

**EL COSTE SOCIAL DE LA EFICIENCIA TECNOLÓGICA:
INTELIGENCIA ARTIFICIAL, DISCRIMINACIÓN INVISIBLE Y LA
TUTELA DE LOS DERECHOS FUNDAMENTALES**

**THE SOCIAL COST OF TECHNOLOGICAL EFFICIENCY: ARTIFICIAL
INTELLIGENCE, INVISIBLE DISCRIMINATION AND THE
PROTECTION OF FUNDAMENTAL RIGHTS**

**O CUSTO SOCIAL DA EFICIÊNCIA TECNOLÓGICA: INTELIGÊNCIA
ARTIFICIAL, DISCRIMINAÇÃO INVISÍVEL E A TUTELA DOS
DIREITOS FUNDAMENTAIS**

Daniel Martínez Cristóbal*

1 Introducción. 2 Marco conceptual y de gobernanza de la Inteligencia Artificial. 2.1 El problema técnico-jurídico de la caja negra y el conflicto de bienes jurídicos. 2.2 La gobernanza institucional en España: el rol pionero y sancionador de la AESIA. 3 El impacto de la Inteligencia Artificial en los derechos fundamentales. 3.1 Derecho a la intimidad y protección de datos (artículo 18 CE): el choque frontal con el big data y la biometría. 3.2 Principio de igualdad y no discriminación (artículo 14 CE): el sesgo algorítmico, los *proxies* y el hito de la Ley Rider. 3.3 Libertad de expresión e información (artículo 20 CE): los retos de la moderación algorítmica, el sobrebloqueo y la censura privatizada. 4 Retos para el Estado de Derecho: administración pública y justicia en España. 4.1 La actuación administrativa automatizada: los límites dogmáticos y las lecciones del caso Bosco. 4.2 Tutela judicial efectiva y el riesgo de indefensión algorítmica: el escrutinio de los sistemas Viogén y RisCanvi. 4.3 El deber de motivación y la consagración del principio de reserva de humanidad. 5 La aplicación normativa europea y la conexión con el constitucionalismo español. 5.1 El derecho a no ser objeto de decisiones individuales automatizadas. 5.2 La Carta de Derechos Digitales de España como instrumento de interpretación. 5.3 El debate del constitucionalismo español frente a la IA: entre la reforma y la mutación constitucional. 6 Conclusiones. Referencias.

* Profesor Titular en la Universidad Rey Juan Carlos. Licenciado en Derecho por la Universidad Complutense de Madrid, y Doctor en Derecho por la Universidad de Alcalá de Henares, con el que obtuvo la mención Cum Laude. Autor de diversos artículos publicados en revistas de impacto, libros y capítulos de libro y colaboraciones. Sus líneas de investigación son el constitucionalismo histórico español y la eficacia de los derechos dentro del marco de la gobernanza global y las nuevas tecnologías. Madrid, Espanha. E-mail: danielmcrystal@gmail.com. Orcid: <https://orcid.org/0000-0001-9754-5688>



RESUMEN

Contexto: El uso generalizado de la Inteligencia Artificial (IA) representa un desafío sin precedentes al modelo tradicional de Estado de Derecho, impulsando una transición hacia un modelo de Estado algorítmico. En este nuevo escenario, la prioridad otorgada a la eficiencia tecnológica pone en grave riesgo derechos fundamentales consolidados.

Objetivos: Analizar las tensiones sociojurídicas derivadas de la automatización de decisiones, evaluando de manera rigurosa la resiliencia del ordenamiento constitucional español y del marco normativo europeo frente a la creciente indefensión algorítmica.

Metodología: Se emplea un análisis dogmático y sociojurídico de la Constitución Española, el Reglamento Europeo de IA (AI Act) y la incipiente labor de agencias supervisoras como la AESIA. El estudio se centra en el obstáculo técnico-jurídico de la caja negra y el sesgo algorítmico.

Resultados: Se evidencia un conflicto estructural entre los sistemas predictivos de alto riesgo y los derechos fundamentales. Destaca la vulneración de la intimidad por el procesamiento extractivista de datos y del principio de igualdad mediante una discriminación indirecta camuflada a través de variables subrogadas (*proxies*). Asimismo, la opacidad tecnológica, escudada en el secreto empresarial, genera una asimetría informativa para la ciudadanía.

Conclusiones: Es imperativo promover una reinterpretación constitucional garantista que consagre la transparencia algorítmica y la reserva de humanidad. La tutela judicial efectiva exige redefinir la gobernanza tecnológica, garantizando un control socio-legal y una supervisión humana ineludible sobre las decisiones automatizadas.

Palabras clave: Inteligencia Artificial; Estado de Derecho; discriminación algorítmica; derechos fundamentales; eficiencia tecnológica.

ABSTRACT

Context: The widespread use of Artificial Intelligence (AI) represents an unprecedented challenge to the traditional model of the Rule of Law, driving a transition towards an algorithmic State model. In this new scenario, the priority given to technological efficiency places consolidated fundamental rights at serious risk.

Objectives: To analyse the socio-legal tensions arising from the automation of decision-making, rigorously evaluating the resilience of the Spanish constitutional order and the European regulatory framework against growing algorithmic defencelessness.

Methodology: A dogmatic and socio-legal analysis of the Spanish Constitution, the European

AI Regulation (AI Act), and the incipient work of supervisory agencies such as the AESIA is employed. The study focuses on the technical-legal obstacle of the black box and algorithmic bias.

Results: A structural conflict between high-risk predictive systems and fundamental rights is evidenced. The infringement of privacy through the extractivist processing of data and of the principle of equality through indirect discrimination camouflaged via proxies stand out. Furthermore, technological opacity, shielded by trade secrets, generates an information asymmetry for citizens.

Conclusions: It is imperative to promote a guarantee-oriented constitutional reinterpretation that enshrines algorithmic transparency and the reservation of humanity. Effective judicial protection demands redefining technological governance, guaranteeing socio-legal control and unavoidable human supervision over automated decisions.

Keywords: Artificial Intelligence; Rule of Law; algorithmic discrimination; fundamental rights; technological efficiency.

RESUMO

Contexto: O uso generalizado da Inteligência Artificial (IA) representa um desafio sem precedentes ao modelo tradicional de Estado de Direito, impulsionando uma transição para um modelo de Estado algorítmico. Neste novo cenário, a prioridade conferida à eficiência tecnológica coloca em grave risco direitos fundamentais consolidados.

Objetivos: Analisar as tensões sociojurídicas decorrentes da automatização de decisões, avaliando de forma rigorosa a resiliência do ordenamento constitucional espanhol e do quadro normativo europeu face à crescente indefesa algorítmica.

Metodologia: Emprega-se uma análise dogmática e sociojurídica da Constituição Espanhola, do Regulamento Europeu de IA (AI Act) e do trabalho incipiente de agências de supervisão como a AESIA. O estudo centra-se no obstáculo técnico-jurídico da caixa negra e do viés algorítmico.

Resultados: Evidencia-se um conflito estrutural entre os sistemas preditivos de alto risco e os direitos fundamentais. Destaca-se a violação da reserva da intimidade pelo processamento extrativista de dados e do princípio da igualdade mediante uma discriminação indireta camuflada através de variáveis de substituição (*proxies*). Da mesma forma, a opacidade tecnológica, escudada no segredo comercial, gera uma assimetria informativa para os cidadãos.

Conclusões: É imperativo promover uma reinterpretação constitucional garantista que

consagre a transparência algorítmica e a reserva de humanidade. A tutela jurisdiccional efetiva exige redefinir a governança tecnológica, garantindo um controlo sociojurídico e uma supervisão humana iniludível sobre as decisões automatizadas.

Palavras-chave: Inteligência Artificial; Estado de Direito; discriminação algorítmica; direitos fundamentais; eficiência tecnológica.

1 INTRODUCCIÓN

El vertiginoso desarrollo, la proliferación y la implementación masiva de la Inteligencia Artificial (IA) representan, sin lugar a dudas, uno de los mayores desafíos regulatorios, dogmáticos y filosóficos a los que se ha enfrentado el constitucionalismo contemporáneo desde su consolidación. Históricamente, el Derecho ha avanzado a un ritmo notablemente más pausado que la disrupción tecnológica, actuando tradicionalmente de forma reactiva para encauzar los cambios sociales, económicos y culturales dentro de los cauces de la legalidad imperante. Sin embargo, la naturaleza profundamente transformadora de la Inteligencia Artificial trasciende con creces la mera digitalización de los procesos burocráticos o la automatización industrial (Tahirí Moreno, 2025). Su capacidad intrínseca para perfilar ciudadanos a gran escala, predecir comportamientos futuros, procesar volúmenes inabarcables de datos masivos y, fundamentalmente, automatizar la toma de decisiones que afectan a la esfera personal y patrimonial de los individuos, ha generado una fricción inédita con los pilares estructurales del Estado de Derecho.

El paradigma actual evidencia un riesgo latente, advertido por la doctrina científica, de transitar desde un Estado Constitucional y Democrático de Derecho clásico hacia un modelo de Estado algorítmico, un ecosistema procedimental donde la eficiencia computacional, la optimización estadística y la velocidad de procesamiento amenazan con desplazar de manera silenciosa las garantías constitucionales forjadas durante siglos.

En el contexto específico de España, la irrupción de la Inteligencia Artificial no opera en un vacío normativo ni ético, sino que debe someterse imperativamente al estricto marco de convivencia establecido por la Constitución Española, que exige que cualquier ejercicio de poder, sea este analógico o digital, público o corporativo, quede subordinado al respeto de los derechos fundamentales y las libertades públicas (Cotino Hueso, 2024). No obstante, el uso progresivo de algoritmos predictivos y sistemas de decisión automatizada por parte de los poderes públicos y el sector privado amenaza con desdibujar garantías constitucionales clásicas ante la pasividad inicial del legislador.

