FACULTAD DE DERECHO

LA PROTECCIÓN DE DATOS EN LA INTELIGENCIA ARTIFICIAL DESDE LA PERSPECTIVA CONSTITUCIONAL

Claudia Vivas Sainz de la Torre

5º E3 Analytics

Derecho Constitucional

Tutor: Miguel Ayuso Torres

Madrid

Marzo 2025

RESUMEN

El siguiente trabajo tiene como objetivo principal analizar el impacto de la inteligencia artificial (IA) en los derechos fundamentales del ciudadano. En la era digital, la inteligencia artificial se halla presente en multitud de sectores, automatizando procesos y facilitando la toma de decisiones. No obstante, al ser una tecnología reciente que avanza mucho más rápido que el Derecho, su marco legislativo está aún por explorar, lo que puede desembocar en vulneraciones de los derechos fundamentales. Por ello, el presente trabajo se centra en analizar los desafíos jurídicos que presenta la IA actualmente, enfocándose en tres derechos específicos: el derecho a la igualdad y no discriminación, el derecho a la libertad de expresión y el derecho a la privacidad y protección de datos personales.

A lo largo del trabajo, en primer lugar, se analizará la base teórica que rodea a la inteligencia artificial, así como el marco legal actual sobre el que ésta se sustenta. Posteriormente, se procederá a analizar minuciosamente cada derecho mencionado, estudiando los perjuicios que puede causar la IA al ciudadano en cada ámbito, y abordando su marco legal y lagunas legales existentes. Por último, se analizarán los desafíos éticos y jurídicos que existen para el legislador a la hora de promover la innovación tecnológica respetando los derechos fundamentales.

Palabras clave: inteligencia artificial, derechos fundamentales, discriminación algorítmica, desinformación, ciberataques, innovación tecnológica, ética digital.

ABSTRACT

The main objective of this paper is to analyze the impact of artificial intelligence (AI) on citizens' fundamental rights. In the digital age, AI is present in a wide range of sectors, automating processes and facilitating decision-making. However, as a rapidly evolving technology that advances faster than the law, its legislative framework is still underdeveloped, which may lead to violations of fundamental rights. For this reason, the present study focuses on examining the current legal challenges posed by AI, with a specific focus on three key rights: the right to equality and non-discrimination, the right to freedom of expression, and the right to privacy and personal data protection.

Throughout the paper, the theoretical foundations surrounding artificial intelligence are first examined, along with the current legal framework on which it is based. Then, each of the aforementioned rights is thoroughly analyzed, considering the potential harm that AI may cause to individuals in each area, as well as addressing the existing legal frameworks and their regulatory gaps. Finally, the paper explores the ethical and legal challenges faced by legislators when promoting technological innovation while safeguarding fundamental rights.

Key words: artificial intelligence, fundamental rights, algorithmic discrimination, disinformation, cyberattacks, technological innovation, digital ethics.

ÍNDICE

LISTADO DE SIGLAS Y ABREVIATURAS

AEPD (Agencia Española de Protección de Datos)

AESIA (Agencia Española de Supervisión de la Inteligencia Artificial)

ANN (Artificial Neural Networks / Redes Neuronales Artificiales)

Art. o Arts. (Artículo/s)

CDFUE (Carta de los Derechos Fundamentales de la Unión Europea)

EE.UU. (Estados Unidos)

ENIA (Estrategia Nacional de Inteligencia Artificial)

IA (Inteligencia Artificial)

LOPDGDD (Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales)

ML (Machine Learning / Aprendizaje Automático)

PLN (Procesamiento del Lenguaje Natural)

RGPD (Reglamento General de Protección de Datos)

UE (Unión Europea)

CAPÍTULO I: INTRODUCCIÓN

1. JUSTIFICACIÓN Y RELEVANCIA DEL TEMA

¿Cuántas veces hemos escuchado o hemos dicho la siguiente frase: "Alexa, pon música"? ¿O "Alexa: dime qué tiempo va a hacer hoy"? Cada vez son más los hogares que cuentan con asistentes virtuales como Siri o Alexa, los cuales responden a órdenes sencillas como actualizar la lista de la compra, reproducir una canción o, incluso, grabar un mensaje de voz. No obstante, detrás de estas acciones aparentemente simples, se encuentra una tecnología compleja que transforma y analiza grandes conjuntos de datos.

Aparte de estos asistentes virtuales, podemos pensar en otros ejemplos en los que la inteligencia artificial (en adelante, IA) juega un papel fundamental en nuestra rutina, como tener abierta una cuenta de alguna red social como Instagram, o ver películas en plataformas de streaming como Netflix, las cuales utilizan algoritmos de *machine learning* para enseñarnos anuncios personalizados a nuestras preferencias y consumos habituales. Estos sistemas funcionan gracias a un continuo intercambio de datos, tanto de carácter personal, como datos financieros o incluso secretos comerciales; entre usuarios, máquinas y empresas.

Como vemos, la IA, ha adoptado un papel fundamental en nuestro día a día. Además, la cantidad de datos que generan tanto personas como máquinas está creciendo desmesuradamente, manifestándose en multitud de sectores. Es tal la presencia de sistemas que utilizan esta tecnología, que es fundamental conocer cómo funcionan y, principalmente, qué regulación les respalda.

Por ello, los organismos internacionales y gobiernos de distintos países tienen como objetivo elaborar un marco legal efectivo que proteja los derechos fundamentales de los ciudadanos frente a los riesgos que presenta esta tecnología tan avanzada. De hecho, la presidenta de la Comisión Europea, Úrsula von der Leyen, ya enfatizó la necesidad de lograr un *equilibrio en el flujo y el uso de datos al mismo tiempo que se preservaran altos estándares de privacidad, seguridad y ética*[1].

[1] Von der Leyen, U., "Europe's choice. Political guidelines for the next European Commission 2024-2029", Comisión Europea (disponible en e6cd4328-673c-4e7a-8683-f63ffb2cf648_en; última consulta 28/01/2025).

Es evidente, pues, que resulta imprescindible fomentar la transparencia y la seguridad en el uso de datos masivos, así como desarrollar un plano normativo que no entre en conflicto con los derechos fundamentales, y que permita impulsar la innovación tecnológica de manera eficiente y sostenible.

2. OBJETIVOS Y METODOLOGÍA DEL TRABAJO

El presente trabajo tiene como objetivo principal el análisis de la actual regulación de la protección de datos en la IA, y el consiguiente estudio de cómo ésta es capaz de afectar a los derechos fundamentales recogidos en la Constitución.

Para ello, en primer lugar, abordaremos el marco teórico que rodea a la IA, analizando su definición y evolución histórica, los tipos de IA en función de su capacidad, sus modos de trabajo principales y su impacto en la sociedad, destacando varios sectores en los que está presente a día de hoy.

En segundo lugar, analizaremos las bases legales, tanto a nivel europeo como a nivel nacional, sobre las que se sustentan este tipo de sistemas. Por un lado, estudiaremos las normativas que regulan la IA, y, por otro lado, haremos un análisis específico sobre las normas de protección de datos de la IA. En el primer grupo, hablaremos del reciente AI Act[2] y de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación[3], entre otras. En el segundo grupo, hablaremos, a nivel nacional, del artículo 18.4 CE, y de la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)[4]; y, a nivel europeo, nos centraremos en el Reglamento General de Protección de Datos (RGPD)[5], el

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

[3] Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación (BOE 13 de julio de 2022).

[4] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 6 de diciembre de 2018).

[5] 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

Data Act[6] y el Data Governance Act[7]. También comentaremos los organismos e instituciones que se encargan de aplicar las regulaciones en esta materia, tanto en España como en Europa.

Por último, realizaremos un minucioso estudio de cómo los sistemas de IA pueden vulnerar los derechos fundamentales, concretamente, el derecho a la igualdad y no discriminación, el derecho a la libertad de expresión, y el derecho a la privacidad y protección de datos personales del ciudadano. Además, analizaremos cómo se protege al ciudadano de tales vulneraciones en nuestro país, y qué desafíos éticos y jurídicos encuentra el legislador a la hora de establecer una base legal sólida sobre la IA.

esos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE 4 de mayo de 2016).

[6] Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (DOUE 22 de diciembre de 2023).

[7] Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).

CAPÍTULO II: MARCO TEÓRICO

1. LA INTELIGENCIA ARTIFICIAL: INTRODUCCIÓN

La Inteligencia Artificial (IA) es la tecnología a través de la cual las máquinas son capaces de simular habilidades y comportamientos propios del ser humano, como la capacidad de razonar y resolver problemas. Según la Comunicación sobre Inteligencia Artificial para Europa de 2018, *el término «inteligencia artificial» (IA) se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos*[8].

No obstante, hemos de tener en cuenta otras definiciones de IA más antiguas, como la de Barr y Feigenbaum, de 1981, según la cual la IA es una *rama de las ciencias de la computación que trata del diseño de sistemas inteligentes, es decir, sistemas que presentan características que normalmente asociamos con la inteligencia humana: comprensión del lenguaje, razonamiento, aprendizaje, resolución de problemas, etc*[9]. Por otro lado, Rich y Knight definían este campo, en 1991, como *el estudio de cómo hacer que los ordenadores realicen tareas cognoscitivas que, por ahora, las personas hacen mejor*[10].

Resulta curioso y fascinante estudiar cómo la IA ha evolucionado a lo largo de la historia, creándose distintos hitos que poco a poco fueron definiendo las máquinas que conocemos actualmente.

Ya en la mitología griega se hablaba de Talos, un gigante de bronce, creado por el dios Dédalo para defender la isla de Creta, que lanzaba piedras a los invasores que llegaban a través del mar. Este se considera uno de los primeros ejemplos mitológicos de lo que consideramos actualmente como "robot", pues simboliza el deseo del hombre de ser capaz de crear máquinas que actuasen como los seres humanos[11].

---

[8] Comisión Europea. (2018). "Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Inteligencia Artificial para Europa" (COM(2018) 237 final) (disponible en AI Communication, última consulta 21/02/2025).
[9] Barr, A., y Feigenbaum, E., The Handbook of Artificial Intelligence, HeurisTech Press, Standford, 1981.
[10] Rich,E., y Knight, K., Artificial Intelligence, McGraw-Hill, Nueva York, 1991.
[11] Ramos Cabrer, M. "Fundamentos de la Inteligencia Artificial: Tema 1-Introducción", Universidad de Vigo.

Posteriormente, Herón de Alejandría, en torno al año 70 d.C., plasmó en sus escritos ciertas máquinas, que posteriormente se conocerían como "autómatas", y que se utilizaban para representar escenas de la guerra de Troya. Además, durante la Edad Media también surgieron otras ideas de máquinas automáticas, como el león mecánico de Leonardo Da Vinci en el s.XV, o el "Ars Magna" (El Gran Arte) de Ramón Llull, obra en la que el filósofo del s. XIII trató de automatizar el razonamiento lógico y propio del ser humano[12]. No obstante, lo más innovador de la Edad Moderna llegó de la mano de René Descartes, en su "Discurso sobre el método" de 1637, donde prefigura: *Cuántos autómatas diferentes o máquinas en movimiento pueden ser fabricados por la industria del hombre... Porque podemos entender fácilmente que una máquina esté constituida para que pueda pronunciar palabras, e incluso emitir algunas respuestas a la acción sobre ella de tipo corpóreo, que provoca un cambio en sus órganos; por ejemplo, si se toca en una parte particular, puede preguntarnos qué queremos decirle; si en otra parte puede exclamar que está siendo lastimado, y así sucesivamente*[13].

Sin embargo, el principal impulsor del concepto de IA fue el conocido como "el padre de la informática", Alan Turing, un matemático británico que, en 1950, comenzó a cuestionarse si las máquinas eran capaces de razonar como los seres humanos, y desarrolló el "Test de Turing", según el cuál, si una máquina es capaz de emular la inteligencia humana de tal manera que el ser humano no pueda identificar cuál es la máquina y cuál es el humano, entonces esa máquina se puede calificar como "inteligente". Este experimento, que plasmó en su trabajo "Computing Machinery and Intelligence", ha desencadenado que se desarrollen algoritmos para crear sistemas cada vez más avanzados de IA, como el famoso ChatGPT de la empresa OpenAI.

Como vemos, Descartes introduce en su día lo que muchos años después se convertiría en el Test de Turing. Ambos comparten la idea de que tanto las máquinas como los humanos se pueden distinguir por su capacidad de mantener una conversación y su lenguaje. No obstante, lo que no pensó Descartes es que las máquinas llegarían a simular a los humanos hasta tal punto de pasar desapercibidas, como ocurre actualmente con el desarrollo de la IA.

[12] Ramos Cabrer, M. "Fundamentos de la Inteligencia Artificial: Tema 1-Introducción", Universidad de Vigo. Op.cit. p9.
[13] Descartes, R., Discurso sobre el método, Leiden, 1637.

2. TIPOS DE INTELIGENCIA ARTIFICIAL

Las inteligencias artificiales se pueden clasificar en tres niveles dependiendo de su alcance y de su capacidad: IA Débil (Narrow AI), IA General (AGI) y Superinteligencia (ASI).

Hablemos primero de la IA Débil. Este tipo de IA se caracteriza por estar diseñada por una tecnología muy sencilla y limitada, de forma que sus sistemas se utilizan para realizar tareas simples sin intentar replicar en conciencia la inteligencia humana. Funcionan a base de algoritmos y reglas predefinidas, utilizando una gran cantidad de datos; así como técnicas de *machine learning* que les permiten reconocer y detectar patrones. Su inteligencia se limita a saber realizar las funciones para las que están específicamente programados, las cuales versan desde el reconocimiento de imágenes y voz, hasta la traducción de idiomas y la recomendación de anuncios personalizados[14].

Margaret Rouse, experta en tecnología, explica perfectamente el concepto de este tipo de IA, especificando que *un muy buen ejemplo de IA débil es Siri, de Apple, que tiene Internet detrás como potente base de datos. Siri parece muy inteligente, ya que es capaz de mantener una conversación con personas reales, incluso hacer comentarios sarcásticos y algunos chistes, pero en realidad funciona de una manera muy sencilla y predefinida*[15]. Como Siri, existen otros asistentes virtuales (Alexa, Google Assistant), que utilizan técnicas de IA débil, como el Procesamiento del Lenguaje Natural (PLN), para detectar la consulta del usuario y ofrecer la respuesta adecuada. Asimismo, la IA débil tiene un papel fundamental, curiosamente, en invenciones actuales como los vehículos autónomos, pues permite que el coche detecte a los peatones en la carretera y reconozca señales de tráfico para evitar accidentes.

[14] Rouse, M., "Inteligencia artificial débil", Techopedia. (disponible en ¿Qué significa la inteligencia artificial débil?, última consulta 13/01/2025).
[15] Rouse, M., "Inteligencia artificial débil", Techopedia. (disponible en ¿Qué significa la inteligencia artificial débil?, última consulta 13/01/2025). Op.cit. p.11.

Dentro de esta primera clasificación, debemos mencionar dos subtipos de IA débil analizados por la Scientific Foresight Unit (STOA) del Parlamento Europeo[16]: la IA Simbólica y las Técnicas de Aprendizaje Automático o *Machine Learning*.

En primer lugar, la IA Simbólica, desarrollada entre los años 1950 y 1990, utiliza el razonamiento simbólico y el conocimiento codificado para resolver problemas. Mediante el procesamiento de caracteres, sus algoritmos utilizan reglas para hacer predicciones y deducciones, por ejemplo, "si X=Y e Y=Z, entonces X=Z"[17]. Uno de los principales experimentos que utiliza este tipo de IA es el sistema experto MYCIN, desarrollado en la Universidad de Standford en 1970, el cuál estudiaba si una máquina era capaz de detectar una enfermedad en función de los síntomas que presentaba el paciente. Utilizaba reglas como: *SI el paciente tiene fiebre Y el paciente tiene tos Y el paciente tiene dificultad para respirar, ENTONCES el paciente puede tener neumonía*[18]. En base a esta información, el algoritmo era capaz de hacer recomendaciones al personal sanitario sobre el tratamiento de la enfermedad.

Como vemos, si bien esta IA es muy útil y se utiliza como medidas de apoyo en muchos campos, también presenta claras limitaciones de funcionamiento, pues estos sistemas requieren que los humanos codifiquemos nuestros conocimientos de manera que la máquina pueda reconocerlos y tomar una decisión. Por ello, en las últimas décadas se han desarrollado lo que se conoce como técnicas de aprendizaje automático o *machine learning*, las cuales permiten que sus algoritmos se entrenen a sí mismos e incorporen mejoras, ampliando el conocimiento codificado previamente por el ser humano. Existen muchas técnicas de *machine learning*, entre las que destacamos las ANNs (Artificial Neural Networks) o Redes Neuronales Artificiales, las cuales emulan el comportamiento de las redes neuronales del ser humano.

