IMPACTO DEL ANTEPROYECTO DE LEY PARA EL BUEN USO Y LA GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL: CONEXIÓN CON EL REGLAMENTO (UE) 2024/1689 Y SU AFECTACIÓN A LOS ÓRGANOS DE CONTRATACIÓN PÚBLICA EN ESPAÑA

Impact of the draft bill on the proper use and governance of artificial intelligence: connection with regulation (EU) 2024/1689 and its effect on public procurement bodies in Spain

Marcos Sánchez Siles
Abogado

Resumen: El presente artículo analiza en profundidad el impacto jurídico-administrativo del Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia Artificial en España, en estrecha conexión con el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024. Tras una contextualización general del contenido de ambos instrumentos, se identifican las obligaciones transversales que imponen a todos los operadores jurídicos involucrados en el ciclo de vida de los sistemas de IA. Especial atención se dedica a las obligaciones específicas de los órganos de contratación y poderes adjudicadores, examinado los riesgos jurídicos que entraña la adopción de IA en la esfera pública, los desafíos operativos para su cumplimiento y las nuevas responsabilidades que asumen dichas entidades. Asimismo, se incorpora una perspectiva autonómica a partir del caso de Cataluña, abordando los retos normativos, institucionales y operativos que surgen en la implementación territorial de la gobernanza de la IA. Se concluye subrayando la necesidad de una adaptación proactiva de las Administraciones públicas al nuevo marco regulatorio, equilibrando la innovación con la garantía de los derechos fundamentales.

Abstract: This article provides an in-depth legal analysis of Spain's Draft Law for the Good Use and Governance of Artificial Intelligence, examining its impact on administrative law and its interplay with Regulation (EU) 2024/1689 of 13 June 2024. After a broad context overview of both the national draft law and the European AI Regulation, the general obligations imposed on all actors involved in the AI lifecycle are identified. Special focus is given to the specific obligations of public contracting authorities and awarding entities, including the legal risks of adopting AI in the public sector, operational challenges for compliance, and new responsibilities these entities must undertake. A regional perspective is added through the case of Catalonia, discussing normative, institutional, and operational challenges in the territorial implementation of AI governance. The conclusions highlight the need for proactive adaptation by public administrations to this new regulatory framework, balancing innovation with the protection of fundamental rights.

Palabras clave: Inteligencia Artificial; Contratación Pública; Gobernanza; Reglamento (UE) 2024/1689; Cataluña.

Keywords: Artificial Intelligence; Public Procurement; Governance; Regulation (EU) 2024/1689; Catalonia.

SUMARIO

I. **Introducción y contextualización general:** El auge regulatorio de la IA, del marco europeo a la respuesta española

II. **Marco normativo europeo y nacional:** El Reglamento (UE) 2024/1689 y el Anteproyecto de Ley: ámbito de aplicación, sujetos obligados y principios generales

III. **Obligaciones impuestas a los actores de la IA:** Deberes generales para proveedores, usuarios (despliegue), distribuidores y otros intervinientes en el ciclo de vida de la IA

IV. **Contratación pública y poderes adjudicadores:** Obligaciones específicas de los órganos de contratación y poderes adjudicadores: cumplimiento normativo, riesgos jurídicos, desafíos operativos y nuevas responsabilidades

V. **Perspectiva autonómica: el caso de Cataluña:** Retos normativos, institucionales y operativos en la implementación territorial de la gobernanza de la IA

VI. **Conclusiones**

VII. **Bibliografía**

I. Introducción y contextualización general

El exponencial desarrollo de la Inteligencia Artificial (IA) en la última década ha motivado una intensa actividad regulatoria tanto a nivel internacional, europeo como estatal, fundamentalmente dirigida a asegurar un uso ético, seguro y respetuoso con los derechos fundamentales de estas tecnologías.

Organismos como la OCDE ya en 2019 establecieron principios rectores –actualizados en 2024 para abarcar avances como la IA generativa– enfatizando la necesidad de que la IA respete los derechos humanos, la democracia y la responsabilidad en su desarrollo. En el ámbito europeo, tras publicarse las Directrices Éticas para una IA fiable (Grupo de Expertos de Alto Nivel en IA, 2019) y ante la ausencia de un marco vinculante, la Unión Europea dio un paso pionero al proponer un Reglamento de IA bajo un enfoque común de riesgo. Esta iniciativa cristalizó en el 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 (conocido coloquialmente como "Ley europea de IA").

Este se trata del primer marco jurídico exhaustivo sobre IA a nivel global, concebido para situar a Europa a la vanguardia de una IA "fiable". El Reglamento 2024/1689, de aplicación directa en todos los Estados miembros, sigue un enfoque basado en los niveles de riesgo que pueden entrañar los sistemas de IA, prohibiendo ciertos usos considerados inaceptables y estableciendo requisitos proporcionales para los sistemas de mayor.

