Facultad de Derecho

ICADE

DESAFÍOS REGULATORIOS DE LA ERA DIGITAL
UN ANÁLISIS COMPARADO

Autor: Begoña Astarloa Domínguez

Tutor: Luis Bueno Ochoa

MADRID | Junio 2026

Resumen

El desarrollo acelerado de la inteligencia artificial ha situado al ordenamiento jurídico ante el reto de garantizar que el avance tecnológico no se produzca a costa de los derechos y bienes jurídicos que los sistemas normativos han tardado décadas en consolidar. Desde una perspectiva de derecho comparado, este trabajo analiza las respuestas que la Unión Europea y Estados Unidos han articulado frente a este reto en dos ámbitos en los que el uso intensivo de datos genera conflictos de especial intensidad: la protección de la privacidad y los datos personales, y la propiedad intelectual. La hipótesis de partida es que las divergencias entre ambos sistemas no responden a diferencias técnicas o institucionales, sino a perspectivas regulatorias distintas sobre la relación entre mercado, tecnología y derechos individuales, y que ninguno de los dos modelos ha logrado hasta la fecha un equilibrio estable entre el fomento de la innovación y la protección efectiva de los derechos que esa innovación pone en riesgo.

Palabras clave

Inteligencia artificial, protección de datos, propiedad intelectual, derecho comparado, Efecto Bruselas.

Abstract

The rapid development of artificial intelligence has confronted legal systems with the challenge of ensuring that technological progress does not come at the expense of the rights and legal interests that normative frameworks have taken decades to consolidate. From a comparative law perspective, this paper examines the responses that the European Union and the United States have developed in two areas where the intensive use of data generates especially acute legal conflicts: the protection of privacy and personal data, and intellectual property. The working hypothesis is that the divergences between the two systems do not reflect differences in technical or institutional design, but structurally distinct governance philosophies regarding the relationship between markets, technology and individual rights, and that neither model has yet achieved a stable equilibrium between fostering innovation and effectively protecting the rights that innovation puts at risk.

Keywords

Artificial intelligence, personal data protection, intellectual property, comparative law, Brussels Effect.

Abreviaturas

AI Act: Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial.

ASA: Australian Society of Authors

CEDH: Convenio Europeo de Derechos Humanos

CDFUE: Carta de los Derechos Fundamentales de la Unión Europea

COPPA: Children's Online Privacy Protection Act

CCPA: California Consumer Privacy Act

CPRA: California Privacy Rights Act

DOUE: Diario Oficial de la Unión Europea

DPC: Data Protection Commission

DSM: Directiva sobre derechos de autor en el mercado único digital (Digital Single Market) (Directiva (UE) 2019/790)

EE. UU.: Estados Unidos

FCRA: Fair Credit Reporting Act

FTC: Federal Trade Commission

GDPR: General Data Protection Regulation *(*forma anglosajona del RGPD, usada en algunas citas)

HAI: Human-Centered Artificial Intelligence

HIPAA: Health Insurance Portability and Accountability Act

IA: Inteligencia artificial

LLM/LLMs: Large Language Model/s (modelo/s de lenguaje de gran escala)

RGPD: Reglamento General de Protección de Datos

TDM: Text and Data Mining

TFUE: Tratado de Funcionamiento de la Unión Europea

UE: Unión Europea

USCO: United States Copyright Office

Tabla de contenido

Introducción

La inteligencia artificial (en adelante IA) se ha consolidado en los últimos años como la tecnología más transformadora de nuestra era, con una capacidad de impacto que alcanza simultáneamente la economía, la comunicación, la cultura y las relaciones sociales. Su desarrollo acelerado plantea al ordenamiento jurídico una pregunta que no admite respuesta sencilla: cómo garantizar que el avance tecnológico no se produzca a costa de los derechos y bienes jurídicos que los sistemas normativos han tardado décadas en construir y consolidar.

Esta pregunta no recibe una respuesta uniforme. Ante unos mismos fenómenos tecnológicos, la Unión Europea y Estados Unidos han adoptado enfoques regulatorios profundamente distintos, y esa divergencia no es casual ni coyuntural. Refleja concepciones de fondo sobre la relación entre el mercado, la tecnología y los derechos individuales que preceden a la era digital y que se proyectan ahora, con consecuencias concretas y medibles, sobre los conflictos jurídicos que la inteligencia artificial genera. La pregunta que vertebra este trabajo es, precisamente, la siguiente: ¿Cómo están respondiendo los ordenamientos jurídicos de la Unión Europea y de Estados Unidos a los desafíos regulatorios que plantea el desarrollo de la IA en materia de protección de datos personales y propiedad intelectual, y en qué medida sus respuestas reflejan filosofías de gobernanza diferentes sobre la relación entre mercado, tecnología y derechos individuales?

Objetivos

La hipótesis que orienta este trabajo es que las diferencias observadas entre el ordenamiento jurídico de la Unión Europea y el de Estados Unidos en materia de protección de datos personales y propiedad intelectual no responden a divergencias técnicas o institucionales sino a filosofías de gobernanza estructuralmente distintas sobre la relación entre mercado, tecnología y derechos individuales, y que ninguno de los dos modelos ha logrado hasta la fecha un equilibrio estable entre el fomento de la innovación tecnológica y la protección efectiva de los derechos que esa innovación pone en riesgo.

El objetivo general de este trabajo es analizar de forma comparada como responden el ordenamiento jurídico de la Unión Europea y el de Estados Unidos ante los desafíos regulatorios que plantea el desarrollo de la IA, con particular atención a los conflictos que genera el uso intensivo de datos en dos ámbitos jurídicos específicos: la protección de la privacidad y datos personales, y la propiedad intelectual.

Para alcanzar este objetivo general, el trabajo se articula en torno a tres objetivos específicos. El primero es establecer un marco conceptual que permita comprender por qué la IA plantea dificultades regulatorias específicas, atendiendo tanto a las características propias de esta tecnología como a las limitaciones estructurales de los modelos de regulación ex ante y ex post, y justificar el interés del enfoque comparado desde una perspectiva filosófico-jurídica. El segundo es identificar y analizar las diferencias entre ambos ordenamientos en materia de protección de datos personales, examinando el fundamento, los principios rectores y la efectividad real de cada modelo. El tercero es analizar comparativamente el tratamiento jurídico del entrenamiento de modelos de IA con obras protegidas, valorando los mecanismos que cada sistema ofrece para superar la infracción prima facie y las tensiones que generan entre innovación y protección de derechos de autor.

Metodología

El presente trabajo adopta un enfoque jurídico-doctrinal articulado a través del método del derecho comparado. El análisis se sustenta en el estudio de las fuentes normativas primarias vigentes en cada jurisdicción, en particular el Reglamento General de Protección de Datos, el Reglamento de Inteligencia Artificial y la Directiva sobre derechos de autor en el mercado único digital en el ámbito europeo, y la doctrina del *fair use*, la FTC Act y la normativa sectorial de privacidad en el ámbito americano. El estudio de la legislación se complementa con el análisis de jurisprudencia relevante, especialmente la doctrina emergente de los tribunales americanos en materia de entrenamiento de IA y *fair use*, y con el apoyo en literatura académica especializada procedente de revistas jurídicas de referencia en ambas jurisdicciones.

La estructura del trabajo sigue el modelo propio de los artículos científicos en ciencias sociales. Cada uno de los dos capítulos sustantivos se organiza en un apartado de resultados, en el que se identifican y sistematizan las principales diferencias entre ambos

ordenamientos a través de tablas comparativas y un apartado de discusión, en el que se analizan esas diferencias, se valoran sus implicaciones y se contrasta con la doctrina académica relevante. El trabajo se cierra con unas conclusiones numeradas que sintetizan los hallazgos del análisis comparado.

CAPÍTULO 1: El derecho ante las tecnologías disruptivas

El presente capítulo tiene por objeto establecer el marco conceptual sobre el que se asienta el análisis comparado que desarrollan los capítulos siguientes. Con ese fin, se abordan cuatro cuestiones sucesivas y encadenadas. En primer lugar, se examina el fenómeno de las tecnologías disruptivas y el papel paradigmático que ocupa la inteligencia artificial en el contexto tecnológico actual. A continuación, se analizan las dificultades estructurales que el cambio tecnológico plantea al ordenamiento jurídico, tanto desde la perspectiva de la regulación ex ante como desde los mecanismos de respuesta ex post. En tercer lugar, se identifica el dato como elemento central a través del cual el desarrollo de la IA genera sus principales impactos jurídicos. Por último, se justifica el interés del enfoque comparado entre la Unión Europea y Estados Unidos como marco metodológico para el análisis de estos conflictos.

1.1 Tecnologías disruptivas y transformación del entorno digital

Los primeros planteamientos en torno a la posibilidad de desarrollar máquinas capaces de realizar tareas propias de la inteligencia humana pueden situarse en los trabajos pioneros de Alan Turing en la década de 1950, quien abrió el debate sobre si las maquinas podían pensar y comportarse de manera inteligente[1]. No obstante, fue John McCarthy quien, algunos años más tarde, acuñó el término "inteligencia artificial" y lo definió como "la ciencia y la ingeniería orientadas a la creación de máquinas inteligentes, en especial programas informáticos inteligentes"[2], sentando así las bases conceptuales de esta disciplina. El propio McCarthy recurría a una cita de T.H. Huxley para ilustrar el alcance transformador que podría llegar a tener: "*Extinguished philosophies lie about the cradle of every science as the strangled snakes besides that of Hercules*."[3][4] Y es que la imagen

[1] A. M. Turing, *Computing Machinery and Intelligence*, 59 MIND 433, 442 (1950).
[2] McCarthy, J., "What Is Artificial Intelligence?", Stanford University, 2007.
[3] *Ibid*, p.1.
[4] "Las filosofías extintas yacen alrededor de la cuna de toda ciencia como las serpientes estranguladas junto a la de Hércules".

escogida ejemplifica la capacidad potencial que tiene la IA, como innovación científica, de acabar con paradigmas consolidados, como Hércules con las serpientes, y alumbrar una nueva era de pensamiento y transformación de las categorías sobre las que se asienta el conocimiento. Desde entonces, y de manera especialmente intensa en los últimos años, la IA ha experimentado un desarrollo acelerado, impulsado por el avance de la capacidad computacional y por la disponibilidad de grandes volúmenes de datos. En su estado actual, estos sistemas son capaces, entre otras funciones, de analizar y procesar información a gran escala, aprender de forma autónoma a partir de datos, automatizar procesos complejos, generar contenidos, realizar predicciones y tomar decisiones con un grado creciente de autonomía. Cada vez más rápido, la IA va consolidando su presencia en nuevos sectores y se integra cada vez más en la vida cotidiana, una tendencia que con gran seguridad continuará en el futuro, hasta alcanzar nuevos límites que puede que no seamos capaces ni de imaginar[5], y revolucionando e incluso creando nuevos sectores.

En 1997, Clayton Christensen introduce por primera vez el término "innovación disruptiva" para describir aquellos procesos de innovación que no se limitan a mejorar productos o servicios existentes, sino que alteran de manera profunda los modelos tradicionales sobre los que se asientan determinados sectores[6]. Las innovaciones disruptivas, generan una ruptura de las estructuras previas, desplazando practicas consolidadas y obligando a replantear las reglas del sistema. Este concepto, fue formulado inicialmente en un contexto empresarial, sin embargo, su utilidad transciende dicho contexto y resulta especialmente relevante para comprender el impacto de determinadas tecnologías en el ordenamiento jurídico. En efecto, cuando una innovación altera de forma sustancial los modelos sociales, económicos o comunicativos, el Derecho, como sistema normativo diseñado para ofrecer estabilidad y seguridad jurídica, se ve necesariamente afectado.

Este nuevo escenario tecnológico, marcado por el uso intensivo de datos y la automatización de procesos, evidencia un desfase entre la rapidez de la innovación y la capacidad de adaptación del Derecho, sobre todo a la hora de establecer un orden que permita mantener el desarrollo de estas tecnologías, sin poner en riesgo derechos fundamentales y bienes jurídicos consolidados. Se plantea entonces la necesidad de

[5] Kelly, K., "The Future of Artificial Intelligence", *Wired*, 27 de octubre de 2014.
[6] Christensen, C. M., Raynor, M. and McDonald, R. (2015). 'What is disruptive innovation?'. *Harvard Business Review,* 93, 44–53.

examinar como los ordenamientos jurídicos están respondiendo, o tratando de responder a los desafíos regulatorios derivados de las tecnologías disruptivas. Y es que, y como explica Bennett, la dificultad de adaptar los marcos regulatorios a las circunstancias cambiantes suele representarse con la imagen del Derecho perdiendo una carrera[7].

1.2 Dificultad de adaptación del Derecho al cambio tecnológico

En este contexto de rápido avance tecnológico, incluso los grandes magnates de la industria han llegado a mostrarse preocupados por cómo se puede articular legalmente este proceso y cual ha de ser el nivel de injerencia regulatoria del Estado. El propio Elon Musk, en una entrevista ante el AeroAstro Simposio del MIT en el 2014, mostró abiertamente su preocupación por la falta de regulación de la inteligencia artificial: "sin una estricta regulación y cuidado, el desarrollo de la inteligencia artificial podría convertirse en algo incontrolable (…) con la inteligencia artificial, es como invocar al demonio."[8]

Más allá de estas advertencias procedentes del ámbito tecnológico y empresarial, la preocupación por los efectos del desarrollo tecnológico ha sido asumida también desde el plano jurídico y teórico. En efecto, el avance de las tecnologías como la IA no solo plantea interrogantes sobre el alcance de la intervención regulatoria del Estado, sino que interpela directamente a los juristas, filósofos y teóricos del Derecho, llamados a reflexionar de manera crítica sobre las implicaciones jurídicas de estos procesos. En este sentido, se ha puesto de relieve la necesidad de desarrollar una auténtica "conciencia tecnológica", en términos formulados por Vittorio Frosini, entendida como una actitud reflexiva, crítica y responsable frente a los nuevos problemas que la tecnología suscita en las distintas áreas del acontecer social, y ante los cuales ni el Derecho ni quienes lo aplican o estudian pueden permanecer ajenos[9].