Siendo los párrafos anteriores ejemplos de la IA débil, pasemos ahora a analizar el segundo tipo de IA: la IA general (AGI), una superinteligencia artificial que se prevé que se desarrolle en las próximas décadas. Esta propuesta ya se discutió en 1955 por cuatro

[16] Boucher, P. Artificial intelligence: How does it work, why does it matter, and what can we do about it?,European Parliamentary Research Service (EPRS), Bruselas, 2020.
[17] Rodríguez, S. "IA neurosimbólica, todo lo que debes saber", Big Data Magazine. (disponible en IA neurosimbólica, todo lo que debes saber - Big Data Magazine; última consulta 18/12/2024).
[18] Sancho Azcoitia, S., "MYCIN, El comienzo de la Inteligencia Artificial en el mundo de la medicina", Telefónica Tech (disponible en MYCIN, El comienzo de la Inteligencia Artificial en el mundo de la medicina, última consulta 30/01/2025).

investigadores: Jon McCarthy, Marvin Minsky, Nathaniel Rochester y Claude Shannon; los cuales organizaron un seminario que daría pie a un nuevo campo de investigación: la Inteligencia Artificial.

Ésta se asemejará aún más a la inteligencia humana, y será capaz de desarrollar algoritmos que permitan a las máquinas liberarse del control humano, de tal manera que serán dotadas con capacidades de comprensión, aprendizaje y razonamiento. No obstante, a día de hoy no conocemos ningún ejemplo específico de este tipo de tecnología, aunque no será de extrañar que en los próximos años surjan ejemplos concretos. De hecho, existen algunas organizaciones que se han puesto en marcha para crear IAs seguras para el usuario, como OpenAI o DeepMind. Además, según McKinsey & Company, se espera que dentro de unas décadas la IA Generativa pueda competir con hasta el 25% de la población trabajadora en diferentes industrias, sobre todo en áreas como en la educación, las artes, ramas tecnológicas e incluso el derecho[19].

Por último, nos encontramos con la Superinteligencia Artificial (ASI). Esta avanzada tecnología aún no se ha desarrollado, pues hemos de esperar a que se aplique la IA general primero. Para que la ASI pueda convertirse en una realidad, es necesario que sus componentes básicos terminen su proceso de desarrollo. En primer lugar, lo más probable es que ASI exija tratar conjuntos de grandes cantidades de datos, lo que requiere el avance de técnicas como los modelos lingüísticos (LLM) y el procesamiento del lenguaje natural (PLN). Además, ASI probablemente demandará de redes neuronales mucho más complejas que las que existen actualmente; así como algoritmos más sofisticados[20].

Por tanto, si bien es cierto que se prevé la creación de IAs muy avanzadas, de momento solo tenemos constancia de una IA débil, que, aunque resulte sencilla y limitada, está presente en multitud de sectores, mejorando la eficiencia de la toma de decisiones.

[19] Chui, M., "et al", "The economic potential of generative AI: The next productivity frontier", European Parliamentary Research Service (EPRS), disponible en the-economic-potential-of-generative-ai-the-next-productivity-frontier-vf.pdf; última consulta 28/01/2025).

[20] Hernández Escobar, C., "¿Qué es la superinteligencia artificial y por qué podría ser necesaria para el futuro?", OpenSistemas, (disponible en ¿Qué es la superinteligencia artificial y por qué podría ser necesaria para el futuro? - OpenSistemas, última consulta 21/01/2025).

3. MODOS DE TRABAJO DE LA INTELIGENCIA ARTIFICIAL

La IA se ha convertido en una de las tecnologías más avanzadas de la era digital, la cual está presente en numerosos aspectos de nuestra vida cotidiana. Para entender cómo funciona, es fundamental conocer los pilares sobre los que ésta se sustenta. Entre las técnicas más comunes de la IA, destacan las siguientes:

Machine Learning o Aprendizaje Automático

Machine Learning (en adelante, ML) hace referencia a una subcategoría de IA débil, cuyo objetivo reside en que las máquinas entrenen sus algoritmos encontrando patrones entre los distintos datasets, para mejorar la experiencia del usuario y aumentar la eficacia en la toma de decisiones. Como vemos, el ML es un tipo de aprendizaje que depende del ser humano hasta cierto punto, pues se programa a las máquinas para que sean capaces de mejorar y superar obstáculos por sí solas[21].

Issam El Naqa, Ruijiang Li y Martin J.Murphy definen los algoritmos de ML en su libro "Machine Learning in Radiation Oncology" como *un proceso computacional que utiliza datos de entrada para lograr una tarea deseada sin ser literalmente programado (es decir, "codificado de forma rígida") para producir un resultado particular. Estos algoritmos están, en cierto modo, "codificados de manera flexible" en el sentido de que alteran o adaptan automáticamente su arquitectura a través de la repetición (es decir, la "experiencia") para volverse cada vez mejores en la realización de la tarea deseada*[22].

Estas técnicas se utilizan, por poner un ejemplo, en plataformas de streaming como Netflix o Spotify, las cuales aplican sistemas de recomendación que predicen las películas, series o canciones que le pueden gustar al usuario en base a sus preferencias.

[21] El Naqa, I., "et al", Machine Learning in Radiation Oncology: Theory and Applications, Springer, Nueva York, 2015).
[22] El Naqa, I., "et al", Machine Learning in Radiation Oncology: Theory and Applications, Springer, Nueva York, 2015). Op.cit. p.14.

Redes Neuronales Artificiales (ANN)

Otra técnica de IA que no pasa desapercibida son las Redes Neuronales Artificiales, o Artificial Neural Networks (en adelante, ANN), *aquellas redes en las que existen elementos procesadores de información de cuyas interacciones locales depende el comportamiento del conjunto del sistema*[23]. Claudio Javier Tablada y Germán Ariel Torres definen la red neuronal artificial, en un artículo publicado en la Revista de Educación Matemática, como *un modelo matemático inspirado en el comportamiento biológico de las neuronas y en la estructura del cerebro. Esta también puede ser vista como un sistema inteligente que lleva a cabo tareas de manera distinta a como lo hacen las computadoras actuales*[24].

Por tanto, estas se comportan como un cerebro humano, el cual obtiene aprendizaje extrayendo conocimiento a través de un conjunto de datos. De esta manera, al igual que nuestro cerebro, las ANNs están formadas por nodos que simulan las neuronas, las cuales reciben *inputs* o datos de entrada, realizan los cálculos pertinentes, y emiten un *output* o dato de salida.

En cuanto a sus aplicaciones prácticas, son técnicas de IA débil que se utilizan, principalmente, para identificar imágenes y objetos, reconocer la voz, o incluso diagnosticar enfermedades a través del reconocimiento de patrones en diversas radiografías.

Un ejemplo práctico que analizaremos es el de AlphaGo de DeepMind. AlphaGo es un sistema que utiliza IA, y que fue desarrollado por la empresa DeepMind para jugar al Go, un juego de mesa virtual, utilizando ANNs. El objetivo de estas técnicas es que el sistema aprenda a jugar por sí solo analizando la probabilidad de ganar la partida desde cualquier posición del tablero, siendo, de esta manera, capaz de vencer a seres humanos[25].

---

[23] Hilera, J., y Martínez, V., Redes Neuronales Artificiales: Fundamentos, modelos y aplicaciones, RA-MA, Madrid, 1995.

[24] Tablada, C.J. y Ariel Torres, G., "Redes Neuronales Artificiales", Revista de Educación Matemática, vol.24, n. 3, 2009).

[25] Moliné, A. "La máquina contra el ser humano: AlphaGo vs humanity", Acento (disponible en La máquina contra el ser humano: AlphaGo vs humanity | Acento, última consulta 29/01/2025).

Algoritmos de Optimización

Por último, hablemos de los algoritmos de optimización. La Investigación Operativa es una disciplina matemática relativamente reciente, pues surgió durante la Segunda Guerra Mundial en Inglaterra, donde el gobierno británico agrupó a varios matemáticos, científicos y físicos con el objetivo de analizar problemas militares para gestionar recursos y tomar decisiones bélicas de manera eficaz. Tal y como analiza Rafael Martí Cunquero, en "Algoritmos Heurísticos en Optimización Combinatoria", *en el lenguaje coloquial, optimizar significa poco más que mejorar; sin embargo, en el contexto científico la optimización es el proceso de tratar de encontrar la mejor solución posible para un determinado problema. En un problema de optimización existen diferentes soluciones, un criterio para discriminar entre ellas y el objetivo es encontrar la mejor*[26].

De esta manera, un algoritmo de optimización hace referencia a una herramienta matemática utilizada para maximizar o minimizar una función objetivo, intentando encontrar la mejor respuesta a un problema, siendo las soluciones infinitas.

Estas técnicas son comúnmente utilizadas en empresas vanguardistas como Amazon, que analizan qué rutas siguen sus repartidores, cuánto tiempo tardan en llegar desde el almacén a la dirección de entrega, y estudian cómo la empresa puede optimizar dichas rutas para ahorrar en costes, tiempo y consumo de combustible. Estas novedades de vez en cuando derivan en despidos gestionados por una máquina, como le ocurrió a Stephen Normandin, un ex trabajador de la empresa de Jeff Bezos en Arkansas, EE.UU. Spencer Soper, en su artículo "Fired by bot at Amazon, 'it's you against the machine'" comenta la situación de Normandin, y analiza los problemas que puede causarle al trabajador este tipo de tecnología, pues se enfrenta a la posibilidad de recibir un email comunicándoles su despido y consecuente reemplazo por una máquina que haga más eficientemente su trabajo. Según Soper, *cada vez más, la empresa está cediendo su operación de recursos humanos a las máquinas, utilizando software no solo para gestionar a los trabajadores en sus almacenes, sino también para supervisar a los conductores contratados, las empresas de reparto independientes e incluso el desempeño de sus empleados de oficina*[27].

---

[26] Martí Cunquero, R., "Algoritmos Heurísticos de Optimización Combinatoria", Valencia.
[27] Soper, S., "Fired by Bot at Amazon: 'It's You Against the Machine'", *Bloomberg*, (disponible en Fired by Bot: Amazon Turns to Machine Managers And Workers Are Losing Out - Bloomberg, última consulta 20/01/2025).

4. APLICACIONES DE LA INTELIGENCIA ARTIFICIAL

Cuando pensamos en posibles aplicaciones que tiene la IA en nuestra vida cotidiana, lo más probable es que se nos vengan a la cabeza las más comunes o conocidas: desde chatbots como ChatGPT o Siri, hasta los anuncios personalizados que saltan al consumidor en plataformas de streaming como Netflix o Prime Video. O, sin ir más lejos, podemos fácilmente pensar en el funcionamiento de las redes sociales como Instagram o TikTok, las cuales utilizan algoritmos de *machine learning* para personalizar las publicaciones que le salen al usuario, en base a sus preferencias y su comportamiento en las redes.

Sin embargo, la IA va más allá de eso. Lo cierto es que ésta ya no es una mera promesa de futuro, sino que es un hecho presente, de tal manera que está totalmente impregnada en nuestra vida diaria, transformando gran variedad de sectores, y ofreciendo soluciones rápidas y sencillas a sus consumidores. Algunas áreas, a modo de ejemplo, en las que está presente la IA son las siguientes:

Sector Sanitario

La IA está revolucionando el ámbito sanitario. Investigadores de todo el mundo examinan la manera de utilizar algoritmos, no solo para mejorar diagnósticos y tratamientos, sino también para optimizar el acceso a la atención médica.

Actualmente, los sanitarios están comenzando a utilizar algoritmos de *machine learning* para analizar imágenes como radiografías o resonancias magnéticas y detectar patrones que un humano podría pasar fácilmente por alto. Un ejemplo destacado es el uso de la IA para detectar pacientes con cáncer, a través del análisis de mamografías, por ejemplo, para detectar cáncer de mama; o a través del análisis de lesiones cutáneas para detectar pacientes con cáncer de piel[28].

[28] Roch Moraguez, E., "Inteligencia Artificial en Medicina: Cómo la IA Está Salvando Vidas", LovTechnollogy, (disponible en Inteligencia Artificial en Medicina: Cómo la IA Está Salvando Vidas, última consulta 20/01/2025).

Por otro lado, se está convirtiendo una práctica muy común en el sector sanitario recopilar datos genómicos para elaborar un tratamiento adaptado al paciente, ofreciéndole una atención médica personalizada. Asimismo, se están incluso desarrollando *chatbots* de salud, que los usuarios pueden utilizar para obtener un diagnóstico médico sin necesidad de acudir al centro sanitario. En este aspecto, destaca el proyecto de "Análisis Inteligente Multilingüe de Textos en Salud" de KConnect[29], financiado por la Unión Europea, el cual tiene como objetivo facilitar a los usuarios el acceso a la información médica independientemente de su ubicación geográfica.

Sector Financiero

La IA también se ha introducido en el sector financiero, creando el fenómeno que se conoce como tecnología financiera o *FinTech*. Ésta comprende, como analiza Eloi Noya en "Fintech: ahorro e inversión en la era financiera digital", *aplicaciones en línea [...], cuyo objetivo es facilitarnos la gestión de nuestras finanzas personales* y *ayudarnos en la tarea de ahorrar e invertir en carteras diversificadas con unos costes menores a los bancarios. Estas innovadoras empresas pretenden, por tanto, hacernos la vida más sencilla y menos costosa y aprovechar la tecnología para ponerla a nuestro servicio, haciendo del ahorro y de la investigación algo sencillo y asequible a cualquier usuario*[30]. Como vemos, las *FinTech* son combinaciones de servicios financieros tradicionales con tecnología avanzada, que permiten al usuario reducir costes y mejorar sus procesos financieros.

Un ejemplo práctico de cómo la IA se ha introducido en el mundo financiero es la aplicación Revolut, un banco digital que utiliza esta tecnología cognitiva para optimizar la seguridad bancaria y mejorar la experiencia del usuario. Además, utiliza algoritmos de *machine learning* para monitorear los movimientos del usuario, identificar patrones de compra y detectar fraudes y actividades inusuales.

[29] Comisión Europea. (2017). KConnect – Servicios de extracción de información y búsqueda semántica para aplicaciones médicas multilingües (Proyecto n.º 644753). CORDIS (disponible en Khresmoi Multilingual Medical Text Analysis, Search and Machine Translation Connected in a Thriving Data-Value Chain | KConnect | Project | Fact sheet | H2020 | CORDIS | European Commission, última consulta 23/01/2025).
[30] Noya, E., Fintech: ahorro e inversión en la era financiera digital, LID Editorial, Barcelona, 2021.

Sector Empresarial

Considero de gran importancia comentar la introducción de la IA en el sector empresarial, pues ha supuesto en las últimas décadas una transformación clave entre empresas competidoras.

Por un lado, estas tecnologías se están utilizando como medio para acortar y automatizar procesos largos, reduciendo tiempo y errores, por ejemplo, para llevar a cabo tareas administrativas. Asimismo, la atención al cliente está en proceso de completa automatización, pues actualmente se utilizan *chatbots* o asistentes virtuales para responder a las consultas de los usuarios.

Por otro lado, estos sistemas de automatización inteligente se utilizan como arma de reclutamiento en los departamentos de Recursos Humanos, a través de aplicaciones como LinkedIn Talent Insights, que realizan automáticamente una criba de currículums en base a las preferencias de la empresa para un puesto concreto. Si bien es cierto que con estas aplicaciones la empresa se ahorra tiempo en los procesos de selección, hay que tener cuidado con los posibles sesgos y discriminaciones que puede dirigir la máquina hacia los candidatos, como veremos más adelante.

Por último, estas tecnologías permiten el análisis de grandes cantidades de datos para realizar previsiones de ventas y fluctuaciones del mercado. Además, mediante herramientas de visualización de datos como PowerBI o Tableau, la empresa desarrolla gráficos interactivos para visualizar sus datos maestros y mejorar su toma de decisiones frente a empresas competitivas en el mercado.

Sector Jurídico

La IA está llegando a transformar incluso el ámbito jurídico, el cual, hasta hace unos años, era muy rudimentario. A pesar de ello, a día de hoy se están desarrollando diferentes aplicaciones, tanto para realizar pequeñas tareas, como la gestión de documentos y el tratamiento de datos de los clientes, hasta para mejorar la eficiencia en un juicio, mediante la automatización del proceso judicial[31].

En concreto, herramientas como LawGeex o Kira Systems están en un continuo desarrollo, las cuales sirven para analizar las cláusulas de un contrato de manera automatizada, acelerando el proceso judicial y facilitando el acceso a la justicia. Otras herramientas, como Modria[32], son utilizadas incluso para resolver disputas sin necesidad de acudir a un letrado. Este software, original de California, se está llegando a utilizar para resolver principalmente divorcios.

Además, actualmente existen plataformas que ofrecen a los letrados apoyo en el proceso judicial, como ROSS Intelligence, o se ha llegado incluso a crear el "primer abogado robot": DoNotPay[33], el cual fue creado por Joshua Browder en 2015 y se ha convertido en una aplicación que facilita el acceso a la justicia a los ciudadanos, haciéndolo más rápido y menos costoso que las vías tradicionales.

Con esto, vemos que los sistemas de IA están en auge, implementándose en multitud de sectores y ámbitos de nuestra vida cotidiana. Con el procesamiento y tratamiento de grandes volúmenes de datos, las máquinas son capaces de realizar tareas propias del ser humano en menor tiempo y menor coste, una ventaja competitiva de la que desean aprovecharse empresas e instituciones, y para la que se está invirtiendo multitud de recursos.

---

[31] Garrido Jiménez, D., "Inteligencia artificial y el derecho", Garrido y Doñaque Abogados (disponible en La Inteligencia Artificial y Derecho: su jurisprudencia, última consulta 12/01/2025).

