tiempo.

Partiendo de esta problemática, el presente Trabajo de Fin de Grado se centra en determinar quién debe responder por los daños derivados del uso de la inteligencia artificial en el comercio electrónico y bajo qué condiciones, articulando el análisis en torno a tres ejes principales. El primero es la diligencia que resulta exigible al órgano de administración de la sociedad operadora o al departamento responsable de la contratación del servicio en su decisión de implantar, supervisar y mantener sistemas automatizados en su comercio en línea. El segundo es el reparto contractual del riesgo entre dicha sociedad y los proveedores tecnológicos que suministran, configuran y actualizan estos sistemas. El tercero, está integrado dentro de los dos anteriores, se trata del problema probatorio, esto es, el papel que la trazabilidad y la documentación técnica desempeñan tanto para acreditar la diligencia desplegada como para asignar responsabilidades cuando el daño llega a producirse.

La tesis que se defiende a lo largo del trabajo es que no existe una respuesta definitiva a esta cuestión, pues no la podemos encontrar en un único sujeto ni en una única norma, sino que el camino a seguir es la combinación coherente de una diligencia del administrador o responsable adaptada a las particularidades de la inteligencia artificial y de un reparto contractual realista entre los distintos actores que intervienen en la relación, sostenido todo ello sobre un soporte probatorio mínimo que permita reconstruir los hechos y delimitar las responsabilidades. La diligencia hacia adentro de la sociedad y la disciplina contractual hacia afuera funcionan como dos planos complementarios del mismo gobierno del riesgo.

El trabajo se estructura en seis capítulos. El primero delimita conceptualmente la inteligencia artificial en el contexto del *e-commerce*, identifica sus principales casos de uso y describe el mapa de actores que intervienen en las decisiones automatizadas. El segundo examina el marco normativo europeo aplicable a la responsabilidad por daños derivados de sistemas de inteligencia artificial, prestando especial atención a las novedades introducidas por la Directiva (UE) 2024/2853 y al Reglamento (UE) 2024/1689, así como a las consecuencias de la retirada de ciertas propuestas. El tercero analiza la relación de ese marco con la normativa española aplicable y la transposición de la Directiva (UE) 2024/2853. El cuarto aborda la figura del administrador societario, sus deberes y el estándar de diligencia exigible conforme a los artículos 225 y 226 de la Ley de Sociedades de Capital, figura que podría compararse al responsable del sector encargado de la contratación del sistema automatizado. Los capítulos quinto y sexto, que constituyen el núcleo aplicado del trabajo, proponen un

modelo de gobierno del riesgo articulado en los dos planos comentados; hacia adentro de la sociedad,

La metodología empleada es jurídica y doctrinal, con una orientación práctica. Se ha partido del estudio de la manualística, la doctrina y la legislación vigente en materia de responsabilidad civil, Derecho de sociedades y regulación específica de la inteligencia artificial. La jurisprudencia española y europea sobre fallos de sistemas de inteligencia artificial es todavía escasa, lo que ha obligado a recurrir, por una parte, a resoluciones análogas en otros ámbitos del Derecho de daños y, por otra, a casos relevantes resueltos en jurisdicciones extranjeras que ilustran con claridad los problemas de imputación que el trabajo aborda. Este análisis jurídico se ha complementado con la explicación de los conceptos tecnológicos imprescindibles para comprender el funcionamiento de los sistemas estudiados y con el examen de supuestos habituales en los que la inteligencia artificial falla en el comercio electrónico, identificando así los principales puntos de fricción jurídica. Sobre esta base, el trabajo propone unos criterios operativos para actuar con diligencia y un esquema de cláusulas contractuales jurídicamente defendible y realista, prestando especial atención a los elementos probatorios que permiten acreditar qué medidas se adoptaron y cómo funcionaba el sistema en el momento del incidente.

1. LA INTELIGENCIA ARTIFICIAL EN EL E-COMMERCE: DELIMITACIÓN CONCEPTUAL, USOS Y RIESGO

1.1. El Concepto de Inteligencia Artificial y su aplicación al *e-commerce*

El crecimiento de la inteligencia artificial durante los últimos cinco años ha sido totalmente exponencial; ha pasado de ser un sector de nicho experimental a que la mayoría de la población la utilice prácticamente a diario. Es una herramienta ampliamente extendida, pero conviene precisar qué se entiende por inteligencia artificial.

Se podría definir como un campo de la informática con el objetivo de desarrollar sistemas que sean capaces de llevar a cabo tareas que normalmente necesitarían discernimiento humano. Esto abarca un amplio abanico de capacidades, entre las que se encuentran el aprendizaje, el razonamiento, la comprensión e incluso la creación de arte. El objetivo de la IA es dotar a las máquinas de una “inteligencia”, permitiendo así la ejecución de actividades complejas de forma independiente. A diferencia de los programas tradicionales de informática, que siguen unas instrucciones fijas para realizar una tarea, la IA se basa en algoritmos que permiten a las máquinas entrenar con experiencias o datos y aprender a través de la prueba y el error, adaptándose a nuevas situaciones y realizando tareas de forma flexible y autónoma.¹

Desarrollada esta definición, es necesario discernir entre el concepto general de IA ya explicado y lo que es un agente de IA, que es lo que se emplea en el campo del *e-commerce*.

Un agente es cualquier cosa que sea capaz de percibir su entorno a través de sensores y actuar en este entorno a través de actuadores. Para entenderlo, un “agente humano” tiene ojos, oídos y órganos que actúan como sensores; y manos, piernas y voz que actúan como actuadores. Siguiendo la misma línea, un agente de software recibe paquetes de red, contenido de archivos, entradas humanas (teclado, ratón, pantalla táctil...) y actúa sobre este entorno enviando los paquetes de red, escribiendo los archivos y mostrando información o generando sonidos.²

Por lo tanto, la distinción radica en que la IA tradicional es reactiva, esperando a que el usuario le pida algo a través de un *prompt* (“el *prompt* es una instrucción, pregunta o información que se da a un sistema de IA para que genere una respuesta o complete una tarea”)³ para actuar y realizar su tarea, respondiendo solo a comandos directos; en cambio, el agente de IA tiene acceso a herramientas y memoria para planificar y ejecutar tareas por

¹ SUAVE, André Augusto, *Inteligência Artificial*, 1ª ed., Freitas Bastos, 2024, p. 8, consultado en ProQuest Ebook Central (UAB).

² RUSSELL, Stuart y NORVIG, Peter, *Artificial Intelligence: A Modern Approach, Global Edition*, 4ª ed., Pearson Education, Limited, 2021, p. 54.

³ GONZÁLEZ AROCHA, Jorge, “Fenomenología crítica del prompting en la inteligencia artificial”, *Sophia. Colección de Filosofía de la Educación*, núm. 39, 2025, pp. 141-165, p. 142 (pág. 3 del PDF), DOI: 10.17163/soph.n39.2025.04.

sí mismo hasta alcanzar una meta, trabajando por su cuenta en segundo plano tras recibir un input.

1.2. Los Principales casos de uso de Inteligencia Artificial en tiendas online y marketplaces

Como ya se ha explicado, el verdadero poder de la inteligencia artificial reside en los agentes de IA, que tienen cierta autonomía para cumplir el propósito por el que han sido creados. En el campo del *e-commerce* son comunes ciertos agentes específicos que ayudan a optimizar al máximo estas plataformas en línea, entre estos agentes encontramos: *chatbots*, recomendadores de productos o *repricing* automático.

Un *chatbot* es un programa de software de diálogo capaz de interactuar con los usuarios y procesar sus entradas en lenguaje natural. Entre los usos de los *chatbots* se incluyen la entrega de información por demanda y la respuesta a preguntas frecuentes formuladas por los consumidores.⁴ Entre los agentes de IA, se trata de uno de los más sencillos y básicos, pero también de los más utilizados. Cada vez más compañías y plataformas web incorporan un botón desplegable que, al pulsarlo, despliega un *chatbot*. Su carácter básico radica en que, en esencia, opera como un modelo de lenguaje de propósito general, como puede ser Claude, chat gpt o Gemini, adaptado a la empresa o plataforma digital que lo utiliza, al que el usuario formula sus dudas y que responde con la información con la que ha sido programado. Es decir, se interactúa con un modelo de lenguaje al que se ha entrenado previamente para que asimile la información de la empresa en cuestión.

En cuanto a los recomendadores de productos, son utilizados por numerosas empresas en el ámbito del *e-commerce*, con el objetivo de proporcionar una recomendación lo más acertada posible de los productos ofrecidos y una personalización de la oferta, basándose en las opiniones, gustos, frecuencia de compras y transacciones previas realizadas por el usuario.⁵ Este nivel de personalización, que antes solo era realizable manualmente por vendedores muy experimentados que conocían bien a sus clientes, ahora es posible conseguirlo de forma automatizada para todas las empresas, gracias a algoritmos que cruzan centenas de variables por cliente.⁶

El concepto de precio dinámico puede entenderse como una estrategia de fijación de precios basada en ajustar de manera flexible los precios de los productos o servicios de una

⁴ HUANG, Weijiao; HEW, Khe Foon y FRYER, Luke K., “Chatbots for language learning—Are they really useful? A systematic review of chatbot-supported language learning”, *Journal of Computer Assisted Learning*, vol. 38, n.º 1, 2022, pp. 1–21, p. 1, DOI: 10.1111/jcal.12610.

⁵ BUITRAGO-RODRÍGUEZ, Mariana del Valle, “El comercio electrónico y la inteligencia artificial”, *Revista Gestión y Desarrollo Libre*, año 8, n.º 16, 2023, pp. 1–13, p. 5, DOI: 10.18041/2539-3669/gestionlibre.16.2023.10490.

⁶ TROYA TERRANOVA, Tayron Cesar, “Aplicación de la Inteligencia Artificial en la Dirección de Ventas para la Predicción del Comportamiento del Cliente: Revisión Bibliográfica (2020–2025)”, *Sinergia Académica*, vol. 8, n.º 7, 2025, pp. 694–708, p. 700.

plataforma en línea en respuesta a las condiciones cambiantes del mercado.⁷ Estas condiciones cambiantes pueden sintetizarse en cuatro factores clave: las personas, es decir, los consumidores individuales; las configuraciones de los productos; los periodos y el tiempo; y los lugares y ubicaciones. Dicho de otra forma, los precios dinámicos ajustan el coste de cada producto para adaptarse a las variaciones de la demanda en función de los cuatro elementos explicados.⁸ Cabe destacar que los precios dinámicos pueden tener un impacto negativo o positivo desde la perspectiva del consumidor, dependiendo de la calidad de los procesos de comunicación entre la empresa y el cliente. No obstante, cuando se aplica de la manera correcta, suele conducir a una situación beneficiosa para todas las partes, en la que tanto las empresas como los consumidores salen más beneficiados en comparación con la estrategia de ofrecer un precio estático óptimo.⁹

1.3. El Mapa de actores

El presente mapa de actores se trata de una enumeración de las partes que intervienen en las decisiones automatizadas dentro del comercio electrónico. En el *e-commerce*, la decisión que impacta en el consumidor o en terceros no suele depender siempre de un único sujeto, sino que es el resultado de una cadena técnica y organizativa donde participan diferentes partes como pueden ser los responsables de la empresa o plataforma en línea, los diversos proveedores y, en ocasiones, una plataforma intermediaria. Indicar correctamente las partes que intervienen en el proceso es de extrema importancia, pues la imputación de responsabilidad se relaciona directamente con la persona que configura, ejecuta, supervisa y puede corregir la decisión automatizada.

En primer lugar, el operador del *e-commerce* (*merchant*), titular de la tienda online o canal de venta, que decide la incorporación de herramientas, define el flujo de compra y las políticas comerciales (devoluciones, atención al cliente, descuentos) y mantiene la relación directa con el consumidor. Básicamente, es el empresario que tiene

En segundo lugar, se sitúan los proveedores tecnológicos (SaaS/IA), que suministran las herramientas concretas ya explicadas (recomendadores de productos, *chatbots*, precios dinámicos...), realizan actualizaciones y prestan soporte. En el ámbito del comercio electrónico, los proveedores tecnológicos suelen operar bajo el modelo SaaS (*Software as a Service*), que es el más relevante a efectos de este trabajo.¹⁰ Cabe definir el modelo SaaS

⁷ NOWAK, Marcin y PAWLOWSKA-NOWAK, Marta, “Dynamic Pricing Method in the E-Commerce Industry Using Machine Learning”, *Applied Sciences*, vol. 14, 2024, art. 11668, p. 2, DOI: 10.3390/app142411668.