La IA presenta dificultades específicas desde un punto de vista regulatorio, especialmente si se compara con otras fuentes de riesgo público tradicionalmente abordadas por el

---

[7] Lyria Bennett, *Agents of Change. How the Law 'Copes? With Technological Change*, Griffith Law Review 20, 763 (2014), p 1.
[8] Aileen Graef, *Elon Musk: We Are "Summoning a Demon" with Artificial Intelligence*, UPI (Oct. 27, 2014, 7:50 AM), http://www.upi.com/Business_News/2014/10/27/Elon- Musk-We-are-summoning-a-demon-with-artificial-intelligence/4191414407652/ [https://perma.cc/M98J-VYNH].
[9] Pérez Luño, A. E., "El Derecho ante las nuevas tecnologías", *El Notario del Siglo XXI*, n.º 41, 2012, p. 1.

Derecho. Tal y como se ha señalado desde la doctrina, la complejidad, opacidad y capacidad evolutiva de estos sistemas hacen que su regulación resulte particularmente problemática, al no ajustarse fácilmente a los esquemas normativos clásicos[10]. Esta dificultad, no deriva únicamente de la novedad tecnológica, sino de las características propias de la IA como tecnología disruptiva, capaz de desarrollarse y desplegarse de forma dinámica, con efectos potenciales que no siempre son plenamente previsibles en el momento de su diseño o implementación[11]. Ello obliga a reflexionar sobre el modo en que el Derecho puede y debe intervenir frente a este tipo de fenómenos.

Para comprender esta problemática, resulta fundamental atender a las dimensiones temporales del fenómeno normativo. En el ámbito jurídico, la creación de normas puede distinguirse, en función del momento en que se produce la intervención regulatoria, entre una regulación ex ante y una regulación ex post. En este sentido, Marie-Anne Frison-Roche desarrolla conceptualmente ambos modelos regulatorios:

> El ex ante es la intervención sobre un fenómeno antes de que éste se cristalice, mientras que el ex post es la intervención sobre un fenómeno después de su advenimiento. El ex ante manifiesta la voluntad normativa, el post manifiesta la reacción. El ex ante toma como principio el gobierno de las acciones, el ex post toma como principio la libertad de las acciones[12].

Esta distinción resulta especialmente relevante en el contexto de las tecnologías disruptivas, donde el legislador se enfrenta al dilema de anticipar los riesgos antes de que se materialicen o de reaccionar una vez los daños ya se han producido.

Por un lado, la regulación ex ante de la IA plantea importantes dificultades derivadas de las propias características del proceso de desarrollo de esta tecnología. En este sentido, Matthew U. Scherer ha señalado que el desarrollo de la IA se caracteriza por ser discreto, difuso, no continuo y opaco, lo que complica de manera significativa cualquier intento de anticipación normativa. Es discreto en la medida en que puede llevarse a cabo sin necesidad de grandes infraestructuras ni de una visibilidad pública evidente, permitiendo

[10] Scherer, M. U., "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies", *Harvard Journal of Law & Technology*, vol. 29, n. º 2, 2016, p. 362.
[11] *Id.*
[12] Frison-Roche, M. A., "Ex ante – ex post, justificación de un derecho propio y específico de la regulación", *Responsabilidad Civil y Seguros*, año XI, n.º 10, octubre de 2010, p. 5.

que avances relevantes se produzcan sin ser fácilmente detectables por reguladores. Es difuso porque los equipos de desarrollo suelen estar distribuidos geográficamente, con individuos situados en distintos países y jurisdicciones, lo que introduce problemas de fragmentación normativa y de coordinación regulatoria a escala global. Asimismo, es no continuo, ya que los elementos de desarrollo pueden realizarse de forma independiente y no necesariamente sincronizada, avanzando en paralelo sin una coordinación temporal estricta. Finalmente, el proceso resulta opaco, dado que el desarrollo de sistemas de IA suele mantenerse deliberadamente protegido y oculto, en un contexto de competencia en el que el conocimiento y los avances constituyen una ventaja estratégica[13].

La concurrencia de estas características genera para los legisladores dificultades que no son únicamente jurídicas, sino también de carácter práctico y casi logístico, al dificultar la identificación temprana de riesgos y la delimitación de un marco normativo preventivo eficaz. En un escenario en el que los potenciales efectos de la IA son, en muchos casos, inciertos o difícilmente previsibles, la regulación ex ante se enfrenta al riesgo de resultar incompleta, desfasada o inadecuada frente a problemas que aún no han llegado a manifestarse plenamente.

Por otro lado, frente a las limitaciones de la regulación ex ante, Scherer plantea que la respuesta ex post se articula principalmente a través de mecanismos del derecho de la responsabilidad por daños. No obstante, la aplicación de estos principios clásicos a los sistemas de IA presenta importantes dificultades. Las características propias de la IA tensionan elementos esenciales de la responsabilidad civil, en particular la previsibilidad del daño, la determinación de la causalidad y la identificación del sujeto responsable. La autonomía funcional y el comportamiento parcialmente imprevisible de estos sistemas dificultan la valoración de la previsibilidad del daño, mientras que su complejidad técnica complica la identificación de la causa jurídica del perjuicio, al no resultar siempre claro si esta deriva del diseño del sistema, de su entrenamiento con determinados datos o de decisiones adoptadas de manera autónoma. A ello se añade la insuficiencia o pérdida de control humano efectivo, lo que plantea serias dudas sobre quien debe responder jurídicamente por los daños causados.[14]

---

[13] Scherer, M. U., "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies", *Harvard Journal of Law & Technology*, vol. 29, n. º 2, 2016, p. 362.
[14] *Ibid*., p. 388.

Estas dificultades se ven agravadas por el carácter reactivo del Derecho de daños, que interviene cuando el perjuicio ya se ha producido. En el ámbito del tratamiento de datos, esta lógica resulta especialmente problemática, pues una vez que la información personal ha sido recopilada, procesada o difundida indebidamente, por ejemplo, mediante sistemas de perfilado algorítmico o filtraciones masivas, la pérdida de control sobre los datos y la afectación a la privacidad son en gran medida, irreversibles[15]. Por último, el enfoque judicial centrado en litigios individuales y daños concretos puede conducir a una respuesta fragmentaria, en la que se sobre regular usos visibles de la inteligencia artificial, mientras que otros riesgos más difusos, pero potencialmente más graves, permanecen insuficientemente abordados.[16]

En conjunto, las limitaciones tanto de la regulación ex ante como de los mecanismos ex post ponen de manifiesto que el Derecho se enfrenta a dificultades estructurales para responder de forma eficaz a los retos planteados por la IA u otras tecnologías disruptivas. Estas dificultades no se proyectan de manera abstracta, sino que se concretan especialmente en aquellos ámbitos en los que el funcionamiento de estas tecnologías descansa sobre el uso intensivo y masivo de datos. Precisamente esta centralidad del dato explica que los principales impactos jurídicos del desarrollo de la IA se manifiesten con especial intensidad en la protección de los derechos fundamentales, y en la salvaguarda de bienes jurídicos tradicionales, cuestiones que se analizan en el apartado siguiente.

1.3 El uso intensivo de datos en la inteligencia artificial y su impacto jurídico

La IA no constituye un fenómeno jurídicamente problemático en abstracto. Uno de sus principales impactos sobre el ordenamiento jurídico y el que será objeto de nuestro análisis, se produce a través de un elemento concreto y específico: la necesidad de obtener y tratar datos a una escala sin precedentes históricos. A diferencia de los sistemas informáticos tradicionales, los modelos de IA no ejecutan instrucciones predefinidas, sino que aprenden a partir de grandes volúmenes de información que les permiten identificar patrones, establecer correlaciones y generar resultados de manera autónoma. Es precisamente esta dependencia estructural del dato la que convierte el desarrollo de la IA en un fenómeno con consecuencias jurídicas directas e inevitables: no es posible

[15] *Ibid*., p. 390.
[16] *Ibid*., p. 392.

desarrollar estos sistemas sin obtener información, y no es posible obtener información a esta escala sin entrar en tensión con los marcos normativos existentes.

Tanto la recopilación de datos necesaria para el entrenamiento de modelos de IA como la posterior producción, tratamiento y reutilización de información en su funcionamiento ordinario generan una serie de dilemas jurídicos específicos que trascienden el ámbito meramente técnico. En efecto, el uso intensivo de datos en el desarrollo de estas tecnologías plantea interrogantes relevantes sobre la licitud de su obtención, las condiciones de su tratamiento y los límites de su utilización, cuestiones que afectan directamente a distintos niveles de protección jurídica.

En primer lugar, estos procesos inciden de manera directa en el derecho a la privacidad y en la protección de los datos personales, en la medida en que el entrenamiento y funcionamiento de sistemas de IA se basa frecuentemente en el tratamiento masivo de información vinculada a personas físicas, lo que puede entrar en tensión con los principios de control, transparencia y minimización que caracterizan este derecho fundamental. En segundo término, la utilización de datos y contenidos preexistentes como insumo para el entrenamiento de modelos plantea problemas relevantes en relación con la propiedad intelectual, al cuestionar los límites del uso legítimo de obras protegidas y la adecuación de las categorías jurídicas tradicionales frente a nuevas formas de explotación informacional. Son precisamente estos dos planos de conflicto los que estructuran el análisis comparado que desarrollamos en los capítulos siguientes.

1.4 El interés del análisis comparado en la regulación de tecnologías disruptivas

Los desafíos regulatorios que plantea el desarrollo de la IA no reciben respuestas distintas en la Unión Europea y en Estados Unidos por razones de capacidad legislativa ni por diferencias de grado en la percepción del riesgo tecnológico. La divergencia es de naturaleza más profunda: refleja filosofías de gobernanza fundamentalmente distintas sobre la relación entre el individuo, el mercado y el Estado, que preceden a la era digital y que se proyectan ahora sobre los nuevos problemas que plantea la tecnología. La Unión Europea parte de una concepción centrada en el ser humano y los derechos

fundamentales[17], que antepone transparencia, la rendición de cuentas y la protección del ciudadano por encima de la velocidad de la innovación, bajo la premisa de que la confianza pública solo puede construirse sobre una regulación estricta que garantice la seguridad y la ética desde el diseño[18]. Estados Unidos, en cambio, construye su respuesta desde una filosofía orientada al mercado y a la innovación, que confía en la autorregulación de la industria y en marcos de cumplimiento frecuentemente voluntarios, bajo la premisa de que evitar cargas regulatorias excesivas es condición necesaria para preservar el dinamismo tecnológico[19]. No se trata, por tanto, de dos respuestas distintas a un mismo problema, sino de dos problemas distintos planteados desde concepciones jurídicas irreconciliables.

Esta oposición adquiere una dimensión especialmente significativa si se atiende al peso global de cada uno de estos bloques. La Unión Europea es el principal referente mundial en materia de regulación tecnológica: ninguna otra jurisdicción ha producido un marco normativo de la densidad, coherencia y alcance extraterritorial del RGPD o del Reglamento de Inteligencia Artificial. Estados Unidos, por su parte, es el epicentro indiscutible de la innovación tecnológica global: las empresas que han definido arquitectura de la economía digital, y que hoy lideran el desarrollo de los modelos de IA más avanzados, son en su gran mayoría americanas. Nos encontramos, en definitiva, ante el mayor regulador del mundo frente al mayor innovador del mundo[20], lo que convierte su comparación no en un ejercicio académico sino en el análisis de la tensión que vertebra el debate jurídico-tecnológico de nuestro tiempo. El análisis comparado de estos dos modelos no persigue determinar cuál es superior, sino identificar que tensiones genera cada uno, que bienes jurídicos prioriza y a que costes. Es precisamente desde esa perspectiva crítica desde la que se abordan, en los capítulos siguientes, los dos conflictos jurídicos que el uso intensivo de datos plantea con mayor intensidad: la protección de la privacidad y la salvaguarda de la propiedad intelectual.

[17] Ijaiya, H. y Odumuwagun, O. O., "Advancing artificial intelligence and safeguarding data privacy: a comparative study of EU and US regulatory frameworks amid emerging cyber threats", *International Journal of Research Publication and Reviews*, vol. 5, n. º 12, 2024, p. 3366.
[18] *Ibid*., p. 3361.
[19] Kumari, P., "Legal frameworks for AI regulation: a comparative study", *Advances in Consumer Research*, vol. 2, n. º 2, 2025, p. 219.
[20] Bradford, A., "The false choice between digital regulation and innovation", *Northwestern University Law Review*, vol. 119, 2024, p. 381.

CAPÍTULO 2: Protección de la privacidad y de los datos personales

El presente capítulo analiza el primero de los dos conflictos jurídicos que el uso intensivo de datos plantea en el contexto del desarrollo de la inteligencia artificial: la protección de la privacidad y los datos personales. Para ello, se parte de la constatación de que la Unión Europea y Estados Unidos han construido respuestas normativas que no solo difieren en sus soluciones técnicas, sino en las premisas filosóficas sobre las que se asientan. El capítulo se organiza en tres bloques. En primer lugar, se sistematizan las principales diferencias entre ambos ordenamientos a través de tablas comparativas que cubren la arquitectura y fundamento del sistema, los principios rectores del tratamiento y la efectividad real de cada modelo. A continuación, se analiza el significado y las implicaciones de esas diferencias, prestando especial atención a las dos filosofías regulatorias que las explican, al fenómeno del efecto Bruselas como mecanismo de proyección global del modelo europeo, y a la comparación entre los sistemas de garantía y sanción de cada ordenamiento. El capítulo concluye con un párrafo de transición hacia el segundo eje del análisis comparado.