Casos recientes y altamente paradigmáticos en el panorama jurisprudencial y administrativo nacional han puesto de manifiesto la intensidad de esta tensión estructural.

La controversia jurídica generada en torno a la aplicación informática BOSCO, utilizada por la Administración para la concesión del bono social eléctrico, ha evidenciado los enormes peligros que conlleva la opacidad del código fuente frente a los administrados, desatando un debate de primer orden sobre los límites de la propiedad intelectual frente a la transparencia de los poderes públicos (Moreno García, 2025).

Del mismo modo, el uso de complejas herramientas de valoración de riesgo en el ámbito policial y penitenciario, como los sistemas VioGén a nivel estatal y RisCanvi en la comunidad autónoma de Cataluña, confrontan directamente la legítima búsqueda de la eficiencia administrativa y la seguridad pública con el derecho fundamental a la tutela judicial efectiva, la necesaria motivación de las resoluciones restrictivas de derechos, y la proscripción de la arbitrariedad consagrada en el artículo 9.3 de la Constitución.

La esencia técnica y jurídica de este complejo escenario radica en el conocido fenómeno de la caja negra (*black box*). Este concepto describe la incapacidad estructural, tanto desde el punto de vista de la ingeniería informática como desde la perspectiva jurídica, de comprender, auditar y trazar el camino lógico mediante el cual un modelo de aprendizaje automático (*machine learning*) o de redes neuronales profundas (*deep learning*) llega a una conclusión específica (Pacheco Jiménez, 2024).

A diferencia de la programación tradicional, donde las reglas son dictadas por un humano, la IA infiere sus propias reglas a partir de los datos de entrenamiento. Cuando esta opacidad tecnológica intrínseca se protege y se blindo bajo el escudo jurídico del secreto empresarial o la propiedad intelectual corporativa, se produce una preocupante privatización material de la justicia y de la función pública, dejando al ciudadano en una posición de asimetría informativa insalvable. Resulta absolutamente imperativo, por tanto, analizar si el ordenamiento constitucional español y la naciente estructura normativa europea ofrecen respuestas materiales y procesales con la robustez suficiente para evitar la indefensión algorítmica y garantizar el principio de reserva de humanidad en la toma de decisiones críticas.

El objetivo principal es analizar las tensiones jurídicas derivadas de la implantación de sistemas de Inteligencia Artificial frente al marco constitucional español. Se busca evaluar de manera rigurosa la resiliencia, la ductilidad y la permeabilidad de nuestro sistema de protección de derechos fundamentales y garantías procedimentales ante el avance inexorable de la toma de decisiones automatizadas, identificando las grietas del sistema y proponiendo soluciones interpretativas.

La Constitución Española, interpretada bajo la fecunda doctrina del árbol vivo que le otorga la capacidad de adaptarse hermenéuticamente a las realidades sociales y tecnológicas de su tiempo, no requiere de una reforma estructural por los complejos cauces de los artículos

167 o 168, ni de la inclusión expresa de un nuevo catálogo de neuroderechos constitucionales para hacer frente al fenómeno de la IA. Por el contrario, la respuesta dogmática más solvente y jurídicamente viable reside en una profunda mutación constitucional impulsada a través de una reinterpretación garantista y expansiva por parte de los máximos intérpretes del ordenamiento, el Tribunal Constitucional y el Tribunal Supremo (Balaguer Callejón, 2022). Esta exégesis evolutiva debe estar orientada a consagrar la transparencia algorítmica y la exigencia ineludible de supervisión humana significativa como condiciones insoslayables para el despliegue de la IA en sectores que supongan un alto riesgo para la ciudadanía.

2 MARCO CONCEPTUAL Y DE GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL

Desde una perspectiva técnico-jurídica, el Reglamento (UE) 2024/1689 (AI Act) define la Inteligencia Artificial fundamentándose en su capacidad de inferencia, su nivel de autonomía operativa para generar resultados (*outputs* tales como predicciones, recomendaciones, contenidos generativos o decisiones directas) y su capacidad para influir de manera material en los entornos físicos o virtuales en los que se despliega (Huergo Lora, 2024).

Sin embargo, resulta imprescindible distinguir entre verdaderos sistemas de Inteligencia Artificial (aquellos basados en modelos probabilísticos, redes neuronales y aprendizaje inductivo a partir del entrenamiento masivo con datos) y los meros sistemas informáticos instrumentales o algoritmos de corte puramente determinista. Un algoritmo tradicional se limita a mecanizar una serie de instrucciones lógicas y secuenciales preconcebidas de antemano por un programador humano para aplicar una norma (funcionando en la práctica como una calculadora compleja o un motor de reglas). Estos algoritmos deterministas no extraen nuevos criterios de los datos, no aprenden de la experiencia iterativa ni poseen una autonomía decisional real, por lo que su tratamiento jurídico y su régimen de impugnación difieren sustancialmente de la verdadera IA.

El Reglamento de Inteligencia Artificial (AI Act) estructura su nivel de intervención normativa en torno a cuatro categorías fundamentales basadas en el riesgo, determinando la intensidad de la intervención normativa en función del daño potencial infligido a los derechos fundamentales y la seguridad ciudadana (Jove Villares, 2025).

En primer lugar, se contempla el riesgo inaceptable, que engloba aquellas prácticas tecnológicas taxativamente prohibidas en el territorio de la Unión por considerarse radicalmente contrarias a los valores europeos y vulnerar el núcleo duro de la dignidad humana. Ejemplos paradigmáticos de esta categoría incluyen los sistemas de puntuación

social ciudadana (*social scoring*) por parte de autoridades, la manipulación cognitiva subliminal y la identificación biométrica remota en tiempo real en espacios públicos, salvo excepciones policiales hiper-restringidas.

En un segundo escalón se sitúa el alto riesgo, compuesto por sistemas lícitos y permitidos, pero sujetos a un férreo escrutinio y a requisitos *ex ante* sumamente estrictos antes de su comercialización o despliegue. Para garantizar su viabilidad, se exigen altos estándares de transparencia, supervisión humana ininterrumpida y mitigación proactiva de sesgos. Las aplicaciones típicas de este nivel son las herramientas de IA empleadas en la Administración de Justicia, el control migratorio, la selección de personal y recursos humanos, la gestión de infraestructuras críticas y la concesión de ayudas públicas (Martínez Gutiérrez, 2023).

A continuación, la normativa define el riesgo limitado, aplicable a sistemas que imponen obligaciones de transparencia básicas y específicas diseñadas para evitar el engaño, la confusión o la manipulación del usuario final. El paradigma de este nivel son los *chatbots* conversacionales, donde la persona debe ser explícitamente advertida de que interactúa con una máquina, así como los sistemas de generación de contenido sintético o *deepfakes*, que quedan sujetos a estrictas obligaciones de marcaje de agua.

Finalmente, la estructura regulatoria se asienta sobre el riesgo mínimo. Este nivel abarca los sistemas de uso cotidiano que no presentan amenazas significativas y que operan sin obligaciones jurídicas adicionales bajo el paraguas del AI Act, fomentándose únicamente su adhesión a códigos de conducta voluntarios (Presno Linera, 2025). En la práctica, esto incluye herramientas como los filtros automatizados de correo no deseado (spam), los algoritmos integrados en videojuegos comerciales o la IA de uso puramente instrumental o de entretenimiento menor.

La mayor tensión constitucional en el marco del Estado español se concentra, indiscutiblemente, en la categoría de Alto Riesgo. Es en este estrato donde se engloban los sistemas algorítmicos adquiridos y desplegados por los poderes públicos para el ejercicio de potestades administrativas y judiciales que inciden de forma directa, coactiva y a menudo limitativa en la esfera jurídica de los ciudadanos.

2.1 EL PROBLEMA TÉCNICO-JURÍDICO DE LA CAJA NEGRA Y EL CONFLICTO DE BIENES JURÍDICOS

El principal obstáculo estructural para la integración pacífica, garantista y armónica de la Inteligencia Artificial en el seno de un Estado de Derecho es la caja negra (*black box*). Los modelos algorítmicos contemporáneos más avanzados, particularmente aquellos basados en técnicas de aprendizaje profundo (*deep learning*) y sustentados sobre redes neuronales

artificiales con miles de millones de parámetros ajustables, operan con un nivel de multidimensionalidad matemática y abstracción estadística que hace que sus procesos internos resulten materialmente inescrutables (Fortes Martín, 2025).

Esta opacidad no es meramente un defecto de diseño, sino una característica inherente a la forma en que la máquina optimiza la resolución de problemas. Se produce así una paradoja epistemológica de profundas consecuencias jurídicas, ya que los desarrolladores y usuarios conocen perfectamente los datos masivos introducidos en el sistema (*inputs*) y observan con claridad la decisión, probabilidad o predicción final generada (*outputs*), pero ignoran de manera absoluta el razonamiento lógico exacto, la ponderación específica de las variables o el *iter* deductivo que condujo inequívocamente a dicho resultado.

Esta opacidad intrínseca genera un conflicto directo e intenso de bienes jurídicos protegidos al más alto nivel constitucional. Por un lado, se erige de forma imperativa el derecho fundamental de los ciudadanos a la tutela judicial efectiva y a no padecer indefensión (artículo 24 CE), el derecho a obtener resoluciones judiciales y administrativas debidamente motivadas (artículo 120.3 CE) y el principio rector de transparencia de la actuación de los poderes públicos (artículo 105.b CE). El administrado exige comprender las razones por las cuales se le deniega una prestación, se le clasifica con un alto riesgo de reincidencia o se descarta su candidatura laboral (Gutiérrez García, 2024).