⁸ KOPALLE, Praveen K.; PAUWELS, Koen; AKELLA, Laxminarayana Yashaswy y GANGWAR, Manish, “Dynamic pricing: Definition, implications for managers, and future research directions”, *Journal of Retailing*, vol. 99, 2023, pp. 580–593, p. 581.

⁹ NOWAK, Marcin y PAWLOWSKA-NOWAK, Marta, “Dynamic Pricing Method...”, cit., p. 2.

¹⁰ CORONADO GARCÍA, Beatriz, *Implantación de aplicaciones web en entornos internet, intranet y extranet. MF0493*, 1.ª ed., Editorial Tutor Formación, Logroño, 2024, p. 61.

como aquel en el que las aplicaciones se ejecutan en la nube y los usuarios acceden a ellas a través de Internet. Este modelo ofrece actualizaciones automáticas, escalabilidad y facilidad de acceso desde cualquier lugar, pero depende de la conectividad a Internet y puede implicar costes recurrentes. Ejemplos conocidos de SaaS son Google Workspace, Microsoft 365 o Salesforce.¹¹ En esencia, el proveedor tecnológico es quien instala la automatización en el negocio que le ha contratado.

En tercer lugar, en algunos casos específicos cuando la venta se canaliza a través de una plataforma, puede intervenir un *Marketplace*, que puede condicionar el resultado mediante reglas de publicación, posicionamiento, moderación de contenidos, asignación de visibilidad o gestión de disputas. Un *Marketplace* es un sitio donde vendedores ofrecen sus productos a compradores, en una relación comercial virtual que equivale a los mercados tradicionales en el mundo físico. En este tipo de plataformas existen canales ya tipificados donde los vendedores pueden ofrecer su producto de una determinada manera y en el que los usuarios pueden igualmente realizar búsquedas o comparaciones, de una forma sencilla, estructurada y rutinaria.¹² El modelo de *Marketplace* ha ido subiendo en popularidad los últimos años, esto se debe a que tiene diferentes ventajas. Por ejemplo, la mejora en la capacidad instalada, pues no ofrece servicios ni productos, sino que comercializa los existentes, esto hace que en muchos casos no se deba invertir en infraestructura. En cualquier caso, el dueño de la plataforma suele ganar por comisión realizada en esta; es decir, que obtiene un beneficio. Este aspecto resultará relevante a la hora de determinar responsabilidades.¹³ Algunos ejemplos actuales de *Marketplace* son Amazon, Aliexpress o Temu, plataformas que dominan gran parte del comercio electrónico actual.

Junto a ellos, pueden intervenir proveedores de infraestructura en la nube (*cloud/hosting* y servicios asociados), que condicionan la disponibilidad, rendimiento y una parte de la seguridad técnica del servicio. Su uso aporta escalabilidad, ajustando recursos en picos de demanda; también aporta coste variable, por el pago por uso; y mantenimiento básico a cargo del proveedor; sin embargo, también tiene algunos puntos negativos, por ejemplo, introduce dependencia de la conexión y del propio proveedor y genera posibles costes acumulados a largo plazo y menor control sobre la infraestructura subyacente, lo que puede resultar relevante cuando un incidente como una caída o un fallo de seguridad o de latencia afecta al funcionamiento del sistema de IA o a la prestación del servicio en el *e-commerce*.¹⁴

¹¹ CORONADO GARCÍA, Beatriz, *Despliegue y puesta en funcionamiento de componentes software. UF1291*, 1.ª ed., Editorial Tutor Formación, La Rioja, 2025, p. 31.

¹² HERNÁNDEZ RAMOS, Eva María, *Manual del comercio electrónico: técnicas, modelos, normativa y casos prácticos*, Marge Books, Barcelona, 2018, p. 127.

¹³ ROJAS GARCÍA, José Antonio y MOORE TORRES, Rosa Karol, *Emprendimiento digital: herramientas y metodologías aplicadas para pymes*, 1.ª ed., Universidad Peruana de Ciencias Aplicadas (UPC), Lima, 2024, p. 168.

¹⁴ CORONADO GARCÍA, Beatriz, *Implantación de aplicaciones web en entornos internet, intranet y extranet. MF0493*, 1.ª ed., Logroño, Editorial Tutor Formación, 2024.

2. EL MARCO JURÍDICO APLICABLE A LA RESPONSABILIDAD POR IA EN *E-COMMERCE*: LA NORMATIVA DE LA UNIÓN EUROPEA PARA EL USO DE LA IA EN EL MERCADO DIGITAL Y SU TRANSPOSICIÓN A ESPAÑA

Este capítulo aborda en un mismo bloque el marco europeo aplicable a la responsabilidad por daños derivados del uso de inteligencia artificial y su proyección sobre el Derecho español. La unidad de tratamiento responde al hecho de que el régimen europeo —integrado, esencialmente, por el Reglamento (UE) 2024/1689 y la Directiva (UE) 2024/2853— opera por armonización directa el primero y por transposición nacional el segundo, de modo que su análisis conjunto permite ofrecer una imagen completa del marco vigente sin desdoblarse artificialmente la exposición. El capítulo se estructura en tres epígrafes principales: el marco general europeo e internacional, la regulación específica de la responsabilidad por fallo o error de la inteligencia artificial y la transposición al ordenamiento español de la Directiva (UE) 2024/2853.

2.1. El marco general de la regulación de la IA en la Unión Europea y en los Organismos Internacionales

La necesidad de enfrentar los retos normativos de la inteligencia artificial es cada vez más urgente, sobre todo si tenemos en cuenta todos los avances que se han ido consiguiendo en los últimos años, como el de la computación cuántica, que permite tratar los datos de entrada (*input*) de forma exponencial y sin un límite aparente.¹⁵

En esa misma línea, las Recomendaciones que sugiere la UNESCO respecto a la Ética de la Inteligencia Artificial, se presentan como una aproximación mundial al fenómeno, ya que acepta la incorporación de estas tecnologías en las políticas públicas de los Estados y sugiere la adopción de medidas legislativas reguladoras destinadas a evitar sus repercusiones negativas sobre derechos y libertades.¹⁶

De la misma forma, la Comisión Europea, bajo la presidencia de Ursula von der Leyen, anunció en sus primeros cien días de mandato un paquete legislativo destinado a abordar las implicaciones éticas y humanas de la IA, incluyendo una regulación específica sobre la materia.¹⁷

Los principios y valores europeos y de la UNESCO se sintetizan en la idea de que la inteligencia artificial debe quedar subordinada al ser humano, y no a la inversa, haciendo mucho hincapié en las personas y sus derechos fundamentales. En particular, el respeto de la dignidad humana, de los ecosistemas y de la diversidad e inclusión se sitúan como base

¹⁵ FARÍÑAS DULCE, María José; OLIVA MARTÍNEZ, José Daniel y PÉREZ MACÍAS, Iván Antonio, *Los retos normativos de la inteligencia artificial*, 1.ª ed., Dykinson, Madrid, 2024, p. 158.

¹⁶ RIVERO ORTEGA, Ricardo, *Derecho e inteligencia artificial*, 1.ª ed., Ediciones Olejnik, Argentina, 2023, p. 48.

¹⁷ OJEDA TACORONTE, Carlos José (coord.), *Una mirada jurídica poliédrica a la normativa europea sobre inteligencia artificial*, 1.ª ed., Dykinson, Madrid, 2025, p. 373.

para orientar la regulación de la IA. Este énfasis de las instituciones en garantizar los derechos fundamentales es la reacción a una preocupación clara por los posibles usos indebidos, confusiones y riesgos que pueden llegar a generar los algoritmos y la inteligencia artificial.¹⁸

Aun después de tanto debate y discusión sobre la regulación a aplicar, no fue hasta el 21 de abril de 2021 que la Comisión Europea presentó su Propuesta de reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial y se modifican determinados actos legislativos de la Unión; la llamada “Propuesta de Ley de IA”.¹⁹

El Reglamento (UE) 2024/1689, conocido como Ley de IA, supone un hito legislativo en la regulación de la inteligencia artificial ética, transparente y confiable, y resulta especialmente relevante para los operadores del comercio electrónico. En particular, cuando los sistemas utilizados en el *e-commerce* se califican como de alto riesgo, sus proveedores y, en su caso, los proveedores tecnológicos, asumen obligaciones concretas como el establecimiento de un sistema de gestión de riesgos, la trazabilidad mediante registros (*logs*) que permitan reconstruir lo ocurrido, la supervisión humana efectiva, la transparencia frente al usuario y la notificación a las autoridades competentes de los incidentes graves. Estas obligaciones son las que, en el plano interno, conectan directamente con la diligencia exigible al administrador y, en el plano externo, con el reparto contractual del riesgo, análisis que se desarrollará en los capítulos posteriores.²⁰

El camino para la adopción de la Ley de IA puede entenderse como un proceso en dos fases. Tras una fase técnica preparatoria que consolidó un enfoque basado en el riesgo, en la que las exigencias se intensifican cuanto mayores son los efectos potenciales del sistema. Posteriormente, se abrió la fase legislativa que culminó con la aprobación del Reglamento por el Parlamento Europeo el 13 de marzo de 2024 y por el Consejo el 21 de mayo de 2024.²¹

2.2. La regulación específica sobre la responsabilidad en caso de fallo o error de una Inteligencia Artificial

En la Unión Europea, la responsabilidad por daños vinculados a sistemas de IA se había abordado, hasta su retirada formal por la Comisión Europea en octubre de 2025, mediante la propuesta de Directiva sobre responsabilidad por IA (AILD), que se examina a continuación a título de antecedente, pues, pese a no haberse aprobado, ofrece una imagen muy útil del

¹⁸ RIVERO ORTEGA, Ricardo, *Derecho e inteligencia artificial...*, cit., p. 48.

¹⁹ FARÍÑAS DULCE, María José; OLIVA MARTÍNEZ, José Daniel y PÉREZ MACÍAS, Iván Antonio, *Los retos normativos de la inteligencia artificial...*, cit., p. 158-180

²⁰ LÓPEZ-AMO SAINZ, Ángel Pablo, *La Ley de la Inteligencia Artificial. Parte I*, 1.^a ed., RA-MA Editorial, Madrid, 2024, p. 24.

²¹ FARÍÑAS DULCE, María José; OLIVA MARTÍNEZ, José Daniel y PÉREZ MACÍAS, Iván Antonio, *Los retos normativos de la inteligencia artificial...*, cit., p. 158-180

modelo regulatorio que el legislador europeo llegó a proyectar y de los problemas que el actual marco deja sin resolver. En esa propuesta no se creaban nuevos deberes de diligencia, sino que la apreciación de la culpa por incumplimiento de deberes se hacía conforme al Derecho de la Unión aplicable y, en lo no armonizado, conforme al Derecho nacional del Estado en cuestión. Por esta razón, la propuesta no pretendía alterar regímenes europeos ya consolidados en áreas específicas, como puede ser el funcionamiento jurídico de plataformas y servicios intermediarios en línea, donde ya existen reglas sobre responsabilidad y obligaciones de conducta; tampoco pretendía desplazar la normativa sectorial aplicable en otras materias como los derechos de autor. La lógica del texto era, en esencia, probatoria. Buscaba reducir la asimetría informativa típica de estos sistemas mediante mecanismos de exhibición de evidencias y, cuando la falta de transparencia hiciera muy difícil probar la relación entre el funcionamiento de la IA y el daño, permitía al juez presumir esa relación siempre que fuera razonable pensar que el incumplimiento de diligencia había influido en el resultado, sin perjuicio de la prueba en contrario por el demandado. La retirada de la propuesta en octubre de 2025 ha eliminado estos mecanismos armonizados, lo que refuerza la importancia de los dos planos sobre los que se construyen los capítulos siguientes: la diligencia interna del administrador y el reparto contractual del riesgo con los proveedores tecnológicos.²²

Otro punto de vista a la hora de encajar a la IA en la evolución del régimen de responsabilidad por productos defectuosos en la era digital es el que tiene en cuenta un problema más práctico, la dificultad de delimitar si se está ante producto o servicio cuando se trata de software. Desde ahí, recoge que las propuestas europeas pretenden aclarar el encaje de los programas informáticos como producto también cuando se suministran de forma independiente y que, además, cobra importancia el servicio conexo cuando es determinante para que el producto cumpla sus funciones, conectándolo con la idea de control del fabricante. Igualmente se insiste en que, por la complejidad técnica y los rasgos de autonomía/opacidad, las víctimas pueden tener serias dificultades para probar defecto y causalidad, lo que empuja a mecanismos como revelación de información y ajustes probatorios, enlazando esto con cuestiones de ciberseguridad y actualizaciones, señalando que la seguridad del producto, incluido el software, y las mejoras o actualizaciones pueden ser relevantes en la valoración del defecto y en el análisis de responsabilidades.²³

Históricamente, la normativa que se ha encargado de regular la responsabilidad civil por los daños causados por productos defectuosos en la Unión Europea ha sido la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985. Sin embargo, esta norma, aunque completa, se estaba quedando muy atrás y no tenía en cuenta nuevos conceptos modernos como el software o los agentes automatizados, hecho que llevó a su posterior derogación.²⁴ Aparte

²² DONADO VARA, Alejandro y JIMÉNEZ MUÑOZ, Francisco Javier (coords.), *La responsabilidad civil de la IA*, 1.ª ed., Dykinson, Madrid, 2024, p. 100.