[32] Rajmil, M., "Modria, un software para resolver divorcios u otras disputas jurídicas vía Internet", Digital Trends Español (disponible en Modria, un software para resolver divorcios y otras disputas jurídicas vía Internet | Digital Trends Español, última consulta 12/01/2025).

[33] García, E., "DoNotPay: El abogado robot de la IA", Ser Inteligencia Artificial (disponible en DoNotPay: El abogado robot de IA - Inteligencia Artificial, última consulta 12/01/2025).

CAPÍTULO III: MARCO LEGAL

1. INTRODUCCIÓN

La IA es una tecnología que se encuentra en un continuo desarrollo y que presenta bastantes desafíos a nivel internacional para elaborar un marco legal completo y detallado[34].

Uno de los principales problemas con los que se encuentra el legislador a la hora de establecer una regulación detallada es la velocidad a la que avanzan los sistemas que utilizan IA. Estos desarrollos ocurren a tan gran escala que muchas veces los legisladores carecen de tiempo suficiente para comprender a fondo el funcionamiento de esta tecnología antes de que llegue al usuario, lo que deja a la sociedad expuesta a los riesgos que estos sistemas presentan.

Por otro lado, otro desafío es la gran variedad de aplicaciones y de sistemas de la IA que existen. Actualmente, esta tecnología, como avanzábamos en el punto 2.4, está presente en gran variedad de sectores, desde la educación, la industria, y el comercio; hasta la sanidad, el transporte e incluso el sistema judicial. No todos estos sectores necesitan la misma regulación, sino que cada uno cuenta con características propias que demandan normas específicas, por lo que supone una dificultad añadida para desarrollar el sistema legislativo.

Además, uno de los principales problemas que hasta hace unos meses presentaba un auténtico reto era la falta de consenso sobre los riesgos éticos presentes en la IA. Es evidente que, dependiendo del tipo de sector en el que se aplique, se han de utilizar unos estándares de evaluación de riesgos u otros. Por ejemplo, en el caso del sector sanitario, los riesgos se relacionan con el tratamiento que haya proporcionado la IA al paciente o con el diagnóstico automatizado que ésta ha propuesto. Sin embargo, en otros sectores como el sector del transporte, concretamente en los vehículos autónomos que utilizan esta tecnología para desplazarse, el riesgo puede residir en un fallo en el sistema de reconocimiento de peatones, provocando graves accidentes.

[34] Saione, M., "Regulación de la IA: un reto global", Meer, (disponible en Regulación de la inteligencia artificial: un reto global | Meer, última consulta 30/01/2025).

No obstante, como veremos a continuación, cada vez son más los esfuerzos por superar estas barreras, para conseguir un esquema legal exhaustivo que establezca un equilibrio entre la protección de los derechos fundamentales de los ciudadanos y el impulso de la innovación tecnológica.

Para ello, en las siguientes secciones (3.2 y 3.3), analizaremos el marco legislativo que rodea, por un lado, a la IA, y, por otro lado, a la protección de datos. Esta separación, a mi juicio, resulta bastante necesaria, pues, aunque ambos temas están relacionados, no tienen el mismo objetivo y alcance. Por un lado, la regulación de la IA se enfoca fundamentalmente en controlar los riesgos que pueden causar estos sistemas al usuario, fomentando su uso transparente, responsable y seguro; abordando los problemas éticos, técnicos y sociales que pueden surgir. En cambio, la regulación de la protección de datos tiene como objetivo principal proteger, principalmente, los derechos fundamentales del usuario frente a estos sistemas, garantizándole el control sobre su información personal.

2. REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL

2.1 A nivel europeo

En Europa, el pasado 12 de julio de 2024 se aprobó la Ley de la IA de la Unión Europea (AI Act)[35], la cual supone el primer reglamento a nivel global sobre la IA. Esta nueva ley representa un marco legislativo que establece distintos parámetros normativos en función del nivel de riesgo que conlleve un sistema específico de IA. De esta manera, se ha llegado a un consenso sobre el riesgo, clasificándose en varios niveles:

En primer lugar, encontramos los sistemas que presentan un riesgo inaceptable, los cuales Europa ha prohibido por considerarlos gravemente nocivos para los derechos fundamentales del ciudadano. Dentro de esta categoría entrarían, por ejemplo, sistemas que

[35] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). Op.cit. p.7.

son capaces de manipular cognitivamente al usuario, como aquellos juguetes que incitan a los menores a realizar acciones peligrosas. En segundo lugar, se encuentran los sistemas de IA que presentan alto riesgo para el usuario, los cuales han de someterse a una estricta evaluación previa a su lanzamiento en el mercado. En tercer lugar, nos encontraríamos con los sistemas de riesgo limitado, que son aquellos que tienen una repercusión menor en los derechos del usuario, pero que, en determinadas circunstancias y haciendo mal uso de estos sistemas, pueden ser perjudiciales, como los chatbots o asistentes virtuales. Por último, se posicionan los sistemas de mínimo riesgo, los cuales no siguen ninguna regulación explícita, como los videojuegos.

Por otro lado, la Ley de la IA introduce normas dedicadas a fomentar la transparencia y la responsabilidad en estas nuevas tecnologías, tales como controles exhaustivos previos a su llegada al consumidor, o informes en caso de graves incidencias ante la Comisión Europea.

Como vemos, esta nueva ley europea tiene como principal objetivo el equilibrio de la protección de los derechos fundamentales y la seguridad del ciudadano, con el fomento y el impulso de la innovación de sistemas tecnológicos, además de promover un único mercado para utilizar de manera fiable aquellas aplicaciones desarrolladas por la IA[36].

Por último, el 24 de enero de 2024 se aprobó la Decisión de la Comisión por la que se crea la Oficina Europea de Inteligencia Artificial[37]. Según la Comisión Europea, es tan rápido el progreso de la IA que medidas excepcionales son necesarias para su regulación y minimización de riesgos. De este modo, continúa la Comisión, *deben sentarse las bases de un sistema único de gobernanza de la IA en la Unión mediante el establecimiento de una estructura que supervise los avances en los modelos de inteligencia artificial, en particular en lo que respecta a los modelos de IA de uso general, la interacción con la comunidad científica —con un papel clave en las investigaciones y las pruebas— y la ejecución de las normas; dicha estructura debe tener una vocación mundial. Por consiguiente, debe crearse una Oficina Europea de Inteligencia Artificial en el seno de la Comisión como parte de la estructura administrativa de la Dirección General de Redes de Comunicación, Contenido y*

[36] Herrero Maortua, F., "Marco regulatorio actual sobre inteligencia artificial", PWC (disponible en Marco regulatorio actual sobre inteligencia artificial, última consulta 12/01/2025)
[37] Decisión de la Comisión que dará lugar a la creación de una Oficina Europea de Inteligencia Artificial (DOUE 14 de febrero de 2024).

Tecnologías y que dependa de su plan de gestión anual. Siendo esto así, este organismo se encargará de supervisar la aplicación de las normas reguladoras de la IA y revisar los riesgos que de ella derivan, así como sancionar las posibles infracciones de dicho marco normativo.

2.2 A nivel nacional

En España, de momento no tenemos ninguna ley específica que regule todos los aspectos de la IA, sino que su regulación se sustenta en varias leyes y planes del gobierno[38].

Por un lado, hemos de mencionar la Estrategia Nacional de Inteligencia Artificial (en adelante, ENIA), de noviembre de 2020, un plan del gobierno español cuyo principal objetivo es favorecer la innovación tecnológica y el uso de sistemas de IA en nuestro país. Forma parte del Plan de Recuperación, Transformación y Resiliencia de la economía española, y versa como uno de los vértices de la Agenda España Digital 2026. Esta incluye varios objetivos perfectamente delimitados, entre ellos, incorporar sistemas de IA en las empresas, fomentando la eficacia empresarial y administrativa, pero respetando al trabajador y evitando violaciones de sus derechos individuales y colectivos; además del desarrollo de tecnologías que proyecten la lengua española a nivel global[39].

Por otro lado, la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación[40], tiene como objetivo principal la garantía de la no discriminación del ciudadano en distintos ámbitos, destacando el uso de la IA. Esta se ha convertido en una base reguladora que introduce estándares de transparencia y ética para el uso de la IA en nuestro país, siguiendo las normas europeas.

---

[38]Perezagua Naharro, M., "Marco regulatorio de la inteligencia artificial en España", Auditat. (disponible en Marco regulatorio de la inteligencia artificial en España | Audidat, última consulta 19/01/2025).

[39] Secretaría de Estado de Comunicación. (2020, 2 de diciembre). Estrategia Nacional de Inteligencia Artificial (ENIA). Gobierno de España, (disponible en Pedro Sánchez presenta la Estrategia Nacional de Inteligencia Artificial con una inversión pública de 600 millones en el periodo 2021-2023, última consulta 16/01/2025)

[40]Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación (BOE 13 de julio de 2022). Op.cit. p.7.

En concreto, su art.23.1 dice así: *En el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial, las administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio.*

Además, hemos de destacar la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA)[41], un órgano cuya creación se aprobó en agosto de 2023, y cuya sede se encuentra en La Coruña. Concretamente, se trata de un organismo del gobierno que asumirá las competencias de IA como miembro de la Unión Europea. De hecho, don José Luis Escrivá, ministro para la Transformación Digital y de la Función Pública, comentaba en una rueda de prensa que "*la AESIA es pionera en Europa y sus funciones son clave para avanzar hacia una IA confiable y ética*"[42].

En cuanto a sus funciones, la AESIA se encarga fundamentalmente de coordinar la aplicación de las normas europeas relativas a la IA en nuestro país; así como promover la innovación tecnológica tanto en organismos del sector público como del privado. Además, pretende actuar, y cito textualmente, como "think & do tank"[43], que se refiere a actuar como un organismo que comparta información acerca de las últimas tendencias tecnológicas y advierta sobre los riesgos de la IA.

[41] Fernández-Miranda, F., "Marco regulatorio actual sobre la inteligencia artificial", PWC (disponible en Marco regulatorio actual sobre inteligencia artificial, última consulta 15/01/2025).
[42] Escrivá, J., "AESIA", Digital. Gob, 19 de junio de 2024 (disponible en 20240619_NdP_AESIA_Coruna.pdf, última consulta 16/01/2025).
[43] El término "think & do tank" hace referencia a una organización que combina acciones de investigación (think tank) con la puesta en práctica de proyectos (do tank). Cuevas, J.M., "¿Qué es un 'think tank'?, El Orden Mundial, (disponible en ¿Qué es un 'think tank'? - El Orden Mundial - EOM, última consulta 20/01/2025).

3. REGULACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES

3.1 A nivel europeo

En cuanto a la regulación de la protección de datos en Europa, en primer lugar, hemos de mencionar la Carta de los Derechos Fundamentales de la Unión Europea[44] (en adelante, CDFUE), la cual, como su propio nombre indica, protege los derechos fundamentales de los ciudadanos residentes en los Estados Miembros. Concretamente, su art.8 recoge el derecho a la protección de datos de carácter personal:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

Por otro lado, Reglamento General de Protección de Datos (en adelante, RGPD)[45], teniendo como principio fundamental el artículo de la CDFUE mencionado previamente, recoge un marco regulatorio dedicado a proteger los datos personales de los ciudadanos frente a su uso por parte de organizaciones públicas y empresas privadas. Tal y como se establece en el preámbulo de la ley, *para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados*

[44] Carta de los Derechos Fundamentales de la Unión Europea (DOUE 30 de marzo de 2010).
[45] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE 4 de mayo de 2016). Op.cit. p.7.

miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros[46]. De esta manera, el RGPD refuerza los derechos de los ciudadanos frente al uso de sistemas de la IA, y establece normas para las empresas que utilizan dichos datos.

Por otra parte, en las últimas décadas, la Comisión Europea ha lanzado un nuevo proyecto como parte de su Programa de Trabajo de 2020, la "Estrategia Europea de Datos", cuyo principal objetivo es la creación de un único mercado de datos en la Unión Europea, implementando medidas para favorecer el intercambio seguro y transparente de datos personales y no personales en multitud de sectores, e incitando al cumplimiento estricto del Reglamento General de Protección de Datos (RGPD), para evitar vulneraciones de los derechos fundamentales del usuario. Con esto, Europa pretende situarse como referente en la economía basada en el intercambio de datos.

Como parte de este proyecto, se han aprobado dos leyes fundamentales que promueven el respeto de los derechos fundamentales y el desarrollo tecnológico simultáneamente: las conocidas como Data Act[47] y Data Governance Act[48], las cuales son complementarias al RGPD.

En primera instancia, el Reglamento del Parlamento Europeo y del Consejo sobre normas armonizadas para un acceso justo a los datos y su utilización, también conocido como Ley de Datos (Data Act), entró en vigor el pasado 11 de enero de 2024, como un esfuerzo europeo para establecer normas que promuevan la transformación digital de manera segura y transparente. Uno de sus principales objetivos reside en permitir a los gobiernos de las

[46] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE 4 de mayo de 2016). Op.cit. p.7.

[47] Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (DOUE 22 de diciembre de 2023). Op.cit. p.8.

[48] Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). Op.cit. p.8.

naciones pertenecientes a la UE el acceso a datos generados por empresas, con la limitación de que ha de producirse una situación excepcional, como catástrofes naturales o crisis sanitarias. Además, pretende facilitar el acceso del usuario a sus datos personales generados en las distintas empresas, promoviendo así la transparencia y seguridad de los datos. Asimismo, esta nueva ley intenta crear un ecosistema de datos justo, mejorando las cláusulas de los contratos de datos entre proveedores.

Por otro lado, nos encontramos con el Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos), e inglés conocido como Data Governance Act. Esta norma pretende, al igual que el Data Act, crear un entorno de intercambio de datos seguro entre países europeos, que afecte tanto al sector público como al privado. De esta manera, tiene como metas, por un lado, optimizar el intercambio de datos entre usuarios (B2C), empresas (B2B) y organismos del sector público, creando una nueva figura, la del "intermediario de datos", cuya función principal es favorecer la transferencia de información entre las partes. Además, permite que los datos generados por organismos públicos sean más accesibles para empresas privadas, impulsando la innovación y el desarrollo de sistemas tecnológicos, mediante la creación de "repositorio de datos públicos".

3.2 A nivel nacional

En primer lugar, debemos mencionar el artículo 18.4 de la Constitución Española, que garantiza la protección de los ciudadanos en relación con el tratamiento de datos personales como un derecho fundamental: *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

En la STC 94/1998, de 4 de mayo[49], el Tribunal Constitucional señala que se trata de un derecho fundamental a la protección de datos, es decir, el ciudadano encuentra garantizado todo control sobre sus datos personales, de tal manera que se le permite oponerse ante

[49] Sentencia del Tribunal Constitucional, núm. 94/1998 de 4 de mayo, [versión electrónica - base de datos Aranzadi Digital. Ref. RTC\1998\94]. Fecha de última consulta: 28 de enero de 2025.

cualquier uso de sus datos que no sea aquel que justificó su recopilación. Por su parte, la STC 292/2000, de 30 de noviembre[50], considera este derecho fundamental como un derecho independiente, lo que permite a las personas decidir si comparten sus datos personales con un tercero o no, ya sea este tercero el Estado o un particular.

A nivel legislativo, el derecho de la protección de las personas físicas en relación con el tratamiento de sus datos personales se regula principalmente en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD). Esta ley hace un esfuerzo por adaptar el RGPD al marco legal español, estableciendo las bases para el tratamiento de datos personales y la regulación de los sistemas propios de la IA.

Según ambos textos, el tratamiento de datos personales debe realizarse de manera clara, justa y lícita; limitándose además a los fines para los cuales fueron recopilados. Además, reconoce a los ciudadanos derechos sobre sus datos, tales como el derecho de rectificación, acceso, supresión y oposición, los cuales deberán ser siempre respetados por sistemas que implementan IA.

Por otro lado, tenemos la Carta de Derechos Digitales aprobada en 2021, un plan del gobierno para acotar los derechos de los ciudadanos en la era digital, con el objetivo de proteger al usuario de los riesgos que pueden derivar de las nuevas tecnologías. En concreto, y en relación con la IA, destacan los siguientes:

Derecho a la Protección de Datos:

1. Con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

[50] Sentencia del Tribunal Constitucional, núm. 292/2000, de 30 de noviembre [versión electrónica - base de datos Aranzadi Digital. Ref. RTC\2000\292]. Fecha de última consulta: 28 de enero de 2025.

2. Estos datos serán tratados respetando los principios de licitud, lealtad, transparencia, minimización, integridad, confidencialidad y limitación por la finalidad y plazo de conservación, con base en las garantías de su protección desde el diseño y por defecto.

3. El tratamiento de datos personales se fundamentará en las bases jurídicas que la mencionada normativa prevé.

4. Toda persona tiene derecho a ser informada en el momento de la recogida de los datos sobre su destino y los usos que se hagan de los mismos, a acceder a los datos recogidos que le conciernan y a ejercer sus derechos de rectificación, oposición, cancelación, portabilidad de los datos, y derecho a la supresión (derecho al olvido) en los términos previstos en la normativa de protección de datos nacional y europea.

5. El respeto de este derecho estará sujeto al control de la Autoridad de Protección de Datos y el resto de organismos competentes en la materia[51].