A pesar de ello, estos derechos ciudadanos colisionan frontalmente con el marco de la economía de mercado y la innovación corporativa en el derecho a la libertad de empresa (artículo 38 CE) y la imperiosa necesidad de la industria tecnológica de proteger la propiedad intelectual y el secreto empresarial del código fuente y la arquitectura de sus algoritmos. En el ordenamiento español, este interés corporativo se encuentra fuertemente tutelado por la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, así como por la legislación en materia de propiedad intelectual (Jove Villares; Presno Linera, 2025).

A pesar de la contundencia de este choque de trenes normativo, la jurisprudencia y la doctrina constitucional mayoritaria han comenzado a asentar y consolidar el criterio jurídico de que, cuando un sistema algorítmico se emplea para el ejercicio de potestades públicas con capacidad de imperio, o en contextos sociolaborales que afectan el disfrute de derechos fundamentales, el secreto corporativo no puede operar jamás como un escudo opaco de carácter absoluto frente a la ciudadanía. Surge de este modo la exigencia del derecho a la transparencia algorítmica como derecho de nueva generación, y que obliga a la Administración responsable o a la empresa empleadora a traducir la compleja lógica matemática a un lenguaje comprensible y jurídicamente evaluable, permitiendo de facto al afectado articular una defensa material y cuestionar la validez sustantiva de los criterios estadísticos aplicados (Miranzo Díaz, 2023).

2.2 LA GOBERNANZA INSTITUCIONAL EN ESPAÑA: EL ROL PIONERO Y SANCIONADOR DE LA AESIA

Ante la inmensa complejidad de los desafíos técnicos y jurídicos, el diseño de una estructura institucional ágil y dotada de amplios poderes resulta perentorio para asegurar el control real y efectivo del cumplimiento normativo en todo el territorio. En este ámbito específico, el Estado español ha asumido un liderazgo dentro de la Unión Europea al crear la Agencia Española de Supervisión de Inteligencia Artificial (AESIA), convirtiéndose en el primer país europeo en dotarse de una autoridad de esta naturaleza.

Constituida mediante el Real Decreto 729/2023, la AESIA se erige y configura como la autoridad nacional competente, dotada de plena independencia técnica, autonomía funcional y capacidad de gestión. Su mandato orbita en torno a la supervisión integral, el control del cumplimiento normativo del AI Act y el fomento de un ecosistema nacional de inteligencia artificial caracterizado por la ética, la seguridad y el respeto a los derechos de la ciudadanía.

El despliegue operativo de la AESIA se produjo el 2 de febrero de 2025, centrándose inicialmente en la persecución de las prácticas prohibidas dictadas por Europa. Posteriormente, la agencia asumió la plena potestad sancionadora a partir del 2 de agosto del mismo año. Esta potestad punitiva faculta a la agencia para incoar expedientes e imponer multas coercitivas de extrema severidad, las cuales pueden llegar a alcanzar la cifra de 35 millones de euros por infracciones consideradas graves contra la normativa europea en el diseño o despliegue de sistemas algorítmicos.

La filosofía de la AESIA no se agota en su vertiente estrictamente punitiva o inspectora, sino que ejerce paralelamente una labor de gobernanza anticipatoria, pedagógica y orientadora de enorme valor para el tejido productivo y el sector público. Para facilitar la comprensión, asimilación y aplicación práctica del intrincado articulado del Reglamento de IA, la agencia ha elaborado y publicado un exhaustivo conjunto de dieciséis guías prácticas y técnicas dirigidas a orientar paso a paso a los desarrolladores, proveedores y responsables de despliegue de IA en territorio español.

Dentro de este catálogo destacado de 2025, adquiere especial relevancia la Guía 06 sobre Vigilancia humana. Este documento desarrolla las complejas exigencias del artículo 14 del AI Act, imponiendo el diseño de interfaces efectivas y estableciendo modelos de gobernanza como el *Human-in-the-loop* (HITL). Su objetivo es garantizar que las decisiones generadas por sistemas de alto riesgo sean ineludiblemente auditadas por personas físicas dotadas de la capacidad material y legal para invalidar o revertir los resultados (Lazcoz Moratinos, 2024).

En íntima conexión, la Guía 07 de Gobernanza de datos fija protocolos científicos y procedimentales sumamente rigurosos para el diseño, depuración y enriquecimiento de los conjuntos de datos de entrenamiento. En la práctica, exige exámenes estadísticos preventivos para detectar, evaluar y mitigar sesgos discriminatorios latentes que puedan derivar en afectaciones a los derechos fundamentales.

Por su parte, la Guía 11 de Ciberseguridad establece exigentes medidas organizativas y técnicas, como el control de accesos RBAC y auditorías específicas, para blindar los modelos de IA de alto riesgo frente a manipulaciones externas y ataques adversarios sofisticados. El texto hace especial hincapié en la prevención del envenenamiento de datos (*data poisoning*) y los ataques de evasión durante la fase de inferencia. Como complemento temporal a estas medidas de seguridad, la Guía 13 de Vigilancia poscomercialización obliga a la puesta en marcha de sistemas de monitoreo y telemetría continua. Estos mecanismos resultan indispensables para detectar derivas estadísticas en el rendimiento del modelo, caídas de precisión o impactos negativos imprevistos sobre colectivos de personas una vez que la IA se encuentra plenamente operativa en el mercado o en la administración.

Finalmente, para vertebrar el cumplimiento normativo de manera práctica, la Guía 16 (Manual de checklist de guías de requisitos) funciona proporciona herramientas de autoevaluación estructuradas en formato matriz, permitiendo a las empresas auditar su nivel de madurez tecnológica y trazar planes de adaptación certeros para cumplir con los doce requisitos primordiales del Reglamento europeo.

Junto a esto, España ha complementado su visión de gobernanza integral con la articulación pionera del primer entorno controlado de pruebas (*sandbox* regulatorio) de la Unión Europea con la aprobación del Real Decreto 817/2022, permitiendo a las administraciones públicas y al sector tecnológico privado testar, tensionar y validar sistemas de IA de alto riesgo en condiciones controladas de seguridad jurídica y técnica antes de su comercialización generalizada (Cotino Hueso, 2024). Esta herramienta de derecho experimental resulta vital para integrar la protección y el cumplimiento de los derechos fundamentales desde la fase misma de diseño e ingeniería del *software* (*ethics and fundamental rights by design*), materializando un modelo de regulación verdaderamente proactivo.

3 EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LOS DERECHOS FUNDAMENTALES

La irrupción de la Inteligencia Artificial en la sociedad contemporánea no sólo representa un cambio de herramienta técnica, sino que modifica desde sus cimientos las coordenadas fácticas bajo las cuales se ejercen, tutelan y garantizan los derechos

fundamentales. La estructura intrínseca de esta tecnología exige de la comunidad jurídica una urgente relectura y reinterpretación material del Título I de la Constitución Española. De no acometerse esta tarea hermenéutica, se corre el riesgo inminente de provocar la obsolescencia práctica de la Constitución frente al poder fáctico de los gigantes tecnológicos.

Hay que tener en cuenta que el marco constitucional se forjó en un mundo analógico, por lo que el Derecho no debe limitarse a un enfoque puramente restrictivo. Ante la presente metamorfosis digital, los poderes públicos tienen la obligación de promover la adopción de la IA en áreas donde su precisión salva vidas o mejora sustancialmente el bienestar general (por ejemplo, en el diagnóstico médico o la sostenibilidad). Sin embargo, este derecho a la IA debe equilibrarse indisolublemente con la contención estricta hacia la propensión a la autonomía descontrolada y la generación de daños colectivos (Landa Reza, 2025).

3.1 DERECHO A LA INTIMIDAD Y PROTECCIÓN DE DATOS (ARTÍCULO 18 CE): EL CHOQUE FRONTAL CON EL BIG DATA Y LA BIOMETRÍA

El modelo hegemónico de desarrollo y evolución de la Inteligencia Artificial contemporánea, con particular incidencia en las ramas del aprendizaje automático y el aprendizaje profundo, posee una naturaleza esencial e insoslayablemente extractivista. Para que logren un grado óptimo de precisión y operatividad, resulta imperativo entrenarlas mediante el procesamiento masivo de conjuntos de datos históricos de dimensiones inabarcables (*Big Data*).

Esta insaciable demanda algorítmica de datos, ejecutada frecuentemente a través de técnicas de extracción automatizada a gran escala (*web scraping*), colisiona de forma frontal con los cimientos del derecho a la protección de datos. Dicha confrontación se hace evidente al contraponer los principios de minimización de datos (recabar solo lo estrictamente necesario) y limitación de la finalidad (usarlos solo para el propósito original explícito), consagrados en el artículo 5 del Reglamento General de Protección de Datos (RGPD).