2.1 El dato personal como primer frente de conflicto

El capítulo anterior puso de manifiesto que el desarrollo de la IA descansa de forma estructural sobre la obtención y el tratamiento masivo de datos. Cuando esos datos están vinculados a personas físicas, el conflicto jurídico adquiere su dimensión más inmediata: el mismo proceso que alimenta los modelos algorítmicos opera sobre información que los ordenamientos jurídicos han decidido proteger como expresión de la dignidad y la autonomía individual. La privacidad y la protección de datos personales constituyen así el primer frente en el que el desarrollo tecnológico colisiona con los derechos fundamentales.

Sin embargo, como se anticipó en el capítulo 1, esta colisión no recibe una respuesta uniforme. La Unión Europea y Estados Unidos han construido marcos normativos que no solo difieren en sus soluciones técnicas, sino en las premisas filosóficas sobre las que se asientan. Analizar esta divergencia es el objeto de este capítulo, que se organiza en torno a tres ejes: la arquitectura y el fundamento del sistema de protección en cada ordenamiento, los principios que rigen el tratamiento de datos y su impacto específico en

el contexto de la IA, y la efectividad real de cada modelo a través de los derechos que reconoce a los individuos y del régimen sancionador que lo respalda.

2.2 Resultados

Los resultados del análisis comparado se presentan en las tres tablas siguientes.

2.2.1 Fundamento y arquitectura del sistema de protección

El primer bloque comparativo examina la estructura de base sobre la que cada ordenamiento construye la protección de datos personales: su naturaleza jurídica, la existencia o ausencia de un marco normativo general, el modelo regulatorio adoptado, su alcance territorial y la autoridad competente para su aplicación. En el caso europeo, el texto de referencia es el Reglamento (UE) 2016/679 (RGPD), en particular sus artículos 1, 3 y 51 a 59. En el caso americano, la comparación se articula a partir de la FTC Act y la legislación sectorial federal, con especial atención a la CCPA como referente estatal más desarrollado.

Tabla 1: Fundamentos jurídicos del sistema de protección de datos

Ítem	**Unión Europea**	**Estados Unidos**
Naturaleza jurídica del derecho	Derecho fundamental autónomo y explícito	Derecho implícito, de construcción jurisprudencial: sin reconocimiento constitucional expreso
Existencia de marco normativo general	Si: RGPD (2016/679) de aplicación directa y uniforme en todos los Estados miembros	No: ausencia de ley federal general, regulación sectorial y fragmentada (HIPAA, FCRA, COPPA, CCPA…)

Modelo regulatorio	Integral, horizontal y basado en derechos fundamentales	Sectorial, fraccionado y orientado al mercado (*notice and choice*)
Alcance territorial	Extraterritorial: se aplica a cualquier responsable que trate datos de personas en la UE, con independencia de su sede (art. 3 RGPD)	Territorial: alcance en materia de privacidad determinado en gran medida a nivel estatal, sin régimen general de aplicación extraterritorial
Autoridad de control	Autoridades independientes de protección de datos + Comité Europeo de Protección de Datos (CEPD)	Federal Trade Commission (FTC), sin mandato exclusivo ni específico en materia de privacidad.

2.2.2 Principios rectores del tratamiento

El segundo bloque examina las condiciones bajo las cuales cada ordenamiento permite el tratamiento de datos personales: los principios de licitud, la configuración del consentimiento y las obligaciones de minimización y limitación de finalidad. Los textos de referencia en el ámbito europeo son los artículos 5, 6 y 7 del RGPD. En el ámbito americano, la comparación toma como referencia la Section 5 de la FTC Act y el modelo del *notice and choice* predominante en la práctica regulatoria federal, así como las disposiciones relevantes de la CCPA.

Tabla 2: Principios rectores del tratamiento de datos personales

Ítem	**Unión Europea**	**Estados Unidos**

Principio de licitud	Tratamiento solo posible si existe base jurídica tasada (art. 6 RGPD)	Sin principio general equivalente, el tratamiento es lícito salvo práctica engañosa o desleal (FTC Act, s.5)
Consentimiento	Libre, específico, informado e inequívoco, revocable en cualquier momento (art 7 RGPD)	Modelo de *notice and choice*: basta con informar en la política de privacidad
Minimización y limitación de finalidad	Obligatorios: solo datos necesarios para fines determinados y explícitos (art 5 RGPD)	Sin obligación general equivalente a nivel federal.

2.2.3 Efectividad del sistema: derechos individuales y régimen sancionador

El tercer bloque analiza la efectividad real de cada sistema, atendiendo al catálogo de derechos reconocidos a los individuos, al régimen sancionador y al principio de accountability. Los textos de referencia europeos son los artículos 15 a 22, 83 y 5.2 y 24.1 del RGPD. En el ámbito americano, la comparación se articula nuevamente a partir de la FTC Act y la práctica de los *consent decrees* como principal mecanismo de garantía del cumplimiento.

Tabla 3: Derechos individuales, régimen sancionador y *accountability*

Ítem	**Unión Europea**	**Estados Unidos**
Catálogo de derechos del interesado	Amplio y uniforme: acceso, rectificación, supresión, portabilidad, oposición, y derecho a no ser objeto de decisiones	Derechos sectoriales o estatales, sin catálogo federal general ni

	automatizadas (arts. 15-22 RGPD)	equivalente al art. 22 RGPD.
Régimen sancionador	Multas de hasta 20M o el 4% de la facturación global anual (art. 83 RGPD): por ejemplo, la sanción de 1200M a Meta (2023)	Sanciones variables, acuerdos administrativos con la FTC (*consent decrees*) sin multa proporcional a la facturación global
Principio de accountability	Obligación estructural y proactiva: el responsable debe demostrar el cumplimiento, incluye evaluaciones de impacto (art. 5.2, 24.1 y 35 RGPD)	Sin principio estructural equivalente, cumplimiento esencialmente reactivo

2.3 Discusión

Los resultados obtenidos permiten ahora valorar el alcance y las implicaciones de las divergencias identificadas. El análisis se estructura en torno a tres planos: el filosófico, que examina los fundamentos que explican la distancia entre ambos modelos, el internacional, que atiende a como esa distancia se proyecta más allá de las fronteras de cada ordenamiento, y el práctico, que evalúa la capacidad real de cada sistema para garantizar la protección efectiva de los ciudadanos.

2.3.1. Dos filosofías regulatorias irreconciliables

La divergencia entre los sistemas de protección de datos de la Unión Europea y Estados Unidos no responde a una mera diferencia técnica o institucional, sino a una diferencia de fondo en el espíritu regulatorio de ambos ordenamientos. Cada sistema articula una respuesta distinta a una misma pregunta: ¿Cuál es la relación que debe existir entre el mercado, la tecnología y los derechos individuales? La UE parte de un modelo basado en

derechos fundamentales, mientras que EE.UU. construye su respuesta desde la lógica del mercado y la posición del individuo consumidor.

El derecho a la protección de datos en la Unión Europea encuentra su consagración en el artículo 8 de la Carta de los Derechos Fundamentales: "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"[21], y de forma paralela en el artículo 16 del Tratado de Funcionamiento de la Unión Europea[22]. Este derecho no surge de forma autónoma, sino como desarrollo de la intimidad y la privacidad, reconocidas históricamente en el Convenio Europeo de Derechos Humanos[23] y profundamente arraigadas en la tradición jurídica continental, particularmente a través de la teoría de las esferas del derecho alemán (*Sphärentheorie*), que distingue distintos niveles de protección de la esfera personal en función de su grado de intimidad. Como explica Dopazo, la protección de datos se fundamenta intrínsicamente en esos derechos vinculados a la esfera personal, siendo la privacidad el presupuesto que hace posible su autonomía como categoría jurídica propia[24].

Sobre esa base filosófica, el RGPD articula un marco normativo estructurado en torno a seis principios rectores que, como sistematiza Barrio, son: legitimidad, proporcionalidad, empoderamiento, transparencia, *accountability* y seguridad[25]. De este conjunto se desprende con claridad el espíritu del modelo europeo: la protección de datos no es una cuestión de cumplimiento contractual ni de gestión de riesgos empresariales, sino una obligación jurídica estructural cuyo centro de gravedad es el individuo y su dignidad. El mercado puede operar, pero dentro de los límites que impone el respeto a los derechos fundamentales. Esta premisa contrasta de forma radical con la lógica sobre la que se construye el sistema norteamericano.

---

[21] Carta de los Derechos Fundamentales de la Unión Europea (CDFUE), *Diario Oficial de la Unión Europea* C 326, de 26 de octubre de 2012, art. 8.
[22] Tratado de Funcionamiento de la Unión Europea (TFUE), versión consolidada, *Diario Oficial de la Unión Europea* C 202, de 7 de junio de 2016, art. 16.
[23] Consejo de Europa, Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), Roma, 4 de noviembre de 1950: *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su corresponde ncia."*.
[24] Dopazo Fraguío, M. P., "Protección de datos en el Derecho de la Unión Europea: principales aportaciones doctrinales y marco regulatorio vigente", *Revista de Derecho Europeo*, n.º 68, 2018, p. 130
[25] Barrio Andrés, M., "Los principios estructurales del Reglamento General de Protección de Datos", *Actualidad Jurídica Iberoamericana*, n.º 20, febrero de 2024, pp. 1326 - 1337.

Si el modelo europeo ancla la privacidad en la dignidad de la persona, al otro lado del Atlántico el concepto se desarrolló sobre una base filosófica distinta: la libertad individual frente a la intromisión del Estado[26]. Su cimiento doctrinal se encuentra en el influyente artículo "*The Right to Privacy*", publicado en 1890 por Samuel Warren y Louis Brandeis en la Harvard Law Review[27], en el que ambos autores reaccionaban a las intromisiones de la prensa amarilla en la vida privada de los ciudadanos y reclamaban el reconocimiento de un derecho a ser dejado en paz (*the right to be let alone*). Sin embargo, este derecho no alcanzó consolidación jurisprudencial hasta mediados del siglo XX, a través de la intervención del Tribunal Supremo.

En Katz v. United States (1967)[28], el Tribunal vinculó la privacidad con la Cuarta Enmienda, estableciendo el criterio de la "expectativa razonable de privacidad" en el ámbito de las comunicaciones. En Griswold v. Connecticut (1965)[29], reconoció un derecho constitucional implícito a la privacidad construido a partir de las "penumbras" de las enmiendas constitucionales, doctrina posteriormente extendida en Roe v. Wade (1973)[30]. Lo que estas sentencias tienen en común es su orientación: en todos los casos, la privacidad opera como escudo frente al poder del Estado, no como límite a la actuación de los particulares o las empresas[31].

Esta orientación tiene consecuencias directas en el ámbito de los datos personales. A diferencia del modelo europeo, en EE.UU. rige un principio de libre circulación de la información, conforme al cual el tratamiento de datos personales es en principio lícito salvo que una norma específica lo restrinja[32]. La protección no es la regla sino la excepción: fuera de los sectores con regulación específica[33], HIPAA para el ámbito sanitario, FCRA para los datos crediticios o COPPA para menores, el tratamiento de datos

[26] Whitman, J. Q., "The two western cultures of privacy: Dignity versus liberty", *The Yale Law Journal*, vol. 113, 2004, p. 1161.
[27] Warren, S. D. y Brandeis, L. D., "The right to privacy", *Harvard Law Review*, vol. 4, n. º 5, 1890, pp. 193-220
[28] *Katz v. United States*, 389 U.S. 347 (1967).
[29] *Griswold v. Connecticut*, 381 U.S. 479 (1965).
[30] *Roe v. Wade*, 410 U.S. 113 (1973).
[31] Whitman, *op.cit*., p. 1161.
[32] Sobrino, J., "Protección de datos y privacidad: estudio comparado entre la Unión Europea y Estados Unidos", *Revista de Derecho UNED*, n.º 25, 2019, p.709.
[33] DLA Piper, "Data Protection Laws of the World: United States", 2024, p. 11. (disponible en https://www.dlapiperdataprotection.com; última consulta 26/03/2026)

se articula de forma contractual[34]. Las empresas elaboran sus propias políticas de privacidad y el consumidor contrata con ellas. La protección de datos no es una garantía jurídica estructural, sino el resultado de una negociación entre partes desiguales. A nivel federal, la Federal Trade Commission (FTC), que estudiaremos a continuación[35] actúa como referente institucional en materia de privacidad, protegiendo al individuo en su calidad de consumidor frente a prácticas desleales o engañosas, pero sin reconocimiento de un derecho vinculado a la dignidad personal. Con todo, no han faltado intentos de aproximarse al modelo europeo siendo California el ejemplo más destacado a nivel estatal con la CCPA[36] y su posterior reforma mediante la CPRA[37], sobre las que volveremos más adelante[38] . La consecuencia, visible en la tabla 2.1, es un sistema fragmentado donde el nivel de protección del ciudadano depende del sector o del estado en que se encuentre. Esta falta de uniformidad regulatoria complica el cumplimiento normativo y la seguridad jurídica, y deja a los consumidores sin un entendimiento real de sus derechos sobre sus datos personales[39]; una asimetría especialmente problemática en el entorno digital, donde los datos no tienen frontera.