Derecho a la Igualdad y a la No Discriminación en el Entorno Digital:

1. El derecho y el principio a la igualdad inherente a las personas será aplicable en los entornos digitales, incluyendo la no discriminación y la no exclusión. En particular, se promoverá la igualdad efectiva de mujeres y hombres en entornos digitales. Se fomentará que los procesos de transformación digital apliquen la perspectiva de género adoptando, en su caso, medidas específicas para garantizar la ausencia de sesgos de género en los datos y algoritmos usados.

2. En los procesos de transformación digital se velará, con arreglo a la normativa aplicable, por la accesibilidad de toda clase[52].

[51]Secretaría de Estado de Digitalización e Inteligencia Artificial. (2021). Carta de derechos digitales. Ministerio de Asuntos Económicos y Transformación Digital.
[52]Secretaría de Estado de Digitalización e Inteligencia Artificial. (2021). Carta de derechos digitales. Ministerio de Asuntos Económicos y Transformación Digital. Op.cit. p.30.

Derechos ante la Inteligencia Artificial:

1. La inteligencia artificial deberá asegurar un enfoque centrado en la persona y su inalienable dignidad, perseguirá el bien común y asegurará cumplir con el principio de no maleficencia.

2. En el desarrollo y ciclo de vida de los sistemas de inteligencia artificial: a) Se deberá garantizar el derecho a la no discriminación cualquiera que fuera su origen, causa o naturaleza, en relación con las decisiones, uso de datos y procesos basados en inteligencia artificial. b) Se establecerán condiciones de transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza. En todo caso, la información facilitada deberá ser accesible y comprensible. c) Deberán garantizarse la accesibilidad, usabilidad y fiabilidad.

3. Las personas tienen derecho a solicitar una supervisión e intervención humana y a impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial[53].

[53]Secretaría de Estado de Digitalización e Inteligencia Artificial. (2021). Carta de derechos digitales. Ministerio de Asuntos Económicos y Transformación Digital. Op.cit. p.30.

CAPÍTULO IV: VULNERACIÓN DE DERECHOS FUNDAMENTALES POR SISTEMAS DE INTELIGENCIA ARTIFICIAL

1. INTRODUCCIÓN

Los sistemas de inteligencia artificial están desarrollándose a velocidades inauditas, de manera que cada vez son más los datos recopilados por este tipo de infraestructuras tecnológicas. De hecho, según el informe "Artificial Intelligence Index Report 2024" de la Universidad de Standford, la IA está presente en multitud de sectores, como el financiero, el sanitario o el energético, realizando tareas propias del ser humano que llevan a una mejora en la toma de decisiones. Además, se están destinando millones de euros a la investigación y desarrollo de la IA generativa. De hecho, estas inversiones llegaron a alcanzar 25.200 millones de dólares en 2023[54].

Una herramienta que está en auge constante es el famoso Chat GPT, de la empresa OpenAI, el cual utiliza IA para proporcionar al usuario información de todo tipo. Es más, el informe incluye una encuesta llevada a cabo en más de 20 países sobre el uso y consciencia de dicha herramienta. En los resultados, el 63% de los encuestados confirmaban tener conocimiento de la aplicación, e incluso el 36% confesaba utilizarla semanalmente. Con esto vemos la importante presencia de estos sistemas en nuestras vidas, ante los cuales nuestros datos personales y financieros se encuentran completamente expuestos[55].

Es por ello fundamental una extensa regulación de los sistemas que funcionan mediante IA, y un marco normativo sólido que incluya los posibles riesgos que conllevan para el usuario. En este apartado realizaremos un análisis de cómo la IA es capaz de perjudicar al ciudadano, centrándonos en tres de sus derechos fundamentales recogidos en la Constitución: el derecho a la igualdad y no discriminación, el derecho a la libertad de expresión y el derecho a la privacidad y protección de datos personales.

---

[54] Zhang, S., et all, "Artificial Intelligence Report 2024", Standord Institute for Human-Centered Artificial Intelligence.

[55] Zhang, S., et all, "Artificial Intelligence Report 2024", Standord Institute for Human-Centered Artificial Intelligence. Op.cit. p.32.

2. DERECHO A LA IGUALDAD Y NO DISCRIMINACIÓN

2.1 Sesgos y Discriminación Algorítmica

En primer lugar, veamos cómo los sistemas de IA pueden vulnerar el derecho a la igualdad y no discriminación del ciudadano. Si bien es cierto que uno de los objetivos de la IA consiste en mejorar la eficiencia en la toma de decisiones, éstas pueden deberse a discriminaciones y sesgos algorítmicos que afectan a determinados grupos sociales.

Por tanto, uno de los principales riesgos del uso de la IA es la reproducción de sesgos, reflejando discriminaciones por edad, género o incluso raza en los datos que se utilizan para entrenar al algoritmo. Estos problemas reflejan una falta de objetividad de la IA, de la cual se espera un comportamiento completamente imparcial y que está demostrando todo lo contrario, lo que altera la confianza de los usuarios en este tipo de sistemas. Además, se fomenta la desigualdad social, pues aumenta las injusticias históricas que se están tratando de extinguir[56].

Estos sesgos algorítmicos son notables en distintas etapas del uso y desarrollo de sistemas de la IA: en los datos de entrenamiento, en el progreso del propio algoritmo o incluso en la interpretación de resultados. Además, cada vez son más los escenarios en los que se pueden dar sesgos algorítmicos: en la contratación de empresas, en sistemas de reconocimiento facial o incluso en métodos que predicen la reincidencia de delincuentes.

El caso más sonado hasta el momento de discriminación logarítmica es el de Amazon de 2018. En esa época, la empresa había desarrollado un sistema tecnológico que ayudaría en el departamento de Recursos Humanos a seleccionar currículums que pasarían a la fase de la entrevista en un proceso laboral, con el objetivo de automatizar dicho proceso y, por tanto, reducir costes y tiempo. El sistema utilizaba datos históricos de Amazon para entrenar el algoritmo y tomar las decisiones más eficientes para la empresa. Sin embargo, no contaron con que estos datos reflejaban un sesgo importante, pues la mayoría de los puestos técnicos de la empresa habían sido ocupados en su día por hombres. Jeffrey Dastin, periodista experto en

[56] Flores Anarte, L., "Sesgos de Género en la Inteligencia Artificial: el Estado de Derecho frente a la Discriminación Algorítmica por Razón de Sexo", Universidad de Sevilla, (disponible en 95-120 Sesgos.pdf, última consulta 23/03/2025).

tecnología, explicaba en Reuters que, *en efecto, el sistema de Amazon se enseñó a sí mismo que los candidatos masculinos eran preferibles. Penalizaba los currículos que incluían la palabra "femenino", como en "capitana del club de ajedrez femenino". Y degradó a las graduadas de dos universidades exclusivamente femeninas*[57]. Por tanto, al estar las mujeres considerablemente menos representadas, el sistema mostraba preferencia por los candidatos masculinos. Como consecuencia, la empresa decidió abandonar el proyecto de contratación automatizada por considerarse vulnerador del derecho a la igualdad y no discriminación de las posibles candidatas a los puestos de trabajo.

Además, en las últimas décadas, la IA se ha ido introduciendo en multitud de sectores, como comentábamos en el capítulo II. Si bien se encuentra presente en el ámbito laboral, también podemos encontrarla en otros sectores en los que no está dispensada de desafíos éticos y jurídicos: el sector financiero y el sector judicial.

Por un lado, resulta habitual la presencia de algoritmos en sistemas utilizados en el sector bancario, pues las entidades financieras utilizan infraestructuras de *machine learning* para analizar variables del cliente y estudiar su solvencia a la hora de conceder créditos bancarios y préstamos hipotecarios. Entre estas variables se encuentra el historial de ingresos y gastos del cliente, su situación laboral, su nivel educativo y su registro de créditos anteriores. A pesar de su aparente objetividad, encontramos situaciones reales en las que estos algoritmos han desembocado en situaciones discriminatorias para el cliente, ya sea por razones de raza, género o incluso estado civil. En 2018, sin ir más lejos, se realizó un estudio en la Universidad de California, EE.UU. , en el que se analizaron multitud de solicitudes de hipotecas en el país, y se llegó a la conclusión de que los algoritmos que decidían conceder el préstamo seguían patrones históricos y geográficos que desembocaban en una discriminación racial, de tal manera que los clientes hispanos y afroamericanos pagaban un 0,079% más de interés que los clientes americanos, o en otras palabras, los intereses anuales para los primeros aumentaban en 500 millones de dólares adicionales.

[57] Dastin, J., "Insight-Amazon scraps secret AI recruiting tool that showed bias against women", Reuters, (disponible en Insight - Amazon scraps secret AI recruiting tool that showed bias against women | Reuters, última consulta 10/02/2025)

En esta línea se encuentra la práctica bancaria del *scoring*, la cual está completamente prohibida a día de hoy. El *scoring* es un sistema que utiliza algoritmos de *machine learning* para analizar el riesgo de impago de un cliente, evaluando sus datos financieros y personales. Este sistema se puso de manifiesto en el Asunto C-634/21 – OQ contra Land Hessen[58], el cual responde a una petición de decisión prejudicial por parte del Tribunal de lo Contencioso-Administrativo de Wiesbaden (Alemania) ante el TJUE. En este caso, SCHUFA Holding AG, una empresa alemana, evaluaba la concesión de préstamos y servicios financieros en función de la puntuación sobre el cliente que generara el sistema del *scoring.* No es de esperar que este sistema pudiera resultar perjudicial para el cliente si se utilizaba de manera difusa, tal y como sostenía el demandante.

Como conclusión, el TJUE consideró que esta práctica por parte de SCHUFA podría constituir una "decisión individual automatizada"[59] si influye de manera directa en una decisión externa para aprobar o rechazar un contrato con el afectado (en este caso, si influye directamente en la decisión de un banco de conceder o no el crédito al cliente). Esta práctica está prohibida por el artículo 22.1 RGPD, que dice lo siguiente: *Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*[60].

Como consecuencia, este fallo del TJUE subraya la necesidad de una regulación clara y exhaustiva en el uso de sistemas de IA, especialmente en ámbitos que impactan directamente en los derechos de los ciudadanos. Además, refuerza la aplicación del RGPD, estableciendo que toda "decisión individual automatizada" que pueda afectar de manera significativa a una persona debe estar sujeta a un control humano riguroso y a una regulación detallada. Asimismo, la sentencia aboga por la implementación de sistemas más transparentes, garantizando que los afectados tengan acceso a información clara sobre el proceso de toma de

---

[58] Sentencia del Tribunal de Justicia de la Unión Europea, núm C-634/2021, de 7 de diciembre [versión electrónica - base de datos Aranzadi. Ref TJCE\2023\146]. Fecha de última consulta: 7 de marzo de 2025.

[59] *La generación automatizada, por una agencia de información comercial, de un valor de probabilidad a partir de datos personales relativos a una persona y acerca de la capacidad de esta para hacer frente a compromisos de pago en el futuro constituye una «decisión individual automatizada», en el sentido de la mencionada disposición, cuando de ese valor de probabilidad dependa de manera determinante que un tercero, al que se comunica dicho valor, establezca, ejecute o ponga fin a una relación contractual con esa persona.* (Sentencia del Tribunal de Justicia de la Unión Europea, núm C-634/2021, de 7 de diciembre [versión electrónica - base de datos Aranzadi. Ref TJCE\2023\146]. Fecha de última consulta: 7 de marzo de 2025). Op.cit. p.35.

[60] 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 (DOUE 4 de mayo de 2016).

decisiones. Finalmente, enfatiza la importancia de ofrecer mecanismos efectivos para impugnar decisiones injustas, asegurando así la protección de los derechos fundamentales en el contexto de la automatización y la inteligencia artificial.

Por otro lado, la IA se utiliza también en el ámbito judicial, fundamentalmente mediante sistemas que miden la probabilidad de reincidencia de presos o que recomiendan medidas cautelares en función del delito cometido. Concretamente, en España existe un caso bastante sonado: el de la Tabla de Variables de Riesgo (TVR) que llevan utilizando las prisiones españolas desde hace más de 30 años. Este sistema evalúa diez variables, como la extranjería, la drogodependencia o la peligrosidad del interno, entre otras, para evalúar la concesión al preso de la libertad condicional. Con éstas *se alcanza una tasa de posible mal uso de la salida cuya concesión se valora –sea esto bien en forma de comisión de nuevo delito, bien de quebrantamiento de la condena-*, comentan Puerto Solar Calvo y Pedro Lacal Cuenca en Legal Today[61]. El problema de dicho sistema reside en su antigüedad, ya que, desde su implementación en 1993, no ha sido actualizado, por lo que no refleja correctamente la realidad de hoy en día. Es por ello por lo que presenta discriminaciones y sesgos hacia determinados internos, principalmente a los reclusos extranjeros, ya que *su mera consideración arroja un mínimo de 85% de riesgo si el interno en cuestión es ciudadano de la Unión Europea. Riesgo que alcanza el 90-100% si consideramos a internos de fuera de la UE*, continúan los autores.

Con esto, vemos que, a pesar de que la IA se presupone una tecnología objetiva e imparcial, lo cierto es que todavía presenta sesgos que dan lugar a decisiones discriminatorias, vulnerando el derecho a la igualdad del ciudadano.

[61] Solar Calvo, P., y Lacal Cuenca, P., "Inteligencia artificial en el medio penitenciario", LegalToday, (disponible en Inteligencia artificial en el medio penitenciario - LegalToday, última consulta 07/03/2025).

2.2 Regulación del Derecho a la Igualdad y No Discriminación

Como hemos analizado, los sistemas de IA pueden ser susceptibles de vulnerar derechos fundamentales, como el derecho a la igualdad y a la no discriminación. Para mitigar estos riesgos, considero esencial la implementación de un esquema normativo sólido y completo que garantice la transparencia, la seguridad y la responsabilidad en el uso de la IA.

Para analizar su marco regulatorio, resulta primordial estudiar cómo se legisla el derecho a la igualdad y no discriminación en nuestro ordenamiento jurídico. Este se contempla principalmente en el art.14 CE, que dice lo siguiente: *Los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social*[62].

Además, el Estado tiene la obligación de garantizar una igualdad efectiva, formalizándose ésta en el art. 9.2 CE: *Corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social*[63].

Ahora bien, ¿cómo se protege al ciudadano de la discriminación algorítmica en España?

Por un lado, en 2024 la Unión Europea diseñó el AI Act, el cual, como veíamos en el punto 3.1.2, clasifica los sistemas en función del riesgo que se considera que presenta para el ciudadano.

Por otro lado, el RGPD, como veíamos previamente en el Asunto C-634/21 – OQ contra Land Hessen, prohíbe en su art.22 la utilización de decisiones automatizadas sin intervención humana en casos significativos como en la asignación de créditos o en contrataciones laborales. Esto se refuerza en nuestro ordenamiento jurídico con la STC 41/2020, de 9 de marzo[64], en la que se impugnó una decisión de la Consejería de Educación

[62] Constitución Española (BOE 29 de diciembre de 1978).
[63] Constitución Española (BOE 29 de diciembre de 1978). Op.cit. p.37.
[64] Sentencia del Tribunal Constitucional, núm 41/2020, de 9 de marzo [versión electrónica - base de datos Aranzadi. Ref. RTC\2020\41]. Fecha de última consulta: 8 de marzo de 2025.

de la Comunidad de Madrid por vulnerar el derecho a la igualdad y no discriminación de una ciudadana. La perjudicada era víctima en un caso de violencia de género, pero su condición de víctima no se tuvo en cuenta por la Administración porque utilizó un sistema de IA con datos del Ministerio del Interior, entre los que no se encontraban los de la víctima, negándole la ayuda necesaria. Como vemos, estos sistemas, sin una supervisión humana, pueden dar lugar a errores y discriminaciones. Por ello, el Tribunal Constitucional aboga por un uso responsable de los sistemas de IA, de tal manera que deben ser revisados por la acción humana en todo momento.

Además, hemos de mencionar la Ley 15/2022, que, en su artículo 23.1, fomenta el uso transparente de los sistemas que utilicen IA: *En el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial, las administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio*[65].

A su vez, esta obligación de transparencia en la toma de decisiones automatizadas para evitar discriminaciones se refuerza en el art.11 LOPDGDD, que obliga a la entidad que recoge los datos a informar al afectado sobre la finalidad de la recopilación y sobre los derechos que tiene para protegerlos. Entre estos, se encuentran el derecho de acceso del interesado, el derecho de rectificación, el derecho de supresión, el derecho a la limitación del tratamiento, la obligación de notificación relativa a la rectificación o supresión de datos personales, el derecho a la portabilidad de los datos y el derecho de oposición, recogidos en los arts. 15-21 RGPD.

Por otro lado, hemos de mencionar otras normas que fomentan el derecho de información del ciudadano respecto del uso de sus datos personales[66]. Entre ellas, destaca el Real Decreto-ley 9/2021, de 11 de mayo, que introduce un nuevo artículo, el 64.4.d), el cual

[65] Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación (BOE 13 de julio de 2022) Op.cit. p.7.
[66] Digital Future Society. (2022). La discriminación algorítmica en España: límites y potencial del marco legal. Digital Future Society, (disponible en Discriminacion_algoritmica_Espana_marco_legal.pdf, última consulta 15/03/2025).

dice lo siguiente: *El comité de empresa, con la periodicidad que proceda en cada caso, tendrá derecho a: d) Ser informado por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles*[67]. Mediante este artículo se estipula el derecho de los representantes de los trabajadores a conocer los sistemas de IA utilizados por la empresa en la toma de decisiones automatizadas (por ejemplo, en casos de contrataciones).