En el ordenamiento constitucional español, la salvaguarda jurídica frente a esta voracidad tecnológica se estructura en dos niveles. Por un lado, el artículo 18.1 CE, que tutela el derecho a la intimidad personal y familiar frente a intromisiones externas. Y por otro, a través del artículo 18.4 CE que otorga a la persona el poder activo de control, disposición y trazabilidad sobre sus datos personales (*habeas data*), con la intención de neutralizar los abusos de la informática, reafirmado en la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

El conflicto con las garantías constitucionales adquiere un cariz crítico ante la masificación y el abaratamiento tecnológico de los sistemas de identificación biométrica y

reconocimiento facial integrados en las infraestructuras de videovigilancia de los espacios públicos. Estas tecnologías de IA poseen la capacidad técnica de rastrear, perfilar, analizar emociones e identificar a millones de ciudadanos de forma masiva, indiscriminada y totalmente automatizada en tiempo real. Esto supone una intromisión letal en la expectativa de anonimato en el espacio público, generando un efecto disuasorio (*chilling effect*) que socava el libre desarrollo de la personalidad (artículo 10.1 CE), y el derecho de reunión y manifestación (Ridaura Martínez, 2024)

En respuesta a este desafío, el Reglamento de IA (AI Act) ha tipificado la identificación biométrica remota en tiempo real en espacios públicos con fines policiales como una práctica prohibida por constituir un riesgo inaceptable. La activación de estas tecnologías de vigilancia queda circunscrito a supuestos restringidos y condicionados a una autorización judicial previa y motivada. Su uso se admite exclusivamente como ultima ratio en escenarios de extrema gravedad, tales como la localización de víctimas de secuestro o la prevención de una amenaza terrorista inminente y contrastada.

3.2 PRINCIPIO DE IGUALDAD Y NO DISCRIMINACIÓN (ARTÍCULO 14 CE): EL SESGO ALGORÍTMICO, LOS PROXIES Y EL HITO DE LA LEY RIDER

Existe una falacia ampliamente extendida en el debate público que tiende a revestir a los sistemas algorítmicos y matemáticos de un aura de neutralidad, objetividad e infalibilidad técnica, asumiendo que el código informático está exento de los prejuicios humanos. Nada más alejado de la realidad, ya que los algoritmos son construcciones innegablemente sociotécnicas. Los modelos de IA no nacen en un vacío moral, sino que aprenden inductivamente a partir de bases de datos generadas por la sociedad.

En el supuesto de que estos inmensos repositorios de información oculten sesgos sistémicos, déficits de representatividad o dinámicas históricas de exclusión (ya sea por género, etnia, orientación sexual o estrato social), el sistema lejos de corregir estas taras sociales, el algoritmo absorberá esa visión sesgada del mundo para mecanizarla, dotarla de una falsa legitimidad científica y blindarla tras la impenetrabilidad del código. Con ello multiplicará exponencialmente esta discriminación al momento de dictar resoluciones o reconocer prerrogativas.

Este grave fenómeno, denominado sesgo algorítmico, atenta contra la misma esencia de la igualdad formal consagrada en el artículo 14 de la Constitución Española. Este precepto consagra el principio de igualdad ante la ley y la prohibición absoluta de toda discriminación por razón de nacimiento, raza, sexo, religión o cualquier otra condición personal o social. Simultáneamente, el sesgo algorítmico neutraliza y vacía de contenido el mandato material

contenido en el artículo 9.2 CE, que obliga positivamente a los poderes públicos a remover los obstáculos y promover las condiciones para que la igualdad del individuo sea real y efectiva.

El mayor desafío jurídico a la hora de evaluar la constitucionalidad material de un modelo de IA radica en la detección de la discriminación indirecta. En la inmensa mayoría de los casos de diseño de sistemas de *machine learning*, los programadores eliminan cautelarmente de las bases de datos aquellas variables protegidas de forma expresa por la ley (como el sexo o la etnia). Sin embargo, dada su formidable capacidad para encontrar correlaciones invisibles al ojo humano, el algoritmo de IA identifica patrones discriminatorios utilizando variables subrogadas, también conocidas en la literatura técnica como *proxy variables*. Estos datos, aparentemente insignificantes y neutrales desde una perspectiva legal, guardan en la realidad social una altísima correlación estadística y de probabilidad con la pertenencia a una minoría étnica o a un estrato de renta desfavorable (Palma Ortigosa, 2024). El resultado final es idéntico a una discriminación explícita, pero su detección y conflicto probatorio en un tribunal resulta extraordinariamente complejo.

A nivel nacional, la creciente asimilación institucional de los estragos que la gobernanza algorítmica puede causar sobre la igualdad material ha derivado en avances normativos y jurisprudenciales pioneros a escala global. En el terreno del Derecho Laboral, es imperativo destacar la reforma del Estatuto de los Trabajadores articulada mediante la Ley 12/2021, o Ley Rider. Su valor histórico trasciende la mera presunción de laboralidad en el entorno de las plataformas digitales, consagrando en el artículo 64.4.d) del ET un inédito y vanguardista derecho a la transparencia algorítmica en el seno de las relaciones laborales (Gómez Abeja, 2022).

Este precepto otorga a los representantes sindicales el derecho a ser informados por la empresa empleadora sobre los parámetros, las reglas lógicas y las instrucciones básicas en los que se fundamentan los algoritmos o sistemas de inteligencia artificial que afectan sustancialmente a la toma de decisiones empresariales. Esto abarca sistemas que inciden en las condiciones de trabajo, la organización de turnos, el acceso al empleo, las penalizaciones de rendimiento y, por supuesto, el despido (incluyendo la elaboración automatizada de perfiles o *profiling*).

Esta consagración del derecho a abrir la caja negra corporativa ha sido corroborada por la jurisprudencia social española y apuntalada por los tribunales comunitarios, especialmente tras la sentencia C-203/22 del TJUE sobre *scoring* (Dun & Bradstreet Austria), sentando las bases de un nuevo Derecho Laboral adaptado a la era digital (Barrio Andrés, 2025). Se eleva así el listón del control institucional sobre los algoritmos que organizan la vida laboral, limitando drásticamente el uso abusivo del secreto empresarial cuando este se

esgrime para encubrir prácticas directivas opacas, sesgadas o discriminatorias.

3.3 LIBERTAD DE EXPRESIÓN E INFORMACIÓN (ARTÍCULO 20 CE): LOS RETOS DE LA MODERACIÓN ALGORÍTMICA, EL SOBREBLOQUEO Y LA CENSURA PRIVATIZADA

El artículo 20 de la Constitución Española reconoce, protege y garantiza el derecho fundamental a expresar y difundir libremente pensamientos, ideas y opiniones mediante cualquier medio de reproducción. Para dotar a este derecho de una eficacia real frente a los abusos del poder, el apartado segundo del citado artículo impone como garantía inquebrantable e imperativa que el ejercicio de estos derechos no pueda restringirse mediante ningún tipo de censura previa.

No obstante, en el entramado de la sociedad digital contemporánea, los espacios públicos de reunión presencial física han sido reemplazados, en gran medida, por las infraestructuras de telecomunicación gestionadas por corporaciones privadas. Las grandes plataformas de redes sociales, repositorios de vídeos y sistemas de microblogging operan materialmente como la nueva plaza pública (*public square*) donde la ciudadanía ejerce diariamente su libertad de expresión y conforma el debate político.

Ante el volumen inabarcable e incesante de información que se carga en estas redes cada minuto, la supervisión humana directa se ha tornado materialmente inviable. Como única alternativa de viabilidad técnica y financiera, las plataformas han delegado casi la totalidad de las labores de censura previa, filtrado y bloqueo de perfiles a inteligencias artificiales, modelos de Procesamiento de Lenguaje Natural (PLN) y visión artificial. Sin embargo, tras su aparente complejidad técnica, estos algoritmos operan en base a correlaciones estadísticas entre patrones léxicos o visuales, careciendo de comprensión semántica profunda, matices socioculturales y discernimiento ético (García Sanz, 2025).

Como consecuencia directa, estas inteligencias artificiales se muestran manifiestamente incapaces de distinguir de manera fidedigna entre un discurso de odio ilícito, apología del terrorismo o pornografía infantil (que las plataformas están legalmente obligadas a erradicar) y manifestaciones discursivas plenamente lícitas y amparadas por el artículo 20 CE. La máquina no comprende el sarcasmo, la ironía fina, la crítica política mordaz, la denuncia periodística cruda o el debate académico legítimo sobre temas controvertidos.

El resultado directo de esta delegación es el fenómeno conocido como el sobrebloqueo (*overblocking*). Impulsadas por el temor a represalias económicas severas, las empresas configuran sus algoritmos con parámetros de tolerancia mínimos, derivando en la

eliminación automáticamente de contenidos perfectamente lícitos sin intervención humana previa (Olivé Busquets, 2020). Paralelamente, emergen mecanismos de censura subrepticia aún más lesivos, como el silenciamiento algorítmico o bloqueo en la sombra (*shadowbanning*), donde el contenido no se borra, pero se reduce drásticamente la visibilidad de un usuario sin notificarle, limitando su alcance y el contenido deja de aparecer en búsquedas o *hashtags*, usualmente por violar normas de comunidad o spam.

Esta dinámica configura un escenario como una forma de censura previa automatizada, ejecutada por plataformas a escala global y operando prácticamente al margen del control legal y jurídico. Como respuesta para neutralizar y acotar legalmente estos riesgos se aprobó a nivel europeo el Reglamento (UE) 2022/2065 de Servicios Digitales de la UE (*Digital Services Act*, DSA), vigente desde febrero de 2024, por el que se modificó la Directiva 2000/31/CE (Reglamento de Servicios Digitales). Este Reglamento ha introducido un corpus de obligaciones de transparencia específicas para los sistemas algorítmicos de recomendación y censura de contenidos, por el que exige a las plataformas de muy gran tamaño (VLOPs) la realización sistemática de evaluaciones de impacto sobre el debate público y los procesos electorales. Pero el verdadero hito garantista de esta disposición radica en la exigencia de dotar a los usuarios de canales eficaces y rápidos de revisión humana y queja ante las decisiones automatizadas de retirada de contenido o suspensión de cuentas, buscando restablecer la primacía de los derechos fundamentales en el entorno de las redes.