La distancia entre ambos sistemas se concreta de forma especialmente nítida en el tratamiento del consentimiento, que actúa como espejo de las dos filosofías descritas. En la UE, el art. 7 del RGPD exige que el consentimiento sea libre, específico, informado e inequívoco, revocable en cualquier momento[40]: no puede inferirse del silencio ni de casillas premarcadas. En EE.UU., el sistema predominante es el *opt-out*: el tratamiento de datos es lícito por defecto, y corresponde al usuario solicitar activamente que cese, salvo en categorías especialmente sensibles donde se exige *opt-in*[41]. El silencio equivale

[34] Bradford, A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020, p. 23.
[35] Ver capítulo 2, punto 2.3.3.
[36] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 *et seq.* (2018).
[37] California Privacy Rights Act (CPRA), Proposition 24, Cal. Civ. Code § 1798.100 *et seq.* (2020), en vigor desde el 1 de enero de 2023.
[38] Ver capitulo 2, punto 2.3.2.
[39] Barrio Andrés, M., "La regulación del derecho a la protección de datos en los Estados Unidos: hacia un RGPD norteamericano", *Cuadernos de Derecho Transnacional*, vol. 14, n.º 2, 2022, p. 189.
[40] 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), *Diario Oficial de la Unión Europea* L 119, de 4 de mayo de 2016, art. 7.
[41] DLA Piper, *op.cit.,* p.3.

a consentimiento, y ese consentimiento se articula mediante la política de privacidad como instrumento contractual, no como garantía jurídica de un derecho fundamental.

Esta diferencia no es menor. En contexto de la IA, implica que cualquier empresa que pretende utilizar datos personales para entrenar un modelo en la UE debe identificar previamente una base jurídica habilitante de las tasadas en el art. 6 del RGPD, consentimiento, interés legítimo, ejecución contractual u otras, antes de iniciar el tratamiento[42]. En EE.UU., en ausencia de norma sectorial aplicable, ese tratamiento es libre por defecto. En definitiva, mientras que en la UE la protección de datos es la norma y el tratamiento la excepción que requiere justificación, en EE.UU. ocurre exactamente lo contrario. Esta inversión de la lógica regulatoria no es un detalle técnico: es la expresión más clara de las dos filosofías irreconciliables que vertebran el análisis comparado de este capítulo.

2.3.2 La fragmentación norteamericana y el efecto Bruselas

El análisis comparado de los sistemas de protección de datos pone de manifiesto una asimetría estructural de primer orden. La Unión Europea ha construido un modelo sólido y coherente, articulado a través del RGPD, que ofrece una protección integral mediante un conjunto de herramientas que actúan de forma coordinada: principios rectores de aplicación transversal, bases jurídicas tasadas para el tratamiento, un catálogo amplio de derechos del interesado y un régimen sancionador con capacidad disuasoria real. Frente a ello, el sistema americano presenta una fragmentación que dificulta estructuralmente la protección del derecho a la privacidad: la ausencia de un marco federal general, la dispersión sectorial de la regulación y lógica contractual que rige el tratamiento de datos generan un entorno en el que el nivel de protección del ciudadano varía en función del sector económico en el que opere la empresa que trata sus datos, del estado en que resida, o de la política de privacidad que haya aceptado sin necesariamente haberla leído ni comprendido.

Sin embargo, en el contexto digital en que se inscribe el tratamiento de datos personales, esta divergencia regulatoria adquiere una dimensión adicional que complica el análisis. Los datos personales no reconocen fronteras geográficas ni espacios: una empresa con

[42] RGPD, art. 6.

sede en California puede recoger datos de ciudadanos europeos, procesarlos en servidores ubicados en terceros países y utilizarlos para finalidades que jamás fueron previstas por el usuario en el momento de facilitarlos. Esta realidad plantea un desafío de fondo para cualquier sistema de protección de datos con vocación territorial: ¿Cómo garantizar derechos cuyo objeto, el dato, circula de forma instantánea y transfronteriza por infraestructuras que escapan a la jurisdicción del legislador nacional?

La Unión Europea respondió a este desafío mediante una decisión de alcance normativo singular: el artículo 3 del RGPD establece que el Reglamento se aplica al tratamiento de datos de personas que se encuentren en la Unión con independencia de que el responsable o encargado esté establecido o no en territorio europeo[43]. Esta extensión extraterritorial, ya reflejada en la tabla 2.1, convierte el RGPD en un instrumento de vocación universal: cualquier empresa que trate datos de ciudadanos europeos queda sujeta a sus exigencias, opere desde California, Singapur o Dublín. Es precisamente sobre esta base donde cobra relevancia el fenómeno identificado por Anu Bradford.

Bradford acuñó el concepto de "efecto Bruselas" para describir el proceso mediante el cual las normas y regulaciones emanadas de Bruselas han penetrado múltiples aspectos de la vida económica, tanto dentro como fuera de Europa, a través de lo que la autora denomina "globalización regulatoria unilateral", es decir, la capacidad de la UE para exportar sus estándares al resto del mundo sin necesidad de acuerdos internacionales ni de mecanismos de coerción directa, sino como consecuencia lógica de su peso como mercado.[44] Bradford desdobla el fenómeno en dos ramas. Por un lado, el efecto Bruselas *de facto* se produce cuando las empresas multinacionales, ante el coste de mantener estándares diferenciados para distintos mercados, optan por aplicar globalmente el estándar europeo, más exigente, como política única.[45] La lógica es puramente económica, resulta más eficiente homogeneizar hacia arriba que gestionar la complejidad de operar bajo sistemas paralelos. Un ejemplo paradigmático de las consecuencias de este efecto es la sanción de 1200 millones de euros impuesta por la autoridad irlandesa de protección de datos a Meta en 2023 por la transferencia ilícita de datos de usuarios

[43] RGPD, art. 3.
[44] Bradford, A., "The Brussels Effect", *Northwestern University Law Review*, vol. 107, n. º 1, 2012, p.3. El concepto fue posteriormente desarrollado en extenso en Bradford, A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020.
[45] Bradford (2012), *op.cit.,* p.6.

europeos a servidores estadounidenses[46], que forzó a la compañía a revisar su arquitectura de transferencia de datos a escala global. Por otro lado, el efecto Bruselas *de iure* se produce en una segunda instancia, una vez que las empresas exportadoras han adaptado sus prácticas al estándar europeo, tienen incentivos para presionar a sus gobiernos domésticos para que adopten esos mismos estándares, igualando así las condiciones de competencia frente a sus competidores internos que no están sujetos a las mismas exigencias.[47]

Este efecto de iure es visible en la práctica empresarial y en la evolución legislativa americana. Microsoft y Meta, entre otras compañías, han anunciado la extensión voluntaria de elementos clave del RGPD a sus políticas internas con carácter global, aplicando derechos de acceso, supresión y portabilidad a usuarios situados fuera del territorio europeo , no por globalización jurídica sino por coherencia operativa y gestión reputacional.[48] A nivel legislativo, California ha liderado este proceso con la CCPA y la CPRA, que reflejan de forma clara la influencia del modelo europeo en el reconocimiento de derechos de acceso, supresión y *opt-out.* Otros estados avanzan en la misma dirección: Virginia con la Consumer Data Protection Act, Colorado con la Colorado Privacy Act y Connecticut con la Data Privacy Act han aprobado legislación que sigue patrones similares[49], configurando un mosaico regulatorio estatal que, pese a su fragmentación, apunta progresivamente hacia los estándares que el RGPD ha consolidado en Europa.

Con todo, no puede atribuirse la fortaleza regulatoria europea exclusivamente a motivaciones de protección de derechos fundamentales. Algunos autores han apuntado, con cierto fundamento, que la legislación europea en materia digital responde también a una lógica de soberanía y posicionamiento estratégico internacional. La Unión Europea carece de grandes empresas tecnológicas propias y no cuenta con un equivalente al Silicon Valley americano ni a los gigantes tecnológicos chinos. En este contexto, la regulación se convierte en un instrumento de poder: a través de normas de aplicación extraterritorial

[46] Comisión de Protección de Datos de Irlanda (*Data Protection Commission*), Decisión en el asunto Meta Platforms Ireland Limited, Referencia IN-20-8-1, de 12 de mayo de 2023 (disponible en https://finreg360.com/wp-content/uploads/2023/05/final_for_issue_ov_transfers_decision_12-05-23-1.pdf; última consulta 28/03/2026).
[47] Bradford (2012), *op.cit*., p.6.
[48] Brill, J., "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data", *Microsoft On the Issues*, 21 de mayo de 2018 (disponible en https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/; última consulta 28/03/2026).
[49] DLA Piper, *op.cit*., p.4.

como el RGPD, la UE proyecta influencia sobre la economía digital global y reafirma su peso como actor internacional. Este proceso de resoberanización europea en el ámbito digital se remonta a 2013, cuando responsables políticos franceses advirtieron por primera vez que Europa corría el riesgo de convertirse en una "colonia digital" de sus aliados occidentales, atrapada entre el poderío tecnológico estadounidense y las aspiraciones hegemónicas chinas.[50] Desde esta perspectiva, el efecto Bruselas no es solo una consecuencia involuntaria del peso del mercado europeo, sino también, al menos en parte, un objetivo deliberado de política regulatoria.

2.3.3 Efectividad real: ¿sancionar o disuadir?

El análisis de la efectividad de ambos sistemas exige ir más allá de la arquitectura normativa y preguntarse por los mecanismos concretos a través de los cuales cada ordenamiento garantiza el cumplimiento de sus mandatos. Como veremos, la UE apuesta por un modelo que combina la prevención estructural con la sanción disuasoria, mientras que en EE.UU. opera de forma predominantemente reactiva, interviniendo una vez que el daño ya se ha producido.

El modelo europeo articula una primera capa de protección de naturaleza ex ante a través del principio de responsabilidad proactiva o *accountability*, recogido en los artículos 5.2[51] y 24.1[52] del RGPD. Este principio exige al responsable del tratamiento no solo cumplir con las obligaciones que impone el Reglamento, sino estar en condiciones de demostrar activamente ese cumplimiento mediante registros de actividad de tratamiento, evaluaciones de impacto sobre la protección de datos en los supuestos de tratamiento de alto riesgo, y la adopción de medidas técnicas organizativas adecuadas desde el diseño y por defecto. Como señala Estepa, el principio de *accountability* supone una transformación estructural en la lógica del cumplimiento normativo: el responsable no espera a ser inspeccionado o sancionado para adecuar sus prácticas, sino que interioriza

[50] Nocetti, J., "Will Europe remain a 'digital colony'?", en Gomart, T. y Hecker, M. (dirs.), *European Elections 2019: Structuring the Debate*, Institut Français des Relations Internationales, París, 2019, p. 41.
[51] RGPD, art. 5.2: **"**El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)."
[52] RGPD, art. 24.1: "Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario."

el cumplimiento como parte de su funcionamiento ordinario.[53] Esta dimensión preventiva es especialmente relevante en el contexto del tratamiento masivo de datos propio de los sistemas de inteligencia artificial, donde el daño potencial sobre los derechos de los interesados puede producirse a gran escala antes de que ninguna autoridad tenga ocasión de intervenir.

Sobre esta base preventiva, el RGPD superpone un potente régimen sancionador que constituye uno de los pilares del sistema. El articulo 83 del Reglamento estructura las sanciones en dos tramos: el primero permite imponer multas de hasta diez millones de euros o el dos por ciento de la facturación global anual de la empresa infractora para las infracciones de menor gravedad; el segundo eleva ese umbral hasta veinte millones de euros o el cuatro por ciento de la facturación global para las infracciones más graves, aplicándose la cifra de mayor cuantía.[54] La magnitud de estas cifras no es casual: el legislador europeo diseñó deliberadamente un régimen cuya proporcionalidad respecto a la facturación global busca que ninguna empresa, por grande que sea, pueda calcular el incumplimiento como una opción económicamente rentable. El ejemplo más ilustrativo de este potencial disuasorio es la antes mencionada[55] sanción récord de 1200 millones de euros impuesta a Meta en 2023.[56] Se trata de la mayor sanción impuesta hasta la fecha bajo el RGPD, y constituye una demostración inequívoca de la capacidad efectiva del sistema europeo para disciplinar a los grandes operadores tecnológicos.

Frente a este modelo, el sistema estadounidense opera desde una lógica radicalmente distinta. A nivel federal, la Federal Trade Commission actúa como principal garante de los derechos de los consumidores en materia de privacidad, con competencia para perseguir las prácticas desleales o engañosas de las empresas al amparo de la Section 5 de la FTC Act[57]. Sin embargo, su actuación es de naturaleza estrictamente ex post: la FTC

[53] Estepa Montero, M., "El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas", *Anuario Jurídico y Económico Escurialense*, n.º 55, 2022, p. 72.
[54] RGPD, art. 83.
[55] Ver capítulo 2, punto 2.3.2.
[56] DPC, *op.cit.*
[57] Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) (1914, enmendado): "The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations (…) from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."

no establece estándares preventivos de cumplimiento ni interviene antes de que se produzca una infracción, sino que reacciona una vez que el daño ya ha tenido lugar.[58]

La mayoría de los procedimientos iniciados por la FTC en materia de privacidad concluyen sin resolución sancionadora formal[59], mediante acuerdos negociados con las empresas investigadas conocidos como *consent decrees*. Como señalan Solove y Hartzog, estos acuerdos han adquirido una relevancia práctica notable en un ámbito donde el *case law* es escaso, ya que las investigaciones raramente llegan a resolución judicial. Entonces, son los propios *consent decrees* los que funcionan en la práctica como referente y guía para el resto de empresas del sector, conformando así una suerte de *common law* análogo.[60] Sin embargo, la doctrina identifica dos deficiencias estructurales de este sistema que limitan seriamente su eficacia. En primer lugar, Becker explica que estos acuerdos no generan verdaderos precedentes jurídicos: la ausencia de reglas claras sobre que constituye una práctica de seguridad "irrazonable" o "desleal" en los términos de la FTC Act, unida a la falta de especificidad de los documentos publicados por la Comisión, que se limitan a afirmaciones genéricas sin detallar que medidas concretas se consideran adecuadas, impide que las empresas puedan orientar preventivamente sus políticas de tratamiento de datos[61]. En segundo lugar, por su propia naturaleza, estos acuerdos solo pueden activarse ex post, una vez que la FTC constata que se ha producido una brecha. Entonces, este enfoque reactivo invita a una aplicación arbitraria de la norma, ya que lo que realmente desencadena la intervención de la FTC no es la evaluación de si las medidas de seguridad adoptadas por la empresa eran razonables antes del incidente, sino la constatación de que el incidente ya se produjo[62].