A pesar de la existencia de varias leyes que regulen la materia, desgraciadamente siguen existiendo vacíos legales que dejan al descubierto el derecho a la igualdad y no discriminación del ciudadano.

En primer lugar, no existe una definición específica sobre el concepto de "discriminación algorítmica" en ninguna norma, por lo que resulta muy fácil para las entidades evadirse de dicha acusación. Por lo tanto, considero necesaria la elaboración de una ley clara y específica sobre qué elementos conforman la discriminación algorítmica[68].

Además, si bien es cierto que una medida complementaria eficaz sería el sometimiento de los sistemas de IA a auditorías externas periódicas para asegurarse de que no hay posibles sesgos, no existe ninguna norma que regule eficazmente esa obligación. El AI Act europeo, que clasifica los sistemas de IA en función del riesgo que conllevan para el ciudadano, incluye en su art.43 los procedimientos de evaluación que deben cumplimentar los proveedores de los sistemas calificados como de alto riesgo. Incluye dos tipos de procedimientos en función del nivel de riesgo del sistema: evaluaciones internas de la empresa (para aquellas tecnologías que presentan riesgo alto pero que son menos críticas, por ejemplo, la IA que se utiliza en sistemas de Recursos Humanos pero que no toma decisiones importantes) y auditorías externas (para los sistemas de alto riesgo que pueden afectar a los derechos fundamentales) llevadas a cabo por un organismo independiente acreditado por la UE. No obstante, este artículo, a mi juicio, resulta insuficiente, pues, ¿no sería necesario que

[67] Real Decreto-ley 9/2021, de 11 de mayo, por el que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales (BOE 12 de mayo de 2021).
[68] Digital Future Society. (2022). La discriminación algorítmica en España: límites y potencial del marco legal. Digital Future Society, (disponible en Discriminacion_algoritmica_Espana_marco_legal.pdf, última consulta 15/03/2025). Op.cit. p.38.

todos los sistemas que se califican como de alto riesgo se someten al control de un órgano independiente para evitar conflictos de interés?

Por último, si bien es cierto que el RGPD garantiza medidas al ciudadano para proteger sus derechos personales, la realidad es que no existen mecanismos de reclamación rápida tipificados, sino que los procesos son tan lentos que el perjudicado por discriminación algorítmica prefiere no llegar a juicio. Esto supone un verdadero problema, ya que, por un lado, los ciudadanos que ven su derecho a la igualdad vulnerado no reciben compensación alguna porque no llegan a denunciar y, por otro, los algoritmos sesgados siguen en vigor, pues la entidad que los utiliza no se siente coaccionada para modificarlos. A pesar de ello, el Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial, otorga a la AESIA en sus arts. 4 y 10 *la función de inspección, comprobación, sanción y demás que le atribuya la normativa europea que le resulte de aplicación y, en especial, en materia de inteligencia artificial*[69]. Por lo tanto, este organismo podrá sancionar a aquellas entidades que no cumplan con lo estipulado en el AI Act, de forma que se iniciará la lucha en nuestro país contra los sistemas de IA sesgados y discriminatorios. Sin embargo, según respondió el propio Gobierno en el Congreso, esta potestad sancionadora será asumida por la AESIA a partir del 2 de agosto de 2025[70]. Por tanto, hasta esa fecha, la AESIA no tendrá la capacidad sancionadora plenamente desarrollada, y el derecho a la igualdad y no discriminación del ciudadano seguirá expuesto a posibles vulneraciones.

En definitiva, el derecho a la igualdad y no discriminación del ciudadano puede verse vulnerado por sistemas de IA, si es que éstos se basan en datos históricos sesgados, o si toman decisiones sin intervención humana, entre otras vías. Para evitarlo, es necesario un marco regulatorio que luche contra la discriminación algorítmica y limite las decisiones individuales automatizadas. Con todo, a pesar de los esfuerzos legislativos tanto en España como en Europa, en realidad siguen existiendo multitud de vacíos legales, de manera que se evidencia que el legislador todavía no está a la altura de los avances tecnológicos tan veloces que estamos viviendo en estos tiempos.

[69] Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial (BOE 2 de septiembre de 2023).
[70] Gobierno de España. (2024, 11 de diciembre). Respuesta del Gobierno a las preguntas escritas del Congreso sobre la Agencia Española de Supervisión de Inteligencia Artificial (AESIA) (Preguntas 184/16529 a 184/16531). Secretaría de Estado de Relaciones con las Cortes y Asuntos Constitucionales.

3. DERECHO A LA LIBERTAD DE EXPRESIÓN

3.1 Censura Algorítmica, Desinformación y Fake News

En la era digital en la que vivimos, las redes sociales han experimentado un crecimiento exponencial, convirtiéndose en espacios de interacción masiva con millones de usuarios registrados en plataformas como Instagram, Facebook o TikTok. Ante la enorme cantidad de contenido que se genera a diario, estas empresas han implementado diversas estrategias para moderarlo, asegurando que se cumplan sus normas comunitarias y evitando la difusión de publicaciones que puedan resultar perjudiciales.

Para ello, han desarrollado herramientas avanzadas de control, como sistemas de reconocimiento de palabras clave que detectan expresiones de odio o incitación a la violencia, tecnologías de identificación de imágenes con contenido sexual o violento, e incluso mecanismos de denuncia por parte de los propios usuarios. A través de estos métodos, las plataformas pueden evaluar y, si es necesario, eliminar aquellas publicaciones que infrinjan sus políticas, garantizando así un entorno más seguro y respetuoso para su comunidad.

No obstante, estos sistemas de moderación de contenido presentan un desafío importante, ya que, si no se utilizan correctamente, pueden llegar a vulnerar el derecho a la libertad de expresión de los usuarios. Como hemos analizado a lo largo de este trabajo, la IA sigue siendo una tecnología imperfecta, en constante evolución, lo que obliga al ser humano a implementar mejoras continuas para corregir sus deficiencias.

En este contexto, pueden surgir situaciones en las que el algoritmo malinterprete el significado o la intención de una publicación y la censure de manera errónea. Asimismo, existe el riesgo de que algunos usuarios hagan uso abusivo del mecanismo de denuncia, logrando que se eliminen contenidos que, en realidad, no infringen las normas de la plataforma. Estos errores evidencian la necesidad de desarrollar sistemas más precisos y equitativos, que garanticen un equilibrio entre la moderación de contenido y el respeto por la libertad de expresión.

En este contexto, debemos mencionar una política que sigue la red social X (antiguo Twitter): el *Shadow Ban*. Esta práctica limita el contenido y el alcance de las publicaciones de un usuario por decisión de la plataforma, de manera que éstas dejan de ser visibles para el resto de la comunidad, pero el creador sigue viendo esa publicación. Si bien este sistema se

utiliza por razones lícitas, por ejemplo, si la plataforma piensa que el usuario puede haberse creado una cuenta falsa, o si el usuario sube tweets ofensivos; el problema viene cuando X no avisa al usuario de que ha sido *shadow baneado,* lo que puede generar problemas a la hora de garantizar la transparencia a los usuarios[71].

Por otro lado, hablemos de la desinformación. A diario, miles de personas consumen en diversas redes sociales contenido de distinta naturaleza: noticias, moda, cocina, deportes, etc. Sin embargo, no toda la información que se publica en las redes es verídica, de manera que la desinformación y las noticias falsas o *fake news* se han convertido en una amenaza mundial en diferentes ámbitos.

De esta manera, *la desinformación se define como la difusión deliberada de información falsa o engañosa con el objetivo de confundir o manipular a las personas. A menudo, la desinformación se crea con fines políticos, económicos o ideológicos*. Por otro lado, *las noticias falsas (o "fake news") son un tipo específico de desinformación que se presenta como contenido periodístico legítimo pero que es completamente falso o contiene elementos distorsionados de la verdad*[72].

Según un estudio realizado en marzo de 2018 en el Instituto Tecnológico de Massachusetts (MIT)[73], las noticias falsas tienen un 70% más de probabilidades de ser compartidas que las verdaderas. Es decir, las *fake news* se difunden a una velocidad mucho más rápida, lo que es realmente preocupante, ya que incluyen principalmente noticias políticas, sociales e incluso sanitarias de las que el receptor no duda de su veracidad. Un ejemplo actual es el reciente caso de la DANA, un fenómeno meteorológico que causó fuertes inundaciones por la zona del Levante y que, lamentablemente, dejó 232 personas fallecidas. Durante la catástrofe, se vivieron en España algunos días de incertidumbre, los cuales fueron aprovechados en redes sociales para propagar noticias falsas, creando páginas de recaudación de ayudas que posteriormente se calificaron de estafas, tal y como explica la agencia EFE[74].

---

[71] Abdulhafeez Y., "Shadowbanned or Deboosted Twitter: What It Means and How to fix it", Incognition (disponible en Shadowbanned or Deboosted Twitter: What It Means and How to fix it - Incogniton, última consulta 08/03/2025).

[72] González Valderrama, D.A., "Desinformación y noticias falsas: Cómo identificar y combatir el fenómeno en la era digital", CuriosoTeatro Global, (disponible en Desinformación y noticias falsas: Cómo identificar y combatir el fenómeno en la era digital - CuriosoTeatro Global: Innovación en Cultura y Educación, última consulta 08/03/2025).

[73] Vosoughi S,. et all, (2018). The spread of true and false news online. Science, 359(6380), 1146-1151.

[74] Hernández, S., "Desinformación sobre la DANA: causas y consecuencias", EFE Verifica (disponible en Desinformación sobre la dana: causas y consecuencias, última consulta 08/03/2025).

Además, la desinformación se utiliza comúnmente como herramienta para perjudicar o favorecer elecciones en distintos países, como el caso de las recientes elecciones presidenciales de EE.UU., de noviembre de 2024, en las que se crearon imágenes falsas del actual presidente, Donald Trump, con afroamericanos, para conseguir el voto de los ciudadanos negros, tal y como comenta Marianna Spring en la BBC[75].

Ahora bien, ¿cómo afecta la desinformación al derecho a la libertad de expresión? La propagación de *fake news* resulta perjudicial para la libertad de expresión del ciudadano, pues da pie a la censura de determinadas publicaciones en redes sociales y noticias en medios de comunicación. La libertad de expresión, tal y como analiza Irene Khan, Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión en su informe "La desinformación y libertad de opinión y expresión", la libertad de expresión *solo puede restringirse de conformidad con el artículo 19, párrafo 3, del Pacto Internacional de Derechos Civiles y Políticos, que exige que todas las restricciones estén fijadas por la ley y sean necesarias para el fin legítimo de respetar los derechos y la reputación de los demás y proteger la seguridad nacional, el orden público o la salud o la moral públicas. A la luz de la importancia fundamental de este derecho para el disfrute de todos los demás derechos humanos, las restricciones deben ser excepcionales e interpretarse de manera estricta*[76]. Por lo tanto, si bien es cierto que las noticias falsas pueden colisionar con la libertad de expresión del ciudadano, esta censura debe estar explícitamente justificada en las causas del artículo 19.3, evitando así un uso arbitrario de ésta.

[75] Spring, M., "Las imágenes falsas creadas con IA para intentar atraer el apoyo de los votantes negros hacia Trump", BBC News, (disponible en Elecciones en Estados Unidos: las imágenes falsas creadas con IA para intentar atraer el apoyo de los votantes negros hacia Trump - BBC News Mundo, última consulta 08/03/2025).

[76] Khan, I. (2021). *La desinformación y la libertad de opinión y de expresión: Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*. Naciones Unidas. Consejo de Derechos Humanos, 47º período de sesiones. [A/HRC/47/25] (disponible en A/HRC/47/25: La desinformación y la libertad de opinión y de expresión Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan | OHCHR, última consulta 08/03/2025)

3.2 Regulación del Derecho a la Libertad de Expresión

La protección del derecho a la libertad de expresión es muy complicada, pues es necesario encontrar un balance entre la lucha contra la desinformación y la limitación de la censura para proteger dicho derecho[77]. En el siguiente apartado analizaremos cómo se protege en nuestro país el derecho de libertad de expresión del ciudadano frente a la lucha contra las noticias falsas y desinformación.

En primer lugar, el derecho a la libertad de expresión se recoge como derecho fundamental en el art.20 CE, que dice lo siguiente:

Se reconocen y protegen los derechos:

a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.
b) A la producción y creación literaria, artística, científica y técnica.
c) A la libertad de cátedra.
d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades[78].

A su vez, este derecho se recoge en el art. 19 de la Declaración Universal de los Derechos Humanos, según la cual *todo el mundo tiene derecho a la libertad de opinión y expresión; este derecho incluye la libertad a mantener opiniones sin interferencias y a buscar, recibir e impartir información e ideas a través de cualquier medio sin tener en cuenta las fronteras*[79].

[77] Quiñónez, H.A., "La desinformación vulnera el derecho a la libertad de expresión| Por: Herly Alejandra Quiñónez", MujerAnalítica, (disponible en La desinformación vulnera el derecho a la libertad de expresión| Por: Herly Alejandra Quiñónez - Mujer Analítica, última consulta 18/03/2025).

[78] Constitución Española (BOE 29 de diciembre de 1978). Op.cit. p.37.

[79] Naciones Unidas. (1948). Declaración Universal de Derechos Humanos.

Ahora bien, ¿cómo se intenta combatir la desinformación en España?

A nivel europeo, el Reglamento (UE) 2022/2065, comúnmente conocido como la Ley de Servicios Digitales, incluye pretensiones para combatir la desinformación en el contenido publicado en las plataformas digitales. En su art. 34, se incluye la obligación de realizar evaluaciones de riesgos anuales mediante las que se *detectarán, analizarán y evaluarán con diligencia cualquier riesgo sistémico en la Unión que se derive del diseño o del funcionamiento de su servicio y los sistemas relacionados con éste, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios*[80]. Por tanto, este reglamento incluye la obligación de las plataformas digitales de realizar evaluaciones periódicas para detectar contenido ilegal o falso.

Además, hablemos también del Código de Buenas Prácticas en materia de Desinformación. Se trata de una iniciativa de la Unión Europea para establecer una serie de pautas que han de seguir las plataformas digitales para combatir el problema[81]. Si bien es cierto que es un código de aplicación voluntaria, ya ha sido firmado por varias plataformas digitales como X o TikTok[82], y algunas de sus disposiciones han sido plasmadas en la Ley de Servicios Digitales mencionada previamente. Entre sus preceptos más relevantes contra la desinformación, destacan aquellos que proponen canales de denuncia de contenidos falsos, además de los que impiden que los propagadores de las noticias falsas se lucren con la desinformación, y de los que introducen el *fact-checking*, una herramienta que permite verificar el origen de la información compartida y garantizar su veracidad[83]. Con esto, hemos de tener en cuenta que las plataformas digitales cuentan además con su propia regulación interna, adoptando las medidas necesarias para luchar contra la desinformación, como el etiquetado de contenido erróneo o la eliminación de publicaciones que no cumplen con su normativa interna.

---

[80] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (DOUE 27 de octubre de 2022).

[81] European Commission. (2022). Code of Practice on Disinformation. Publications Office of the European Union, (disponible en Guidance on Strengthening the Code of Practice on Disinformation | Shaping Europe's digital future, última consulta 17/03/2025).

[82] Goñi, E., "Una imagen que vale mil engaños", El País, 17 de febrero de 2025 (disponible en Una imagen que vale mil engaños | Opinión | EL PAÍS, última consulta 23/03/2025).

[83] Ognyanova, K., "Fact-Checking: Journalistic Strategies and Audience Outcomes in Diverse National Contexts", SageJournals (disponible en Fact-Checking: Journalistic Strategies and Audience Outcomes in Diverse National Contexts - Katherine Ognyanova, 2024, última consulta 17/03/2025).

Simultáneamente, en España se aprobó, en 2020, la Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. Su principal objetivo reside en la captación de publicaciones falsas que promuevan la desinformación social y su consecuente eliminación. Para ello, se estableció un plan de actuación formado por cuatro niveles: desde analizar posibles casos de desinformación hasta implementar un plan gubernamental para su erradicación[84]. No obstante, podemos encontrar casos de empresas que han denunciado este procedimiento por considerarlo vulnerador del derecho a la libertad de expresión, como ocurrió en la STS 1238/2021, de 18 de octubre, donde el Tribunal Supremo desestimó el recurso por encontrar este procedimiento perfectamente constitucional[85].

Por otro lado, debemos mencionar la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación, el cual implica que: *Toda persona, natural o jurídica, tiene derecho a rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio. Podrán ejercitar el derecho de rectificación el perjudicado aludido o su representantes y, si hubiese fallecido aquél, sus herederos o los representantes de éstos*[86]. Como vemos, esta norma tiene como objetivo principal evitar la propagación de bulos o noticias falsas, de manera que garantiza mecanismos de defensa para que el perjudicado pueda denunciar la falta de veracidad de la información difundida por el medio de comunicación pertinente. No obstante, se trata de una ley que no está actualizada a la era digital actual, por lo que el legislativo pretende ampliar el alcance de la norma a los conocidos *influencers*, que, según don Félix Bolaños, ministro de Presidencia, Justicia y Relaciones con las Cortes adelantó para El País, se definen como *aquellos que tienen más de 100.000 seguidores en una sola red social o más de 200.000 en varias de ellas*[87].