4 RETOS PARA EL ESTADO DE DERECHO: ADMINISTRACIÓN PÚBLICA Y JUSTICIA EN ESPAÑA

La progresiva y ambiciosa integración de sistemas de Inteligencia Artificial y plataformas predictivas en el seno de la Administración Pública, las Fuerzas de Seguridad y la Administración de Justicia transforma radicalmente el paradigma histórico de las relaciones entre el Estado y la ciudadanía. El uso de la tecnología genera una profunda asimetría informativa a favor de quien posee y controla los datos. Cuando el titular de esa opaca caja negra no es una corporación mercantil sometida a las leyes del mercado, sino el propio poder público, la opacidad algorítmica amenaza con dinamitar las bases mismas del Estado de Derecho, el control de legalidad de los actos administrativos (artículo 106.1 CE) y la interdicción de la arbitrariedad (artículo 9.3 CE).

4.1 LA ACTUACIÓN ADMINISTRATIVA AUTOMATIZADA: LOS LÍMITES DOGMÁTICOS Y LAS LECCIONES DEL CASO BOSCO

Lejos de ignorar la transformación tecnológica del sector público, el legislador ha procurado dotar de seguridad jurídica a esta transición, principalmente a través del artículo

41 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Este precepto regula y habilita la actuación administrativa automatizada, definiéndola como cualquier acto o resolución de trámite o definitiva realizada íntegramente a través de medios electrónicos en el marco de un procedimiento administrativo, sin que exista intervención o validación humana directa en el proceso de emisión.

Sin embargo, esta cobertura legal genérica no constituye, bajo ningún concepto, una patente de corso para el despliegue de una administración algorítmica sin límites. Resulta imprescindible trazar una frontera conceptual infranqueable entre el ejercicio de potestades estrictamente regladas y el de potestades discrecionales (Moreno García, 2025).

En el ámbito de las potestades regladas, la automatización algorítmica y el uso de sistemas informáticos no suscita mayor controversia. En estos escenarios, el algoritmo opera como un mero instrumento técnico, que coadyuva a la eficacia, eficiencia y celeridad que debe regir en la actuación administrativa según el artículo 103 de la Constitución.

En las antípodas se sitúa el ejercicio de las potestades discrecionales o la necesidad de valorar conceptos jurídicos indeterminados frente a un caso concreto. Son aquellos supuestos donde la ley otorga un margen de apreciación a la Administración para decidir lo más conveniente. En estos casos, delegar por completo la decisión final en un sistema de Inteligencia Artificial basado en modelos matemáticos y aprendizaje automático resulta problemático, ya que estos métodos carecen de la aptitud para ponderar valores éticos en colisión (Velasco Rico, 2024).

El conflicto real sobre los límites a la opacidad quedó reflejado en la Sentencia 1119/2025 de 11 de septiembre de la Sala Tercera de lo Contencioso-Administrativo del Tribunal Supremo sobre el acceso al código fuente de la aplicación informática estatal BOSCO marca un hito en materia de transparencia algorítmica, buena administración y control democrático de decisiones automatizadas de la administración pública que condicionan el acceso a derechos sociales.

Este *software* fue desarrollado y es utilizado en exclusiva por el Ministerio para la Transición Ecológica para verificar, cruzando de forma masiva datos tributarios y de padrón, si los solicitantes en situación de pobreza energética cumplían de forma objetiva con los requisitos legales para ser considerados consumidores vulnerables y obtener, en consecuencia, el bono social eléctrico que aplicaban las empresas comercializadoras. Ante quejas sobre errores de diseño en el programa que provocaban la denegación masiva e injustificada de ayudas a ciudadanos en extrema necesidad, la Fundación Civio solicitó amparo a la Ley de Transparencia para acceder al código fuente y poder auditar independientemente cómo la máquina cruzaba los datos. Tras el silencio administrativo y una resolución del Consejo de Transparencia y Buen Gobierno (CTBG), que solo permitió la entrega de documentación

técnica y rechazó la del código fuente de BOSCO, amparándose en la protección de los derechos de propiedad intelectual y apelando a informes que alegaban riesgos para la ciberseguridad nacional (Moreno García, 2025).

Tras un largo periplo judicial en el que el Juzgado Central de lo Contencioso-Administrativo n.º 8 (2021) y la Audiencia Nacional (2024) confirmaron la negativa a proporcionar el código fuente, apoyándose en varios límites de la Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno (LTAIBG), Civio recurrió en casación y el Tribunal Supremo estimó el recurso y reconoció el derecho de la Fundación a acceder al código fuente de la aplicación, fundamentándose en el principio de transparencia algorítmica, vinculado directamente al artículo 105.b de la Constitución y a la consolidación de una verdadera democracia digital (Pertíñez Vílchez, 2024).

El fallo del Tribunal Supremo determinó y fijó como doctrina que, en el marco de la actuación administrativa automatizada, donde la justificación jurídica, fáctica y el razonamiento de la decisión se encuentran íntimamente parametrizados y codificados en el diseño del *software*, el acceso al código fuente resulta ser un mecanismo indispensable y un derecho instrumental para que la sociedad civil pueda fiscalizar si el sistema informático aplica correctamente las previsiones legales vigentes que el legislador pretendía que se aplicaran. Esta sentencia consagra de manera indubitada que el Estado no puede alegar el régimen del secreto empresarial o la propiedad intelectual para levantar parcelas de inmunidad que eludan el control de legalidad de los actos que afectan a los derechos sociales de los ciudadanos más vulnerables.

Sin embargo, es necesario subrayar que el programa BOSCO, a diferencia de sistemas probabilísticos como el del caso *Schufa* ante el TJUE (Asunto C-634/21), no es propiamente un modelo de Inteligencia Artificial dotado de autonomía para extraer nuevos criterios de los datos. Su naturaleza jurídica se reduce a la de una calculadora procedimental, encargada exclusivamente de mecanizar la comprobación de variables y requisitos legales (renta y configuración familiar) fijados de antemano por la norma (López-Tarruella Martínez, 2024). En este caso, al tratarse de requisitos tasados, los solicitantes a los que se le denegó la ayuda pueden acreditar documentalmente su situación fáctica y comprobar que cumple los requisitos, demostrando el error del sistema y logrando la anulación del acto mediante recurso ordinario.

Pero el verdadero problema y el fallo estructural del sistema BOSCO no residía en la opacidad de la programación interna, sino en el incumplimiento del deber de motivación. El diseño institucional del procedimiento se concibió para que el sistema devolviera únicamente una respuesta binaria afirmativa o negativa a las empresas eléctricas comercializadoras, con el objetivo de salvaguardar la intimidad fiscal de los solicitantes. Esto provocó el desastre

jurídico de denegar miles de solicitudes carentes de argumentación, dejando al solicitante en la indefensión de no saber qué parámetro concreto (si la renta, el empadronamiento o el tipo de familia) fue el que provocó el rechazo.

4.2 TUTELA JUDICIAL EFECTIVA Y EL RIESGO DE INDEFENSIÓN ALGORÍTMICA: EL ESCRUTINIO DE LOS SISTEMAS VIOGÉN Y RISCANVI

El artículo 24 de la Constitución Española garantiza a todas las personas, sin excepción, el derecho fundamental a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, estableciendo en su redacción la proscripción absoluta y taxativa de que, en ningún caso, pueda producirse indefensión.

La introducción de sistemas predictivos de IA y perfilado algorítmico en el ámbito policial, penitenciario y judicial ha dado lugar a la aparición de un fenómeno que la doctrina jurídica califica como indefensión algorítmica. Esta patología procesal se materializa en la incapacidad fáctica, material y jurídica a la que se ve abocado un investigado para rebatir o articular una estrategia de defensa eficaz frente a un dictamen, una acusación o una predicción de peligrosidad que ha sido generada por un modelo estadístico y cuyo funcionamiento interno es inescrutable tanto para su defensa letrada como para el propio tribunal que asume el informe.

El impacto de estos sistemas predictivos sobre el núcleo de la tutela judicial es altamente sensible cuando se aplican en el contexto del Derecho Penal, penitenciario y de seguridad ciudadana en España. Dos paradigmas indiscutibles de este debate en el panorama nacional son los sistemas de apoyo RisCanvi y VioGén.

En primer lugar, cabe analizar el caso de RisCanvi, un algoritmo predictivo diseñado e implementado extensamente por la administración penitenciaria de la Generalitat de Cataluña. Su finalidad central radica en procesar decenas de factores sobre el interno para emitir predicciones estadísticas acerca del riesgo futuro de que el recluso cometa un acto de violencia dentro de centros penitenciarios, reincida en el delito violento tras su liberación o quebrante permisos (Molina Sánchez, 2025). Los resultados arrojados por esta herramienta operan como el eje que condiciona materialmente resoluciones vitales adoptadas por las Juntas de Tratamiento y los Juzgados de Vigilancia Penitenciaria, tales como la progresión al tercer grado, la concesión de permisos de salida y la libertad condicional.

Sin embargo, múltiples informes y estudios del Síndic de Greuges han lanzado alarmas sobre RisCanvi. Se denuncian graves carencias estructurales en materia de transparencia de cara a los afectados, vulnerándose sus derechos de acceso a los datos personales que nutren el sistema. Asimismo, los estudios señalan patologías de discriminación algorítmica,

evidenciando que el sistema penaliza sistemáticamente y sobreestima la peligrosidad real en colectivos en situación de extrema vulnerabilidad psicosocial (personas que padecen adicciones severas, diagnósticos de salud mental o que provienen de entornos de marginación económica profunda). En esta línea, la conversión de la gestión del riesgo puro en el fin último de la pena choca frontalmente con el mandato expreso del artículo 25.2 de la Constitución, que exige orientar ineludiblemente la ejecución penitenciaria hacia la reeducación y la reinserción social del condenado, y no hacia su inmovilización preventiva por un riesgo estadístico abstracto (Aleman Aróstegui, 2023).