En definitiva, la comparación entre ambos sistemas revela una diferencia que va más allá del régimen sancionador en sentido estricto: mientras que la UE construye la efectividad del sistema sobre la combinación de prevención estructural y sanción proporcional, EE.UU. delega la protección en la reacción posterior al daño. En un entorno donde el tratamiento masivo de datos puede comprometer los derechos de millones de personas de

[58] Becker, T., "When Congress makes no policy choice", *Columbia Law Review*, vol. 120, n. º 5, 2020, p.142.
[59] Solove, D. J. y Hartzog, W., "The FTC and the new common law of privacy", *Columbia Law Review*, vol. 114, 2014, p.585.
[60] *Ibid* p. 619.
[61] Becker, *op.cit.,* p.142.
[62] *Ibid*, p. 143.

forma simultánea e instantánea, la pregunta sobre si sancionar o disuadir no es retórica, tiene consecuencias reales para la protección efectiva de los ciudadanos.

2.4 De la privacidad a la autoría: el dato como elemento disruptivo

La protección de datos constituye, como hemos analizado, la primera línea de tensión dentro del desarrollo de las tecnologías digitales y los derechos individuales. Sin embargo, el impacto de estas tecnologías sobre el ordenamiento jurídico no se agota en la esfera de la privacidad. El entrenamiento de los modelos de IA exige, además de datos personales, acceder a volúmenes ingentes de contenido creativo protegido por derechos de autor, abriendo un segundo frente de conflicto que, vinculado al anterior por el mismo elemento detonante, presenta una naturaleza jurídica propia. A él dedicamos el capítulo siguiente.

CAPÍTULO 3: Propiedad intelectual y entrenamiento de modelos de IA

El presente capítulo analiza el segundo de los conflictos jurídicos que el uso intensivo de datos plantea en el contexto del desarrollo de la inteligencia artificial: la utilización de obras protegidas por derechos de autor como material de entrenamiento de modelos de IA. Para ello, se parte de la constatación de que tanto el ordenamiento europeo como el estadounidense reconocen que dicho uso constituye, en principio, una infracción, pero articulan mecanismos distintos para superarla, reflejo de las mismas filosofías de gobernanza que ya identificamos en el capítulo anterior. El capítulo se organiza en tres bloques. En primer lugar, se sistematizan las principales diferencias entre ambos ordenamientos a través de tablas comparativas que cubren la base jurídica del entrenamiento con obras protegidas, los límites y el equilibrio con los titulares de derechos, y los mecanismos de transparencia y control. A continuación, se analiza el significado y las implicaciones de esas diferencias, atendiendo a la infracción prima facie como punto de partida común, a la tensión entre innovación y protección de derechos de autor, y al papel del AI Act como capa regulatoria complementaria al sistema de la Directiva DSM. El capítulo concluye con un párrafo de transición hacia las conclusiones del trabajo.

3.1 La obra protegida como dato de entrenamiento

El desarrollo de modelos de inteligencia artificial, y en particular de los modelos de IA generativa y los grandes modelos de lenguaje (Large Language Models o LLMs), ha conocido una aceleración sin precedentes en los últimos años, transformando de forma radical las posibilidades de generación automatizada de texto, imágenes, audio y otros contenidos. Este desarrollo, sin embargo, no es gratuito en términos jurídicos: para que un modelo pueda generar contenido de forma autónoma, debe ser previamente entrenado, y ese entrenamiento se lleva a cabo mediante técnicas de minería de texto y datos (*text and data mining o TDM)*, definidas en el artículo 2.2 de la Directiva (UE) 2019/790 como "toda técnica analítica automatizada destinada a analizar textos y datos en formato digital a fin de generar información que incluye, sin carácter exhaustivo, pautas, tendencias o correlaciones".[63]

El propio legislador europeo ha reconocido la dimensión del problema. El considerando 105 del Reglamento de Inteligencia Artificial de la UE advierte que el desarrollo y entrenamiento de estos modelos "requiere acceder a grandes cantidades de texto, imágenes, videos y otros datos", y que las técnicas de TDM "pueden utilizarse ampliamente en este contexto para la recuperación y el análisis de tales contenidos, que pueden estar protegidos por derechos de autor y derechos afines", añadiendo que "todo uso de contenidos protegidos por derechos de autor requiere la autorización del titular de los derechos de que se trate, salvo que se apliquen las excepciones y limitaciones pertinentes".[64] Esta advertencia no es retorica, sitúa el conflicto entre el desarrollo de la IA y la propiedad intelectual en el centro de la agenda regulatoria europea.

La oficina de Copyright de Estados Unidos, en un informe emitido en 2025, detalla con precisión como las obras protegidas entran en juego durante el desarrollo del modelo de IA. El proceso comienza con la recopilación y curación del conjunto de datos de entrenamiento, que implica descargar obras de fuentes públicas o adquirirlas por otras vías, transferirlas entre sistemas, convertirlas en distintos formatos y organizarlas en

[63] Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital, art. 2.2, DOUE L 130, de 17 de mayo de 2019.
[64] 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, Considerando 105, DOUE L 1689, de 12 de julio de 2024.

subconjuntos filtrados. A continuación, durante el entrenamiento propiamente dicho, las obras son reproducidas en bloques sucesivos y mostradas al modelo para que este ajuste sus parámetros internos. Finalmente, el modelo resultante puede en ciertos casos memorizar expresiones protegidas de las obras de entrenamiento y reproducirlas en sus salidas. En cada una de estas fases, el uso de obras protegidas sin autorización puede constituir una infracción de los derechos de sus titulares[65].

Es en este contexto donde se inscribe el análisis comparado que desarrollamos a continuación: como responden el ordenamiento europeo y el estadounidense ante un conflicto que enfrenta la lógica de la innovación tecnológica con la protección de la propiedad intelectual como un bien jurídico consolidado.

3.2 Resultados

3.2.1 Base jurídica del entrenamiento con obras protegidas

El primer bloque comparativo examina el fundamento normativo sobre el que cada ordenamiento permite el entrenamiento de modelos de IA con obras protegidas: la naturaleza del mecanismo habilitante, el carácter del análisis que exige y el grado de seguridad jurídica que ofrece. El texto de referencia europeo son los artículos 3 y 4 de la Directiva (UE) 2019/790, que introducen excepciones específicas para la minería de textos y datos. En el ordenamiento americano, el texto de referencia es el § 107 del Copyright Act, que codifica la doctrina del *fair use* mediante un test de cuatro factores de aplicación judicial caso por caso.

Tabla 4: Fundamentos jurídicos del entrenamiento de IA con obras protegidas

Ítem	**Unión Europea**	**USA**
Fundamento normativo	Directiva UE 2019/790, arts. 3 y 4 (Directiva DSM)	*Fair use* (17 U.S.C. §107)

[65] U.S. Copyright Office, *Copyright and Artificial Intelligence, Part 3: Generative AI Training*, Pre-Publication Version, U.S. Copyright Office, Washington D.C., 2025, Sección II, pp. 4-25.

Naturaleza del mecanismo	Excepción legislativa específica para minería de textos y datos (TDM)	Doctrina jurisprudencial de aplicación abierta
Carácter del análisis	Regla previa con condiciones objetivas predeterminadas	Test de 4 factores aplicado caso por caso
Grado de seguridad jurídica	Previsibilidad formal en cuanto al texto, incertidumbre interpretativa en su aplicación a la IA	Incierto hasta decisión judicial

3.2.2 *Límites y equilibrio con los titulares de derechos*

El segundo bloque examina los mecanismos que cada ordenamiento articula para proteger los intereses de los titulares de derechos en el contexto del entrenamiento de IA: la posibilidad de oposición, su efectividad práctica, el papel del impacto en el mercado, el carácter transformativo del uso, la compensación y la distribución del riesgo entre las partes. El texto de referencia europeo es el articulo 4.3 de la Directiva DSM, que regula el mecanismo de *opt-out*. En el ordenamiento norteamericano, la comparación se articula a partir de los cuatro factores del *fair use* del § 107 del Copyright Act, con especial atención al factor del daño al mercado potencial de la obra, que la jurisprudencia ha identificado como el más relevante del test.

Tabla 5: Límites y equilibrio con los titulares de derechos

Ítem	**Unión Europea**	**USA**
Posibilidad de oposición del titular	*Opt-out* expreso del titular (art 4.3 DSM).	Sin mecanismo formal equivalente.

Efectividad práctica del *opt-out*	Limitada: ausencia de estándar técnico específico.	Sin mecanismo equivalente, la oposición depende de negociación contractual o litigio.
Impacto en el mercado	No explicitado en la excepción. No hay evaluación caso por caso.	Factor central del fair use (*market harm*).
Carácter transformativo del uso	No opera como categoría autónoma en la excepción TDM.	Factor clave del *fair use*, objeto de debate judicial en litigios de IA.
Compensación obligatoria	No prevista en la excepción general.	No automática, depende del juicio.
Distribución del riesgo	Riesgo regulatorio estructurado, el incumplimiento activa el régimen de la Directiva.	Riesgo litigioso trasladado a tribunales.

3.2.3 Mecanismos de transparencia y control sobre el uso de obras protegidas

El tercer bloque examina las obligaciones de transparencia que cada ordenamiento impone sobre el uso de obras protegidas en el entrenamiento de modelos de IA: el sujeto obligado, el alcance territorial de la obligación y su efectividad práctica. El texto de referencia europeo es el articulo 53.1.c) del Reglamento de Inteligencia Artificial, que obliga a los proveedores de modelos de IA de uso general a identificar y respetar las reservas de derechos expresadas conforme al articulo 4.3 de la Directiva DSM, en conjunción con el considerando 106 del mismo Reglamento en cuanto a su alcance extraterritorial. El ordenamiento norteamericano carece de una obligación equivalente a

nivel federal, por lo que la comparación refleja en este caso una asimetría estructural entre ambos sistemas.

Tabla 6: Transparencia y control sobre el uso de obras protegidas

Ítem	**Unión Europea**	**USA**
Obligación de transparencia sobre datos de entrenamiento	Si, los proveedores de modelos de IA de uso general deben identificar y respetar las reservas de derechos expresadas conforme al art 4.3 DSM (AI Act, art 53.1.c).	Sin obligación equivalente a nivel federal.
Sujeto obligado	El proveedor del modelo.	Sin sujeto obligado equivalente.
Alcance territorial	Aplicable a todo proveedor que introduzca un modelo en el mercado europeo, con independencia de dónde se haya realizado el entrenamiento (AI Act, considerando 106).	Sin régimen general de aplicación extraterritorial.
Efectividad del mecanismo	Incierta, condicionada a la existencia de estándares técnicos que permitan identificar y verificar el cumplimiento de las reservas.	Sin mecanismo equivalente, la transparencia depende de la voluntad de las empresas.

3.3 Discusión

Los resultados obtenidos permiten ahora examinar el alcance de las divergencias identificadas. El análisis se estructura en torno a tres planos: el punto de partida común, que examina como cada sistema califica y permite superar la infracción prima facie, la tensión de fondo entre innovación y protección de derechos de autor, que subyace a todas las diferencias observadas, y el papel del AI Act como elemento que completa y refuerza el modelo europeo más allá de lo que la Directiva DSM por si sola puede garantizar.

3.3.1 Dos modelos ante un mismo conflicto: la infracción como punto de partida

Como se ha expuesto, el desarrollo de modelos de IA generativa exige el procesamiento de cantidades masivas de contenido para que el algoritmo pueda identificar patrones, estructuras y relaciones entre datos. Este proceso, que constituye el núcleo técnico del entrenamiento, tiene una consecuencia jurídica inmediata e inevitable: la reproducción de obras protegidas por derechos de autor. Tanto el ordenamiento europeo como el estadounidense coinciden en que dicha reproducción constituye, en principio, una infracción. Sin embargo, la forma en que cada sistema articula esta calificación, y sobre todo las vías que ofrece para superarla, revela diferencias estructurales.