España ha emprendido la adecuación de su ordenamiento interno a dicho marco comunitario, anticipando incluso algunas medidas. El Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial (en adelante, Anteproyecto de Ley de IA) –aprobado en Consejo de ministros el 11 de marzo de 2025– representa la respuesta normativa española para articular la aplicación efectiva del Reglamento europeo en nuestro país.

Este Anteproyecto consta de 37 artículos, distribuidos en cuatro capítulos (más disposiciones adicionales y finales), y persigue garantizar un uso ético, inclusivo y beneficioso de la IA, adaptando la legislación española al referido Reglamento (UE) ya en vigor. Como se expondrá, la Ley proyectada se centra especialmente en desarrollar aspectos que el Reglamento delega a los Estados miembros –como el régimen sancionador y la estructura de gobernanza nacional– y en establecer salvaguardas adicionales en ámbitos sensibles (por ejemplo, el uso de sistemas de identificación biométrica en espacios públicos).

En este contexto general, resulta esencial comprender la conexión entre el Anteproyecto español y el Reglamento europeo. El propio texto proyectado reconoce que su finalidad principal es desarrollar a nivel nacional las disposiciones del Reglamento de IA. Al ser el Reglamento un acto directamente aplicable y de alcance universal (cubre cualquier sistema de IA comercializado o utilizado en la UE, incluso si se desarrolló fuera) la norma española no duplica sus normas técnicas, sino que complementa y ejecuta aquellos aspectos que requieren actuación estatal. En particular, el Reglamento europeo obliga a los Estados a crear un régimen de sanciones efectivo y a designar autoridades nacionales de supervisión y aplicación. Asimismo, habilita a los Estados para autorizar excepciones en supuestos muy específicos (uso de sistemas de identificación biométrica en tiempo real para fines de seguridad, bajo ciertas condiciones). El Anteproyecto de Ley de IA da cumplimiento a esas obligaciones: establece un completo régimen jurídico sancionador para las infracciones del Reglamento en te-

rritorio español, organiza el sistema de gobernanza nacional designando autoridades competentes, y regula el procedimiento para autorizar los usos excepcionales de IA de alta sensibilidad.

La importancia de este Anteproyecto trasciende la mera transposición operativa del Derecho de la UE puesto que su aprobación convertiría a España en uno de los primeros países en contar con un marco integral nacional sobre IA, complementando el europeo con particularidades propias. Entre ellas destaca la incorporación de un "nuevo derecho digital" en favor de las personas: la posibilidad de solicitar la retirada provisional del mercado español de sistemas de IA que hayan provocado incidentes graves (p. ej. la autoridad competente podrá ordenar la desconexión inmediata de un sistema que haya causado la muerte de una persona). Este mecanismo, que refuerza la protección cautelar, encuentra sustento en el artículo 73.8 del Reglamento europeo y refleja la voluntad del legislador español de dotar de eficacia inmediata a la tutela de derechos frente a riesgos de la IA.

Igualmente, el Anteproyecto prevé un derecho de reclamación administrativa específico: a partir del 2 de agosto de 2026 cualquier persona física o jurídica podrá instar el inicio de un expediente sancionador por incumplimientos del Reglamento de IA. Para facilitarlo, se articulará un canal centralizado –gestionado por la Agencia Española de Supervisión de IA– que incluso admitirá informaciones anónimas como base para abrir.

Otro elemento para destacar es la anticipación institucional de España en materia de IA. Antes incluso de la aprobación definitiva del Reglamento (UE) 2024/1689, el Gobierno español impulsó la creación de la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA)[1], con sede en A Coruña, concebida como el organismo público encargado de supervisar el desarrollo y uso de la IA de forma ética y segura. La AESIA tiene la misión de liderar y coordinar la vigilancia del cumplimiento normativo tanto en el sector público como en el privado, protegiendo derechos fundamentales como la privacidad y la igualdad. Así mismo su establecimiento se enmarca en la Estrategia Nacional de IA y en la apuesta de España por avanzar en la implantación de entornos de prueba controlados (o *sandboxes*). Es más, el Reglamento europeo exige a cada país miembro que, máxime en 2026, ponga en marcha al menos un *sandbox* para proyectos de IA

España ya lanzó a finales de 2024 una convocatoria piloto seleccionando 12 sistemas de IA de alto riesgo para participar en un entorno de pruebas supervisado durante un con el objetivo de que las enseñanzas derivadas de ese piloto sirvan para elaborar guías técnicas de cumplimiento, experiencia que ilustra la voluntad de combinar la innovación responsable con la preparación temprana de todos los actores ante las exigencias legales venideras.