Por otro lado, resulta ineludible examinar el sistema estatal de seguimiento integral VioGén (y su evolución hacia VioGén 2), coordinado por el Ministerio del Interior y utilizado por las Fuerzas y Cuerpos de Seguridad del Estado en todo el territorio nacional. Su función primordial es evaluar metódicamente el nivel de riesgo objetivo de revictimización en los casos denunciados de violencia de género, determinando el alcance y la contundencia de las medidas de protección policial que el Estado debe brindar imperativamente a las víctimas para proteger su integridad y su vida. La actualización normativa plasmada en la Instrucción 1/2025 de la Secretaría de Estado de Seguridad ha incorporado parámetros de valoración mucho más refinados, exigiendo un escrutinio adicional sobre la presencia de menores convivientes a cargo y una evaluación pormenorizada de las amenazas surgidas en el ecosistema digital y la ciberseguridad, así como pautando reevaluaciones más rigurosas de la evolución del riesgo.

Si bien VioGén es un instrumento irrenunciable para salvar vidas, la doctrina advierte de un peligro latente en la praxis de la tutela judicial debido al sesgo de automatización. Este fenómeno sociológico y psicológico describe la tendencia del agente policial evaluador, e incluso del juez de instrucción al adoptar órdenes de alejamiento, a acatar y homologar acríticamente la predicción matemática emitida por la pantalla del algoritmo, abdicando de su responsabilidad de valoración casuística (Martínez Garay *et al.*, 2025). El funcionario teme contradecir a un sistema amparado por el Estado por miedo a las consecuencias disciplinarias o penales si su juicio personal errara, lo que termina por petrificar la decisión. Ante esta realidad, es imperativo señalar que las diligencias formales de valoración emitidas por los agentes operando sobre VioGén poseen plena naturaleza de actos administrativos que influyen en los derechos de las partes y, como tales, son susceptibles de ser sometidos a control y recurso jurisdiccional ante los tribunales.

La verdadera amenaza de estas herramientas de apoyo es la automatización encubierta de las decisiones públicas. Escudándose en la gestión científica del riesgo, los funcionarios y magistrados pueden llegar a delegar el peso material de sus resoluciones en la estructura del software (García Ortiz; Molina Sánchez, 2023). Esto supone desvirtuar una herramienta

meramente consultiva para convertirla en la única instancia que, de manera inapelable, decide sobre el futuro de un individuo.

4.3 EL DEBER DE MOTIVACIÓN Y LA CONSAGRACIÓN DEL PRINCIPIO DE RESERVA DE HUMANIDAD

En el supuesto de que una Administración pública delegue la restricción de libertades o derechos sociales basándose de manera principal en el dictamen de un sistema algorítmico opaco convierte material y jurídicamente inviable cumplir con el deber de motivación exigido por nuestro ordenamiento. Si el diseño operativo del aprendizaje profundo (*deep learning*) impide descifrar una justificación lógica sobre cómo el algoritmo ha llegado a asignar un nivel de peligrosidad determinado a un ciudadano, cualquier resolución al amparo de dicha predicción carecerá de todo sustento argumentativo e incurrirá necesariamente en un vicio de nulidad de pleno derecho por ausencia de justificación material.

Ante este callejón sin salida procedimental provocado por la intrusión de la opacidad estadística se debe imponer la existencia de espacios de decisión que sean áreas exclusivas del ser humano, subrayando la existencia de la reserva de humanidad como principio irrenunciable en la protección innegociable de la dignidad humana. Los sistemas de IA carecen ontológicamente del sentimiento de empatía, imprescindible para comprender la situación y dictar una solución justa y equitativa (Cotino Hueso, 2024).

La decisión final que restringe derechos constitucionales en el seno de un procedimiento administrativo o judicial, especialmente en aquellos ámbitos que demandan el ejercicio de potestades discrecionales (donde se exige desplegar un juicio moral, ponderar valores constitucionales en colisión, valorar contextos excepcionales y aplicar compasión y empatía) no puede ser delegada a una máquina (García-Pérez Calabuig; Rodríguez Fernández; Galán Casado, 2025). La resolución final, la asunción de la firma y el peso ético de las consecuencias de la decisión deben recaer, de manera ineludible y mediante un análisis crítico, no meramente de firma formal (*rubber-stamping*), sobre una persona, sujeto a la exigencia de responsabilidad civil, penal, disciplinaria y patrimonial que impone nuestro ordenamiento.

5 LA APLICACIÓN NORMATIVA EUROPEA Y LA CONEXIÓN CON EL CONSTITUCIONALISMO ESPAÑOL

El reciente Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial o AI Act) se consolida como el vértice de la pirámide regulatoria sobre la materia, situando a

Europa en la vanguardia normativa. La virtualidad revolucionaria y disruptiva que aporta el AI Act reside en su decidido cambio de paradigma filosófico y regulatorio, abandonando el ineficaz y dilatado modelo tradicional de procedimiento judicial para imponer un sistema eminentemente preventivo, reflejado en su artículo 27 con la exigencia de llevar a cabo una exhaustiva evaluación de impacto en los derechos fundamentales (EIDF).

La EIDF impone a la Administración pública el deber de detallar exhaustivamente los procedimientos donde se incardinará la inteligencia artificial, acotando su vigencia, frecuencia de uso y delimitando con riguroso celo qué estratos ciudadanos y colectivos vulnerables quedarán sujetos a dicho escrutinio algorítmico (Pérez-Ugena, 2024). El núcleo de esta exigencia radica en forzar a la Administración a realizar un mapa de riesgos sobre posibles vulneraciones a la igualdad material, la privacidad o la libertad ideológica de la ciudadanía. Fundamentalmente, esta evaluación fuerza a las instituciones obligándoles a diseñar e integrar protocolos preventivos de mitigación, mecanismos de reclamación ágiles y a detallar documentalmente cómo se ejercerá la medida de supervisión humana real que evitará el abandono a las decisiones de la máquina, operando como un nuevo filtro o control previo de constitucionalidad técnica a gran escala.

5.1 EL DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS

Mientras que el vasto y complejo articulado del AI Act asume la misión de establecer los requisitos de seguridad técnica, gobernanza organizativa y el diseño del producto tecnológico que supone la IA en el mercado interior, el Reglamento General de Protección de Datos (RGPD) se erige sistemáticamente como el escudo normativo destinado a conferir el blindaje procesal y la protección directa e individualizada del titular de los datos (Covilla Martínez, 2025).

Dentro de este ecosistema garantista, el artículo 22 del RGPD se ha consolidado en la doctrina y jurisprudencia europea como la principal línea de defensa del ciudadano. Este precepto, concebido para evitar la cosificación absoluta del ser humano, consagra el derecho inalienable e incondicionado de todo individuo 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.

A este respecto, la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) a través de la sentencia C-203/22, de 27 de febrero de 2025, junto a su predecesora sobre el caso alemán Schufa C-634/21, dota a la interpretación del articulado del RGPD de un carácter marcadamente activista y expansivo en favor del garantismo del ciudadano frente a

las corporaciones gestoras de bases de datos masivas.

La Gran Sala del Tribunal de Justicia ha dictaminado con rotundidad que la simple elaboración automatizada de perfiles de conducta y la atribución de un índice de probabilidad predictiva a un individuo (patentes en los sistemas de *scoring* crediticio, los algoritmos para el cribado de currículos o las herramientas penales predictivas de niveles de riesgo de reincidencia) constituye en sí misma una decisión individual automatizada sujeta a la prohibición y al régimen de garantías del artículo 22 (Ponce Solé, 2024). Esta calificación aplica en todos los supuestos donde dicho valor probabilístico determine y condicione la resolución final de un tercero (ya sea una entidad financiera denegando crédito, una empresa descartando a un candidato o una Administración denegando una ayuda).

Esta interpretación impuesta por la justicia comunitaria acarrea consecuencias estructurales tanto al sector público como al privado al implementar de forma material el principio del humano en el bucle (*human in the loop*). Exige, además, que en aquellos casos donde la ley permita la toma de decisiones automatizadas de forma excepcional y restrictiva, deba estar siempre acompañada del derecho a recabar una intervención y revisión humana, así como el derecho a recibir, de acuerdo al artículo 15.1.h) del RGPD, la información significativa sobre la lógica algorítmica aplicada (Hernández San Juan, 2025).

5.2 LA CARTA DE DERECHOS DIGITALES DE ESPAÑA COMO INSTRUMENTO DE INTERPRETACIÓN

En el año 2021, España se situó a la vanguardia global en la articulación de políticas públicas sobre gobernanza tecnológica, gracias a la elaboración de la Carta de Derechos Digitales por parte del Ministerio de Asuntos Económicos y Transformación Digital. Fue aprobada por el Gobierno con el objetivo de establecer un conjunto de derechos que protejan los intereses y las libertades de los ciudadanos en el ámbito digital, garantizando su privacidad y seguridad en internet, así como su derecho a la neutralidad de la red y a una educación digital adecuada.