En el ordenamiento europeo, la normativa de derechos de autor protege cualquier reproducción directa o indirecta de una obra, sea temporal o permanente, parcial o total.[66] El proceso de entrenamiento de un modelo de IA activa esta protección en múltiples momentos: cuando el desarrollador descarga obras de fuentes públicas para construir el conjunto de datos, cuando las transfiere entre sistemas de almacenamiento, cuando las convierte en otros formatos, y cuando el propio proceso de entrenamiento las reproduce en bloques sucesivos para mostrarlas al modelo. Se produce así lo que la doctrina ha denominado el “problema del contenedor”: no es posible utilizar los datos, que en sí mismos no están protegidos, sin reproducir la obra protegida que los contiene, generando una derivación de protección que extiende el control del titular de derechos más allá de la expresión creativa y hacia los hechos y datos en ella incorporados.[67] A ello se añade la

[66] Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, *Diario Oficial de la Unión Europea* L 167, de 22 de junio de 2001, art. 2.
[67] Margoni, T. y Kretschmer, M., "A deeper look into the EU text and data mining exceptions: harmonisation, data ownership, and the future of technology", *GRUR International*, vol. 71, n. º 8, 2022, p. 690.

dimensión de las bases de datos, cuya protección en el derecho europeo opera en un doble plano: el derecho de autor sobre su estructura, cuando la selección o disposición de datos sea original, y el derecho sui generis sobre la inversión realizada para obtener, verificar o presentar esos datos.[68] La extracción y reutilización de partes sustanciales de una base de datos para entrenar un modelo de IA activa ambas capas de protección, complicando aún mas el acceso a los volúmenes de información que el desarrollo tecnológico exige.

En el ordenamiento estadounidense, el análisis de la infracción parte de los derechos exclusivos reconocidos al titular en el 17 U.S.C. § 106[69], reproducción, distribución, exhibición pública, ejecución publica y preparación de obras derivadas, y exige para su acreditación dos elementos: la titularidad de un copyright valido y la copia de elementos originales de la obra.[70] Aplicado al entrenamiento de la IA, la Oficina de Copyright de Estados Unidos (USCO) concluye en su informe de 2025 que el proceso genera múltiples actos de reproducción claramente identificables: la descarga de obras para construir el conjunto de datos, su transferencia entre sistemas de almacenamiento, su conversión a distintos formatos, y su reproducción en bloques durante el entrenamiento.[71] La Oficina añade que, en aquellos casos en que el modelo memoriza expresión protegida de las obras de entrenamiento y es capaz de reproducirla en sus salidas sin necesidad de que dicha expresión le sea suministrada externamente, los propios pesos del modelo pueden constituir una infracción del derecho de reproducción o del derecho sobre obras derivadas.[72]

Establecida la infracción prima facie en ambos ordenamientos, la pregunta que vertebra el resto del análisis comparado es como cada sistema permite superarla. En la Unión Europea, la respuesta se articuló mediante las excepciones específicas para minería de textos y datos introducida por la Directiva (UE) 2019/790. El artículo 3 prevé una excepción de carácter no renunciable para organismos de investigación e instituciones de patrimonio cultural, que pueden realizar TDM sin necesidad de autorización previa[73]; sin

---

[68] Geiger, C., Frosio, G. y Bulayenko, O., "Text and data mining: Articles 3 and 4 of the Directive 2019/790/EU", en *Propiedad intelectual y mercado único digital europeo*, Tirant lo Blanch, Valencia, 2019, p. 9.
[69] Copyright Act, 17 U.S.C. § 106 (1976).
[70] U.S. Copyright Office, *Copyright and Artificial Intelligence, Part 3: Generative AI Training*, 2025, pp. 26-31.
[71] *Ibid*., pp. 26-29.
[72] *Id.*
[73] Directiva (UE) 2019/790, *op. cit.*, art. 3.

embargo, su ámbito subjetivo excluye expresamente a las empresas comerciales y a las start-ups, que quedan obligadas a negociar licencias individuales. El articulo 4 extiende la excepción a cualquier persona, pero introduce a cambio un mecanismo de *opt-out* que permite a los titulares de derechos reservar expresamente sus obras mediante medios legibles por maquina; ejercido el *opt-out*, el entrenamiento sobre esa obra vuelve a ser potencialmente ilícito en ausencia de licencia.[74]

En Estados Unidos, la respuesta no proviene del legislador sino de la doctrina del *fair use*, codificada en el § 107 del Copyright Act[75], que establece que el uso leal de una obra protegida constituye una infracción, que sin embargo podría estar amparado por esta doctrina y somete su determinación a un test de cuatro factores: la finalidad y el carácter del uso, incluyendo si tiene naturaleza comercial o educativa sin ánimo de lucro, la naturaleza de la obra protegida, la cantidad y sustancialidad de la parte utilizada en relación con el conjunto de la obra, y el efecto del uso sobre el mercado potencial de la obra o su valor.[76] Estos factores no se aplican de forma mecánica ni generan reglas claras de antemano, se exige ponderación judicial caso por caso.

Es precisamente esta naturaleza abierta del *fair use* la que convierte el conflicto entre IA y derechos de autor en un campo de batalla judicial en tiempo real. A diferencia del modelo europeo, donde la excepción TDM ofrece al menos una referencia normativa previa, el sistema americano está siendo construido por los tribunales a medida que se suceden los litigios. Como señala Durantaye, todas las grandes empresas de IA han sido demandadas en múltiples ocasiones por titulares de derechos individuales o por grupos de demandantes, concentrándose la mayoría de los procedimientos en el Distrito Norte de California.[77]

Las primeras resoluciones judiciales sobre entrenamiento de IA y *fair use* comenzaron a dictarse en 2025: en *Bartz et al. v. Anthropic*[78], el tribunal consideró que el uso de libros adquiridos lícitamente para entrenar modelos de lenguaje constituía *fair use*, subrayando el carácter transformativo de la tecnología. Días después, en *Kadrey et al. v. Meta*

---

[74] *Ibid*., art. 4.
[75] Copyright Act, 17 U.S.C. § 107.
[76] U.S. Copyright Office, *Copyright and Artificial Intelligence, Part 3*, *op. cit.*, Sección IV, p. 32.
[77] De La Durantaye, K., "Control and compensation. A comparative analysis of copyright exceptions for training generative AI", *IIC - International Review of Intellectual Property and Competition Law*, vol. 56, n. º 4, 2025, p 745.
[78] *Bartz et al. v. Anthropic PBC*, No. 3:23-cv-03223 (N.D. Cal. 2023).

Platforms[79], el tribunal alcanzó la misma conclusión, pero advirtió que el daño al mercado, el factor más relevante del test no puede acreditarse por analogía, sino que debe probarse de forma específica. Ambas resoluciones sugieren que la legalidad en la obtención de los datos de entrenamiento y la acreditación del daño de mercado serán los ejes sobre los que pivote la doctrina emergente.

Entre los casos aún sin resolver, destaca el litigio iniciado por *The New York Times Co.* contra Microsoft Corp. y OpenAI.[80] El demandante argumenta que el uso de su material periodístico para entrenar los modelos no constituye *fair use*, por carecer de carácter transformativo y porque los modelos reproducen este material sin atribución adecuada en ocasiones omitiendo la autoría. El Times ha solicitó un requerimiento judicial que incluye la destrucción de los modelos ya entrenados, así como compensación económica en forma de daños y perjuicios y la restitución de los beneficios perdidos o lucro cesante[81]. De resolverse en favor del demandante esta sentencia podría redefinir de forma radical los límites del *fair use* aplicado al entrenamiento de IA. En la misma línea *Andersen v. Stability AI*[82] plantea cuestiones igualmente determinantes sobre el procesamiento masivo de imágenes extraídas de internet para entrenar modelos de generación visual. Las empresas del sector siguen de cerca cada resolución, conscientes de que el marco jurídico que rige su actividad se está definiendo, en sede judicial.

3.3.2 El conflicto entre innovación y protección de derechos de autor

El análisis comparado de los mecanismos mediante los cuales cada ordenamiento aborda la infracción prima facie no puede desvincularse de una pregunta de fondo más amplia: ¿qué pretende conseguir la norma? ¿Debe el derecho decantarse por proteger los derechos de los creadores o por facilitar el desarrollo tecnológico, o es posible encontrar un equilibrio entre ambos? Esta tensión no es nueva, pero adquiere una dimensión especialmente aguda en el contexto del entrenamiento de modelos de IA, donde el volumen de obras afectadas y la velocidad del desarrollo tecnológico dificultan la aplicación de las categorías jurídicas tradicionales.

[79] *Kadrey et al. v. Meta Platforms, Inc.*, No. 3:23-cv-03417 (N.D. Cal. 2023).
[80] *The New York Times Co. v. Microsoft Corp. and OpenAI*, No. 1:23-cv-11195 (S.D.N.Y. 2023).
[81] De La Durantaye (2025), *op.cit.*, p. 746.
[82] *Andersen et al. v. Stability AI Ltd. et al.*, No. 3:23-cv-00201 (N.D. Cal. 2023).

Históricamente, la aproximación regulatoria de EE.UU. y la UE han representado dos filosofías opuestas frente a la innovación tecnológica. Como señala Bradford, las empresas tecnológicas americanas como Google, Microsoft y Apple pudieron crecer y escalar en un entorno regulatorio permisivo, lo que contribuyó de forma directa y significativa a su éxito comercial, mientras que la experiencia europea sirve como advertencia del efecto contrario: regulaciones extensas, pero escasez de empresas tecnológicas europeas con proyección global.[83] Esta tensión estructural entre regulación e innovación es precisamente el telón de fondo sobre el que se desarrolla el debate que analizamos.

Por un lado, permitir el uso libre de obras protegidas para entrenar modelos de IA beneficia el desarrollo tecnológico, pero expone a los titulares de derechos a una potencial pérdida de su mercado. Los autores alegan que sus obras pueden verse sustituidas por los propios modelos que las han consumido como dato de entrenamiento, o que no obtienen remuneración alguna por la explotación de su trabajo[84], lo que podría desincentivar la creación. Como solución, algunos sectores han reclamado la introducción de sistemas de licencias obligatorias o formas de remuneración que garanticen una compensación justa.[85]

En esta línea, la Unión Europea ha intentado mejorar la posición de su sector apostando en un principio por la innovación, pero introduciendo palancas de protección que los titulares de derechos pueden activar. Como señalan Margoni y Kretschmer, las excepciones TDM de la Directiva DSM podrían poner a las empresas europeas, especialmente a las pymes y *startups*, en igualdad de condiciones frente a las grandes plataformas americanas que hasta ahora han podido beneficiarse de marcos jurídicos más permisivos para desarrollar sus modelos sin autorización previa.[86] Sin embargo, se identifican límites relevantes en la formulación de los artículos 3 y 4 de la directiva, existe el riesgo de que si todos los titulares ejercen masivamente el *opt-out* del artículo 4.3, el efecto neto de la excepción puede acabar siendo contraproducente para las propias empresas europeas que pretendía beneficiar.[87] Además, este mecanismo de *opt-out* abre

[83] Bradford, A., (2024), *op.cit*., p.379.
[84] Senftleben, M., "AI Act and author remuneration: a model for other regions?", SSRN Working Paper, n. º 4740268, 2024, p. 2.
[85] *Ibid.*, p. 6.
[86] Margoni, T. y Kretschmer, M., "A deeper look into the EU text and data mining exceptions: harmonisation, data ownership, and the future of technology", *GRUR International*, vol. 71, n. º 8, 2022., p. 689.
[87] *Id*.

inevitablemente la puerta a la creación de un mercado de licencias y sistemas de remuneración individual[88] que elevan las barreras de entrada y los costes operativos para las empresas del sector. Como advierte Senftleben, la necesidad de obtener autorizaciones individuales y gestionar pagos de remuneración por el entrenamiento de modelos constituye un factor de coste adicional en forma de gastos de transacción y licencias que, cuando alcanza un nivel excesivo, compromete la capacidad competitiva del sector europeo de IA en el mercado global.[89]

La dificultad de encontrar ese equilibrio no es exclusiva de los grandes bloques regulatorios analizados. Australia ilustra con claridad las tensiones políticas y sociales que genera cualquier intento de reformar el marco de derechos de autor para acomodar el entrenamiento de la IA. En 2024, la Comisión de Productividad australiana propuso introducir una excepción de TDM en la lista de usos permitidos bajo la doctrina del *fair dealing* de la *Copyright Act* de 1968, con el objetivo de facilitar el desarrollo de modelos de IA en el país.[90] La propuesta generó una reacción inmediata y contundente por parte de autores, ilustradores y otros titulares de derechos de autor australianos, que la interpretaron como una autorización encubierta para que las empresas tecnológicas explotaran sus obras sin compensación.[91] El debate australiano es relevante porque pone de manifiesto que la elección entre innovación y protección no es solo una cuestión técnico-jurídica, sino profundamente política: cualquier reforma en este ámbito implica decisiones sobre qué intereses se priorizan y quien asume el coste del desarrollo tecnológico.

En EE.UU., la respuesta al conflicto ha tomado un camino radicalmente distinto: en lugar de legislar, se ha dejado que sean los tribunales quienes definan los límites del *fair use* aplicado al entrenamiento de IA. Este enfoque ha generado una explosión de litigios involucrando a la mayoría de grandes empresas de IA americanas, que han preferido optar por una inversión millonaria en litigación, buscando construir una doctrina favorable en sede judicial, antes que someterse a restricciones legislativas. Según el informe de la IA

[88] De La Durantaye, K., "Garbage in, garbage out. Regulating generative AI through copyright law", *ZUM - Zeitschrift für Urheber- und Medienrecht*, n. º 10, 2023, p. 9.
[89] Senftleben, *op.cit.,* p. 12.
[90] Productivity Commission, *Harnessing Data and Digital Technology: Interim Report*, Australian Government, Canberra, agosto de 2025.
[91] Australian Society of Authors (ASA), "Submission in response to Harnessing Data and Digital Technology Inquiry Interim Report", Productivity Commission, 15 de septiembre de 2025.

de Stanford de 2024, la inversión privada en IA en EE.UU. supera con creces la de cualquier otra región del mundo, lo que ilustra la magnitud de los intereses económicos en juego[92]. Las empresas americanas se han visto beneficiadas por la ausencia inicial de legislación ya que han podido hacer uso de las obras y esperar a que los titulares de los derechos de autor tomen iniciativa legal, con todos los riesgos que esto conlleva[93]. Como señala De la Durantaye, las empresas americanas esperan que los tribunales acaben interpretando el *fair use* de forma amplia, o simplemente prefieren litigar en un sistema que conocen antes que relocalizarse.[94] El resultado es una doctrina en construcción, cuyos contornos dependen de sentencias que aún no han sido dictadas.