Con este ecosistema, la presente investigación se orienta a desentrañar las implicaciones concretas de este nuevo marco normativo, con especial foco en las Administraciones Públicas en su rol de órganos de contratación y poderes adjudicadores. Tradicionalmente, el Derecho Administrativo ha debido adaptarse a las transformaciones tecnológicas (piénsese en la administración electrónica, la protección de datos personales, etc.), asumiendo nuevos deberes y cambiando prácticas para asegurar que la innovación no menoscabara principios básicos como la legalidad, la transparencia o la igualdad. Pero la irrupción de la IA en la función pública –sea para optimizar servicios, agilizar trámites o apoyar la toma de decisiones– plantea desafíos inéditos: desde riesgos de opacidad y sesgos algorítmicos hasta cuestiones de responsabilidad por decisiones automatiza-

das. El Reglamento europeo y el Anteproyecto de Ley de IA imponen un conjunto de obligaciones específicas a los poderes públicos que adoptan estas tecnologías, ya sea como desarrolladores, usuarios o compradores de sistemas de IA. En especial, los órganos de contratación pública (Administraciones, entes, organismos y empresas sujetos a la legislación de contratos del sector público) se sitúan en una posición clave: actúan como garantes tanto de que los sistemas de IA que adquieren a terceros cumplan con la normativa, como de que su propio uso interno de herramientas inteligentes respeten los derechos de los ciudadanos; además de actuar como tractores de un mercado de IA fiable y responsable, incorporando criterios éticos y legales en sus procesos de contratación, alineándose con la noción de "compras públicas innovadoras responsables" promovida desde la UE.

II. Marco normativo europeo y estatal: reglamento (UE) 2024/1689 y anteproyecto de ley de IA

El Reglamento (UE) 2024/1689, en su artículo 2, define un amplio ámbito de aplicación material y subjetivo cubriendo prácticamente todo sistema de IA que se ponga en el mercado o se utilice en la Unión, con independencia de su lugar de desarrollo. Quedan excluidos, eso sí, ciertos usos específicos como los relacionados con la defensa, actividades fuera del mercado (p.ej. investigación sin lanzamiento comercial) u otros expresamente enumerados en el artículo 2.3-2.8 del. En lógica coherencia, el Anteproyecto de Ley de IA español, en su artículo 3, acota su aplicación a los mismos supuestos que el Reglamento, exceptuando aquellos excluidos por este.

Por el lado subjetivo, la Ley española se aplicará a todas las personas jurídicas privadas y entidades del sector público que actúen como "operadores" de sistemas de IA, tal y como los define el Reglamento. Ello incluye, concretamente a: los proveedores que desarrollen sistemas de IA (incluidos proveedores de modelos de IA de uso general); los potenciales proveedores que realicen pruebas en condiciones reales (es decir, quienes participen en *sandboxes* o entornos de experimentación antes de sacar un sistema al mercado); los responsables del despliegue, término con el que se alude a los usuarios que utilizan o implementan sistemas de IA bajo su autoridad (por ejemplo, una empresa o administración que integra una herramienta de IA en sus procesos); los fabricantes de productos que incorporen IA (cuando comercialicen el producto con su propio nombre o marca); los representantes autorizados en la UE de proveedores extracomunitarios; los importadores y distribuidores de sistemas de IA. De igual forma quedan comprendidos los organismos de evaluación de la conformidad (organismos notificados) que intervengan certificando sistemas de IA de alto riesgo. Esta enumeración, detallada y exhaustiva, muestra la clara voluntad del legislador de que prácticamente todo actor en la cadena de valor de un sistema de IA quede sometido a obligaciones normativas específicas.

Tanto el Reglamento europeo como el Anteproyecto asumen un modelo regulatorio gradual según el nivel de riesgo que presenta la aplicación de IA de que se trate, estableciendo cuatro niveles de riesgo: 1- riesgo mínimo o nulo, correspondiente a la mayoría de sistemas de IA cotidianos (ej. filtros de spam, algoritmos de recomendación sencillos, videojuegos con IA) los cuales no están sujetos a requisitos adicionales más allá de la legislación general; 2- riesgo limitado, para sistemas de IA que requieren solo obligaciones de transparencia (por ejemplo, informar a usuarios de que interactúan con una IA, o

etiquetar contenido sintético) pero sin necesidad de evaluación previa de conformidad; 3- alto riesgo, categoría central del Reglamento que abarca aquellos sistemas de IA que pueden suponer amenazas significativas para la seguridad, la salud o los derechos fundamentales de las personas; y 4-) riesgo inaceptable, reservado a usos de IA que se consideran contrarios a valores fundamentales o con impacto inadmisible, los cuales quedan prohibidos totalmente.