No obstante, su mayor trascendencia reside en el Apartado XXV, en el que se estructuran los Derechos frente a la Inteligencia Artificial. En este bloque se formulan prerrogativas contra el avance tecnológico, como el derecho a la no discriminación derivada de procesos y sesgos algorítmicos, el acceso a la transparencia y toma de decisiones del sistema, y la potestad de poder solicitar una revisión humana fundamentada (Tahiri Moreno, 2025).

Es necesario precisar que la Carta de Derechos Digitales pertenece al derecho blando (*soft law*), al carecer de fuerza de ley resulta inviable esgrimirla de manera autónoma ante la jurisdicción para invalidar decisiones automatizadas y algorítmicas. Sin embargo, su

transcendencia sociológica y política permite que su contenido sirva de guía fundamental a todas las instancias judiciales para interpretar y aplicar preceptos constitucionales como el libre desarrollo de la personalidad o el secreto de las comunicaciones frente a la realidad tecnológica actual.

5.3 EL DEBATE DEL CONSTITUCIONALISMO ESPAÑOL FRENTE A LA IA: ENTRE LA REFORMA Y LA MUTACIÓN CONSTITUCIONAL

En la esfera del Derecho Constitucional, el debate gira en torno a la necesidad de actualizar material o formalmente el texto constitucional frente al desafío de los algoritmos y la digitalización. Mientras una parte de la doctrina sugiere una reforma expresa para integrar los neuroderechos (Yuste Rojas, 2025) y nuevas garantías digitales, otra parte de la doctrina sostiene que la Constitución exime al legislador de embarcarse en un proceso complejo y de resultado incierto al cimentarse sobre principios vertebradores amplios.

Introducir y elevar a rango constitucional derechos excesivamente acotados, formulados sobre tecnologías en constante mutación, conlleva el riesgo fatal de que dichos preceptos nazcan obsoletos, sobrepasados por la vertiginosa velocidad de la innovación disruptiva. En consecuencia, la respuesta jurídica e institucional más garantista y perdurable radica en la figura de la mutación constitucional. Lejos de concebirse como una losa inmutable, la Constitución debe entenderse como un organismo en desarrollo (bajo el prisma de la *living tree doctrine*), cuya actualización debe canalizarse a través de la jurisprudencia interpretativas del Tribunal Constitucional complementada por la ineludible labor casacional y unificadora del Tribunal Supremo.

En base a esto último, el Tribunal Constitucional en la STC 292/2000 (y precedentes como la STC 254/1993) fue capaz de delimitar el potente derecho a la protección de los datos personales (el derecho al control del *habeas data*) infiriéndolo del vetusto mandato contenido en la redacción del artículo 18.4 de la CE, que se limitaba simplemente a enunciar el deber de la ley de limitar el uso de la informática. Es preciso ensanchar y redefinir el artículo 24, a partir del derecho a la tutela judicial efectiva, para que albergue el derecho a la explicabilidad algorítmica y la imposibilidad de padecer indefensión técnica ante el Estado. Paralelamente, es urgente dotar de nuevas dimensiones procesales, carga probatoria y fuerza expansiva al principio de igualdad y no discriminación contenido en el artículo 14, utilizándolo para prohibir toda forma de discriminación y marginación indirecta generada mediante el uso de variables y datos *proxies* en manos de los algoritmos corporativos o estatales.

La eficacia de la Constitución Española no radica en una positivación compulsiva de

todos los derechos digitales imaginables sino en mantener intacto el postulado del artículo 10.1 CE en cuanto a la dignidad humana y al respeto a los derechos inviolables que le son inherentes. La premisa del libre desarrollo de la personalidad en la esfera digital es la que debe erigirse en toda circunstancia y ante cualquier avance tecnológico, como límite infranqueable a la cosificación, la robotización, el perfilado invasivo y la automatización indolente de la sociedad y del propio Estado Constitucional.

6 CONCLUSIONES

El presente trabajo ha puesto de manifiesto que el vertiginoso desarrollo y la adopción masiva de la Inteligencia Artificial (IA) no constituyen una mera evolución técnica o una simple digitalización procedimental, sino un auténtico y disruptivo cambio de paradigma que desafía los cimientos mismos del Estado Constitucional y Democrático de Derecho.

La transición hacia lo que la doctrina científica ha denominado el Estado algorítmico encierra el riesgo inminente de subordinar las garantías constitucionales a los nuevos imperativos de la eficiencia digital, la optimización estadística y la indudable velocidad de procesamiento. En este nuevo y complejo ecosistema, el ordenamiento jurídico español se enfrenta al desafío de encauzar la disrupción tecnológica dentro de los cauces de la legalidad, garantizando que todo ejercicio de poder público o privado quede ineludiblemente subordinado al respeto incondicional a los derechos fundamentales y las libertades públicas consolidadas.

El núcleo central de esta constante fricción dogmática y procedimental reside en la opacidad técnica de los sistemas algorítmicos complejos, el conocido fenómeno técnico-jurídico de la caja negra (*black box*), inherente a los modernos sistemas de aprendizaje automático (*machine learning*) y aprendizaje profundo (*deep learning*). Como se ha analizado, esta opacidad algorítmica estructural genera una profunda asimetría informativa que colisiona frontalmente con el derecho a la tutela judicial efectiva, el derecho a la motivación de resoluciones administrativas y judiciales, y la transparencia de los poderes públicos, se ven seriamente amenazados en situaciones como el sistema BOSCO para el bono social o las herramientas predictivas VioGén y RisCanvi.

La protección del secreto empresarial y la propiedad intelectual corporativa, amparada en la libertad de empresa del artículo 38 CE, no puede erigirse como un escudo absoluto que consagre la indefensión algorítmica de los administrados. Por consiguiente, resulta absolutamente imperativo consolidar la transparencia algorítmica como un derecho de nueva generación, dotando a los afectados de las herramientas materiales para investigar, controlar y verificar las lógicas probabilísticas subyacentes.

Frente a este escenario, la respuesta se ha fundamentado en la prevención y gestión del riesgo, encontrando su plasmación jurídica en el Reglamento Europeo de Inteligencia Artificial (AI Act). En este específico contexto normativo, el Estado español ha asumido un liderazgo dentro de la Unión Europea mediante la creación de la Agencia Española de Supervisión de Inteligencia Artificial (AESIA). Su labor combina la potestad sancionadora con una clara vocación pedagógica a través de sus minuciosas guías técnicas, marcando el camino hacia una regulación verdaderamente anticipatoria y proactiva.

La implantación de obligaciones como el control humano mediante modelos *human-in-the-loop*, la vigilancia estricta de los datos para la mitigación preventiva de sesgos y la implementación de severos protocolos de ciberseguridad frente a manipulaciones, evidencian un esfuerzo institucional para conciliar la innovación con el cumplimiento normativo.

De igual forma, el impacto directo y transversal de la Inteligencia Artificial sobre los derechos fundamentales demanda una vigilancia extrema. Por una parte, la voracidad insaciable del Big Data y la proliferación de sistemas de identificación biométrica en espacios públicos amenazan severamente el derecho a la intimidad, la privacidad y la protección de datos personales, resultando vital la restricción y prohibición de estas prácticas para impedir un efecto disuasorio sobre el libre desarrollo de la personalidad.

Por otra parte, la utópica neutralidad matemática ha sido tajantemente desmentida por la persistencia del sesgo algorítmico y la utilización de variables subrogadas (*proxies*), que perpetúan, invisibilizan y automatizan dinámicas de exclusión que vulneran el principio de igualdad y no discriminación. En este ámbito, logros legislativos como la Ley Rider (Real Decreto-ley 12/2021) han demostrado la viabilidad de abrir la caja negra corporativa en el entorno laboral, limitando el abuso del secreto empresarial y cimentando un marco de transparencia vanguardista. Resulta igualmente apremiante atajar el *overblocking* provocado por la moderación automatizada en las plataformas digitales, que socava la libertad de expresión e información, delegando la censura previa a inteligencias artificiales carentes de discernimiento ético y sensibilidad social.

La inevitable convergencia entre la inteligencia artificial y la Constitución Española no precisa de un tortuoso proceso de reforma de esta última, sino que clama por una mutación constitucional abanderada por el Tribunal Constitucional y el Tribunal Supremo. La doctrina del *living tree doctrine* otorga a nuestra Norma Suprema la flexibilidad necesaria para guiar esta metamorfosis digital, condicionada siempre a una interpretación expansiva y garantista de los derechos.

La supervivencia de las garantías que definen al Estado Constitucional frente al envite de la tecnocracia reside en la consagración y salvaguarda del principio de reserva de humanidad en todas las instancias de decisión algorítmica. Ninguna motivación basada en la

eficiencia estadística ni en el secreto empresarial debe exonerar a las administraciones públicas ni a las grandes empresas tecnológicas de la obligación irrenunciable de asegurar que ámbitos críticos como el patrimonio, el empleo y la libertad de los ciudadanos permanezcan siempre bajo el control directo y supervisable de humanos.

Únicamente preservando esta línea roja infranqueable será posible abarcar los innegables y vastos beneficios que brinda el progreso tecnológico, evitando con ello que la ciudadanía quede expuesta, ante el avance de una automatización descontrolada, a una regresión inaceptable de las garantías democráticas y los derechos fundamentales que cimentan nuestro Estado de Derecho.

REFERENCIAS

ALEMÁN ARÓSTEGUI, L. El uso de RISCANVI en la toma de decisiones penitenciarias. **Estudios Penales y Criminológicos**, [s. l.], n. 44, p. 1-43, 2023.

BALAGUER CALLEJÓN, F. **La constitución del algoritmo**. El difícil encaje de la constitución analógica en el mundo digital. Zaragoza: Fundación Manuel Giménez Abad, 2022. p. 29-56.