Ante este panorama, cabe preguntarse si la dicotomía entre innovación y regulación es realmente inevitable, o si se trata, como argumenta Bradford, de un falso paradigma. La autora sostiene que el liderazgo tecnológico de Estados Unidos no se debe a la ausencia de regulación, sino a factores estructurales como la profundidad de sus mercados de capital, su cultura de riesgo y su capacidad de atraer talento global.[95] Desde esta perspectiva, imponer reglas que protejan a los autores no destruiría necesariamente la capacidad innovadora de un país si el resto del ecosistema se mantiene sólido. Es más, Bradford defiende que la regulación puede actuar como motor de innovación social, forzando a las empresas a desarrollar técnicas de entrenamiento más eficientes, sistemas de licenciamiento más creativos y modelos que dependan menos de la copia masiva no consentida. Lo que Bradford denomina, siguiendo la hipótesis de Porter, una reorientación de la innovación hacia estándares más altos de calidad y sostenibilidad.[96] La confianza del público en la IA añade, depende en última instancia de que los ciudadanos perciban que la tecnología opera dentro de los marcos legales y éticos: una IA que explota obras ajenas sin compensación puede generar un rechazo social que resulte más costoso a largo plazo que cualquier obligación regulatoria.

No obstante, la autora reconoce también los argumentos del lado contrario: las obligaciones regulatorias generan costes de cumplimiento que desvían recursos de la investigación, y la reducción del volumen de datos disponibles para el entrenamiento

[92] Stanford Human-Centered Artificial Intelligence (HAI), *AI Index Report 2025*, cap. 4: "Economy", Stanford University, 2025, Chapter 4.
[93] De La Durantaye, (2023), *op.cit*., p. 7.
[94] De La Durantaye (2025), *op. cit.*, p. 764.
[95] Bradford (2024), *op. cit.*, p. 382.
[96] *Ibid*., p. 403.

podría traducirse en modelos de menor calidad frente a los desarrollados en entornos más permisivos.[97] El debate, en definitiva, no está cerrado. Lo que sí puede afirmarse es que ninguno de los dos sistemas ha encontrado todavía un equilibrio estable entre proteger a los creadores y fomentar la innovación: la UE ha apostado por la certeza normativa a costa de un alcance limitado y trasladando la elección a los titulares del derecho, y Estados Unidos ha apostado por la flexibilidad judicial a costa de la incertidumbre. Ambos por vías distintas siguen trasladando el problema sin resolverlo.

3.3.3 El AI Act como capa regulatoria complementaria

El análisis del conflicto entre innovación y derechos de autor no estaría completo sin atender a un elemento que la Unión Europea ha introducido como complemento indispensable al sistema de la Directiva DSM: las obligaciones de transparencia previstas en el Reglamento de Inteligencia Artificial. Para entender su relevancia, conviene partir de la observación de Durantaye, quien identifica el control sobre las obras como uno de los dos ejes centrales del debate sobre el uso de contenido protegido para el entrenamiento de IA, junto con la compensación, señalando que transparencia y seguridad jurídica operan como elementos complementarios de ambos.[98] Sin control efectivo, la compensación es ilusoria; y sin transparencia, el control es imposible.

El problema es que el artículo 4.3 de la Directiva DSM, que permite a los titulares reservar sus derechos mediante declaración expresa en formato legible por máquina[99], presenta en la práctica obstáculos significativos que lo hacen difícilmente operativo. Como señala Durantaye, no existe todavía un estándar técnico específico para declarar válidamente esa reserva: los titulares recurren en la práctica a archivos *robots.txt*, diseñados originalmente para gestionar la indexación por motores de búsqueda, que no permiten diferenciación alguna, si un titular indica que no desea que su sitio sea rastreado con fines de entrenamiento, dejará también de aparecer en los resultados de búsqueda, lo que equivale en la práctica a desaparecer del entorno digital[100]. A ello se añade que muchos conjuntos de datos de entrenamiento no son públicamente accesibles, y que empresas que hasta hace

[97] *Ibid*., p.416.
[98] De La Durantaye (2025)., *op.cit*., p. 738.
[99] Directiva 2019/790, articulo 4.3: "*La excepción o limitación establecida en el apartado 1 se aplicará a condición de que el uso de las obras y otras prestaciones a que se refiere dicho apartado no esté reservado expresamente por los titulares de derechos de manera adecuada, como medios de lectura mecánica en el caso del contenido puesto a la disposición del público en línea*."
[100] De La Durantaye, (2023), *op.cit*., p. 9.

poco presumían de transparencia han optado por no revelar los detalles de sus datos de entrenamiento alegando presiones competitivas[101]. Sin saber qué obras se han utilizado, el titular no puede ni siquiera verificar si su reserva ha sido respetada.

Es en este punto donde interviene el Reglamento de la UE sobre Inteligencia Artificial o AI Act, concretamente a través del articulo 53 que establece obligaciones de transparencia en cuanto a las fuentes utilizadas para entrenar modelos de IA. El artículo 53.1.c) del Reglamento obliga a los proveedores de modelos de IA de uso general a establecer una política de cumplimiento del derecho de la Unión en materia de derechos de autor, incluyendo la identificación y el respeto de las reservas de derechos expresadas conforme al artículo 4.3 de la Directiva DSM, mediante el uso de tecnologías de vanguardia.[102] La UE intenta así recalibrar la balanza entre los intereses de los titulares y los de las empresas tecnológicas, haciendo que sean estas últimas quienes asuman la carga de identificar y respetar las reservas, en lugar de dejar esa responsabilidad en manos de unos titulares que carecen de los medios técnicos para ejercerla eficazmente.[103] El considerando 106 del AI Act refuerza esta lectura al precisar que cualquier proveedor que coloque un modelo de IA de uso general en el mercado europeo debe cumplir esta obligación con independencia de la jurisdicción en que hayan tenido lugar los actos de entrenamiento.[104]

Esta extensión territorial es deliberada y explícita: como señala Senftleben, el propio AI Act reconoce abiertamente su vocación de producir un efecto Bruselas en este ámbito, buscando nivelar el terreno de juego entre proveedores de modelos de IA de forma que ninguno pueda obtener una ventaja competitiva en el mercado europeo aplicando estándares de derechos de autor más bajos.[105] La lógica es la misma que ya identificamos

[101] *Ibid., p. 10.*
[102] AI Act, art. 53.1.c.
[103] De La Durantaye, (2025), *op.cit*., p. 750.
[104] AI Act, considerando 106: "Los proveedores que introduzcan modelos de IA de uso general en el mercado de la Unión deben garantizar el cumplimiento de las obligaciones pertinentes establecidas en el presente Reglamento. A tal fin, los proveedores de modelos de IA de uso general deben adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor y derechos afines, en particular para detectar y cumplir la reserva de derechos expresada por los titulares de derechos con arreglo al artículo 4, apartado 3, de la Directiva (UE) 2019/790. Todo proveedor que introduzca un modelo de IA de uso general en el mercado de la Unión debe cumplir esta obligación, independientemente de la jurisdicción en la que tengan lugar los actos pertinentes en materia de derechos de autor que sustentan el entrenamiento de dichos modelos de IA de uso general. Esta medida es necesaria para garantizar unas condiciones de competencia equitativas entre los proveedores de modelos de IA de uso general que impidan que un proveedor obtenga una ventaja competitiva en el mercado de la Unión aplicando normas en materia de derechos de autor menos estrictas que las establecidas en la Unión."
[105] Senftleben, *op.cit.,* p. 13.

en el capítulo 2 respecto al RGPD: si quieres acceder al mercado europeo, debes respetar las reglas europeas, con independencia de dónde hayas entrenado tu modelo.

Sin embargo, la efectividad real de este efecto Bruselas es, como mínimo, incierta. Como apuntan Sag y Yu, aunque el efecto Bruselas generado por regulaciones europeas anteriores es innegable, no está claro que otros países sientan la misma presión para adoptar legislación compatible con el AI Act, especialmente teniendo en cuenta que las empresas europeas de IA tienen una cuota de mercado muy limitada frente a sus competidoras estadounidenses y chinas. La dominancia de las grandes empresas americanas puede generar la situación inversa: que sean los reguladores europeos quienes deban equilibrar la imposición de obligaciones con el riesgo de que esas empresas amenacen con abandonar el mercado europeo.[106] Las cuestiones de aplicación extraterritorial y de ley aplicable identificadas por la doctrina podrían además atenuar considerablemente el efecto real de la norma más allá de las fronteras de la Unión.

En última instancia, el riesgo que subyace a toda esta arquitectura regulatoria es el que Samuelson ha denominado "*innovation arbitrage"*: si las obligaciones impuestas por la normativa europea resultan excesivamente onerosas, las empresas de IA simplemente optarán por entrenar sus modelos en jurisdicciones más permisivas, dejando a los titulares europeos sin compensación y a la industria europea sin modelos.[107] En este escenario, sería la UE quien saldría perjudicada. Sin embargo, este panorama podría invertirse: si los tribunales estadounidenses acaban interpretando el *fair use* de forma restrictiva en el contexto del entrenamiento de IA , como podría ocurrir en función del resultado de los grandes litigios pendientes, EE.UU. perdería la ventaja regulatoria que hoy lo convierte en destino preferente para el entrenamiento de modelos. En ese caso, la certeza normativa que ofrece el modelo europeo, con todas sus limitaciones, podría acabar siendo un activo y no un lastre.

3.4 Del conflicto normativo a la valoración comparada

El recorrido realizado a lo largo de los dos capítulos sustantivos de este trabajo ha permitido examinar, desde una perspectiva comparada, las respuestas que la Unión

[106] Sag, M. y Yu, P. K., "The globalization of copyright exceptions for AI training", *Emory Law Journal*, vol. 74, 2024, p. 1221.
[107] Samuelson, P., "Generative AI meets copyright", *Science*, vol. 381, n. º 6654, 2023, p. 159.

Europea y Estados Unidos han construido frente a los dos principales conflictos jurídicos que el uso intensivo de datos plantea en el contexto de la inteligencia artificial. La propiedad intelectual constituye, como hemos analizado, el segundo gran frente en el que ese uso intensivo colisiona con el ordenamiento jurídico, prolongando en el ámbito de la autoría la misma tensión que el capítulo anterior identificó en el de la privacidad. En ambos casos, las divergencias observadas no son accidentales ni meramente técnicas, sino expresión de filosofías de gobernanza distintas que se proyectan de forma coherente sobre cada uno de los ámbitos estudiados. Es desde esa constatación desde la que procede formular, a continuación, las conclusiones del trabajo.

CONCLUSIONES

PRIMERA.- La hipótesis que orienta este trabajo queda confirmada por el análisis comparado: las diferencias entre el ordenamiento jurídico de la Unión Europea y el de Estados Unidos en materia de protección de datos personales y propiedad intelectual no responden a divergencias técnicas o institucionales de grado, sino a filosofías de gobernanza estructuralmente distintas. El modelo europeo ancla la protección jurídica en los derechos fundamentales de la persona, concibiendo la regulación como una obligación estructural del Estado. El modelo norteamericano parte de una filosofía orientada al mercado y a la innovación, que confía en la autorregulación de la industria y en la intervención reactiva de las instituciones. Esta divergencia de naturaleza explica por qué ambos sistemas producen respuestas tan distintas ante unos mismos fenómenos tecnológicos, y se proyecta de forma coherente sobre cada uno de los ámbitos analizados.

SEGUNDA.- En materia de protección de datos personales, el análisis comparado revela una asimetría estructural entre un modelo europeo integral, horizontal y extraterritorial, basado en bases jurídicas tasadas, un catálogo amplio de derechos del interesado y un régimen sancionador con capacidad disuasoria real, y un modelo norteamericano sectorial y reactivo, en el que el tratamiento de datos es lícito por defecto y la protección depende del sector económico, del estado de residencia o de la política de privacidad aceptada. La efectividad del sistema europeo descansa sobre la combinación del principio de accountability y la sanción proporcional a la facturación global, elementos que el modelo estadounidense no replica. Con todo, el fenómeno del efecto Bruselas identificado por Bradford introduce una dimensión adicional a través de la aplicación extraterritorial del

RGPD y de la tendencia de las multinacionales a homogeneizar sus estándares hacia el nivel europeo, la regulación europea se proyecta más allá de sus fronteras y actúa como principal exportador global de estándares en materia de privacidad.

TERCERA.- En materia de propiedad intelectual, ambos ordenamientos coinciden en calificar el entrenamiento de modelos de IA como un proceso que genera actos de reproducción de obras protegidas susceptibles de constituir una infracción, pero articulan mecanismos distintos para superarla. La Unión Europea lo hace a través de las excepciones TDM de la Directiva DSM, complementadas por las obligaciones de transparencia del AI Act, que trasladan a los proveedores de modelos la carga de identificar y respetar las reservas de derechos. Estados Unidos delega esa determinación en la doctrina del *fair use*, cuya aplicación al entrenamiento de IA está siendo construida en tiempo real por los tribunales. Ninguno de los dos sistemas ha encontrado un equilibrio estable: la UE apuesta por la certeza normativa a costa de un alcance limitado; EE.UU. apuesta por la flexibilidad judicial a costa de la incertidumbre. Ambos, por vías distintas, siguen trasladando el problema sin resolverlo.