²³ JORQUI AZOFRA, María, *Responsabilidad por los daños causados por productos y sistemas de inteligencia artificial*, 1.ª ed., Dykinson, Madrid, 2023, p. 143.

²⁴ HERRERA DE LAS HERAS, Ramón, *Aspectos legales de la inteligencia artificial: personalidad jurídica de los robots, protección de datos y responsabilidad civil*, 1.ª ed., Dykinson, Madrid, 2020, pp. 75–76.

de lo ya expuesto, uno de los elementos de mayor peso que impulsó una propuesta de modificación de la Directiva 85/374/CEE, fue precisamente el reto que genera en estos días la inteligencia artificial. Por todos estos motivos, el 18 de noviembre de 2024 se publicó en el Diario Oficial de la Unión Europea la nueva Directiva (UE) 2024/2853, entrando en vigor el 9 de diciembre de 2024. Esta nueva normativa sustituye y deroga formalmente a la antigua Directiva 85/374/CEE que, como se ha expuesto, se estaba quedando atrás.

La Directiva (UE) 2024/2853 supone una transformación especialmente profunda del régimen europeo de responsabilidad por productos defectuosos, ya que adapta sus categorías tradicionales a la economía digital. Su relevancia no radica únicamente en el hecho de ampliar el concepto de producto para incluir el software, los archivos digitales y los sistemas de inteligencia artificial, sino también en que reconoce nuevos daños indemnizables, como la destrucción o corrupción de datos. De este modo, la norma abandona una visión exclusivamente material del producto y asume que, en la actualidad, buena parte del riesgo puede encontrarse en elementos intangibles que condicionan la seguridad del bien y el funcionamiento del mercado digital.²⁵

Siguiendo esta misma línea, una de las aportaciones más útiles de la nueva norma es que permite entender que, en los productos digitales, el defecto ya no tiene por qué localizarse únicamente en el soporte físico, sino también en el entorno digital que hace posible su funcionamiento. Así, la responsabilidad puede venir determinada por errores de software, vulnerabilidades críticas, actualizaciones defectuosas, parches de seguridad insuficientes o fallos en servicios digitales integrados. Esta perspectiva resulta especialmente valiosa porque refleja con bastante fidelidad la realidad tecnológica actual, donde, en muchos casos, la seguridad del producto depende más de su mantenimiento digital y de su supervisión constante que de sus componentes materiales.²⁶

Otro aspecto de vital importancia de la Directiva (UE) 2024/2853 es la ampliación del círculo de operadores que pueden llegar a responder por los daños causados por un producto defectuoso. El texto ya no se centra exclusivamente en el fabricante clásico, sino que contempla también supuestos en los que pueden quedar implicados prestadores de servicios logísticos y proveedores de plataformas en línea, especialmente cuando la presentación de la operación induce al consumidor a pensar que el producto es suministrado por la propia plataforma o por un operador bajo su control. Esta ampliación se examinará con mayor detalle en el marco práctico, pues da un gran paso y es de gran ayuda para la determinación

²⁵ SANCHO LÓPEZ, Marina, “Cumplimiento normativo en la era de la inteligencia artificial: Directiva (UE) 2024/2853 sobre productos defectuosos y la responsabilidad de bienes intangibles y servicios digitales”, *Actualidad Jurídica Iberoamericana*, n.º 24, 2026, pp. 184–185 y 214.

²⁶ GARCÍA CORREAS, Javier, “La nueva Directiva (UE) 2024/2853: redefiniendo la responsabilidad por producto defectuoso en la era de la Salud digital”, en prensa, 2025, pp. 5–6

de la responsabilidad en el comercio electrónico y ayuda a comprender la complejidad actual de las cadenas de distribución digitales.²⁷

Desde una perspectiva más general, la evolución normativa europea en materia de responsabilidad por IA muestra que la Unión Europea ha optado por una solución prudente. Frente a propuestas anteriores que apuntaban hacia una eventual “personalidad electrónica” de los sistemas autónomos, el enfoque finalmente consolidado ha sido mucho más conservador, basándose en adaptar los esquemas clásicos del Derecho de daños para incorporar la inteligencia artificial sin romper con sus categorías básicas. En esa línea, la Directiva 2024/2853 no crea una responsabilidad autónoma de la IA, sino que integra estas tecnologías en el régimen ya existente de responsabilidad por productos defectuosos.²⁸

Antes de abordar la transposición de la Directiva (UE) 2024/2853 al ordenamiento español, conviene precisar cómo se articulan entre sí las dos piezas centrales del marco europeo, el Reglamento (UE) 2024/1689 y la propia Directiva (UE) 2024/2853. Ambas operan en planos distintos pero complementarios. El Reglamento (UE) 2024/1689 establece un régimen de obligaciones ex ante —evaluación y gestión de riesgos, trazabilidad mediante registros, supervisión humana, transparencia y notificación de incidentes— dirigido a proveedores y responsables del despliegue de sistemas de IA, en particular los calificados como de alto riesgo. La Directiva (UE) 2024/2853, en cambio, regula la responsabilidad ex post por los daños efectivamente causados por productos defectuosos, incluidos los sistemas de IA y el software. La conexión entre ambas normas es bidireccional, el incumplimiento de las obligaciones ex ante del Reglamento puede operar como indicio del carácter defectuoso del producto a los efectos de la Directiva; recíprocamente, el correcto cumplimiento de aquellas obligaciones refuerza la posición probatoria y exoneratoria del operador frente a las acciones de responsabilidad. Esta articulación entre normativa preventiva y resarcitoria es la que dota de coherencia al marco europeo y la que justifica que, en lo sucesivo, ambas normas se manejen de forma integrada.

2.3. La transposición de la Directiva (UE) 2024/2853

La Directiva (UE) 2024/2853 obliga a repensar el encaje del actual régimen español de productos defectuosos, especialmente el contenido del Libro III del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios. La reforma europea responde a un contexto en el que la digitalización, las plataformas y la inteligencia artificial han alterado profundamente la forma en que se diseñan, comercializan y utilizan los productos,

²⁷ DE LA VEGA GARCÍA, Fernando, “Directiva (UE) 2024/2853, del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y que deroga la Directiva 85/374/CEE”, *Ars Iuris Salmanticensis*, vol. 13, 2025, p. 310.

²⁸ PARRA SEPÚLVEDA, Darío y CONCHA MACHUCA, Ricardo, “La inteligencia artificial explicable como fundamento para su gobernanza: implicancias en la responsabilidad civil”, *Revista Chilena de Derecho y Tecnología*, vol. 14, 2025, e74040, pp. 23–24.

lo que exige una adaptación de la normativa interna. En este sentido, la nueva Directiva no solo moderniza el marco europeo, sino que actúa también como un impulso directo para revisar el Derecho español vigente, tanto por exigencia normativa como por la necesidad práctica de ofrecer respuestas adecuadas a daños causados por productos digitales y sistemas de IA.²⁹

En el plano de la transposición al Derecho español, una de las cuestiones más relevantes que plantea la nueva Directiva es si su incorporación debe seguir haciéndose dentro del TRLGDCU o si, por el contrario, convendría aprobar una ley especial independiente.

Por una parte, existe el pensamiento de que lo más conveniente es seguir una línea continuista y transponer la Directiva (UE) 2024/2853 mediante una reforma del TRLGDCU, manteniendo así la ubicación tradicional del régimen de responsabilidad por productos defectuosos dentro de la normativa de consumo. Esta tesis tiene a su favor un argumento práctico evidente basado en que en el Derecho español vigente esta materia ya se contiene en los artículos 128 a 149 TRLGDCU, de manera que la incorporación de la nueva Directiva podría hacerse, al menos en apariencia, mediante una actualización de esos preceptos.³⁰ Además, esta solución permitiría preservar la conexión sistemática con el resto de normas protectoras del consumidor, algo que no es irrelevante si se tiene en cuenta que uno de los objetivos expuestos de la Directiva sigue siendo garantizar un elevado nivel de protección de los consumidores.³¹ Desde esta perspectiva, la reforma del TRLGDCU ofrecería continuidad normativa, facilitaría la localización del régimen aplicable para los operadores jurídicos y evitaría, en esencia, la dispersión legislativa.³² Esta manera de entender la transposición encaja especialmente bien si se pone el foco en la función protectora del sistema y en el hecho de que muchos de los litigios derivados de productos defectuosos seguirán produciéndose, en la práctica, en relaciones de mercado en las que la persona perjudicada actúa como destinataria final del bien o servicio. No obstante, esta posición encuentra límites importantes, porque la nueva Directiva ya no responde del todo a la lógica clásica del Derecho de consumo, sino que amplía el concepto de producto, de daño y de operadores responsables en un sentido que desborda claramente el esquema tradicional del TRLGDCU.³³

Por otra parte, como consecuencia de esas limitaciones, parte de la doctrina entiende que el contenido de la Directiva (UE) 2024/2853 ya no puede verse como una simple materia de

²⁹ GONZÁLEZ CABRERA, Inmaculada, “El impacto en el TRLGDCU de la Directiva (UE) 2024/2853 sobre responsabilidad civil por daños causados por productos defectuosos”, en prensa, 2025, pp. 138–139 y 181.

³⁰ PÉREZ GARCÍA, Máximo Juan, “La responsabilidad por los daños causados por productos defectuosos: análisis de la Directiva (UE) 2024/2853 y una propuesta de ley ferenda de incorporación al ordenamiento español”, *InDret*, n.º 3/2025, 2025, pp. 230–231.

³¹ SANCHO LÓPEZ, Marina, “Cumplimiento normativo en la era de la inteligencia artificial...”, cit., pp. 189–191.

³² PÉREZ GARCÍA, Máximo Juan, “La responsabilidad por los daños causados por productos defectuosos...”, cit., p. 210.

³³ GONZÁLEZ CABRERA, Inmaculada, “El impacto en el TRLGDCU...”, cit., pp. 139–145

consumo, sino como un verdadero régimen de Derecho de daños, ya que protege a cualquier persona física perjudicada y no únicamente al consumidor en sentido estricto. Desde esta perspectiva, la futura adaptación española no debería limitarse a una mera reforma técnica del texto refundido, sino afrontar de forma más sistemática el nuevo modelo de responsabilidad por productos defectuosos en entornos digitales. Esta segunda posición, que en la doctrina reciente aparece como la más elaborada, parte de la idea de que la Directiva (UE) 2024/2853 no debería entenderse como una mera norma de consumo, sino como una auténtica pieza del Derecho de daños. El argumento central de esta corriente es que la condición de consumidor no constituye el presupuesto decisivo de protección, pues el derecho a ser indemnizado no se reconoce solo al consumidor en sentido técnico, sino a cualquier persona física que sufra daños causados por un producto defectuoso. A ello se suma que la Directiva introduce una regulación mucho más compleja y transversal que la de 1985, al incorporar software, archivos digitales, servicios conexos, plataformas y nuevos operadores económicos, así como reglas probatorias y criterios de imputación que exceden del marco típico de la defensa de consumidores. Desde esta óptica, mantener la transposición dentro del TRLGDCU podría resultar conceptualmente forzado y generar tensiones internas, especialmente porque el propio TRLGDCU maneja una noción de consumidor que, en algunos casos, incluye también a personas jurídicas, mientras que la Directiva restringe su ámbito subjetivo a las personas físicas perjudicadas.³⁴ Por ello, esta segunda tesis sostiene que lo más coherente sería aprobar una ley especial e independiente sobre responsabilidad por daños causados por productos defectuosos, con derogación de los actuales artículos 128 a 149 TRLGDCU y con un régimen transitorio claro para los supuestos anteriores al 9 de diciembre de 2026. Su principal ventaja sería la coherencia sistemática, ya que permitiría construir un régimen autónomo, alineado con la armonización máxima de la Directiva y mejor conectado con el Derecho común de daños, evitando encajar a la fuerza un modelo nuevo en una estructura pensada para otra lógica normativa. Incluso se ha apuntado como alternativa su futura incorporación al Código Civil, aunque esta vía se considera menos realista mientras no exista una reforma integral de la responsabilidad extracontractual.³⁵

A la vista de lo expuesto, este trabajo se inclina por la segunda de las opciones planteadas. Es decir, que la aprobación de una ley especial e independiente para la transposición de la Directiva (UE) 2024/2853 resulta, en efecto, la solución más coherente, pues el nuevo régimen ya no responde plenamente a la lógica clásica del Derecho de consumo, sino que se configura como una verdadera pieza del Derecho de daños con un ámbito subjetivo más amplio y un ámbito objetivo más complejo que el del régimen actual del TRLGDCU. Esta es, por tanto, la postura que se asume en este trabajo y que se confirmará al hilo de las conclusiones finales.