El Reglamento (UE) 2024/1689 identifica expresamente ocho prácticas de IA prohibidas por implicar riesgos inaceptables para las personas. Entre ellas se cuentan: el empleo de técnicas subliminales (estimulación por debajo del umbral de consciencia) para manipular el comportamiento de individuos de forma perjudicial; la explotación de vulnerabilidades de colectivos especialmente protegidos (como menores, personas con discapacidad o situación de vulnerabilidad) para influirles negativamente; los sistemas de "social scoring" o puntuación social generalizada por autoridades públicas (clasificando a ciudadanos en función de su conducta o características con consecuencias discriminatorias); la utilización de IA para evaluación predictiva de comportamientos ilícitos (profiling penal) de manera masiva; ciertos usos de reconocimiento emocional en ámbitos como el laboral o educativo; y, muy relevante, el uso de sistemas de identificación biométrica remota en tiempo real en espacios accesibles al público con fines de seguridad o aplicación de la ley, salvo excepciones.

El Anteproyecto de Ley proscribe estas mismas prácticas en el territorio español, remitiendo al artículo 5.1 del Reglamento). En particular, el texto proyectado reitera la prohibición general de sistemas de reconocimiento facial en vivo por fuerzas policiales en lugares públicos, estableciendo que solo podrán autorizarse en supuestos excepcionales, caso por caso, cuando sean estrictamente necesarios para finalidades muy concretas (búsqueda de víctimas de delitos, prevención de amenazas graves para la vida o la seguridad, o detección/identificación de delincuentes graves). Esta materia se regula con detalle en el Anteproyecto (arts. 10-11, capítulo III), previendo un procedimiento de autorización previa para dichas excepciones, que requerirá órgano competente y garantías específicas.

Por su parte, los sistemas de IA de alto riesgo quedan definidos en el Reglamento a través de dos vías: 1- por su finalidad o ámbito de uso, enumerándose en un anexo (Anexo III del Reglamento) diversos tipos de sistemas presumidos de alto riesgo; y 2-por ser componentes de seguridad de productos regulados por normativa de seguridad ya existente (ej. juguetes, maquinaria, dispositivos médicos, automóviles). Así, en la lista de alto riesgo figuran, entre otros: IA empleada en infraestructuras críticas (transporte, energía) que pueda poner en peligro la vida o salud; sistemas usados en el ámbito educativo o formativo que determinen el acceso a la educación o el trayecto profesional (p.ej. calificación de exámenes); sistemas de reclutamiento o gestión de personal (como software de cribado de CV); sistemas que decidan el acceso a servicios públicos esenciales o prestaciones sociales (vivienda, ayudas) o a servicios privados esenciales como créditos o seguros; ciertas aplicaciones en materia de orden público, control migratorio, asilo y gestión de fronteras; sistemas utilizados en la administración de justicia o procesos democráticos (p.ej. herramientas para preparar resoluciones judiciales). Todos estos sistemas no están prohibidos, pero solo pueden ponerse en el mercado o en servicio si cumplen estrictos requisitos y procedimientos de conformidad ex ante.

El Anteproyecto de Ley español refrenda estos criterios e incorpora algunas matizaciones: Añade la previsión de que la ausencia de

las debidas medidas de supervisión humana en un sistema de IA de alto riesgo puede constituir infracción grave sancionable; destaca la obligación de etiquetar de forma visible toda imagen, audio o vídeo generado o manipulado (deepfakes) por IA que pueda inducir a error sobre la realidad, tipificando como infracción grave el no hacerlo, implementando así una de las obligaciones de transparencia específicas introducidas por el Reglamento (UE).