BARRIO ANDRÉS, M. El derecho a la explicación de la toma de decisiones automatizada: Sentencia del Tribunal de Justicia 27 de febrero de 2025, as. C-203/22: Dun & Bradstreet Austria. **La Ley Unión Europea**, [s. l.], n. 137, 2025.

COTINO HUESO, L. La supervisión del cumplimiento del Reglamento de inteligencia artificial por las autoridades de vigilancia del mercado. **Revista Canaria de Administración Pública**, [s. l.], n. 4, p. 159-186, 2024.

COVILLA MARTÍNEZ, J. C. Inteligencia artificial y discrecionalidad administrativa: explorando adaptaciones y límites, **Revista española de derecho administrativo**, [s. l.], n. 242, 2025.

FORTES MARTÍN, F. La distribución de competencias e imputación de responsabilidades en la actuación administrativa automatizada. En: VAQUER CABALLERÍA, M. (dir.); PEDRAZA CÓRDOBA, J. (coord.). **La actuación administrativa automatizada: sus claves jurídicas**. [S. l.]: Tirant lo Blanch, 2025. p. 395-467.

GARCÍA SANZ, R. M. De la fragmentación, segmentación y descontextualización de la información al splinternet: un derecho a la información en mutación en la era de la inteligencia artificial. **Revista Española de Derecho Constitucional**, [s. l.], v. 135, p. 111-149, 2025.

GARCÍA ORTIZ, A. M.; MOLINA SÁNCHEZ, M. Inteligencia artificial y prevención de la violencia contra las mujeres: la responsabilidad del Estado ante el incumplimiento del deber de debida diligencia. **Estudios Penales Y Criminológicos**, [s. l.], n. 44, p. 1-35, 2023.

GARCÍA-PÉREZ CALABUIG, M.; RODRÍGUEZ FERNÁNDEZ, S.; GALÁN CASADO, D. Análisis de la influencia de la normativa europea en inteligencia artificial en el estigma virtual y la discriminación social. **La Ley Derecho de Familia**, [s. l.], n. 46, p. 71-81, 2025.

GÓMEZ ABEJA, L. Inteligencia artificial y derechos fundamentales. En: GARRIDO MARTÍN, J. *et al.* (dir.). **Inteligencia artificial y Filosofía del derecho**. [S. l.]: Laborum, 2022. p. 91-114.

GUTIÉRREZ GARCÍA, E. **Inteligencia artificial y derechos fundamentales**. Hacia una convivencia en la era digital. [S. l.]: Colex, 2024.

HERNÁNDEZ SAN JUAN, I. Efectos de la automatización sobre la organización administrativa: las organizaciones especializadas. En: VAQUER CABALLERÍA, Marcos (dir.); PEDRAZA CÓRDOBA, Juanita (coord.). **La Actuación Administrativa Automatizada: sus claves jurídicas**. Valencia: Tirant lo Blanch, 2025. p. 347-394.

HUERGO LORA, A. J. Inteligencia artificial y Administraciones públicas: para qué y cómo. **Teoría y Derecho: Revista de Pensamiento Jurídico**, [s. l.], n. 37, p. 40-69, 2024.

JOVE VILLARES, D. La gobernanza de la inteligencia artificial. análisis de las posibilidades autonómicas de supervisión. **Cuadernos Manuel Giménez Abad**, [s. l.], n. 29, 2025.

JOVE VILLARES, D.; PRESNO LINERA, M. Á. La salud en el entorno digital europeo. **Cuadernos Constitucionales**, [s. l.], n. 6, p. 83-107, 2025.

LANDA REZA, I. Entre la innovación y el Derecho: La adecuación de los deathbots al Reglamento de IA. **Revista de Derecho Civil**, [s. l.], v. 12, n. 3, p. 175-206, 2025.

LAZCOZ MORATINOS, G. La vigilancia o supervisión humana en el artículo 14 del Reglamento de inteligencia artificial: un mero requisito obligatorio para los sistemas de alto riesgo. En: COTINO HUESO, L.; SIMÓN CASTELLANOS, P. (dir.). **Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea**. Madrid: Aranzadi, 2024. p. 691.

LÓPEZ-TARRUELLA MARTÍNEZ, A. Derecho a presentar una reclamación y derecho a una explicación. Vías de recurso para los particulares en el reglamento de inteligencia artificial. En: COTINO HUESO, L.; SIMÓN CASTELLANO, P. (dir.). **Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea**. Madrid: Aranzadi, 2024. p.

893-918.

MARTÍNEZ GARAY, L.; BOIX PALOP, A.; BRIZ REDÓN, A.; FLORES GIMÉNEZ, F.; García Ortiz, A.; MOLINA SÁNCHEZ, M.; MONTES SUAY, F.; PALMA ORTIGOSA, A.; PERIS MANGUILLOT, A.; SORIANO ARNANZ, A. **Three predictive policing approaches in Spain: Viogén, RisCanvi and Veripol**. Valencia: Publicaciones Universidad de Valencia, 2025.

MARTÍNEZ GUTIÉRREZ, R. Responsabilidad administrativa por el uso de inteligencia artificial. En: GAMERO CASADO, E (dir.). **Inteligencia artificial y sector público: Retos, límites y medios**. [S. l.]: Tirant Lo Blanch, 2023. p. 227-253.

MIRANZO DÍAZ, J. **Inteligencia artificial y Derecho administrativo**. Especial referencia a los instrumentos de colaboración público-privada y contratación pública. Madrid: ICA-Tecnos, 2023.

MOLINA SÁNCHEZ, M. La diligencia que emite Viogén como acto administrativo: naturaleza jurídica y consecuencias prácticas. **Revista General de Derecho Administrativo**, [s. l.], n. 70, 2025.

MORENO GARCÍA, J. La transparencia de los algoritmos en la STS 1119/2025, de 11 de septiembre de 2025. El caso Bosco, un paso decisivo en la lucha contra la opacidad algorítmica. **Revista Vasca de Administración Pública**, [s. l.], v. 133, p. 317-351, 2025.

OLIVÉ BUSQUETS, P. **Overblocking en redes sociales y otras plataformas: riesgos y remedios para los usuarios proveedores de contenidos**. 2020. Working Paper (Derecho) - Universitat de Barcelona, Càtedra Jean Monnet de Dret Privat Europeu, Barcelona, 2020.

PACHECO JIMÉNEZ, M. N. Sistemas de inteligencia artificial para la toma automatizada de decisiones: algunos problemas de los contratos algorítmicos concluidos con asistente digital. **Cuadernos de Derecho Privado**, [s. l.], v. 4, n. 9, p. 140-171, 2024.

PALMA ORTIGOSA, A. ¿Quién es quién en el Reglamento Europeo de Inteligencia Artificial? Las autoridades notificantes y los organismos notificados. **Actualidad Jurídica Iberoamericana**, [s. l.], n. 21, p. 598-617, 2024.

PÉREZ-UGENA, M. Análisis comparado de los distintos enfoques regulatorios de la inteligencia artificial en la Unión Europea, EE. UU., China e Iberoamérica. **Anuario Iberoamericano de Justicia Constitucional**, [s. l.], v. 28, n. 1, p. 129-156, 2024.

PERTÍÑEZ VÍLCHEZ, F. La contratación entre sistemas de inteligencia artificial. En: ÁLVAREZ LATA, N. *et al.* (coord.). **Derecho de contratos, responsabilidad extracontractual e inteligencia artificial**. Madrid: Aranzadi, 2024. p. 101-122.

PONCE SOLÉ, J. Inteligencia Artificial, decisiones administrativas discrecionales totalmente automatizadas y alcance del control judicial. **Revista de Derecho Público: Teoría y Método**, [s. l.], v. 9, p. 171-220, 2024.

PRESNO LINERA, M. Á. El Reglamento europeo de inteligencia artificial: ¿garantía del mercado o defensa de los derechos? **Revista Española de Derecho Constitucional**, [s. l.], v. 135, p. 13-49, 2025.

RIDAURA MARTÍNEZ, M. J. El reconocimiento facial para preservar la seguridad: nuevo marco del Reglamento de Inteligencia Artificial de la Unión Europea. En: CAAMAÑO DOMÍNGUEZ, F.; JOVE VILLARES, D. (coord.). **Tecnologías abusivas y Derecho**. Valencia: Tirant lo Blanch, 2024.

TAHIRÍ MORENO, J. A. La actuación administrativa algorítmica. Una propuesta doctrinal desde la dogmática de la acción administrativa y la teoría general de los actos, **Revista de Derecho Público: teoría y método**, [s. l.], n. 1 12, p. 85-117, 2025.

VELASCO RICO, C. I. Implementación de sistemas algorítmicos en el sector público, preferencias ciudadanas y obligaciones de transparencia a la luz del Reglamento de IA de la Unión Europea. En: CERRILLO I MARTÍNEZ, A. *et al.* (dir.). **Inteligencia artificial y administraciones públicas: una triple visión en clave comparada**. [S. l.]: Iustel, 2024.

YUSTE ROJAS, R. **Neuroderechos: un viaje hacia la protección de lo que nos hace humanos**. [S. l.]: Ediciones Paidós, 2025. p. 245.

Como citar este documento:

MARTÍNEZ CRISTÓBAL, Daniel. El coste social de la eficiencia tecnológica: Inteligencia Artificial, discriminación invisible y la tutela de los derechos fundamentales. **Revista Opinião Jurídica**, Fortaleza, v. 24, n. 45, e6424, jan./dez. 2026. DOI: <https://doi:10.12662/2447-6641oj.v24i45.6424.pe6424.2026>. Disponível em: link do artigo. Acesso em: xxxx.