³⁴ GONZÁLEZ CABRERA, Inmaculada, “El impacto en el TRLGDCU...”, cit., pp. 306-307.

³⁵ PÉREZ GARCÍA, Máximo Juan, “La responsabilidad por los daños causados por productos defectuosos...”, cit., pp. 228-230.

3. LA DILIGENCIA DEL ADMINISTRADOR Y EL GOBIERNO DEL RIESGO POR IA: LA FIGURA DEL ADMINISTRADOR, SUS DEBERES Y EL ESTÁNDAR DE DILIGENCIA

Una vez delimitado el marco normativo europeo y español aplicable a la responsabilidad por los daños derivados del uso de inteligencia artificial, conviene examinar el plano interno de la sociedad operadora del comercio electrónico. La eficacia práctica de aquel marco depende, en buena medida, de quién decide implantar y supervisar estos sistemas y bajo qué estándar de actuación. Por ello, este capítulo aborda la figura del administrador societario, sus deberes y el estándar de diligencia exigible conforme a los artículos 225 y 226 de la Ley de Sociedades de Capital, que sirven de fundamento al modelo de gobierno del riesgo que se desarrollará en los capítulos siguientes. Es importante destacar que todo lo explicado en este apartado podrá ser de aplicación también al responsable de sector de la empresa que se encargue de dirigir la implantación del sistema, pues el administrador podría no tener nada que ver con esto.

3.1. La figura del administrador

En España, la figura del administrador en las sociedades de capital está regulada principalmente en el Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital; concretamente dentro del Título VI “La administración de la sociedad”, que va de su artículo 209 a su artículo 251.

Los requisitos subjetivos que deben reunir los administradores se hallan en el artículo 212 de esta Ley de Sociedades de Capital, donde se expone que los administradores de la sociedad de capital podrán ser personas físicas o jurídicas; y que, salvo disposición contraria en los estatutos, para ser nombrado administrador no se requerirá la condición de socio. El artículo 212 bis destaca que en caso de que se nombre administrador a una persona jurídica, como podría ser otra sociedad distinta, será necesario que esta designe a una sola persona natural para el ejercicio permanente de las funciones propias del cargo; es decir, que siempre habrá una persona física detrás de esta figura, incluso cuando se trate de una persona jurídica.

En cuanto a sus competencias, la Ley de Sociedades de Capital atribuye al administrador dos esferas de actuación. En primer lugar, en el artículo 209 se expone que la administración o gestión de la empresa de la que es titular la sociedad será competencia del administrador, junto a todos los actos necesarios para el desarrollo de aquellas actividades u operaciones empresariales que integren su objeto social. La otra esfera de actuación está regulada en el

artículo 233, haciendo referencia a que le corresponde al administrador la obligación de representar a la sociedad en sus relaciones jurídicas con terceros.³⁶

Teniendo esto en cuenta, cabe afirmar que, en términos generales, la figura del administrador societario le corresponde a la persona física que ha sido nombrada por la junta general de socios y que es el encargado de ordenar, disponer y organizar los bienes de la sociedad de capital; en este sentido, los administradores realizan la gestión de los negocios de la empresa y, por lo tanto, encarnan las facultades y obligaciones tendentes a la consecución de los fines sociales.³⁷

3.2. Los deberes del administrador

La función más básica y general del administrador, como se ha expuesto, es la realización de toda actividad necesaria para alcanzar el objeto social de la sociedad, siempre velando por el bien y los objetivos de esta. La problemática surge en el momento en que el administrador antepone sus propios intereses por encima de los de la sociedad. Para tener esto bajo control y que exista una regularización fue para lo que se crearon los deberes del administrador, con el fin de crear la obligación de velar por la sociedad y su beneficio.³⁸

Existen varios deberes del administrador, entre ellos se destacan el deber general de diligencia o de cuidado, regulado en el artículo 225 de la Ley de Sociedades de Capital; el deber de protección de la discrecionalidad empresarial, regulado en el artículo 226; y el deber de lealtad, regulado en el artículo 227 de esta misma Ley. El análisis se centrará en los dos primeros, los artículos 225 y 226 LSC, dado que son los que articulan el estándar de diligencia y la regla de protección de la discrecionalidad empresarial sobre los que se apoya el modelo de gobierno del riesgo desarrollado en los capítulos posteriores; el deber de lealtad del artículo 227 LSC se omite por su menor relevancia para el objeto concreto del trabajo.

El artículo 225 LSC parte de la base de que los administradores, como se ha expuesto a lo largo de este apartado, deben actuar con la diligencia de un ordenado empresario, teniendo en cuenta la naturaleza del cargo y las funciones atribuidas a cada uno de ellos, subordinando en todo momento y situación su interés particular al de la empresa. Para conseguir este resultado, los administradores deberán tener la dedicación adecuada y adoptar las medidas precisas para la buena dirección y el control de la sociedad, debiendo exigir y recabar de esta

³⁶ SERRANO SEGARRA, María, *Derecho de Sociedades Mercantiles (Segunda Parte)*, Universidad Miguel Hernández de Elche, 2024, p. 7.

³⁷ HERNÁNDEZ MARTÍNEZ, William David, “Los supuestos de aplicación del administrador de hecho: un análisis del caso español a propósito de la sociedad por acciones simplificada”, *Estudios Socio-Jurídicos*, vol. 14, n.º 2, 2012, pp. 2–3.

³⁸ CASANOVA TORRADO, Miguel José, *La fundamentación de los fiduciary duties de los administradores de sociedades y sus consecuencias en la acción social de responsabilidad*, tesis doctoral, Universidad de Navarra, Pamplona, 2012, p. 251.

la información adecuada y necesaria que le sea de utilidad para el cumplimiento de sus obligaciones.³⁹

3.3. El estándar de diligencia

El concepto de estándar de diligencia del administrador sigue la misma línea expuesta hasta ahora; entendiéndose cumplido, según el artículo 226 LSC, “cuando el administrador haya actuado de buena fe, sin interés personal en el asunto objeto de decisión, con información suficiente y con arreglo a un procedimiento de decisión adecuado”. Por consiguiente, es relevante tener en cuenta la diligencia empleada por el administrador que ha tomado una decisión que implicaba un riesgo y que ha causado un perjuicio al patrimonio ajeno administrado.⁴⁰

La cuestión que emerge en el ámbito de la aplicación de sistemas de inteligencia artificial en el comercio electrónico de la sociedad, es si entra dentro del estándar de diligencia ya comentado que el administrador de dicha sociedad realice una serie de revisiones y estudios razonables para controlar el comportamiento y el rendimiento de las automatizaciones o si, por el contrario, esta acción no entra dentro de sus deberes y responsabilidades como administrador. Si se analizan estrictamente los artículos 225 y 226 LSC respecto a la diligencia del administrador, encontramos frases como “Los administradores deberán desempeñar el cargo con la diligencia de un ordenado empresario” o “Los administradores deberán tener la dedicación adecuada y adoptarán las medidas precisas para la buena dirección y el control de la sociedad”; sin embargo, ¿existe un límite o un estándar medible para que, en caso de que uno de estos sistemas falle, decidir si el administrador no ha hecho todo lo que debía hacer y, por consiguiente, otorgarle algún tipo de responsabilidad por lo ocurrido?

Obviamente, no le puedes exigir al administrador que estudie los posibles fallos y errores en un flujo automatizado como lo haría un ingeniero informático especializado; no obstante, se le puede exigir la implantación de ciertos controles razonables antes de la instalación de dicho sistema en la base de datos de la empresa. Es aquí donde se inicia el debate de hasta qué punto el administrador de la sociedad debe informarse y controlar el software instalado, pues ni en Europa ni en España existe jurisprudencia o normativa que resuelva sobre estos controles mínimos que debe implantar o no el administrador. La concreción de estos controles operativos mínimos, así como del reparto contractual de riesgos con los proveedores tecnológicos, constituye precisamente el objeto del capítulo siguiente.

³⁹ SERRANO SEGARRA, *Derecho de Sociedades Mercantiles...*, cit., p. 8.

⁴⁰ GÁLVEZ JIMÉNEZ, Aixa, *El delito de administración desleal (artículo 252 del Código Penal) en el ámbito de las sociedades de capital*, Dykinson, Madrid, 2019, p. 123.

4. MODELO DE GOBIERNO DEL RIESGO POR IA EN EL E-COMMERCE: LA DILIGENCIA DEL ADMINISTRADOR Y LA IMPLANTACIÓN DE CONTROLES INTERNOS A LOS SISTEMAS DE IA

4.1. Análisis y explicación de los posibles controles y su viabilidad

Como se ha expuesto, el administrador no puede desentenderse de la instalación del sistema de inteligencia artificial, así que la opción de no implantar ningún tipo de control queda totalmente descartada. La importancia de adoptar estos controles efectivos no es una preocupación meramente teórica, sino una solución a problemas prácticos a los que se pueden enfrentar los consumidores, así como muestra el caso resuelto por el *Civil Resolution Tribunal* de la Columbia Británica en febrero de 2024 conocido como *Moffatt vs. Air Canada*, 2024 BCCRT 149. En este asunto, un pasajero recibió de un *chatbot* de la aerolínea información incorrecta sobre las condiciones de la tarifa de duelo o luto, y, al solicitar el reembolso conforme a esa información proporcionada por el chat, Air Canada le denegó dicho reembolso alegando que la política oficial publicada en otra parte de su web exigía un trámite distinto al que le expresó ese *chatbot*. Frente a la defensa de la aerolínea, que sostuvo que el *chatbot* constituía una entidad legal separada, responsable de sus propios actos, el tribunal rechazó esa construcción y consideró a la compañía plenamente responsable de la información ofrecida por su sistema automatizado. Aunque se trate de una jurisdicción extranjera y no vincule directamente a los tribunales españoles, el supuesto ilustra con claridad por qué la implantación de un sistema de IA exige un mínimo de controles internos, pues sin ellos la empresa podría responder por los actos del sistema sin haber tenido capacidad real de prevenir este daño.⁴¹ Establecida la importancia de implantar unos controles suficientes, procede analizar las posibles opciones y valorar su viabilidad a la luz de los criterios defendidos en este trabajo.

La primera posibilidad, que es a la vez la que exige menos esfuerzo para el administrador, es la de que este se asegure de que quien instala el programa de inteligencia artificial sea un equipo o persona cualificados para realizar dicha operación. Es decir, que el administrador debe comprobar que quien automatiza el sistema o flujo es un experto técnico con garantías, ya sea por su formación académica, recorrido profesional o por experiencias contrastadas y reales de haber realizado un buen trabajo. Desde la perspectiva de un administrador que quiere contratar el servicio, es lógico que considere que está procediendo correctamente y que no habrá ningún problema si está contratando a una empresa seria y con experiencia previa en el sector. Esta es una muy buena opción si tenemos en cuenta su agilidad y la poca carga de trabajo que otorga, pues con hacer un estudio de la empresa que instalará el software ya se excluye la responsabilidad, sin tener que entrar a estudiar el sistema que se implanta en la empresa. Sin embargo, la mayor problemática de esta posibilidad es que se basa

⁴¹ BRAND, Joshua L. M., “Air Canada’s chatbot illustrates persistent agency and responsibility gap problems for AI”, *AI & Society*, vol. 40, 2025, pp. 3361–3363.

principalmente en la confianza que tiene el administrador y en un criterio mayormente subjetivo, esto hace que no exista una línea clara para determinar cuándo una empresa se considera fiable o cuándo el administrador ha hecho un estudio suficiente de la oferta en el mercado.