Otro ámbito fundamental es el relativo a la gobernanza del sistema de supervisión y control. El Reglamento 2024/1689 crea un marco institucional multinivel: a nivel de la UE se establece la Oficina de IA (en la Comisión Europea) y el Comité Europeo de IA, encargado este último de asistir a la Comisión y coordinar la aplicación coherente del Reglamento en los Estados. En paralelo, cada Estado miembro debe designar una o varias autoridades nacionales de vigilancia del mercado para velar por el cumplimiento del Reglamento (art. 63 y ss. del Reglamento). El Anteproyecto dedica su Capítulo II (arts. 4 a 9) a esta gobernanza nacional y se designa formalmente como autoridad notificante principal a la Secretaría de Estado de Digitalización e IA, de la cual depende la AESIA, para interactuar con la Comisión en la notificación de los organismos de evaluación de conformidad. Asimismo, el art. 6 del Anteproyecto designa a las autoridades de vigilancia del mercado por sectores, siguiendo un modelo de "descentralización sectorial". En concreto, se nombran: la Agencia Española de Supervisión de IA (AESIA) como autoridad competente general y de coordinación; la Agencia Española de Protección de Datos (AEPD) para sistemas de IA en materias de migración y asilo asociados a Fuerzas y Cuerpos de Seguridad del Estado; el Consejo General del Poder Judicial (CGPJ) para sistemas de IA en la Administración de Justicia; la Junta Electoral Central para sistemas utilizados en procesos electorales; el Banco de España en lo referente a sistemas de IA de evaluación de solvencia crediticia; la Dirección General de Seguros para IA en seguros; y la Comisión Nacional del Mercado de Valores (CNMV) para IA en mercados de capitales. Esta lista corresponde en gran medida a las áreas de alto riesgo definidas en el Reglamento, asignando la supervisión al regulador sectorial ya existente (y aplicando el principio de *mismo supervisor para mismo ámbito*. En todos los casos no cubiertos por un regulador sectorial específico, la autoridad competente será la AESIA, que actuará así de autoridad horizontal de referencia. Además, el Anteproyecto prevé mecanismos de cooperación: la AESIA podrá asistir mediante convenios a las demás autoridades de vigilancia del mercado en el ejercicio de sus funciones, para asegurar una aplicación uniforme y aprovechar la especialización técnica de la agencia nacional de IA.

Finalmente, el núcleo del Anteproyecto español es el régimen de infracciones y sanciones (Capítulo IV, arts. 12 a 34). En cumpliendo del mandato del Reglamento (art. 71 y 83), se establecen infracciones administrativas muy graves, graves y leves, con multas proporcionales a la gravedad: las infracciones muy graves podrían sancionarse con multas de hasta 35 millones de euros (o porcentajes del volumen de negocio mundial, típicamente 6 % como prevé el Reglamento), las graves con hasta 15 millones (o 4 % del negocio), y las leves con hasta 5 millones (o 2 % del negocio.

El Anteproyecto indica que los límites superiores e inferiores de las sanciones administrativas en España serán muy similares a los fijados por el Reglamento General de Protección de Datos (GDPR), estableciendo así una analogía con ese régimen sancionador bien conocido. De hecho, se prevé incluso la posibilidad de optar por apercibimiento sin multa para PYMEs en caso de infracciones leves, obligándoles a cesar la conducta o corregirla,

sin sanción pecuniaria, como permite el art. 99.8 del Reglamento de IA. Asimismo, se habilita la adopción de medidas cautelares durante la tramitación de procedimientos sancionadores, pudiendo la autoridad ordenar la retirada temporal de un sistema de IA del mercado o su desconexión si su continuidad entraña un riesgo grave e inaceptable. Esta medida preventiva constituye un elemento innovador que garantiza la efectividad inmediata de la tutela ante infracciones serias.

III. Obligaciones impuestas a todos los actores en el ciclo de vida de la IA

Tal y como se indicaba, el nuevo régimen jurídico anteriormente expuesto impone un amplio catálogo de obligaciones a los diversos agentes que intervienen en el ciclo de vida de los sistemas de IA y estas varían según el rol (proveedor, usuario desarrollador, distribuidor, etc.) y el nivel de riesgo del sistema de IA de que se trate, pero en conjunto buscan garantizar un estándar elevado de seguridad, transparencia y respeto a los derechos fundamentales en toda la cadena, pudiéndose considerar:

1. Obligaciones de los proveedores de sistemas de IA: Los proveedores (desarrolladores que ponen sistemas de IA en el mercado bajo su nombre) asumen las cargas más exigentes, especialmente cuando se trata de sistemas de alto riesgo. Deben llevar a cabo un análisis de riesgos previo de su sistema y establecer un sistema de gestión de riesgos continuo durante todo el ciclo de vida del producto. Deben diseñar el sistema cumpliendo con principios de seguridad desde el diseño, incorporando medidas técnicas para mitigar riesgos y permitiendo la trazabilidad (por ejemplo, mediante registro de eventos o logs). Asimismo, corresponde al proveedor asegurar la calidad de los datos utilizados para entrenar el modelo (depuración de sesgos, representatividad adecuada) para minimizar resultados discriminatorios. También deben elaborar la documentación técnica completa del sistema, incluyendo descripción de su finalidad, funcionamiento, datos empleados, medidas de seguridad, etc., que será necesaria para evaluaciones de conformidad y para informar tanto a las autoridades como a los usuarios desarrolladores. En sistemas de alto riesgo, el proveedor debe someter el sistema a una evaluación de la conformidad antes de su puesta en mercado: en algunos casos podrá ser una autoevaluación interna, pero en muchos supuestos (p.ej., IA incorporada en productos con marcado CE) será necesaria la intervención de un organismo notificado externo que certifique el cumplimiento. Adicionalmente, el proveedor deberá garantizar la vigilancia postcomercialización, es decir, monitorizar el desempeño del sistema una vez desplegado, recoger feedback de usuarios, informar a autoridades de cualquier incidente grave o mal funcionamiento (notificación obligatoria de incidentes en plazo máximo, según art. 62 del Reglamento). En caso de detectar un sistema no conforme, tiene la obligación de tomar acciones correctivas, incluso retirar el producto del mercado si fuera preciso. Por último, el proveedor debe acompañar al sistema de IA de instrucciones de uso claras y de las informaciones obligatorias (por ejemplo, indicar nombre y datos de contacto, la marca CE de conformidad cuando proceda, la finalidad prevista del sistema, etc.). Cabe resaltar que, según el Anteproyecto español, no marcar el CE un sistema de IA de alto riesgo (o su embalaje/documentos) será infracción leve sancionable.