---

[84] Congreso de los Diputados. (2022). Respuesta del Gobierno a la pregunta escrita 184/73609 sobre la desinformación y la Seguridad Nacional, (disponible en e_0193749_n_000.pdf, última consulta 14/03/2025).

[85] Sentencia del Tribunal Supremo núm.1238/2021, de 18 de octubre [versión electrónica, base de datos Aranzadi. Ref. RJ\2021\4841] Fecha de la última consulta: 17 de marzo de 2025.

[86] Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación (BOE 27 de marzo de 1984).

[87] Navarro, I., "Menos bulos, 'influencers': la nueva ley de rectificación les pondrá al mismo nivel que los medios de comunicación", El País, 19 de enero de 2025 (disponible en Menos bulos, 'influencers': la nueva ley de rectificación les pondrá al mismo nivel que los medios de comunicación | Negocios | EL PAÍS, última consulta 21/03/2025).

Pese a todos estos esfuerzos para combatir la desinformación, lamentablemente, a día de hoy sigue siendo un ámbito muy poco explorado por el legislador, por lo que existen vacíos legales que dejan al ciudadano expuesto ante el riesgo de censura y consecuente vulneración del derecho a la libertad de expresión. Exploremos algunos problemas existentes:

En primer lugar, como ocurría en el derecho a la igualdad, no existe en nuestro país ninguna norma que regule extensamente el concepto de "desinformación" y las consecuencias que conlleva para el derecho a la libertad de expresión del ciudadano. De momento, lo único que podemos encontrar son pinceladas en las leyes mencionadas previamente, que regulan de manera amplia el problema y causan riesgos de ambigüedades a la hora de interpretar la norma. Por otro lado, si bien es cierto que existe una definición de "desinformación" proporcionada por el Tribunal Supremo, según la cual la "desinformación· es la *información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público*[88], ésta no conforma jurisprudencia, pues solamente existe una sentencia que mencione este tema, lo que, en términos prácticos, significa que no tiene fuerza vinculante y que, por lo tanto, el juez puede interpretar la norma en base a su propio criterio sin necesidad de seguir las indicaciones del Tribunal.

Además, recordemos que la Ley de Rectificación, a día de hoy, sigue con su texto original de 1984, por lo que solo cubre la información divulgada por medios de comunicación. Esto supone un problema, ya que en nuestra era digital cada vez es más común la presencia de usuarios en redes sociales con miles de seguidores, cuyas publicaciones tienen un largo alcance. Por tanto, es necesario que se reforme la ley, que sabemos que ya está en proceso, para que, ante una publicación de una noticia falsa por parte de un *influencer*, el usuario perjudicado pueda ejercer su derecho de rectificación y solicitar que se elimine de la plataforma.

En cuanto a las disposiciones sancionadoras vigentes, lo único que podemos encontrar son preceptos en el Código Penal que sancionan diversas conductas relacionadas con la desinformación, como delitos de odio, calumnias e injurias. El problema reside en que las

[88] Sentencia del Tribunal Supremo núm.1238/2021, de 18 de octubre [versión electrónica, base de datos Aranzadi. Ref. RJ\2021\4841] Fecha de la última consulta: 17 de marzo de 2025. Op.cit. p.46.

"noticias falsas" como tal no son punibles, a menos que su contenido se relacione con un delito ya tipificado.

Además, a día de hoy no tenemos constancia de ningún órgano independiente que combata la desinformación. Y es que, si bien es cierto que existe la previamente mencionada Orden PCM/1030/2020, la cual regula un mecanismo para detectar las campañas de desinformación que pueden afectar a la seguridad nacional, la realidad reside en que la Comisión Permanente contra la Desinformación y todos los organismos implicados en ella, como el Departamento de Seguridad Nacional o el Centro Nacional de Inteligencia, entre otros, dependen del Gobierno. Por tanto, se corre el riesgo de que se politice la lucha contra la desinformación y se lleven a cabo decisiones lejos de ser neutrales[89].

No obstante, todas estas propuestas para combatir la desinformación tienen que respetar unos límites para evitar la vulneración del derecho a la libertad de expresión del ciudadano por medio de la censura. El art.20.2 CE, ya nos advierte: *El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa*[90]. Esto implica que la censura previa está completamente prohibida, de manera que solo se permite la adopción de medidas contra la desinformación una vez el usuario haya ejercido su derecho de libertad de expresión. Ahora bien, ¿cómo se limita la censura?

En primer lugar, el art. 53.1 CE establece que el derecho a la libertad de expresión solo puede limitarse por una norma con rango de ley: *Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161, 1, a)*[91].

Además, la STC 136/1999 establece los requisitos que debe tener toda limitación de un derecho fundamental: legalidad (estar recogida en una norma con rango de ley); perseguir un fin legítimo, como motivos de seguridad, salvaguarda del orden público, protección del

[89] Javier Vázquez, V., "La Comisión contra la desinformación y la imposible neutralidad del Gobierno", AgendaPública, (disponible en La Comisión contra la desinformación y la imposible neutralidad del Gobierno, última consulta 21/03/2025).
[90] Constitución Española (BOE 29 de diciembre de 1978). Op.cit. p.37.
[91] Constitución Española (BOE 29 de diciembre de 1978). Op.cit. p.37.

derecho al honor, etc; proporcionalidad y sometimiento de la medida al control judicial[92]. Por lo tanto, toda medida que censure cualquier publicación promulgada por usuarios o medios de comunicación ha de cumplir estos cuatro presupuestos.

Como conclusión, en una era en la que las plataformas digitales están floreciendo a la velocidad de la luz, hay que ser cuidadosos con el contenido que se sube a redes sociales. Ante la dura lucha contra la desinformación, nuestro país está tratando de implementar medidas para disminuir la propagación de noticias falsas pero salvaguardando el derecho a la libertad de expresión y limitando la censura. No obstante, de momento, estas medidas son poco eficaces, por lo que resulta necesario un marco legal completo y extenso sobre la desinformación y la consecuente protección del derecho a la libertad de expresión.

4. DERECHO A LA PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

4.1 Recopilación Masiva de Datos

La regulación de la IA supone un gran desafío en el ámbito de la privacidad, debido a todos los problemas legales y éticos que conlleva la recopilación y el procesamiento de cantidades masivas de datos, tales como la falta de transparencia y la falta de consentimiento del usuario en el uso de estos datos por terceros o en su uso distinto al fin previsto inicialmente.

Según un informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, actualmente se está llevando a cabo una recopilación de datos masiva por parte de empresas y de gobiernos, de manera que *los grandes volúmenes de datos permiten realizar innumerables formas de análisis e intercambio con terceros, lo que suele derivar en más intrusiones en la privacidad y otros impactos adversos en los derechos humanos. [...] Una preocupación particular es la posibilidad de que se anule el anonimato mediante la combinación de datos de diversas fuentes. [...] El almacenamiento prolongado de datos*

[92] Sentencia del Tribunal Constitucional núm 136/1999, de 20 de julio [versión electrónica - base de datos Aranzadi. Ref. RTC\1999\136]

personales también conlleva riesgos, ya que estos pueden ser explotados en el futuro de formas no previstas en el momento de su recopilación. Con el tiempo, los datos pueden volverse inexactos, irrelevantes o conservar errores históricos de identificación, lo que podría causar resultados sesgados o erróneos en futuros procesamientos de datos[93].

Sea por la causa que sea (descuidos, ciberataques, etc), la privacidad en la era digital es vulnerable frente a intromisiones ilícitas. Es por ello que tanto empresas privadas como gobiernos y entidades públicas tienen como principal objetivo proteger la salud y privacidad digital de sus usuarios y ciudadanos, cumpliendo las leyes de privacidad y protección de datos y adoptando las medidas extraordinarias necesarias. Sin embargo, pese a dichos esfuerzos, siguen existiendo casos en los que los datos recopilados se utilizan para fines distintos a los justificados inicialmente, que han dado lugar a vulneraciones del derecho a la privacidad y protección de datos personales de los usuarios[94].

Un claro ejemplo de ello es el caso del escándalo de Cambridge Analytica ocurrido en 2018[95]. Todo comenzó cuando Aleksandr Kogan, un psicólogo de la Universidad de Cambridge, programó una aplicación móvil que ofrecía a sus usuarios un test de personalidad, al cual podían acceder aportando sus datos de Facebook. Esta aplicación accedía a la información personal del usuario y a la de sus seguidores, sin consentimiento de estos últimos. Kogan vendió esta información a la empresa Cambridge Analytica, la cual la utilizó para crear perfiles de posibles votantes y sacar ventaja en las elecciones presidenciales de EE. UU. de 2016, favoreciendo a Donald Trump. El escándalo fue de tal escala que Facebook tuvo que abonar 5.000 millones de dólares en concepto de multa, y su creador, Mark Zuckerberg, testificó ante el Congreso de EE.UU. acerca de la falta de transparencia y de controles de privacidad que presentaba en el momento su aplicación. Como consecuencia, las políticas de privacidad de Facebook fueron reforzadas.

---

[93] United Nations High Commissioner for Human Rights. (2021). The right to privacy in the digital age (A/HRC/48/31). United Nations Humans Rights Council. (disponible en Los riesgos de la inteligencia artificial para la privacidad exigen medidas urgentes –Bachelet | OHCHR, última consulta 09/03/2025).

[94] Cussol, E., "9 Problemas de privacidad de datos que hay que evitar: ejemplos y soluciones", Termly, (disponible en 9 Problemas de privacidad de datos que hay que evitar: Ejemplos y soluciones, última consulta 09/03/2025).

[95] Torrealba, D., "Facebook y Cambridge Analytica: ¿qué pasó y por qué es importante?. Convivencias en red (disponible en Facebook y Cambridge Analytica: ¿qué pasó y por qué es importante?, última consulta 25/02/25).

En España, sin ir más lejos, también se han producido ataques al derecho a la privacidad del ciudadano, incluso por parte de administraciones públicas. Recientemente, la Generalitat Valenciana publicó un vídeo en redes sociales de menores tutelados que visitaban el Bioparc de Valencia, para promover una campaña institucional. El problema radica en que la administración no tomó las medidas necesarias al publicar el vídeo para proteger la identidad de los menores, vulnerando, por tanto, su derecho a la intimidad, a la propia imagen y a la protección de datos. Es por ello por lo que el Síndic de Greuges (Defensor del Pueblo) de la Comunidad Valenciana, Ángel Luna, estima que *se ha vulnerado el derecho a la propia imagen de los menores por no apreciar concurrencia ni de interés público ni de accesoriedad en la fotografía publicada*[96].

4.2 Ataques Cibernéticos

La información es poder. Recopilar datos masivos de carácter personal, empresarial y financiero supone una ventaja competitiva, pero no está exenta de riesgos. Es tal la amenaza que presentan los *hackers* para gobiernos y empresas privadas que países como EE.UU. los han calificado de "terroristas". De hecho, León Panetta, el ex secretario de defensa del país americano, afirmó que un ataque cibernético a las instituciones estadounidenses podría llegar a convertirse en el *próximo Pearl Harbour*[97]. El ciberterrorismo, según el FBI, es *el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos*[98].

A lo largo de la era digital han ocurrido grandes ciberataques que han dado la vuelta al mundo. "Ooops, tus archivos acaban de ser cifrados. Si quieres recuperarlos tendrás que pagar". Esta amenaza apareció el viernes 12 de mayo de 2017 en los ordenadores de los empleados de varias empresas españolas, comenzando lo que actualmente se conoce como el primer ciberataque masivo en el mundo: "WannaCry". Mediante un virus, los *hackers*

[96] Herrero Gutiérrez, A., "El Síndic de Greuges considera que la Generalitat vulneró los derechos de menores tutelados tras la difusión de un video", El País, 7 de marzo de 2025.
[97]Panetta, L. (2012, 12 de octubre). *Discurso sobre ciberseguridad en el Museo Intrepid Sea, Air & Space*. Departamento de Defensa de EE. UU, (disponible en Secretary Leon Panetta on Cybersecurity | C-SPAN.org, última consulta 15/03/2025).
[98] Pollit M., Ciberterrorism: Fact or Fancy, FBI Laboratory.

consiguieron entrar en los sistemas encriptados de más de 10 grandes empresas españolas, entre ellas Telefónica, Iberdrola y Vodafone, pidiendo un rescate a cambio de la liberación de las bases de datos robadas. En cuestión de minutos se convertió en un ciberataque a escala mundial, afectando a otros 149 países, entre ellos, Rusia, Reino Unido, Japón o Alemania. Este ataque podría haber desencadenado una catástrofe mundial, pues afectó, principalmente, a sistemas nacionales de salud (NHS, Reino Unido) que no pudieron acceder a datos de sus pacientes y tuvieron que detener operaciones e intervenciones; a fábricas de automóviles, y a empresas de telecomunicación. Afortunadamente, gracias a numerosos esfuerzos se pudo detener la propagación del virus y no causó daños adicionales. No obstante, este ciberataque sirvió como precedente para reforzar la ciberseguridad, tanto en entidades públicas como en privadas[99].

4.3 Uso de Datos Biométricos

Por otro lado, hablemos del uso de los datos biométricos, especialmente en los sistemas de reconocimiento facial, tan populares a día de hoy. A través de estos mecanismos, una máquina es capaz de detectar a una persona mediante el análisis de su rostro. De hecho, *los sistemas de reconocimiento facial están basados en la capacidad de la IA y los algoritmos de aprendizaje automático (machine learning) para aprender y adaptar patrones a partir de grandes cantidades de datos faciales, procesando atributos faciales tales como la distancia entre los ojos, la forma de la mandíbula, la posición de la nariz y las arrugas alrededor de los ojos*[100]. En otras palabras, estos sistemas, mediante un estudio detallado de las características faciales del individuo, son capaces de identificar secuencias y comparar las imágenes extraídas con el contenido de su base de datos, detectando coincidencias.

[99] Méndez, M.A., "Así fue el primer ciberataque masivo que ha paralizado el mundo", El Confidencial, 27 de junio de 2017 (disponible en Así fue el primer ciberataque masivo que ha paralizado el mundo, última consulta 17/03/2025).
[100] Ricardo, R., "¿Cómo Funcionan los Sistemas de Reconocimiento Facial?", Estudyando, (disponible en ¿Cómo Funcionan los Sistemas de Reconocimiento Facial? | Estudyando, última consulta 11/03/2025).

Los sistemas de reconocimiento facial se utilizan, principalmente, en programas de vigilancia, aunque también se pueden ver en controles de acceso a edificios o plataformas, en campañas de marketing, o incluso en accesos al teléfono móvil. Ahora bien, ¿son sistemas seguros? Como hemos visto durante todo el trabajo, sin una buena regulación, no hay nada seguro. Y es que estos sistemas son susceptibles de vulnerar el derecho a la privacidad y protección de datos del individuo de diversas maneras[101].

En primer lugar, hablemos del riesgo más obvio del reconocimiento facial: la intromisión en la esfera personal del individuo y la consecuente pérdida de la privacidad. Actualmente, nos encontramos continuamente expuestos a cámaras de vigilancia de comercios, bancos, etc, los cuales cuentan con sistemas de reconocimiento facial que analizan nuestro rostro y lo almacenan en su base de datos. Esto supone una continua invasión a la privacidad del individuo, el cual ni siquiera ha sido informado de ello. El problema reside en la falta de conciencia del propio ciudadano, el cual está totalmente acostumbrado a la integración de estos sistemas en su rutina diaria y no se percata de los riesgos que pueden llegar a conllevar. Además, algunos Estados hacen uso arbitrario de estos datos, ejerciendo un control excesivo sobre el ciudadano[102]. Un claro ejemplo de vulneración del derecho a la privacidad es el de China, que *con una población de casi 1.500 millones de habitantes, [...] tiene instaladas más de 700 millones de cámaras de vigilancia, es decir, casi una por cada dos ciudadanos*[103], las cuales se utilizan para fomentar el "sistema de crédito social" chino, que, según fuentes del propio gobierno, ayuda a mejorar el comportamiento social del ciudadano y mejora su confiabilidad para cumplir las normas[104]. El problema es que ya se han empezado a utilizar en otros países democráticos, los cuales necesitan una regulación de la IA extensa para no incurrir en perjuicios al ciudadano.

[101] Aszodi N., y Norga A., "Reconocimiento facial: ventajas e inconvenientes", Liberties, (disponible en Reconocimiento facial: ventajas e inconvenientes | liberties.eu, última consulta 11/03/2025).
[102] Sanabria Moyano, J.E, et all, (2022), "Tecnología de reconocimiento facial y sus riesgos en los derechos humanos". Revista Criminalidad, 64(3), 61-78, (disponible en Tecnología de reconocimiento facial y sus riesgos en los derechos humanos, última consulta 09/03/2025).
[103] Hanna., "Cómo los métodos de vigilancia chinos se están globalizando", Tuta, (disponible en Cómo los métodos de vigilancia chinos se están globalizando. | Tuta, última consulta 11/03/2025).
[104] Serrano Martínez, A., "Crédito social chino: el sistema de puntos que ya se exporta a otras sociedades", El Economista, (disponible en Crédito social chino: el sistema de puntos que ya se exporta a otras sociedades, última consulta 11/03/2025).