Otra posibilidad más exigente sería la obligación de tener en plantilla a un especialista en *compliance* de nuevas tecnologías, a un técnico informático o a cualquier otro experto de características análogas. Obviamente, esta opción no podría ser aplicable a todas las sociedades, pues dejaría a las empresas que no se pueden permitir contratar a un empleado de estas características sin la posibilidad de utilizar una tecnología tan revolucionaria como lo es la inteligencia artificial automatizada, abriendo una brecha de enormes dimensiones entre empresas pequeñas y empresas grandes. La única forma de poder implementar esta opción en la práctica sería si solo fuese aplicable a sociedades de determinadas dimensiones. Los criterios que se utilizan habitualmente para cuantificar la dimensión de una empresa son el balance total, el importe neto de la cifra de negocios y el número de plantilla;⁴² sabiendo esto y siguiendo la misma línea que ha tomado históricamente el estado español con la implementación de gravámenes regulatorios y fiscales a las personas jurídicas con 50 o más trabajadores, se podría tomar el mismo camino e implementar estos requisitos a las sociedades que superen ese número de empleados.⁴³ La justificación de esta medida tiene su base en que se presupone que cuanto más grande es la compañía, más responsabilidades y control debe asumir, pues está llegando a más clientes y, como consecuencia, causará muchos más daños y perjuicios en caso de que falle uno de estos sistemas.

Una vez analizadas las dos posibles opciones de distinta índole para determinar cuándo otorgar la responsabilidad al administrador, una de características esencialmente laxas y otra con rasgos notablemente más estrictos y garantistas, procede introducir el procedimiento que, según se defiende en este trabajo, debería establecerse para determinar o no la responsabilidad en caso de fallo de un sistema de inteligencia artificial en un comercio electrónico. Es decir, los pasos que debe seguir el administrador de una empresa en todo el proceso de instalación y la vida funcional del sistema automatizado para evitar ser responsabilizado personalmente por futuros errores. Este procedimiento consta de cinco fases que deberá cumplir el administrador o responsable del sector encargado de la implementación del sistema en la empresa. Este proceso no constituye una exigencia ajena al Derecho de sociedades, sino la traducción operativa y práctica de los requisitos que el artículo 226 LSC impone para que la decisión empresarial del administrador, en este caso la decisión de implantar y mantener un sistema de IA, quede protegida por la regla de protección de la discrecionalidad empresarial

⁴² GARCÍA GINÉ, Joan, “Efectos legales del tamaño de la empresa”, *Revista de Contabilidad y Tributación*. CEF, n.º 357, 2012, pp. 137–194, p. 143.

⁴³ “Economía española: nuevos retos”, *Cuadernos de Información Económica*, n.º 250, enero/febrero 2016, Funcas, p. 68.

4.2. La evaluación de riesgos y la documentación mínima

La primera fase del procedimiento consiste en la realización de una evaluación de riesgos previa a la implementación del sistema, pues el administrador o responsable de departamento debe ser consciente de que no está contratando un simple sistema informático que afecta a la intranet de la empresa, sino que se trata de una extensión más de la compañía que interactúa directamente con el consumidor; esta es la razón por la que debe incorporar una previsión sobre posibles fallos del sistema y qué consecuencias jurídicas podrían tener dichos errores.

Es de gran importancia tener en cuenta el contexto de la compañía y del comercio electrónico al que se quiere aplicar cada sistema automatizado, pues la evaluación de riesgos que se plantea no puede formularse de manera abstracta siguiendo siempre unos mismos pasos universales, sino que debe estar vinculada a cada caso de uso concreto. Por ejemplo, el nivel de exposición de un sistema que ordena productos en una página web según *Mouse Tracking* creando un mapa de calor, técnica que se basa en monitorear el movimiento del ratón del ordenador para saber dónde está mirando la persona, pues el posicionamiento del ratón coincide al 84% con el movimiento de los ojos, sabiendo así los productos que tienen más éxito en la web,⁴⁴ será muy bajo si lo comparamos con otros sistemas que denieguen devoluciones o respondan automáticamente a las reclamaciones del consumidor. Esto se debe a que, aunque el primero es notablemente más complejo de instalar y programar, es un sistema que afecta indirectamente al consumidor, mientras que es el segundo el que tiene un impacto directo hacia este. Por ello, la evaluación debe identificar, para cada flujo y automatización instalada, cuáles son los escenarios de daño razonablemente previsibles, a quién podrían afectar y cuál sería el impacto probable en términos económicos, reputacionales y normativos.

Sobre esta base, la evaluación de riesgos debe concluir en decisiones prácticas y no solo en una mera descripción de los riesgos del sistema. Es decir, no se entenderá cumplida esta evaluación si únicamente se ha realizado un párrafo teórico sobre el riesgo de un sistema genérico, tarea que cualquier persona puede realizar en pocos segundos con la ayuda de una inteligencia artificial generativa; sino que se exigirá la delimitación de los aspectos del proceso antiguo que quedan ahora automatizados, cuáles quedan reservados a la intervención humana y qué límites se impondrán al sistema en situaciones sensibles. En particular, cuando la automatización puede afectar a los derechos de los consumidores, a la ejecución de un pago o a la contratación, resulta razonable la exigencia de un mayor nivel de cautela y precisión al describir e intentar prever estas situaciones problemáticas. Por último, la evaluación deberá contemplar el papel del proveedor tecnológico, que varía según el sistema o flujo y el nivel de dependencia que tiene el sistema instalado respecto a este, pues muchos sistemas requieren de un mantenimiento mensual o semanal. Este aspecto es de suma importancia, ya que la atribución de responsabilidades en caso de incidencia dependerá en

⁴⁴ PEÑA GONZÁLEZ, Zucel y TRUJILLO CASAÑOLA, Yaimí, “Mapas de calor en sitios web”, *Serie Científica de la Universidad de las Ciencias Informáticas*, vol. 12, n.º 9, 2019, pp. 99–101.

gran medida de quién controla el sistema realmente y de quién conserva las evidencias sobre su funcionamiento.

La documentación mínima es tan importante como la evaluación de riesgos. Esta cumple una función de vital importancia en el procedimiento, convertir esta evaluación en un soporte de diligencia verificable. A efectos prácticos, debe quedar constancia de todos los elementos que se han visto envueltos en la instalación de la automatización para así poder otorgar responsabilidades. Es decir, deberá quedar prueba y documentación de la finalidad del sistema y del proceso de decisión que llevó a su implantación, del proveedor elegido y su alcance de intervención, de los datos o señales que alimentan la automatización en la medida en que sean relevantes, de la configuración esencial del sistema y de los límites establecidos, así como de la versión o estado del sistema en el momento de la revisión o fallo. La idea de implementar esta documentación y prueba mínima no es la de pretender burocratizar el funcionamiento empresarial y tecnológico, sino permitir la reconstrucción de todos los hechos hasta llegar al problema, sabiendo con qué información y bajo qué controles se realizó el proceso. Sin esta trazabilidad fáctica, la defensa posterior del administrador y de la empresa respecto a la responsabilidad se apoya únicamente en afirmaciones sin una base muy difíciles de sostener ante un conflicto, lo que permitiría a todas las partes eludir la responsabilidad y dejaría el perjuicio del consumidor sin una imputación.

4.3. La revisión humana, la monitorización y las métricas

La segunda fase está más centrada en evitar que el sistema funcione sin ningún tipo de supervisión efectiva, sobre todo cuando dicho sistema interviene en decisiones con impacto real y directo hacia los consumidores o terceros o cuando interactúa y se comunica directamente con ellos. Esta revisión humana no debe entenderse como una revisión manual de todas las decisiones que realiza la automatización con inteligencia artificial, esto sería algo inviable en la práctica, pues tendría más sentido contratar a alguien para que realizara directamente esa función en lugar de limitarse a supervisar el sistema buscando algún fallo. Por ende, la supervisión exigible debe entenderse articulada en dos niveles complementarios. En primer lugar, una monitorización automática y continua, basada en indicadores y umbrales objetivos, que vigile el comportamiento del sistema y permita detectar desviaciones, picos o anomalías antes de que escalen. En segundo lugar, una intervención humana reactiva que se active únicamente cuando esos indicadores arrojen alertas o se identifiquen decisiones sensibles, errores significativos o incidencias relevantes. De este modo, el control no exige una vigilancia manual permanente, pero tampoco deja a cargo de la propia que ha fallado el arreglar ese error.

A pesar de lo expuesto, debe reconocerse que un sistema puede generar daños de forma silenciosa durante un tiempo antes de que el problema se haga evidente y afecte a personas que utilizan el portal de la empresa. La inteligencia artificial es tan asombrosa como impredecible, pudiendo evolucionar y mutar sus funciones, objetivos y metas dependiendo

de los comandos y *prompts* con los que se le haya configurado. Existen numerosos ejemplos en los que esto ha sucedido, uno de ellos es el caso del *chatbot* Tay desplegado por Microsoft en Twitter en marzo de 2016. El sistema, diseñado para aprender del lenguaje y la interacción con otros usuarios, fue retirado por la propia compañía en menos de veinticuatro horas, al comprobarse que la falta de límites claros en su aprendizaje había permitido que terceros lo entrenaran de forma masiva con mensajes ofensivos, racistas y discriminatorios, que el sistema acabó reproduciendo. El supuesto evidencia cómo, en ausencia de controles previos sobre los datos de entrada y de mecanismos de supervisión del comportamiento, una IA puede mutar de forma muy rápida y generar consecuencias jurídica y reputacionalmente relevantes para la entidad responsable; un riesgo que, trasladado al comercio electrónico, puede manifestarse no solo en términos reputacionales sino también en perjuicio directo a los consumidores.⁴⁵ Por ello, aun cuando no resulte viable ni necesaria una atención humana absolutamente dedicada al control y la revisión del sistema en todo momento, es muy necesario que la empresa observe el comportamiento del sistema mediante indicadores mínimos que permitan detectar patrones como incrementos anómalos de reclamaciones, picos de transacciones rechazadas, aumento de devoluciones discutidas o reiteración de incidencias por respuestas incorrectas de un *chatbot*. Por lo tanto, no se trata de que un humano revise a la IA, sino de que otra automatización diferente especializada en esta materia vigile estas incidencias y cambios en la normalidad de la compañía. Aunque a primera vista pueda parecer complejo, en la práctica se traduce en añadir una nueva capa al flujo automatizado, intervención perfectamente abordable por un experto en la instalación de este tipo de sistemas.

Conviene retomar en este punto el debate sobre el criterio de proporcionalidad. ¿Todas las empresas pueden desplegar sistemas complejos de seguimiento? Se trata de una cuestión compleja, no solo por un impedimento económico y adquisitivo por parte de la empresa pequeña, sino por una cuestión de desconocimiento sobre la materia. En esencia, la función de esta base es determinar que cuanto más intensa sea la intervención de la IA y la automatización en decisiones relevantes, más necesario será contar con mecanismos de revisión, humanos o artificiales, y con indicadores que alerten de un funcionamiento anómalo. En caso contrario, la empresa corre el riesgo de sostener un sistema automatizado sin una capacidad real de control, lo que debilita en gran medida tanto la prevención del daño como la posibilidad de acreditar la diligencia del administrador o responsable si el daño finalmente se produce.

4.4. El registro de decisiones, la auditoría y la gestión de incidentes

Esta tercera fase aborda el núcleo probatorio del sistema de inteligencia artificial. Para determinar a los sujetos que deben hacerse cargo del daño, otorgándoles así la

⁴⁵ TORRES MANRIQUE, Jorge Isaac y RIBEIRO BRASIL, Deilton, *Inteligencia artificial: omnipresencia, nuevas tendencias e interdisciplinariedad*, 1.ª ed., J.M. Bosch Editor, 2023, pp. 86–88.

responsabilidad, resulta determinante explicar qué fue lo que ocurrió, por qué ocurrió ese error y quién tenía la capacidad de evitarlo o corregirlo; para conseguir esto es esencial poder conocer el contexto de todo el sistema y de la interacción que se ha realizado. En sistemas automatizados con inteligencia artificial esto se traduce en la necesidad de realizar un registro razonable de las decisiones adoptadas y de los elementos esenciales que las sustentan. Es importante destacar que no se trata de un intento de convertir el *e-commerce* en un lugar de permanente vigilancia, sino de garantizar un mínimo de trazabilidad para poder realizar dicho registro. Este registro debe poder reconstruir la decisión automatizada, pues es uno de los elementos más importantes para empezar a saber lo que está causando un error; el momento en que se tomó, para poder dar más contexto a la situación e identificar cambios que se realizaron en esas fechas; el resultado producido, para saber qué es lo que desencadena el error; la configuración o versión vigente, pues muchas veces el error o fallo en el sistema se puede deber a una mala actualización de la versión del sistema instalado; y, cuando exista intervención humana, el motivo y el desenlace final. Sin este registro objetivo y real, cualquier controversia terminaría dependiendo de reconstrucciones hipotéticas e incompletas, cosa que acaba agravando el conflicto y hace que nadie se responsabilice por los perjuicios ocasionados.