2. Obligaciones de los Usuarios o responsables del Despliegue: El usuario en terminología del Reglamento (denominado responsable del despliegue en el Anteproyecto) es la persona física o jurídica que, bajo su autori-

dad, utiliza un sistema de IA (normalmente, el cliente o entidad que emplea una IA adquirida). Sus obligaciones, aunque menos numerosas que las del proveedor, son cruciales para un uso responsable. Debe utilizar el sistema conforme a la finalidad prevista y a las instrucciones facilitadas por el proveedor, evitando usos para los que no esté diseñado y que puedan generar riesgos. En sistemas de alto riesgo, el usuario debe verificar que el sistema ostenta la declaración UE de conformidad y marcado CE, y no efectuar modificaciones que puedan alterar su funcionamiento (pues, de hacerlo, podría ser considerado "proveedor" de un nuevo sistema). Debe también monitorizar el funcionamiento de la IA durante su uso y, si detecta fallos graves o anomalías que supongan riesgos, tiene el deber de informar al proveedor o a las autoridades competentes. Cabe destacar que, en este sentido, el Reglamento exige que determinados usos de IA con impacto significativo vayan acompañados de medidas de supervisión humana apropiadas (art. 29), siendo responsabilidad del usuario implementar dicha supervisión en el contexto concreto de empleo del sistema. Por ejemplo, si un ayuntamiento utiliza un algoritmo para priorizar solicitudes ciudadanas, deberá asegurar que hay control humano que pueda intervenir en caso de decisiones anómalas. Igualmente, el usuario debe conservar registros o logs generados por el sistema si son proporcionados, para fines de trazabilidad. Y una obligación novedosa introducida en la versión final del Reglamento es que, tratándose de administraciones públicas o empresas que utilicen IA de alto riesgo, realicen una Evaluación de Impacto en Derechos Fundamentales (EIDF) antes de su puesta en uso, similar a las evaluaciones de impacto en protección de datos. Ello deriva del artículo 65 del Reglamento, que contempla que los usuarios del sector público evalúen cómo la IA puede afectar derechos como la no discriminación, igualdad y/o privacidad, e incorporen medidas de mitigación. Por ejemplo, si un Servicio Público de Empleo automatiza con IA la preselección de candidatos para cursos, debería analizar el riesgo de sesgo sexista o racista y establecer salvaguardas (supervisión humana, posibilidad de reclamación para rechazados. La falta de esta evaluación de impacto podría considerarse un incumplimiento sancionable. Cabe mencionar que en Cataluña la Autoridad de Protección de Datos (APDCat) ya ha desarrollado una metodología pionera para realizar este tipo de evaluaciones algorítmicas de impacto, ante la ausencia de directrices europeas uniformes, mediante matrices de riesgo que combinan probabilidad y gravedad del posible impacto, ilustrando así la necesidad de materializar en la práctica este nuevo deber para usuarios públicos de IA.

3. Obligaciones de Importadores y Distribuidores: Aquellas empresas que importen un sistema de IA (desde fuera de la UE) o lo distribuyan dentro de la cadena comercial también tienen obligaciones, orientadas a garantizar que solo se comercialicen sistemas conformes. El importador debe verificar que el proveedor extracomunitario ha cumplido sus deberes: que el sistema tiene marcado CE, declaración de conformidad, documentación en idioma requerido, entre otros. Si detecta incumplimientos, debe abstenerse de poner el sistema en el mercado. Además, debe indicar su propio nombre y dirección en el producto para trazabilidad. El distribuidor (comercializador) igualmente debe actuar con la debida diligencia, no pudiendo ofrecer sistemas que sepa (o debiera saber) que incumplen el Reglamento. En caso que tuviera sospechas fundadas de que un sistema no resultara conforme (por ejemplo, por alertas o retiros), debe informar al proveedor o importador y a la autoridad. Tanto importadores como distribuidores, cuando tengan un sistema bajo su responsabilidad, están obligados a conservar copia de la declaración de conformidad y a facilitar a las autoridades toda la información necesaria del producto.