Por otro lado, existe un riesgo potencial de robo de datos personales, como ocurrió en octubre de 2023 en Asia, donde un grupo de *hackers* chinos se dedicaba a sustraer datos de sistemas de reconocimiento facial mediante programas aparentemente lícitos, como el conocido "GoldPickaxe", para acceder a las cuentas bancarias de los usuarios. Tal y como explica James Reddick en The Record, *los hackers se hacían pasar por agencias gubernamentales para engañar a las víctimas. En Tailandia, por ejemplo, los usuarios eran incitados a descargar una aplicación llamada "Digital Pension", supuestamente para recibir su pensión en línea. En otros casos, enviaban notificaciones falsas sobre facturas de servicios públicos, instando a los usuarios a hacer clic en un enlace malicioso*[105]. Como vemos, pese a que el uso de datos biométricos en diferentes ámbitos sea cómodo para el ciudadano, no está exento de riesgos. Por ello, se necesita una completa regulación que aborde, no solo mecanismos de protección del derecho a la privacidad del ciudadano, sino también la asunción de responsabilidades ante un uso incorrecto de la IA.

4.4 Regulación del Derecho a la Privacidad

El derecho a la privacidad se configura para proteger la vida personal y la intimidad de los ciudadanos frente a las intromisiones por parte de terceros, empresas privadas e incluso por parte del gobierno. Se recoge en el art.18 de la Constitución, el cual dice lo siguiente:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

[105] Reddickm J., "Hackers are targeting Asian bank accounts using stolen facial recognition data", The Record, (disponible en Hackers are targeting Asian bank accounts using stolen facial recognition data | The Record from Recorded Future News, última consulta 12/03/2025).

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos[106].

Concretamente, debemos centrarnos en este último apartado, el cual regula el derecho del ciudadano a proteger sus datos personales frente al florecimiento de nuevas tecnologías. Ya en 1978, en los orígenes de la Constitución actual, se consideró necesaria la introducción de un apartado que funcionase como marco de protección contra las posibles vulneraciones que tendría la tecnología en los próximos años. Posteriormente, este artículo se ha ido concretando en otras leyes españolas y europeas.

Una de las principales normativas europeas que protege el derecho a la privacidad y a la protección de datos es el RGPD[107], el cual es adaptado en España por la LOPDGDD[108]. Además, no debemos olvidar la Ley de Inteligencia Artificial de la UE[109], y de mecanismos adicionales a la ley para garantizar el cumplimiento de dichas leyes como la AESIA.

Dicho esto, ¿cómo se protege al ciudadano de ciberataques e intromisiones ilícitas? En primer lugar, para evitar usos ilegales de los datos personales, el RGPD establece seis principios que sientan las bases para la recopilación y el procesamiento de datos de manera transparente, recogidos en su artículo 5.1:

[106] Constitución Española (BOE 29 de diciembre de 1978). Op.cit. p.37.
[107] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE 4 de mayo de 2016). Op.cit. p.7.
[108] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 6 de diciembre de 2018). Op.cit. p.7.
[109] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). Op.cit. p.7.

Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)[110].

[110] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE 4 de mayo de 2016). Op.cit. p.7.

Además, el RGPD garantiza al ciudadano medidas para reforzar la seguridad de los datos personales cuando se produzcan pérdidas o filtraciones en su art. 32:

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Asimismo, en caso de ciberataques e intromisiones ilícitas, se obliga a la entidad recopiladora de datos personales a actuar de manera transparente, de forma que el art.34 RGPD le obliga a notificar al perjudicado inmediatamente, para que este pueda adoptar medidas adicionales de protección de sus datos, como proceder al cambio de contraseñas.

Por otro lado, ¿estamos bien protegidos de las instituciones que recopilan nuestros datos biométricos? Lo cierto es que el uso de datos biométricos en España está fuertemente restringido, sujeto a un marco normativo que, aparentemente, limita su uso para evitar cualquier posible vulneración de los derechos fundamentales del usuario. De esta manera, el RGPD, que califica a los datos biométricos como aquellos datos especiales que necesitan una regulación reforzada[111] , en su artículo 9, prohíbe el uso de datos biométricos a no ser que se

[111] Morell Ramos, J., "¿Hasta qué punto es legal usar un sistema de reconocimiento facial?", Abogacía Española, (disponible en ¿Hasta qué punto es legal usar un sistema de reconocimiento facial? – Abogacía Española, última consulta 13/03/2025).

cuente con el consentimiento explícito del usuario o concurra una causa de interés público, entre otras circunstancias:

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado; [...]

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado[112];

Esta prohibición aparece también recogida en la LOPDGDD, lo que refuerza aún más la protección del ciudadano respecto del uso por terceros de sus datos biométricos.

Además, la AEPD publicó, en Noviembre de 2023, una guía ("Tratamientos de control de presencia mediante sistemas biométricos") sobre el uso de estos datos para el control de acceso, tanto para entornos laborales como para entornos no laborales. Al igual que el RGPD, la AEPD considera estos datos como de alto riesgo, por lo que es necesario evaluar su impacto en la protección de datos de los ciudadanos como paso previo a su implementación

[112] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE 4 de mayo de 2016). Op.cit. p.7.

en estos sistemas[113]. Esta evaluación se recoge en el artículo 35.7 RGPD, que dice lo siguiente:

La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas[114].

Si bien es cierto que uno de los requisitos para la utilización de este tipo de datos en sistemas que utilizan IA era el consentimiento explícito del perjudicado, en algunas circunstancias como en el ámbito laboral el consentimiento del trabajador no resulta suficiente para la utilización de este tipo de datos como herramienta de acceso al puesto de trabajo, al encontrarse trabajando por cuenta ajena. Por ello, la AEPD considera adicionalmente necesaria una norma de rango de ley que justifique el uso de datos biométricos para dicha finalidad. Asimismo, en todo momento ha de respetarse el Principio de Minimización de

[113] Agencia Española de Protección de Datos. (2022). "Guía sobre tratamientos de control de presencia mediante sistemas biométricos". AEPD, (disponible en guia-control-presencia-biometrico.pdf, última consulta 13/03/2025).

[114] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE 4 de mayo de 2016). Op.cit. p.7.

Datos, el cual garantiza que los datos recogidos por dichos sistemas son adecuados y limitados a los fines para los cuales se recogieron[115].

Por último, el derecho a la privacidad y protección de datos personales se refuerza con otros derechos que se garantizan a los ciudadanos sobre sus propios datos, como el derecho de acceso del interesado, regulado en el artículo 15 RGPD, mediante el cual el ciudadano puede recabar información sobre qué datos personales recopilan empresas y la administración pública; el derecho de oposición (artículo 21 RGPD), que permite al ciudadano oponerse en cualquier momento al tratamiento de sus datos personales en causas tasadas; o el derecho al olvido, recogido en el artículo 17 RGPD, que garantiza al ciudadano la eliminación de sus datos personales cuando desee, siempre y cuando ya no sean válidos para el fin para el que se recogieron inicialmente.

Dicho esto, en el derecho a la privacidad existen, como en los otros dos derechos analizados anteriormente, lagunas legales que debemos mencionar en el presente estudio.

Para empezar, actualmente nuestro país carece de una ley explícita sobre la inteligencia artificial. Si bien es cierto que determinadas cuestiones aparecen reguladas en otras leyes europeas y nacionales como en el RGPD o en la LOPDGDD, lo cierto es que, sin un marco normativo completo, hay determinados aspectos que se dejan al descubierto, como la certificación de sistemas de IA o la responsabilidad civil en caso de perjuicios al ciudadano. Esto genera desconciertos en la ciudadanía y respuestas legales difusas[116].

En segundo lugar, tampoco existe en España una ley específica sobre el uso de datos biométricos, sino que estos se regulan parcialmente en leyes como el RGPD, la LOPDGDD y resoluciones de la AEPD. Al no estar regulado suficientemente, hay muchos asuntos que quedan sin supervisión, lo que puede dar casos de vigilancias masivas ilegales. No obstante, el art.5 del AI Act prohíbe tajantemente el uso de cámaras de vigilancia con sistemas de reconocimiento facial, tan populares en países como China, a no ser que su uso se limite a los supuestos tipificados en la ley, entre los que se encuentran la búsqueda de víctimas de delitos

[115] García Herrero, J., "Principio de Minimización de Datos en el RGPD: ¿Por Qué es Bueno para Todos?, Jorge García Herrero, (disponible en Principio de Minimizacion de Datos en el RGPD: ¿Por Qué es Bueno para Todos? - Jorge García Herrero y Asociados, abogados, última consulta 07/03/2025).
[116] Herranz, A., "Necesaria, pero con ciertas lagunas: así es la IA Act europea", La Razón, 15 de diciembre de 2023 (disponible en Necesaria, pero con ciertas lagunas: así es la IA Act europea, última consulta 23/03/2025).

o la prevención de ataques terroristas, entre otros. Sin embargo, el uso de sistemas de vigilancia en entornos privados como comercios o empresas no está expresamente prohibido por la ley, pese a considerarse un "sistema de alto riesgo" si afecta directamente a los derechos fundamentales del ciudadano. Pese a ello, recordemos que esta ley es bastante reciente y todavía no se ha procedido a su completa aplicación, y que en España no existe ninguna ley específica sobre el tema, por lo que, mientras tanto, seguirán existiendo zonas grises que pueden dar lugar a la vulneración del derecho a la privacidad[117].

Como conclusión, el derecho a la privacidad carece, a día de hoy, de regulación suficiente para proteger al individuo de las posibles vulneraciones llevadas a cabo por sistemas de IA. Si bien es cierto que el RGPD establece una base sólida, se necesita un marco regulatorio específico en España para poder abordar temas concernientes a la asunción de responsabilidades o los medios de validación de dichos sistemas. En cuanto a los datos biométricos, estos se están comenzando a utilizar en entornos delicados para el individuo, como en su entorno laboral, por lo que resulta fundamental garantizar un uso transparente y ético de dichos datos. Por último, si bien es cierto que la Comisión Europea realizó un gran trabajo con su propuesta del AI Act, y que éste entró en vigor el 1 de agosto de 2024, su aplicación se realizará de manera progresiva, de forma que hasta el 1 de agosto de 2026 no se implementará totalmente, y seguirán habiendo zonas grises sin regulación, susceptibles de causar perjuicios al ciudadano.

[117] Samhermelando J., "Inteligencia artificial: la UE prohibirá la puntuación social y la vigilancia biométrica masiva", El Español, (disponible en Inteligencia artificial: la UE prohibirá la puntuación social y la vigilancia biométrica masiva, última consulta 14/03/2025).

CAPÍTULO V: CONCLUSIÓN FINAL

Actualmente, la IA está en constante desarrollo, transformando multitud de sectores y mejorando tareas propias de los seres humanos. El acceso de los individuos a sistemas que funcionan con IA implica la recopilación de grandes cantidades de datos personales, financieros, e incluso datos que requieren una protección especial, como los biométricos. Es tal la velocidad a la que avanza esta tecnología, y el volumen de datos que ello conlleva, que resulta fundamental disponer de un marco legal sólido y bien estructurado, que regule detalladamente todos los aspectos que abarca este tipo de tecnología.

En el presente trabajo se ha realizado un estudio de, en primer lugar, el marco teórico que envuelve a los sistemas de IA, incluyendo cómo trabajan y en qué sectores se encuentran presentes. Posteriormente se ha analizado su marco normativo actual, lo cual comprende las leyes en las que aparece regulada y los órganos que se encargan de la correcta implementación de dichas normas. Por último, se ha ahondado en tres derechos principales (igualdad, libertad de expresión y privacidad), estudiando cómo la IA es capaz de vulnerarlos y cómo estamos protegidos ante dicho peligro. Este minucioso estudio me ha permitido establecer una conclusión principal sobre la protección de datos en la IA desde la perspectiva constitucional: el marco jurídico de la IA es muy difícil de establecer.

De entrada, hablemos de lo rápido que avanza la IA, que se encuentra completamente descoordinada del Derecho. Las tecnologías se encuentran desarrollándose a la velocidad de la luz, mientras que los procesos legislativos son lentos y tediosos, por lo que, en el momento en el que una norma se aprueba y se procede a su aplicación, la tecnología para la cual fue implementada ya ha avanzado, dejando estas novedades sin regulación alguna. Un claro ejemplo es el RGPD, aprobado el 27 de abril de 2016. Este recoge normas y principios para el uso transparente y ético de los datos personales del ciudadano, pero no incluye normas relativas a las nuevas tecnologías como el famoso Chat GPT. El legislador, por tanto, tiene una ardua tarea, pues ha de adaptarse al ritmo de desarrollo de la tecnología, creando normas que, además de rápidas, sean robustas y carezcan de zonas grises sin regulación. Este supone un clásico debate de la Filosofía del Derecho: la discusión sobre si la ley debe ser la respuesta a los problemas sociales o si, por el contrario, la ley debe adelantarse para resolver dichos problemas cuando se produzcan en un futuro. Reacción frente a la anticipación

En segundo lugar, el AI Act aprobado en 2024 incluye una definición del sistema de IA en su art.3, entendiéndose por este *un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales*[118]. Pese a ello, esta definición es demasiado amplia, lo que sigue generando inseguridad jurídica e interpretaciones diferentes al considerar si un determinado programa está sujeto al reglamento o no. Por tanto, pese a los esfuerzos del legislador de establecer un esquema legal sobre la IA, estas primeras pinceladas son demasiado generales y, lamentablemente, resultan insuficientes para una implementación de la IA ética y transparente.

En tercer lugar, recordemos que la IA es una tecnología cuya evolución se está produciendo a nivel global, de manera que resulta fundamental armonizar las regulaciones entre los distintos países. Sin embargo, esta tarea resulta bastante complicada, pues cada país tiene una visión distinta sobre una correcta regulación de la IA, lo que ha dado lugar a interpretaciones más garantistas para los derechos fundamentales, como la europea, e interpretaciones más económicas y estratégicas, pero no tan éticas, como las de EE.UU. y China. Consecuentemente, se está produciendo un fenómeno conocido como el *forum shopping*[119], el cual implica que las empresas tecnológicas deciden implantar dichos sistemas en aquellos países con controles más laxos, lo que debilita la eficacia de marcos regulatorios más rígidos como el europeo y pone en peligro los derechos fundamentales del ciudadano. Con esto, no puedo evitar preguntarme cómo me afecta esta cuestión a mí, como ciudadana española. Pues bien, si bien es cierto que en España los sistemas de IA se encuentran regulados por normas europeas como el RGPD y el AI Act, corro el riesgo de que los sistemas de IA a los que me someto hayan sido desarrollados en un país donde no se respetan los estándares éticos, o que mis datos estén siendo almacenados en estos países. Esta falta de

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

[119] García Pascual, L., "Entendiendo el Forum Shopping: Concepto y 3 Ejemplos Esenciales", Derecho Virtual (disponible en ▷ Entendiendo el Forum Shopping: Concepto y 3 Ejemplos Esenciales » Derecho Virtual, última consulta 23/03/2025).

armonización internacional implica, por tanto, un peligro potencial para mis derechos fundamentales.

Por último, un desafío en la regulación de la IA es encontrar un equilibrio entre la propulsión de la innovación tecnológica y la protección de los derechos fundamentales. La inteligencia artificial ha venido para quedarse, pues facilita tareas propias del ser humano en multitud de campos, por lo que resulta conveniente invertir en innovación tecnológica. No obstante, sin una buena regulación, los derechos fundamentales quedan expuestos ante casos de discriminación y sesgos algorítmicos, vigilancia masiva, censura algorítmica y decisiones automatizadas fuera del control humano. Por otro lado, si se aplica una muy estricta regulación, los derechos fundamentales pueden correr riesgos adicionales, como ocurre en el derecho a la libertad de expresión, donde la rígida regulación de la desinformación y las *fake news* puede derivar en publicaciones censuradas inflexiblemente, lo que desemboca en una vulneración del derecho a la libertad de expresión del ciudadano. Por tanto, resulta fundamental desarrollar un marco normativo robusto, que encuentre el equilibrio deseado entre la innovación tecnológica y la protección de los derechos fundamentales.

En definitiva, la inteligencia artificial supone un gran reto para los legisladores actuales, pues no solo hay que tener en cuenta los aspectos técnicos del progreso tecnológico, sino que también hay que salvaguardar la ética y transparencia para implementar estos sistemas de manera responsable. Es por ello por lo que, a mi juicio, resulta fundamental, no solo que el legislador establezca normas claras y concisas sobre la IA a tiempo real, sino que haya consenso entre instituciones de distintos países para establecer marcos normativos sólidos y armonizados.

BIBLIOGRAFÍA

1) LEGISLACIÓN

Carta de derechos digitales. Secretaría de Estado de Digitalización e Inteligencia Artificial. (2021). Ministerio de Asuntos Económicos y Transformación Digital.

Carta de los Derechos Fundamentales de la Unión Europea (DOUE 30 de marzo de 2010).

Constitución Española (BOE 29 de diciembre de 1978).

Decisión de la Comisión que dará lugar a la creación de una Oficina Europea de Inteligencia Artificial (DOUE 14 de febrero de 2024).

Declaración Universal de Derechos Humanos. Naciones Unidas. (1948).

Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación (BOE 13 de julio de 2022).

Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación (BOE 27 de marzo de 1984).

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

Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial (BOE 2 de septiembre de 2023).