Antes de entrar a analizar otras cuestiones de este apartado, conviene precisar cómo se obtiene este registro. En un sistema de inteligencia artificial, la memoria es el mecanismo que permite conservar y reutilizar información más allá de una interacción concreta, de modo que el sistema pueda ajustar sus decisiones a partir de un contexto más amplio;⁴⁶ a efectos jurídicos, lo relevante es que no todas las arquitecturas de memoria permiten reconstruir lo ocurrido. La memoria contextual, basada en *prompts*, se limita a la tarea en curso y, una vez finalizada la inferencia, no permite reconstruir lo ocurrido; es decir, que se olvida de toda la información que le dices cuando le haces una pregunta nueva, haciendo que no pueda tener una conversación. Por el contrario, las memorias a largo plazo, especialmente las estructuradas, conservan información durante períodos prolongados y permiten revisar a posteriori qué falló y por qué. Esta diferencia técnica condiciona directamente la diligencia exigible al administrador, pues elegir una arquitectura sin trazabilidad equivale a impedir el registro de decisiones que el propio Derecho exige.⁴⁷

Por otra parte, existe el deber de la empresa de poder identificar qué se modifica y actualiza en el flujo utilizado en su comercio electrónico, este control de cambios es la llamada auditoría. En sistemas de inteligencia artificial o agentes automatizados, las variaciones en los umbrales establecidos, las integraciones o los parámetros pueden variar el resultado de forma sustancial. Por esta razón, la empresa debe poder identificar qué se ha cambiado en su sistema, cuándo se llevó a cabo, quién aprobó dicho cambio y con qué finalidad lo hizo. Este control no solo tiene valor preventivo, identificando errores producidos por actualizaciones dañinas, sino que permite, además, depurar responsabilidades cuando el fallo

⁴⁶ JIANG, Xun et al., “Long Term Memory: The Foundation of AI Self-Evolution”, *arXiv*, 2025, arXiv:2410.15665v4, pp. 9–10.

⁴⁷ JIANG et al., “Long Term Memory...”, cit., pp. 17–18.

se relaciona con una actualización, con una configuración inadecuada o con una modificación aplicada sin las garantías mínimas.

El caso protagonizado por la empresa de paquetería DPD en enero de 2024 ilustra el por qué es necesaria esta exigencia con claridad. Todo empezó tras una actualización de su sistema, después de la actualización el *chatbot* de atención al cliente comenzó a responder de forma abiertamente hostil hacia la propia compañía, llegando a redactar poemas burlescos y afirmaciones críticas sobre la calidad del servicio cuando los usuarios planteaban dudas o reclamaciones a este chat. La incidencia se difundió en redes sociales y obligó a la empresa a desactivar la funcionalidad de este sistema de IA.⁴⁸ Más allá de la repercusión reputacional hacia la propia empresa, el supuesto evidencia cómo una actualización aprobada sin un control o análisis de cambios adecuado puede transformar un sistema previamente estable en una fuente directa de daño para la imagen de la compañía y, en otras circunstancias, para la seguridad del consumidor.

La cuarta fase, dedicada a la gestión de incidentes, completa este bloque del procedimiento. La compañía o empresa debe contar con un procedimiento claro para detectar y contener los fallos, corregirlos y dejar constancia de las medidas adoptadas. Un incidente en un comercio electrónico no se trata de un simple error técnico, sino de un acontecimiento con una relevancia jurídica potencial que puede afectar a consumidores, a la prestación contractual y a la imagen de la empresa. Esta situación multiplica su riesgo y delicadeza cuando hablamos de grandes *marketplaces* o empresas con una gran tasa de ventas online, pues cuando existe un fallo en el sistema de estos gigantes societarios no se trata de un error específico, sino de un fallo general que afecta a todos los consumidores o interacciones que lo activen. Por todo ello, deben existir responsables definidos y criterios de actuación ante anomalías, incluyendo la coordinación con proveedores cuando el sistema dependa de servicios externos. La finalidad de esta medida tiene su base en que, si el error llega a producirse, la empresa pueda reaccionar con rapidez y documentar de manera ordenada qué sucedió y qué se hizo para limitar el daño, factores que resultan esenciales para sostener un estándar razonable de diligencia.

4.5. Las medidas frente a sesgos, los errores y el *drift* del modelo

Por último, la quinta fase está enfocada a tener lo más controlado posible un rasgo de lo más peligroso y que es bastante común en cualquier derivado de la inteligencia artificial, que es el comportamiento y su tendencia al cambio, pues ya se han visto bastantes casos donde este puede variar con el tiempo. Incluso cuando el sistema se ha implantado correctamente, puede degradarse por cambios en los datos, en el entorno comercial, en los patrones de fraude, en el catálogo o en las propias interacciones con los usuarios. Además, es posible la aparición

⁴⁸ MATECAS, Alexandru-Raul; KIESEBERG, Peter y TJOA, Simon, “Social Engineering with AI”, *Future Internet*, vol. 17, n.º 11, 2025, art. 515, pp. 23–25

de sesgos o errores sistemáticos que, si no se detectan, terminan generando decisiones injustificadas o daños repetidos a ciertos grupos de personas o colectivos. En el ámbito del *e-commerce*, se puede manifestar a través de bloqueos desproporcionados, denegaciones reiteradas de devoluciones, respuestas incorrectas persistentes en atención automatizada o patrones de visibilidad que perjudican sistemáticamente a determinados perfiles o vendedores.

Un buen ejemplo donde se ve ilustrado este tipo de fallos es el sistema interno de selección de personal que Amazon desarrolló entre 2014 y 2018. La compañía detectó que el modelo que implantaron en su intranet penalizaba sistemáticamente los currículums que incluían referencias femeninas y favorecía determinados perfiles masculinos, no por una decisión consciente del diseño, sino porque los datos históricos con los que se había entrenado el sistema reflejaban una composición laboral previa fuertemente masculinizada. El sistema había aprendido del sesgo presente en los datos y lo estaba reproduciendo de forma amplificada. Amazon decidió cancelar el proyecto, pero el supuesto demuestra cómo un sesgo estructural puede instalarse en un sistema correctamente programado sin que nadie se percate y generar decisiones discriminatorias durante años sin ser detectado, a falta de mecanismos de revisión periódica del comportamiento del modelo.⁴⁹

La solución para evitar en la medida de lo posible estos *drifts* o errores de modelo no es exigir una infalibilidad, pues no sería razonable porque estos cambios de comportamiento no se pueden controlar, son intrínsecos a la naturaleza de la IA, que evoluciona en función de los datos y de las interacciones; la solución, de nuevo, radica en establecer controles periódicos y continuados para cortar de raíz cualquier indicio de sesgo en el sistema. Por lo tanto, debe existir una revisión regular del desempeño del sistema, especialmente tras cambios relevantes o tras señales de error detectadas en la monitorización. Esto no debería ser un problema para ninguna compañía, pues ya se suelen realizar controles periódicos del sistema de IA o plataforma para comprobar que todo funciona correctamente, únicamente deberían añadir un nuevo control más enfocado en el comportamiento del sistema y no tanto en su funcionamiento técnico. Asimismo, deben fijarse límites que eviten que una desviación del sistema cause daños masivos sin intervención humana, incluyendo la posibilidad de reducir automatización, elevar revisión humana o suspender temporalmente el sistema cuando los indicadores reflejen un funcionamiento anómalo. Del mismo modo, cualquier actualización o recalibración debe integrarse en el control de cambios, precisamente porque el remedio puede convertirse en una nueva fuente de fallo si se implementa sin trazabilidad.

En esencia, en caso de que el sesgo, el error o la desviación fuesen riesgos previsibles que se podrían haber evitado en mayor o menor medida, y la empresa no hubiese establecido controles mínimos para detectarlos y corregirlos por una escasez de interés, la falta de reacción puede interpretarse como una omisión relevante en el estándar de diligencia y, por

⁴⁹ SILVA, Federico, “La responsabilidad por discriminación algorítmica en los procesos de reclutamiento y selección de personal en la República Argentina”, *Derecho e innovación*, febrero 2026, pp. 23–34.

lo tanto, atribuirle al administrador o encargado del sistema en la empresa la responsabilidad por los daños provocados.

Hasta aquí se han analizado los controles internos que conforman la diligencia exigible al administrador en el gobierno del riesgo. Sin embargo, este gobierno hacia adentro de la sociedad no agota el problema, pues una parte sustancial del control efectivo del sistema corresponde a los proveedores tecnológicos que lo suministran y mantienen. A esta segunda dimensión, la del reparto contractual del riesgo, se dedica el capítulo siguiente.

5. EL MODELO DE GOBIERNO DEL RIESGO POR IA EN EL E-COMMERCE: EL REPARTO CONTRACTUAL DE RIESGOS CON PROVEEDORES TECNOLÓGICOS

5.1. La función del contrato como instrumento de gobierno del riesgo

Desarrollado el plano interno del gobierno del riesgo, la diligencia exigible al administrador y los controles operativos mínimos que de ella se derivan, conviene examinar su plano externo, que se basa en el reparto del riesgo entre la empresa operadora del *e-commerce* que contrata el servicio y los proveedores tecnológicos que suministran, mantienen y actualizan los sistemas de inteligencia artificial. La importancia de esta cuestión se ha visto muy reforzada en los últimos meses debido a que la propuesta de Directiva sobre responsabilidad por inteligencia artificial fue formalmente retirada por la Comisión Europea en octubre de 2025, tras constatarse la imposibilidad de alcanzar un acuerdo entre los Estados miembros y las instituciones europeas.⁵⁰ Esta retirada ha dejado un evidente vacío normativo; pues, como ya se ha explicado anteriormente, el régimen específico de responsabilidad por IA queda hoy compuesto, esencialmente, por el Reglamento (UE) 2024/1689, la Directiva (UE) 2024/2853 sobre productos defectuosos y los respectivos derechos nacionales no armonizados. En este escenario, el contrato suscrito entre el operador del *e-commerce* y sus proveedores tecnológicos adquiere un papel mucho más importante, pues constituye el instrumento jurídico que, dentro de los límites del ordenamiento jurídico y de las normas imperativas de protección al consumidor, permite distribuir los riesgos, asignar las responsabilidades y prever las consecuencias de un eventual fallo del sistema.⁵¹ Aun así, la autonomía contractual no sustituye a la diligencia del administrador o responsable de sector, pero sí la complementa, ofreciendo al administrador o responsable una herramienta para acreditar que el riesgo y la responsabilidad por posibles fallos futuros han sido asignados y gobernados.

5.2. La definición del objeto contratado y el nivel de servicio

El primer bloque de cláusulas contractuales a tener en cuenta en este tipo de relaciones es el relativo a la delimitación precisa del sistema contratado. En entornos tradicionales basta con identificar el bien o servicio adquirido, pero en el ámbito de la instalación de sistemas automatizados con inteligencia artificial esta exigencia se vuelve especialmente compleja, pues el sistema se encuentra en constante evolución, se actualiza y se reentrena con frecuencia. Por ello, es muy importante que el contrato identifique con claridad la versión del sistema entregado, las funcionalidades incluidas, los tipos de decisiones que automatiza,

⁵⁰ GÓMEZ LIGÜERRE, Carlos, “Responsabilidad por daños causados por la inteligencia artificial”, *InDret*, n.º 1/2025, 2025, comentario sobre la retirada de la propuesta de Directiva sobre responsabilidad por IA.