Y, por supuesto, si consideran o descubren que un sistema que distribuyeron presenta un riesgo, deben informar y cooperar en posibles acciones correctivas (retirada, etc.). Estas obligaciones buscan extender la cadena de responsabilidad más allá del fabricante, similar a lo que ocurre en otros reglamentos de producto de la UE.

4. Obligaciones de los Organismos Notificados (evaluadores de conformidad): Aunque no son "operadores" en sentido estricto del mercado, los organismos de certificación acreditados que evalúen sistemas de IA de alto riesgo tienen también deberes bajo el Reglamento. Deben garantizar su independencia, competencia técnica y objetividad en las evaluaciones, evitar conflictos de interés, mantener confidencialidad de la información comercial, y en general cumplir los requisitos del Reglamento 2019/1020 de vigilancia de mercado. El Anteproyecto les extiende la aplicación del régimen sancionador en caso de incumplimientos graves en sus funciones. Esto resulta fundamental para asegurar la credibilidad del sistema de certificación, pues de estos organismos depende en buena medida que los sistemas de alto riesgo inseguros no accedan al mercado europeo.

5. Derechos de las personas afectadas: Si bien no son obligaciones, cabe recordar que el Reglamento consagra algunos derechos en favor de terceros. Por ejemplo, cualquier persona "afectada" por un sistema de IA (concepto amplio que podría incluir a ciudadanos sujetos a una decisión automatizada) tiene derecho a presentar reclamaciones ante las autoridades y a obtener información sobre el uso de IA. España, como vimos, articulará un canal de reclamación específico a través de AESIA. Asimismo, se potencia el derecho a ser informado cuando uno interactúa con una IA o es sujeto de decisiones automatizadas importantes. Este derecho ya estaba parcialmente reconocido en la normativa española: el artículo 13 de la Ley 40/2015, de Régimen Jurídico del Sector Público, y el artículo 46 de la Ley 39/2015, de Procedimiento Administrativo, tras su reforma por la Ley 11/2021, obligan a las Administraciones a informar a los ciudadanos de que se ha utilizado un algoritmo en la toma de una decisión que les afecte, y les permiten solicitar una explicación comprensible de dicha decisión. Esta previsión, pionera a nivel comparado, se alinea con el principio de transparencia algorítmica del Reglamento europeo, reforzando la accountability (rendición de cuentas) de las autoridades que usen IA. De hecho, la propia exposición de motivos del Anteproyecto destaca que España ya cuenta con estos antecedentes normativos que reconocen derechos de los ciudadanos frente a decisiones automatizadas públicas, lo cual facilita la adaptación al nuevo marco europeo.

En síntesis, el entramado de obligaciones anteriormente detallado cubre todo el ciclo de vida de un sistema de IA: desde su concepción y desarrollo (proveedores), pasando por la evaluación previa (organismos notificados), la introducción en el mercado (importadores/distribuidores) y finalmente su uso en entornos reales (usuarios desplegadores), sin olvidar la necesidad de mecanismos de vigilancia continua y respuesta a incidentes. Este modelo integral de corresponsabilidad es semejante al instaurado por la normativa de productos (ej. seguridad de productos, marcado CE) y por la protección de datos (que también impone responsabilidades compartidas entre responsables y encargados). Un efecto inmediato es que todas las organizaciones, públicas o privadas, involucradas en IA deben revisar y adaptar sus prácticas internas. En particular, las Administraciones públicas verán duplicar su rol: muchas de ellas serán usuarias de sistemas de IA (por ejemplo, en salud, educación, gestión administrativa) y simultáneamente, a través de sus unidades de contratación, actuarán como filtro de entrada de soluciones de IA

en el sector público. Y esto último merece un análisis específico en el siguiente apartado.

IV. Órganos de contratación pública y poderes adjudicadores: obligaciones específicas, riesgos y desafíos

Desde una perspectiva de contratación pública, los órganos de contratación y poderes adjudicadores (entendiendo por ellos la acepción referida a estos en la LCSP[2]) desempeñan un papel crucial en la gobernanza de la IA. Estas entidades pueden verse afectadas por la nueva regulación en una triple condición: como compradoras de tecnología IA, como usuarias operativas de sistemas IA, y como garantes de que la IA se integre de forma lícita y ética en la prestación de servicios públicos. A continuación, se abordan las obligaciones y retos específicos que afrontan, estructurados en varios ejes temáticos.