Real Decreto-ley 9/2021, de 11 de mayo, por el que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales (BOE 12 de mayo de 2021).

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 esos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE 4 de mayo de 2016).

Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (DOUE 27 de octubre de 2022).

Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (DOUE 22 de diciembre de 2023).
Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DOUE 12 de julio de 2024).

2) JURISPRUDENCIA

Sentencia del Tribunal Constitucional núm 136/1999, de 20 de julio [versión electrónica - base de datos Aranzadi. Ref. RTC\1999\136].
Sentencia del Tribunal Constitucional, núm. 292/2000, de 30 de noviembre [versión electrónica - base de datos Aranzadi Digital. Ref. RTC\2000\292]. Fecha de última consulta: 28 de enero de 2025.
Sentencia del Tribunal Constitucional, núm 41/2020, de 9 de marzo [versión electrónica - base de datos Aranzadi. Ref. RTC\2020\41]. Fecha de última consulta: 8 de marzo de 2025.
Sentencia del Tribunal Constitucional, núm. 94/1998 de 4 de mayo, [versión electrónica - base de datos Aranzadi Digital. Ref. RTC\1998\94]. Fecha de última consulta: 28 de enero de 2025.
Sentencia del Tribunal de Justicia de la Unión Europea, núm C-634/2021, de 7 de diciembre [versión electrónica - base de datos Aranzadi. Ref TJCE\2023\146]. Fecha de última consulta: 7 de marzo de 2025.
Sentencia del Tribunal Supremo núm.1238/2021, de 18 de octubre [versión electrónica, base de datos Aranzadi. Ref. RJ\2021\4841] Fecha de la última consulta: 17 de marzo de 2025.

3) OBRAS DOCTRINALES

Barr, A., y Feigenbaum, E., The Handbook of Artificial Intelligence, HeurisTech Press, Standford, 1981.

Boucher, P. Artificial intelligence: How does it work, why does it matter, and what can we do about it?,European Parliamentary Research Service (EPRS), Bruselas, 2020.

Descartes, R., Discurso sobre el método, Leiden, 1637.

El Naqa, I., "et al", Machine Learning in Radiation Oncology: Theory and Applications, Springer, Nueva York, 2015).

Hilera, J., y Martínez, V., Redes Neuronales Artificiales: Fundamentos, modelos y aplicaciones, RA-MA, Madrid, 1995.

Martí Cunquero, R., "Algoritmos Heurísticos de Optimización Combinatoria", Valencia.

Noya, E., Fintech: ahorro e inversión en la era financiera digital, LID Editorial, Barcelona, 2021.

Pollit M., Ciberterrorism: Fact or Fancy, FBI Laboratory.

Ramos Cabrer, M. "Fundamentos de la Inteligencia Artificial: Tema 1-Introducción", Universidad de Vigo.

Rich,E., y Knight, K., Artificial Intelligence, McGraw-Hill, Nueva York, 1991.

Tablada, C.J. y Ariel Torres, G., "Redes Neuronales Artificiales", Revista de Educación Matemática, vol.24, n. 3, 2009).

Vosoughi S,. et all, (2018). The spread of true and false news online. Science, 359(6380), 1146-1151.

Zhang, S., et all, "Artificial Intelligence Report 2024", Standord Institute for Human-Centered Artificial Intelligence.

4) RECURSOS DE INTERNET

Abdulhafeez Y., “Shadowbanned or Deboosted Twitter: What It Means and How to fix it”, Incognition (disponible en Shadowbanned or Deboosted Twitter: What It Means and How to fix it - Incogniton, última consulta 08/03/2025).

Agencia Española de Protección de Datos. (2022). “Guía sobre tratamientos de control de presencia mediante sistemas biométricos”. AEPD, (disponible en guia-control-presencia-biometrico.pdf, última consulta 13/03/2025).

Aszodi N., y Norga A., “Reconocimiento facial: ventajas e inconvenientes”, Liberties, (disponible en Reconocimiento facial: ventajas e inconvenientes | liberties.eu, última consulta 11/03/2025).

Chui, M., “et al”, “The economic potential of generative AI: The next productivity frontier”, European Parliamentary Research Service (EPRS), disponible en the-economic-potential-of-generative-ai-the-next-productivity-frontier-vf.pdf; última consulta 28/01/2025).

Comisión Europea. (2017). KConnect – Servicios de extracción de información y búsqueda semántica para aplicaciones médicas multilingües (Proyecto n.º 644753). CORDIS (disponible en Khresmoi Multilingual Medical Text Analysis, Search and Machine Translation Connected in a Thriving Data-Value Chain | KConnect | Project | Fact sheet | H2020 | CORDIS | European Commission, última consulta 23/01/2025).

Comisión Europea. (2018). “Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Inteligencia Artificial para Europa” (COM(2018) 237 final) (disponible en AI Communication, última consulta 21/02/2025).

Congreso de los Diputados. (2022). Respuesta del Gobierno a la pregunta escrita 184/73609 sobre la desinformación y la Seguridad Nacional, (disponible en e_0193749_n_000.pdf, última consulta 14/03/2025).

Cuevas, J.M., “¿Qué es un ‘think tank’?, El Orden Mundial, (disponible en ¿Qué es un 'think tank'? - El Orden Mundial - EOM, última consulta 20/01/2025).

Cussol, E., “9 Problemas de privacidad de datos que hay que evitar: ejemplos y soluciones”, Termly, (disponible en 9 Problemas de privacidad de datos que hay que evitar: Ejemplos y soluciones, última consulta 09/03/2025).

Dastin, J., “Insight-Amazon scraps secret AI recruiting tool that showed bias against women”, Reuters, (disponible en Insight - Amazon scraps secret AI recruiting tool that showed bias against women | Reuters, última consulta 10/02/2025).

Digital Future Society. (2022). La discriminación algorítmica en España: límites y potencial del marco legal. Digital Future Society, (disponible en Discriminacion_algoritmica_Espana_marco_legal.pdf, última consulta 15/03/2025).

Escrivá, J., “AESIA”, Digital. Gob, 19 de junio de 2024 (disponible en 20240619_NdP_AESIA_Coruna.pdf, última consulta 16/01/2025).

European Commission. (2022). Code of Practice on Disinformation. Publications Office of the European Union, (disponible en Guidance on Strengthening the Code of Practice on Disinformation | Shaping Europe’s digital future, última consulta 17/03/2025).

Fernández-Miranda, F., “Marco regulatorio actual sobre la inteligencia artificial”, PWC (disponible en Marco regulatorio actual sobre inteligencia artificial, última consulta 15/01/2025).

Flores Anarte, L., “Sesgos de Género en la Inteligencia Artificial: el Estado de Derecho frente a la Discriminación Algorítmica por Razón de Sexo”, Universidad de Sevilla, (disponible en 95-120 Sesgos.pdf, última consulta 23/03/2025).

García, E., “DoNotPay: El abogado robot de la IA”, Ser Inteligencia Artificial (disponible en DoNotPay: El abogado robot de IA - Inteligencia Artificial, última consulta 12/01/2025).

García Herrero, J., “Principio de Minimización de Datos en el RGPD: ¿Por Qué es Bueno para Todos?, Jorge García Herrero, (disponible en Principio de Minimizacion de Datos en el RGPD: ¿Por Qué es Bueno para Todos? - Jorge García Herrero y Asociados, abogados, última consulta 07/03/2025).

García Pascual, L., “Entendiendo el Forum Shopping: Concepto y 3 Ejemplos Esenciales”, Derecho Virtual (disponible en ▷ Entendiendo el Forum Shopping: Concepto y 3 Ejemplos Esenciales » Derecho Virtual, última consulta 23/03/2025).

Garrido Jiménez, D., “Inteligencia artificial y el derecho”, Garrido y Doñaque Abogados (disponible en La Inteligencia Artificial y Derecho: su jurisprudencia, última consulta 12/01/2025).

Goñi, E., “Una imagen que vale mil engaños”, El País, 17 de febrero de 2025 (disponible en Una imagen que vale mil engaños | Opinión | EL PAÍS, última consulta 23/03/2025).

Gobierno de España. (2024, 11 de diciembre). Respuesta del Gobierno a las preguntas escritas del Congreso sobre la Agencia Española de Supervisión de Inteligencia Artificial (AESIA)

(Preguntas 184/16529 a 184/16531). Secretaría de Estado de Relaciones con las Cortes y Asuntos Constitucionales.

González Valderrama, D.A., "Desinformación y noticias falsas: Cómo identificar y combatir el fenómeno en la era digital", CuriosoTeatro Global, (disponible en Desinformación y noticias falsas: Cómo identificar y combatir el fenómeno en la era digital - CuriosoTeatro Global: Innovación en Cultura y Educación, última consulta 08/03/2025).

Hanna., "Cómo los métodos de vigilancia chinos se están globalizando", Tuta, (disponible en Cómo los métodos de vigilancia chinos se están globalizando. | Tuta, última consulta 11/03/2025).

Hernández Escobar, C., "¿Qué es la superinteligencia artificial y por qué podría ser necesaria para el futuro?", OpenSistemas, (disponible en ¿Qué es la superinteligencia artificial y por qué podría ser necesaria para el futuro? - OpenSistemas, última consulta 21/01/2025).

Herranz, A., "Necesaria, pero con ciertas lagunas: así es la IA Act europea", La Razón, 15 de diciembre de 2023 (disponible en Necesaria, pero con ciertas lagunas: así es la IA Act europea, última consulta 23/03/2025).

Herrero Gutiérrez, A., "El Síndic de Greuges considera que la Generalitat vulneró los derechos de menores tutelados tras la difusión de un video", El País, 7 de marzo de 2025, (disponible en El Síndic de Greuges considera que la Generalitat vulneró los derechos de menores tutelados tras la difusión de un video | Noticias de la Comunidad Valenciana | EL PAÍS, última consulta 12/03/2025).

Herrero Maortua, F., "Marco regulatorio actual sobre inteligencia artificial", PWC (disponible en Marco regulatorio actual sobre inteligencia artificial, última consulta 12/01/2025)

Hernández, S., "Desinformación sobre la DANA: causas y consecuencias", EFE Verifica (disponible en Desinformación sobre la dana: causas y consecuencias, última consulta 08/03/2025).

Javier Vázquez, V., "La Comisión contra la desinformación y la imposible neutralidad del Gobierno", AgendaPública, (disponible en La Comisión contra la desinformación y la imposible neutralidad del Gobierno, última consulta 21/03/2025).

Khan, I. (2021). *La desinformación y la libertad de opinión y de expresión: Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*. Naciones Unidas. Consejo de Derechos Humanos, 47º período de sesiones. [A/HRC/47/25] (disponible en A/HRC/47/25: La desinformación y la libertad de opinión y de expresión Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan | OHCHR, última consulta 08/03/2025).

Méndez, M.A., “Así fue el primer ciberataque masivo que ha paralizado el mundo”, El Confidencial, 27 de junio de 2017 (disponible en Así fue el primer ciberataque masivo que ha paralizado el mundo, última consulta 17/03/2025).

Moliné, A. “La máquina contra el ser humano: AlphaGo vs humanity”, Acento (disponible en La máquina contra el ser humano: AlphaGo vs humanity | Acento, última consulta 29/01/2025).

Morell Ramos, J., “¿Hasta qué punto es legal usar un sistema de reconocimiento facial?”, Abogacía Española, (disponible en ¿Hasta qué punto es legal usar un sistema de reconocimiento facial? – Abogacía Española, última consulta 13/03/2025).

Navarro, I., “Menos bulos, ‘influencers’: la nueva ley de rectificación les pondrá al mismo nivel que los medios de comunicación”, El País, 19 de enero de 2025 (disponible en Menos bulos, ‘influencers’: la nueva ley de rectificación les pondrá al mismo nivel que los medios de comunicación | Negocios | EL PAÍS, última consulta 21/03/2025).

Ognyanova, K., “Fact-Checking: Journalistic Strategies and Audience Outcomes in Diverse National Contexts”, SageJournals (disponible en Fact-Checking: Journalistic Strategies and Audience Outcomes in Diverse National Contexts - Katherine Ognyanova, 2024, última consulta 17/03/2025).

Panetta, L. (2012, 12 de octubre). *Discurso sobre ciberseguridad en el Museo Intrepid Sea, Air & Space*. Departamento de Defensa de EE. UU, (disponible en Secretary Leon Panetta on Cybersecurity | C-SPAN.org, última consulta 15/03/2025).

Perezagua Naharro, M., “Marco regulatorio de la inteligencia artificial en España”, Auditat. (disponible en Marco regulatorio de la inteligencia artificial en España | Audidat, última consulta 19/01/2025).

Quiñónez, H.A., “La desinformación vulnera el derecho a la libertad de expresión| Por: Herly Alejandra Quiñónez”, MujerAnalítica, (disponible en La desinformación vulnera el derecho a la libertad de expresión| Por: Herly Alejandra Quiñónez - Mujer Analítica, última consulta 18/03/2025).

Rajmil, M., “Modria, un software para resolver divorcios u otras disputas jurídicas vía Internet”, Digital Trends Español (disponible en Modria, un software para resolver divorcios y otras disputas jurídicas vía Internet | Digital Trends Español, última consulta 12/01/2025).

Reddickm J., “Hackers are targeting Asian bank accounts using stolen facial recognition data”, The Record, (disponible en Hackers are targeting Asian bank accounts using stolen facial recognition data | The Record from Recorded Future News, última consulta 12/03/2025).

Ricardo, R., "¿Cómo Funcionan los Sistemas de Reconocimiento Facial?", Estudyando, (disponible en ¿Cómo Funcionan los Sistemas de Reconocimiento Facial? | Estudyando, última consulta 11/03/2025).

Roch Moraguez, E., "Inteligencia Artificial en Medicina: Cómo la IA Está Salvando Vidas", LovTechnollogy, (disponible en Inteligencia Artificial en Medicina: Cómo la IA Está Salvando Vidas, última consulta 20/01/2025).

Rodríguez, S. "IA neurosimbólica, todo lo que debes saber", Big Data Magazine. (disponible en IA neurosimbólica, todo lo que debes saber - Big Data Magazine; última consulta 18/12/2024).

Rouse, M., "Inteligencia artificial débil", Techopedia. (disponible en ¿Qué significa la inteligencia artificial débil?, última consulta 13/01/2025).

Saione, M., "Regulación de la IA: un reto global", Meer, (disponible en Regulación de la inteligencia artificial: un reto global | Meer, última consulta 30/01/2025).

Samhermelando J., "Inteligencia artificial: la UE prohibirá la puntuación social y la vigilancia biométrica masiva", El Español, (disponible en Inteligencia artificial: la UE prohibirá la puntuación social y la vigilancia biométrica masiva, última consulta 14/03/2025).

Sanabria Moyano, J.E, et all, (2022), "Tecnología de reconocimiento facial y sus riesgos en los derechos humanos". Revista Criminalidad, 64(3), 61-78, (disponible en Tecnología de reconocimiento facial y sus riesgos en los derechos humanos, última consulta 09/03/2025).

Sancho Azcoitia, S., "MYCIN, El comienzo de la Inteligencia Artificial en el mundo de la medicina", Telefónica Tech (disponible en MYCIN, El comienzo de la Inteligencia Artificial en el mundo de la medicina, última consulta 30/01/2025).

Secretaría de Estado de Comunicación. (2020, 2 de diciembre). Estrategia Nacional de Inteligencia Artificial (ENIA). Gobierno de España, (disponible en Pedro Sánchez presenta la Estrategia Nacional de Inteligencia Artificial con una inversión pública de 600 millones en el periodo 2021-2023, última consulta 16/01/2025)

Serrano Martínez, A., "Crédito social chino: el sistema de puntos que ya se exporta a otras sociedades", El Economista, (disponible en Crédito social chino: el sistema de puntos que ya se exporta a otras sociedades, última consulta 11/03/2025).

Solar Calvo, P., y Lacal Cuenca, P., "Inteligencia artificial en el medio penitenciario", LegalToday, (disponible en Inteligencia artificial en el medio penitenciario - LegalToday, última consulta 07/03/2025).

Soper, S., “Fired by Bot at Amazon: ‘It’s You Against the Machine’”, *Bloomberg*, (disponible en Fired by Bot: Amazon Turns to Machine Managers And Workers Are Losing Out - Bloomberg, última consulta 20/01/2025).

Spring, M., “Las imágenes falsas creadas con IA para intentar atraer el apoyo de los votantes negros hacia Trump”, BBC News, (disponible en Elecciones en Estados Unidos: las imágenes falsas creadas con IA para intentar atraer el apoyo de los votantes negros hacia Trump - BBC News Mundo, última consulta 08/03/2025).

Torrealba, D., “Facebook y Cambridge Analytica: ¿qué pasó y por qué es importante?. Convivencias en red (disponible en Facebook y Cambridge Analytica: ¿qué pasó y por qué es importante?, última consulta 25/02/25).

United Nations High Commissioner for Human Rights. (2021). The right to privacy in the digital age (A/HRC/48/31). United Nations Humans Rights Council. (disponible en Los riesgos de la inteligencia artificial para la privacidad exigen medidas urgentes –Bachelet | OHCHR, última consulta 09/03/2025).

Von der Leyen, U., “Europe’s choice. Political guidelines for the next European Commission 2024-2029”, Comisión Europea (disponible en e6cd4328-673c-4e7a-8683-f63ffb2cf648_en; última consulta 28/01/2025).