⁵¹ AYO FERRÁNDIZ, Cristina; SEIJO BAR, Álvaro; GARRE ANGUERA DE SOJO, Ignacio; GONZÁLEZ GUILLÉN, Pablo, *Responsabilidad civil e inteligencia artificial*, Actualidad Jurídica Uría Menéndez, n.º 67, mayo 2025, pp. 44–52.

los datos de entrada que utiliza y los resultados que genera gracias a estos. A esta delimitación funcional debe añadirse un *service level agreement* (SLA), este concepto hace referencia a un tipo de contrato en el que se establecen de manera cualitativa y cuantitativa las características del servicio que el proveedor del servicio tecnológico debe ofrecer al cliente, que en este caso es la empresa en cuestión.⁵² Se añade este SLA para fijar unos parámetros mínimos de calidad que deben quedar claros desde un inicio como la disponibilidad del sistema, los tiempos máximos de respuesta por parte del instalador de la automatización en caso de fallo, las tasas aceptables de error y las métricas específicas para el caso de uso. Un ejemplo sería, en un sistema de *repricing* dinámico, los márgenes máximos de variación de precio respecto del precio de referencia y el tiempo máximo de reacción del proveedor ante desviaciones anómalas detectadas en la monitorización del sistema. Estos parámetros mencionados no constituyen en sí mismos un simple compromiso técnico, sino un umbral objetivo a partir del cual puede sostenerse el incumplimiento contractual del proveedor. Resulta igualmente conveniente, dada la naturaleza dinámica de estos sistemas, incluir una cláusula de control de cambios que someta las actualizaciones críticas a notificación previa por parte del proveedor y, cuando proceda, a la conformidad expresa del operador; pues, como ya se ha explicado en el apartado anterior de este trabajo, una recalibración o reentrenamiento del agente pueden alterar de forma sustancial el comportamiento del sistema y, con ello, su perfil de riesgo.

5.3. La cooperación técnica y probatoria

El segundo bloque aborda la cooperación del proveedor en la reconstrucción de los hechos cuando se produce un incidente, lo que probablemente sea la cuestión más complicada en este tipo de relaciones. Como ya se ha analizado a lo largo de este trabajo, una de las grandes dificultades de la responsabilidad por los daños a consumidores vinculados a los sistemas de inteligencia artificial es la gran diferencia informativa entre quien sufre el daño, quien crea e instala el sistema y quien lo tiene implementado en su página de comercio electrónico.

Frente a estas dificultades, la propuesta de Directiva sobre responsabilidad por IA preveía mecanismos armonizados de exhibición de pruebas y presunciones probatorias que habrían reducido sensiblemente esa asimetría; al haberse retirado dicha propuesta, la regulación de la materia queda confiada, en gran medida, a la vía contractual, lo que obliga a un cuidado especial en la redacción de las cláusulas correspondientes.⁵³ En este bloque se desarrollan

⁵² MONTERO MOUZO, David; PIÑERO ESCUER, Pedro J.; MANZANARES LÓPEZ, Pilar; MUÑOZ GEA, Juan P., “Monitorización de contratos Service Level Agreement en un entorno de negocio inter-ISP”, comunicación en las Jornadas TELECOM I+D, Universidad Politécnica de Cartagena (ETSIT), 2005, pp. 124–126.

⁵³ MARTÍN CASALS, Miquel, *Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial*, InDret, núm. 3, 2023, pp. 71–74.

tres previsiones esenciales que deberían integrarse en todos los contratos donde un proveedor tecnológico le ofrezca un flujo automatizado a una empresa.

En primer lugar, establecer una obligación clara del proveedor de conservar los registros de funcionamiento del sistema; esto se traduce a las trazas de actividad o *logs*, las configuraciones aplicadas, las versiones desplegadas del sistema y los conjuntos de datos utilizados para su entrenamiento, todo ello durante un plazo razonable acordado por las partes que en ningún caso debería ser inferior al de prescripción de las acciones derivadas del contrato.

En segundo lugar, un derecho de auditoría a favor de la empresa operadora del *e-commerce*, esto con el objetivo de que le permita acceder a esa información mencionada anteriormente, ya sea directamente con algún tipo de contraseña o clave o a través de un tercero independiente sujeto a confidencialidad, especialmente cuando se haya producido un incidente con repercusión en consumidores.

En tercer y último lugar, una obligación contractual de notificación de incidentes en plazos breves, conectada con las obligaciones que el Reglamento (UE) 2024/1689 ya impone a los proveedores de sistemas de IA de alto riesgo, debiendo estos notificar a las autoridades competentes los incidentes graves de los que tengan conocimiento, considerando como tal cualquier mal funcionamiento que provoque daños relevantes a la seguridad, los derechos fundamentales o el patrimonio de las personas; y, en su caso, con las derivadas del Reglamento General de Protección de Datos, que obliga al responsable del tratamiento a notificar las violaciones de seguridad de datos personales a la autoridad de control en un plazo máximo de 72 horas desde su conocimiento. En esencia, todo este bloque permite al operador, llegado el conflicto, aportar la prueba que el régimen general le exige sin depender de la buena voluntad del proveedor.

5.4. La distribución de la responsabilidad y las indemnidades

El tercer bloque se centra en la parte más económica del contrato en caso de fallo del sistema. Aquí deben pactarse las indemnidades cruzadas entre quien contrata los servicios y el proveedor, los límites de la responsabilidad y los seguros que respaldan la cobertura. El planteamiento parte de la base de que existen dos planos de responsabilidad diferentes a tener en cuenta, el plano externo y el interno. En el plano externo, frente al consumidor perjudicado, la Directiva (UE) 2024/2853 establece un régimen de responsabilidad objetiva con causas tasadas de exoneración, sin que la empresa pueda liberarse de él mediante pacto, pues sus disposiciones tienen carácter imperativo en lo que afecta a los derechos del consumidor, y su elusión por vía contractual sería ineficaz por aplicación del artículo 86 del

TRLGDCU.⁵⁴ En el plano interno, en cambio, entre operador y proveedor rige la autonomía de la voluntad, lo que permite pactar quién soporta finalmente el coste de la indemnización satisfecha al consumidor. Las cláusulas contractuales que este trabajo considera razonables para este bloque incluyen una indemnidad del instalador de la automatización por los daños derivados de defectos imputables al sistema, como lo son los errores de diseño, los sesgos no advertidos, las vulnerabilidades de seguridad o las actualizaciones defectuosas; y, recíprocamente, una indemnidad del administrador o sociedad por usos del sistema fuera del ámbito contractualmente previsto o por incumplimiento de las recomendaciones técnicas del proveedor.

Por último, resultaría recomendable que en el contrato se estableciese que el proveedor se encargase del mantenimiento de una póliza de responsabilidad civil con cobertura suficiente, pues la cláusula de indemnidad por sí misma no resulta del todo eficaz si el deudor carece de patrimonio o liquidez en ese momento.

5.5. La terminación, la reversibilidad y la continuidad del servicio

Este último bloque atiende a un posible desenlace entre las dos partes, es decir, a la resolución ordenada del contrato cuando la relación falla. En sistemas de inteligencia artificial integrados en un comercio electrónico, la dependencia tecnológica de la empresa o entidad respecto del proveedor suele ser muy elevada, pues quien contrata los servicios no suele ser un experto en ese ámbito de la tecnología, sino en el ámbito al que se dedica su empresa; debido al desconocimiento razonable del sistema integrado por parte del contratante, una terminación repentina del servicio puede causar tantos o más daños que el propio fallo del sistema. Por ello, el contrato debe prever causas claras de resolución por incumplimiento, entre las que deben figurar el incumplimiento reiterado de los SLA ya mencionados, los incidentes graves no notificados y la negativa a cooperar en la investigación de un incidente. Además, debe garantizarse la reversibilidad del servicio mediante obligaciones de transición ordenada, que comprendan la devolución o portabilidad de los datos del operador, la documentación técnica necesaria para migrar a otro proveedor y un plazo razonable de continuidad mínima del servicio durante la transición. Básicamente, se intenta proteger en cierta medida a la empresa que contrata el servicio tecnológico debido a que, sin estas previsiones, la empresa que recibe los servicios queda atrapada en una relación contractual inexistente o degradada, circunstancia que multiplica el riesgo de incidentes adicionales, porque no hay nadie que se esté haciendo cargo del sistema, y debilita su posición a la hora de exigir responsabilidades, pues ya no existe una relación con quien instaló la automatización.

⁵⁴ DE LA VEGA GARCÍA, Fernando, *Directiva (UE) 2024/2853, del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y que deroga la Directiva 85/374/CEE*, *Ars Iuris Salmanticensis*, vol. 13, 2025, pp. 306–311.

En conjunto, los cuatro bloques analizados conforman un esquema mínimo de reparto contractual del riesgo que, sin ser excesivamente exhaustivo, ofrece al operador del *e-commerce* una base jurídica defendible para gobernar su relación con los proveedores tecnológicos. Este esquema funciona como prolongación natural de los controles internos analizados en el capítulo anterior, pues lo que el administrador debe documentar y supervisar dentro de la sociedad debe quedar también reflejado en los compromisos contractuales que vinculan al proveedor, de modo que la diligencia desplegada hacia adentro encuentre correspondencia en la disciplina contractual que existe fuera. Solo así puede sostenerse, frente al consumidor perjudicado y frente al juez llamado a depurar responsabilidades, que el riesgo derivado del uso de inteligencia artificial fue gobernado de manera efectiva en todas sus dimensiones.

CONCLUSIONES

PRIMERA. - El comercio electrónico contemporáneo se desarrolla en un ecosistema fragmentado en el que las decisiones que impactan al consumidor no dependen de un único sujeto, sino de una cadena en la que intervienen el operador del *e-commerce*, los proveedores tecnológicos, los proveedores de infraestructura en la nube, las plataformas intermediarias y, en su caso, otros actores especializados. Esta fragmentación condiciona de manera decisiva la atribución de responsabilidad por daños derivados del uso de sistemas de inteligencia artificial, pues quien sufre el daño rara vez puede identificar con claridad qué sujeto controlaba realmente el riesgo en el momento del incidente. La consecuencia es una tendencia natural a que la responsabilidad recaiga en el eslabón más visible para el consumidor, el operador del *e-commerce*, mientras los demás actores quedan al margen, a pesar de que en muchos casos sean ellos quienes efectivamente controlan el sistema.

SEGUNDA. - El marco normativo aplicable, a fecha de cierre de este trabajo, no resuelve esa fragmentación, sino que la presupone. La retirada formal de la propuesta de Directiva sobre responsabilidad por inteligencia artificial ha dejado un escenario en el que el régimen específico de responsabilidad por IA queda compuesto, en lo esencial, por el Reglamento (UE) 2024/1689, la Directiva (UE) 2024/2853 sobre productos defectuosos y los derechos nacionales no armonizados de cada Estado miembro. La Directiva (UE) 2024/2853 supone un avance considerable, en la medida en que amplía el concepto de producto al software y a los sistemas de IA, reconoce nuevos daños indemnizables y extiende el círculo de operadores responsables. Sin embargo, este avance no agota el problema. La nueva Directiva sigue articulada en torno a la idea de defecto del producto, lo que deja al margen de su régimen objetivo todos aquellos supuestos en los que el daño no deriva de un defecto en sentido estricto, sino de una decisión automatizada errónea, sesgada o discriminatoria que el sistema produce dentro de su funcionamiento normal. Para esos supuestos, que probablemente serán los más frecuentes en el comercio electrónico, el régimen aplicable seguirá siendo el de la responsabilidad civil general.

TERCERA. - En lo que respecta a la transposición al Derecho español de la Directiva (UE) 2024/2853, se ha defendido en este trabajo que resulta más coherente la opción de aprobar una norma especial e independiente que la opción continuista de reformar los artículos 128 a 149 del TRLGDCU. La razón es que el nuevo régimen ya no responde plenamente a la lógica clásica del Derecho de consumo, sino que se configura como una auténtica pieza del Derecho de daños, con un ámbito subjetivo que protege a cualquier persona física perjudicada y un ámbito objetivo que excede del esquema tradicional al incorporar software, archivos digitales, servicios conexos y nuevos operadores económicos. Forzar su encaje en el TRLGDCU generaría tensiones internas relevantes, especialmente en relación con la noción de consumidor manejada por el texto refundido, que en algunos supuestos comprende

también a personas jurídicas, frente al ámbito subjetivo más restringido de la nueva Directiva.

CUARTA. - Frente a este marco normativo incompleto, la diligencia del administrador adquiere una relevancia que el legislador no ha terminado de explicitar. La aplicación de los artículos 225 y 226 de la Ley de Sociedades de Capital al gobierno de los sistemas de inteligencia artificial obliga a concretar un estándar de diligencia específico, que en este trabajo se ha articulado en cinco fases: evaluación de riesgos previa con documentación mínima, revisión y monitorización proporcionadas al impacto del sistema, registro razonable de decisiones y auditoría de cambios, gestión ordenada de incidentes y control del *drift* y los sesgos a lo largo del tiempo. Estas cinco fases no constituyen una exigencia desproporcionada ajena al Derecho de sociedades, sino la traducción operativa de los requisitos que el propio artículo 226 LSC impone para que la decisión empresarial del administrador quede protegida por la regla de protección de la discrecionalidad empresarial.