CUARTA.- El análisis comparado pone de manifiesto que la dicotomía entre regulación e innovación, frecuentemente presentada como inevitable, responde en realidad a una elección política sobre qué intereses se priorizan y quien asume el coste del desarrollo tecnológico. Como argumenta Bradford, el liderazgo tecnológico no depende estructuralmente de la ausencia de regulación. El riesgo de "*innovation arbitrage*" identificado por Samuelson es real, pero podría invertirse si los tribunales americanos acaban interpretando el *fair use* de forma restrictiva en los grandes litigios pendientes, en cuyo caso la certeza normativa del modelo europeo podría convertirse en una ventaja competitiva. La comparación entre el mayor regulador del mundo y el mayor innovador del mundo no arroja un vencedor claro, sino la constatación de que el derecho, en ambas jurisdicciones, llega tarde a una carrera en la que la tecnología lleva ventaja.

QUINTA.- Los marcos jurídicos analizados no constituyen respuestas definitivas sino estadios provisionales de un proceso regulatorio abierto, condicionado por el propio avance tecnológico y por la experiencia acumulada sobre la efectividad real de las soluciones adoptadas. La resolución de los grandes litigios pendientes en materia de *fair use*, la consolidación de las obligaciones del AI Act y la evolución de la práctica sancionadora del RGPD irán revelando si los mecanismos elegidos son capaces de

alcanzar los objetivos que justificaron su adopción. Cualquier valoración comparada de estos sistemas debe asumirse como parcial y situada en el tiempo: los cambios normativos y jurisprudenciales que inevitablemente se producirán podrán alterar de forma sustancial las conclusiones aquí alcanzadas.

Declaración de Uso de Herramientas de Inteligencia Artificial Generativa en Trabajos Fin de Grado

Por la presente, yo, Begoña Astarloa Domínguez, estudiante de Derecho y Administración y Dirección de Empresas de la Universidad Pontificia Comillas al presentar mi Trabajo Fin de Grado titulado "Desafíos regulatorios de la era digital. Un análisis comparado", declaro que he utilizado la herramienta de Inteligencia Artificial Generativa ChatGPT u otras similares de IAG de código sólo en el contexto de las actividades descritas a continuación:

1. **Crítico:** Para encontrar contra-argumentos a una tesis específica que pretendo defender.

2. **Referencias:** Usado conjuntamente con otras herramientas, como Science, para identificar referencias preliminares que luego he contrastado y validado.

3. **Constructor de plantillas:** Para diseñar formatos específicos para secciones del trabajo.

4. **Corrector de estilo literario y de lenguaje:** Para mejorar la calidad lingüística y estilística del texto.

5. **Sintetizador y divulgador de libros complicados:** Para resumir y comprender literatura compleja.

6. **Revisor:** Para recibir sugerencias sobre cómo mejorar y perfeccionar el trabajo con diferentes niveles de exigencia.

7. **Traductor:** Para traducir textos de un lenguaje a otro.

Afirmo que toda la información y contenido presentados en este trabajo son producto de mi investigación y esfuerzo individual, excepto donde se ha indicado lo contrario y se han dado los créditos correspondientes (he incluido las referencias adecuadas en el TFG y he explicitado para que se ha usado ChatGPT u otras herramientas similares). Soy consciente de las implicaciones académicas y éticas de presentar un trabajo no original y acepto las consecuencias de cualquier violación a esta declaración.

Fecha: 06/06/2026

Firma: Begoña Astarloa Domínguez

BIBLIOGRAFÍA:

Legislación

Instrumentos internacionales

Consejo de Europa, Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), Roma, 4 de noviembre de 1950.

Unión Europea:

Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, *Diario Oficial de la Unión Europea* L 167, de 22 de junio de 2001.

Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE, *Diario Oficial de la Unión Europea* L 130, de 17 de mayo de 2019.

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2022/2555 (*Reglamento de Inteligencia Artificial*), DOUE L 1689, de 12 de julio de 2024.

Unión Europea, Carta de los Derechos Fundamentales de la Unión Europea (CDFUE), *Diario Oficial de la Unión Europea* C 326, de 26 de octubre de 2012.

Unión Europea, Tratado de Funcionamiento de la Unión Europea (TFUE), versión consolidada, *Diario Oficial de la Unión Europea* C 202, de 7 de junio de 2016.

Estados Unidos

California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 *et seq.* (2018).

California Privacy Rights Act (CPRA), Proposition 24, Cal. Civ. Code § 1798.100 *et seq.* (2020), en vigor desde el 1 de enero de 2023.

Copyright Act, 17 U.S.C. §§ 106 y 107 (1976).

Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45 (1914, enmendado).

Jurisprudencia

Tribunal Supremo de los Estados Unidos (U.S. Supreme Court)

Griswold v. Connecticut, 381 U.S. 479 (1965) (disponible en https://supreme.justia.com/cases/federal/us/381/479/; última consulta 04/05/2026)

Katz v. United States, 389 U.S. 347 (1967) (disponible en https://supreme.justia.com/cases/federal/us/389/347/; última consulta 04/05/2026).

Roe v. Wade, 410 U.S. 113 (1973) (disponible en https://supreme.justia.com/cases/federal/us/410/113/; última consulta 04/05/2026).

Tribunales de Estados Unidos

Andersen et al. v. Stability AI Ltd. et al., No. 3:23-cv-00201 (N.D. Cal. 2023).

Bartz et al. v. Anthropic PBC, No. 3:23-cv-03223 (N.D. Cal. 2023).

Kadrey et al. v. Meta Platforms, Inc., No. 3:23-cv-03417 (N.D. Cal. 2023).

The New York Times Co. v. Microsoft Corp. and OpenAI, No. 1:23-cv-11195 (S.D.N.Y. 2023).

Resoluciones y decisiones administrativas

Comisión de Protección de Datos de Irlanda (*Data Protection Commission*), Decisión en el asunto Meta Platforms Ireland Limited, Referencia IN-20-8-1, de 12 de mayo

de 2023 (disponible en https://finreg360.com/wp-content/uploads/2023/05/final_for_issue_ov_transfers_decision_12-05-23-1.pdf; última consulta 28/03/2026).

Informes y documentos institucionales

Australian Society of Authors (ASA), "Submission in response to Harnessing Data and Digital Technology Inquiry Interim Report", Productivity Commission, 15 de septiembre de 2025 (disponible en https://public-website--staging.s3.amazonaws.com/uploads/2025/09/Productivity-Commission-Interim-Report-Australian-Society-of-Authors-Submission.pdf; última consulta 5/04/2026).

DLA Piper, "Data Protection Laws of the World: United States", 2024, (disponible en https://www.dlapiperdataprotection.com; última consulta 26/03/2026).

Productivity Commission, *Harnessing Data and Digital Technology: Interim Report*, Australian Government, Canberra, agosto de 2025 (disponible en https://assets.pc.gov.au/2025-09/data-digital interim.pdf?VersionId=rbzZkLQzxhnPQz4O6MwZ.moIhJRyarOo; última consulta 13/04/2026).

U.S. Copyright Office, *Copyright and Artificial Intelligence, Part 3: Generative AI Training*, Pre-Publication Version, U.S. Copyright Office, Washington D.C., 2025. (disponible en https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf; ultima consulta 04/05/2026).

Obras doctrinales

Aileen Graef, *Elon Musk: We Are "Summoning a Demon" with Artificial Intelligence*, UPI (Oct. 27, 2014, 7:50 AM), http://www.upi.com/Business_News/2014/10/27/Elon- Musk-We-are-summoning-a-demon-with-artificial-intelligence/4191414407652/)

Barrio Andrés, M., "La regulación del derecho a la protección de datos en los Estados Unidos: hacia un RGPD norteamericano", *Cuadernos de Derecho Transnacional*, vol. 14, n.º 2, 2022, pp. 186–193.

Barrio Andrés, M., "Los principios estructurales del Reglamento General de Protección de Datos", *Actualidad Jurídica Iberoamericana*, n.º 20, febrero de 2024, pp. 1322-1341.

Becker, T., "When Congress makes no policy choice", *Columbia Law Review*, vol. 120, n. º 5, 2020, pp. 134-152.

Bennett, L., "Agents of Change. How the Law 'Copes' with Technological Change", *Griffith Law Review*, vol. 20, n.º 3, 2012, pp. 763-794.

Bradford, A., "The Brussels Effect", *Northwestern University Law Review*, vol. 107, n. º 1, 2012, pp. 1-68.

Bradford, A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020.

Bradford, A., "The false choice between digital regulation and innovation", *Northwestern University Law Review*, vol. 119, 2024, pp. 377- 453.

Brill, J., "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data", *Microsoft On the Issues*, 21 de mayo de 2018 (disponible en https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/; última consulta 28/03/2026).

Christensen, C. M., Raynor, M. and McDonald, R. (2015). 'What is disruptive innovation?'. *Harvard Business Review,* 93, 44–53.

De La Durantaye, K., "Garbage in, garbage out. Regulating generative AI through copyright law", *ZUM - Zeitschrift für Urheber- und Medienrecht*, n. º 10, 2023, pp. 645-660.

De La Durantaye, K., "Control and compensation. A comparative analysis of copyright exceptions for training generative AI", *IIC - International Review of Intellectual Property and Competition Law*, vol. 56, n. º 4, 2025, pp. 737-770.

Dopazo Fraguío, M. P., "Protección de datos en el Derecho de la Unión Europea: principales aportaciones doctrinales y marco regulatorio vigente", *Revista de Derecho Europeo*, n.º 68, 2018, pp. 115-148.

Estepa Montero, M., "El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas", *Anuario Jurídico y Económico Escurialense*, n.º 55, 2022, pp. 67-90.

Frison-Roche, M. A., "Ex ante – ex post, justificación de un derecho propio y específico de la regulación", *Responsabilidad Civil y Seguros*, año XI, n.º 10, octubre de 2010, pp. 5-13.

Geiger, C., Frosio, G. y Bulayenko, O., "Text and data mining: Articles 3 and 4 of the Directive 2019/790/EU", en *Propiedad intelectual y mercado único digital europea*, Tirant lo Blanch, Valencia, 2019, pp. 27-71.

Ijaiya, H. y Odumuwagun, O. O., "Advancing artificial intelligence and safeguarding data privacy: a comparative study of EU and US regulatory frameworks amid emerging cyber threats", *International Journal of Research Publication and Reviews*, vol. 5, n. º 12, 2024, pp. 3357-3375.

Kelly, K., "The three breakthroughs that have finally unleashed AI on the world", *Wired*, 27 de octubre de 2014 (disponible en https://www.wired.com/2014/10/future-of-artificial-intelligence/; última consulta 08/03/26).

Kumari, P., "Legal frameworks for AI regulation: a comparative study", *Advances in Consumer Research*, vol. 2, n. º 2, 2025, pp. 216-224.

Margoni, T. y Kretschmer, M., "A deeper look into the EU text and data mining exceptions: harmonisation, data ownership, and the future of technology", *GRUR International*, vol. 71, n. º 8, 2022, pp. 685-701.

McCarthy, J., “What Is Artificial Intelligence?”, Stanford University, 2007 (http://www-formal.stanford.edu/jmc/whatisai.html; última consulta 06/05/2026).

Nocetti, J., "Will Europe remain a 'digital colony'?", en Gomart, T. y Hecker, M. (dirs.), *European Elections 2019: Structuring the Debate*, Institut Français des Relations Internationales, París, 2019.

Pérez Luño, A. E., “El Derecho ante las nuevas tecnologías”, *El Notario del Siglo XXI*, n.º 41, 2012 (disponible en https://legado.elnotario.es/index.php/hemeroteca/revista-41/548-el-derecho-ante-las-nuevas-tecnologias-0-8050094412686392; última consulta el 04/05/2026).

Sag, M. y Yu, P. K., "The globalization of copyright exceptions for AI training", *Emory Law Journal*, vol. 74, 2024, pp. 1163-1227.

Samuelson, P., "Generative AI meets copyright", *Science*, vol. 381, n. º 6654, 2023, pp. 158-161.

Scherer, M. U., “Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies”, *Harvard Journal of Law & Technology*, vol. 29, n. º 2, 2016, pp. 353–400 (disponible en https://perma.cc/M98J-VYNH; última consulta el 04/05/2026).

Senftleben, M., "AI Act and author remuneration: a model for other regions?", SSRN Working Paper, n. º 4740268, 2024 (disponible en https://ssrn.com/abstract=4740268; última consulta 06/04/2026).

Sobrino, J., "Protección de datos y privacidad: estudio comparado entre la Unión Europea y Estados Unidos", *Revista de Derecho UNED*, n.º 25, 2019, pp. 687-713.

Solove, D. J. y Hartzog, W., "The FTC and the new common law of privacy", *Columbia Law Review*, vol. 114, 2014, pp. 583-676.

Stanford Human-Centered Artificial Intelligence (HAI), *AI Index Report 2025*, cap. 4: "Economy", Stanford University, 2025 (disponible en https://hai.stanford.edu/ai-index/2025-ai-index-report/economy; última consulta 28/03/2026).

Turing, A. M., "Computing Machinery and Intelligence", *Mind*, vol. 59, n.º 236, 1950, pp. 433-460.

Warren, S. D. y Brandeis, L. D., "The right to privacy", *Harvard Law Review*, vol. 4, n. º 5, 1890, pp. 193-220.

Whitman, J. Q., "The two western cultures of privacy: Dignity versus liberty", *The Yale Law Journal*, vol. 113, n. º 3, 2004, pp. 1151-1220.