QUINTA. - El problema probatorio ocupa un lugar central en este nuevo marco. La complejidad técnica, la opacidad de los modelos y la dependencia de actualizaciones controladas por terceros convierten la reconstrucción de los hechos en una tarea difícilmente abordable sin trazabilidad fáctica suficiente. A ello se suma que la retirada también ha eliminado los mecanismos armonizados de exhibición de pruebas y las presunciones de causalidad que la propuesta proyectaba. En consecuencia, los registros del sistema, los *logs*, las versiones desplegadas, las configuraciones aplicadas y la documentación de incidentes dejan de ser un elemento técnico secundario y se convierten en el soporte esencial sobre el que se sostiene tanto la posición probatoria del perjudicado como la defensa de la diligencia del administrador y de la empresa. Siendo la trazabilidad una cuestión jurídica de primer orden.

SEXTA. - El segundo eje del trabajo, el reparto contractual del riesgo con los proveedores tecnológicos, se ha revelado como una pieza inseparable de los anteriores. La diligencia hacia adentro de la sociedad y la disciplina contractual hacia afuera funcionan como dos planos complementarios del mismo modelo de gobierno del riesgo. La autonomía de la voluntad, dentro de los límites imperativos de la protección al consumidor, permite ordenar mediante cláusulas precisas el objeto contratado y los niveles de servicio, la cooperación técnica y probatoria del proveedor, la distribución interna de la responsabilidad satisfecha al perjudicado y la salida ordenada del contrato. Tras la mencionada retirada, el contrato adquiere además una función supletoria respecto de los mecanismos armonizados que esta hubiera incorporado, especialmente en materia de obtención y conservación de evidencias. Sin estas previsiones contractuales, la responsabilidad tiende a recaer en el operador del e-

commerce, mientras los proveedores tecnológicos, que en muchos casos controlan efectivamente el sistema, quedan al margen de la reclamación final.

SÉPTIMA. - La respuesta a la pregunta inicial del trabajo no se encuentra, en consecuencia, en un único sujeto ni en una única norma, sino en la combinación coherente de un marco normativo en evolución, de una diligencia del administrador adaptada a las particularidades de la inteligencia artificial y de un reparto contractual realista entre los distintos actores de la cadena. La consolidación de este modelo dependerá, en buena medida, del trabajo que en los próximos años desarrollen tanto la jurisprudencia, llamada a perfilar el contenido concreto de la diligencia exigible, como la práctica contractual, sobre la que recae hoy una parte sustancial del gobierno efectivo del riesgo. Mientras ese desarrollo se produce, el operador del *e-commerce* que aspire a una posición jurídica defendible deberá actuar en los dos planos analizados de forma simultánea, articulando hacia adentro de la sociedad los controles internos que le exige el régimen societario y hacia afuera el reparto contractual de riesgos con sus proveedores. Solo la coordinación efectiva de ambos planos permitirá responder, ante el consumidor perjudicado y ante el juez llamado a depurar responsabilidades, que el riesgo derivado del uso de inteligencia artificial fue gobernado de manera real y verificable en todas sus dimensiones.

BIBLIOGRAFÍA

AYO FERRÁNDIZ, Cristina; SEJO BAR, Álvaro; GARRE ANGUERA DE SOJO, Ignacio; GONZÁLEZ GUILLÉN, Pablo, “Responsabilidad civil e inteligencia artificial”, *Actualidad Jurídica Uría Menéndez*, n.º 67, mayo 2025, pp. 44-52.

BRAND, Joshua L. M., “Air Canada's *chatbot* illustrates persistent agency and responsibility gap problems for AI”, *AI & Society*, vol. 40, 2025, pp. 3361-3363.

BUITRAGO-RODRÍGUEZ, Mariana del Valle, “El comercio electrónico y la inteligencia artificial”, *Revista Gestión y Desarrollo Libre*, año 8, n.º 16, 2023, pp. 1-13. DOI: 10.18041/2539-3669/gestionlibre.16.2023.10490.

CASANOVA TORRADO, Miguel José, *La fundamentación de los fiduciary duties de los administradores de sociedades y sus consecuencias en la acción social de responsabilidad*, tesis doctoral, Universidad de Navarra, Pamplona, 2012.

CORONADO GARCÍA, Beatriz, *Despliegue y puesta en funcionamiento de componentes software. UF1291*, 1.ª ed., Editorial Tutor Formación, La Rioja, 2025.

CORONADO GARCÍA, Beatriz, *Implantación de aplicaciones web en entornos internet, intranet y extranet. MF0493*, 1.ª ed., Editorial Tutor Formación, Logroño, 2024.

DE LA VEGA GARCÍA, Fernando, “Directiva (UE) 2024/2853, del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y que deroga la Directiva 85/374/CEE”, *Ars Iuris Salmanticensis*, vol. 13, 2025, pp. 306-311.

DONADO VARA, Alejandro; JIMÉNEZ MUÑOZ, Francisco Javier (coords.), *La responsabilidad civil de la IA*, 1.ª ed., Dykinson, Madrid, 2024.

“Economía española: nuevos retos”, *Cuadernos de Información Económica*, n.º 250, enero-febrero 2016, Funcas.

FARIÑAS DULCE, María José; OLIVA MARTÍNEZ, José Daniel; PÉREZ MACÍAS, Iván Antonio, *Los retos normativos de la inteligencia artificial*, 1.ª ed., Dykinson, Madrid, 2024.

GÁLVEZ JIMÉNEZ, Aixa, *El delito de administración desleal (artículo 252 del Código Penal) en el ámbito de las sociedades de capital*, Dykinson, Madrid, 2019.

GARCÍA CORREAS, Javier, “La nueva Directiva (UE) 2024/2853: redefiniendo la responsabilidad por producto defectuoso en la era de la Salud digital”, en prensa, 2025.

GARCÍA GINÉ, Joan, “Efectos legales del tamaño de la empresa”, *Revista de Contabilidad y Tributación. CEF*, n.º 357, 2012, pp. 137-194.

GÓMEZ LIGÜERRE, Carlos, “Responsabilidad por daños causados por la inteligencia artificial”, *InDret*, n.º 1/2025, 2025.

GONZÁLEZ AROCHA, Jorge, “Fenomenología crítica del prompting en la inteligencia artificial”, *Sophia. Colección de Filosofía de la Educación*, n.º 39, 2025, pp. 141-165. DOI: 10.17163/soph.n39.2025.04.

GONZÁLEZ CABRERA, Inmaculada, “El impacto en el TRLGDCU de la Directiva (UE) 2024/2853 sobre responsabilidad civil por daños causados por productos defectuosos”, en prensa, 2025, pp. 138-181 y 306-307.

HERNÁNDEZ MARTÍNEZ, William David, “Los supuestos de aplicación del administrador de hecho: un análisis del caso español a propósito de la sociedad por acciones simplificada”, *Estudios Socio-Jurídicos*, vol. 14, n.º 2, 2012, pp. 2-3.

HERNÁNDEZ RAMOS, Eva María, *Manual del comercio electrónico: técnicas, modelos, normativa y casos prácticos*, Marge Books, Barcelona, 2018.

HERRERA DE LAS HERAS, Ramón, *Aspectos legales de la inteligencia artificial: personalidad jurídica de los robots, protección de datos y responsabilidad civil*, 1.ª ed., Dykinson, Madrid, 2020.

HUANG, Weijiao; HEW, Khe Foon; FRYER, Luke K., “Chatbots for language learning—Are they really useful? A systematic review of *chatbot*-supported language learning”, *Journal of Computer Assisted Learning*, vol. 38, n.º 1, 2022, pp. 1-21. DOI: 10.1111/jcal.12610.

JIANG, Xun et al., “Long Term Memory: The Foundation of AI Self-Evolution”, *arXiv*, 2025, *arXiv*:2410.15665v4.

JORQUI AZOFRA, María, *Responsabilidad por los daños causados por productos y sistemas de inteligencia artificial*, 1.ª ed., Dykinson, Madrid, 2023.

KOPALLE, Praveen K.; PAUWELS, Koen; AKELLA, Laxminarayana Yashaswy; GANGWAR, Manish, “Dynamic pricing: Definition, implications for managers, and future research directions”, *Journal of Retailing*, vol. 99, 2023, pp. 580-593.

LÓPEZ-AMO SAINZ, Ángel Pablo, *La Ley de la Inteligencia Artificial. Parte I*, 1.^a ed., RAMA Editorial, Madrid, 2024.

MARTÍN CASALS, Miquel, “Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial”, *InDret*, n.º 3, 2023, pp. 71-74.

MATECAS, Alexandru-Raul; KIESEBERG, Peter; TJOA, Simon, “Social Engineering with AI”, *Future Internet*, vol. 17, n.º 11, 2025, art. 515, pp. 23-25.

MONTERO MOUZO, David; PIÑERO ESCUER, Pedro J.; MANZANARES LÓPEZ, Pilar; MUÑOZ GEA, Juan P., *Monitorización de contratos Service Level Agreement en un entorno de negocio inter-ISP*, comunicación en las Jornadas TELECOM I+D, Universidad Politécnica de Cartagena (ETSIT), 2005, pp. 124–126.

NOWAK, Marcin; PAWLOWSKA-NOWAK, Marta, “Dynamic Pricing Method in the E-Commerce Industry Using Machine Learning”, *Applied Sciences*, vol. 14, 2024, art. 11668. DOI: 10.3390/app142411668.

OJEDA TACORONTE, Carlos José (coord.), *Una mirada jurídica poliédrica a la normativa europea sobre inteligencia artificial*, 1.^a ed., Dykinson, Madrid, 2025.

PARRA SEPÚLVEDA, Darío; CONCHA MACHUCA, Ricardo, “La inteligencia artificial explicable como fundamento para su gobernanza: implicancias en la responsabilidad civil”, *Revista Chilena de Derecho y Tecnología*, vol. 14, 2025, e74040.

PEÑA GONZÁLEZ, Zucel; TRUJILLO CASAÑOLA, Yaimí, “Mapas de calor en sitios web”, *Serie Científica de la Universidad de las Ciencias Informáticas*, vol. 12, n.º 9, 2019, pp. 99-101.

PÉREZ GARCÍA, Máximo Juan, “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*, n.º 3/2025, 2025, pp. 210-231.

RIVERO ORTEGA, Ricardo, *Derecho e inteligencia artificial*, 1.^a ed., Ediciones Olejnik, Argentina, 2023.

ROJAS GARCÍA, José Antonio; MOORE TORRES, Rosa Karol, *Emprendimiento digital: herramientas y metodologías aplicadas para pymes*, 1.^a ed., Universidad Peruana de Ciencias Aplicadas (UPC), Lima, 2024.

RUSSELL, Stuart; NORVIG, Peter, *Artificial Intelligence: A Modern Approach*, Global Edition, 4.^a ed., Pearson Education, Limited, 2021.

SANCHO LÓPEZ, Marina, “Cumplimiento normativo en la era de la inteligencia artificial: Directiva (UE) 2024/2853 sobre productos defectuosos y la responsabilidad de bienes intangibles y servicios digitales”, *Actualidad Jurídica Iberoamericana*, n.º 24, 2026, pp. 184-214.

SERRANO SEGARRA, María, *Derecho de Sociedades Mercantiles (Segunda Parte)*, Universidad Miguel Hernández de Elche, 2024.

SUAVE, André Augusto, *Inteligência Artificial*, 1.^a ed., Freitas Bastos, 2024 (consultado en ProQuest Ebook Central, UAB).

TORRES MANRIQUE, Jorge Isaac; RIBEIRO BRASIL, Deilton, *Inteligencia artificial: omnipresencia, nuevas tendencias e interdisciplinariedad*, 1.^a ed., J.M. Bosch Editor, 2023.

TROYA TERRANOVA, Tayron Cesar, “Aplicación de la Inteligencia Artificial en la Dirección de Ventas para la Predicción del Comportamiento del Cliente: Revisión Bibliográfica (2020-2025)”, *Sinergia Académica*, vol. 8, n.º 7, 2025, pp. 694-708.

Legislación

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 se modifican determinados actos legislativos de la Unión.

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).

Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo.

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

Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.

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.

Jurisprudencia

Moffatt v. Air Canada, 2024 BCCRT 149, Civil Resolution Tribunal of British Columbia, febrero de 2024.