1. Deber de adaptar la contratación pública a las exigencias legales de IA: Una implicación inmediata del Anteproyecto es que la contratación de sistemas de IA por las Administraciones deberá alinearse con el Reglamento (UE) 2024/1689. Esto supone que, en cualquier licitación para adquirir soluciones basadas en IA (por ejemplo, un software de analítica predictiva, un sistema de reconocimiento de imágenes médicas, etc.), el órgano de contratación deberá exigir la conformidad legal del producto. En la práctica, los pliegos de prescripciones técnicas y cláusulas contractuales deberán incorporar requisitos como que el sistema propuesto cuente con marcado CE (si es de alto riesgo), que el licitador/proveedor aporte la declaración UE de conformidad y documentación técnica pertinente, y que detalle las medidas de gestión de riesgos, calidad de datos, supervisión humana, etc., en cumplimiento del Reglamento. En suma, no se debería contratar ni introducir en la Administración un sistema de IA que no haya demostrado su conformidad.

Ello conllevará, necesariamente, un cambio cultural en los departamentos de contratación del conjunto de poderes adjudicadores: así como hoy se exige a los contratistas cumplir con normativas de protección de datos, seguridad informática o accesibilidad, entre (muchos) otros, en adelante habrá que verificar el cumplimiento de la normativa de IA. Incluso podría plantearse condicionar la adjudicación a garantías adicionales éticas o de responsabilidad social por parte del oferente. La Memoria de Impacto Normativo del Anteproyecto sugiere la conveniencia de centralizar recursos y fomentar compras públicas de innovación responsables en materia de IA, lo que apunta a posibles directrices o acuerdos marco que ayuden a los órganos de contratación a evaluar la conformidad de sistemas complejos. Adicionalmente, tras la adjudicación, los contratos de suministro de sistemas de IA deberán incorporar cláusulas que obliguen al proveedor a mantener la conformidad y notificar incidentes durante la ejecución, facilitando a la Administración la información y formación necesaria para un uso seguro. Todo ello exigirá reforzar las capacidades técnicas y jurídicas del personal de contratación: será preciso contar con peritos o asesores en IA que puedan evaluar ofertas técnicamente, y con juristas que integren las obligaciones regulatorias en el clausulado contractual.

2. Obligaciones como usuarios de IA en la gestión pública: Una vez adquirido e implementado un sistema de IA, la Administración pasa a ser un usuario/deployr y, por tanto, le aplican las obligaciones de uso comentadas anteriormente a aquellos que adopten el citado rol. Sin embargo, en el contexto público cobran especial relevancia algunas de ellas: En primer lugar, el deber de realizar una Evaluación de Impacto en Derechos Fundamen-

tales (EIDF) antes de utilizar sistemas de IA de alto riesgo en la función administrativa puede considerarse un requisito de calado, puesto que implica desarrollar metodologías internas para analizar riesgos de la IA sobre, por ejemplo, la igualdad ante la ley, la no discriminación, la protección de datos personales (en conjunción con lo exigido por el RGPD), la tutela judicial efectiva, entre otros. Administraciones pioneras ya están trabajando en este sentido. Por ejemplo, la APDCat en Cataluña presentó en 2025 un sistema para "humanizar los algoritmos", proponiendo matrices de riesgo para cuantificar el impacto en derechos, ante la falta de directrices europeas unificadas. También el Ayuntamiento de Barcelona aprobó en 2021 un Protocolo para la implantación de sistemas algorítmicos que exige, para sistemas de alto riesgo, estudios de impacto algorítmico elaborados por un consejo asesor externo, antes de su puesta en marcha. Estas prácticas anticipan lo que será un estándar: ningún órgano público debería desplegar IA con efectos significativos sin un análisis previo de sus implicaciones y medidas de mitigación.

Conforme a la legislación española vigente, además, las AAPP tienen la obligación de informar a los ciudadanos cuando una decisión administrativa individual haya sido adoptada mediante medios automatizados (art. 41.1.f) de la Ley 40/2015, desarrollado por el art. 13 del RD 203/2021) y debiendo proporcionar, si el interesado lo solicita, una explicación comprensible de la lógica utilizada; conectándose con el derecho a la transparencia algorítmica. Por tanto, los órganos de contratación deberán prever en sus procedimientos cómo cumplir con este deber: por ejemplo, incluyendo en las notificaciones de resoluciones (como concesión o denegación de ayudas, o adjudicación de contratos menores decidida por un algoritmo) una indicación clara de la intervención de IA, y habilitando canales para que el ciudadano pueda pedir aclaraciones o una revisión humana de la decisión. Incumplir estas exigencias no solo vulneraría derechos de los ciudadanos, sino que podría considerarse infracción del Reglamento en la medida en que este prohíbe la toma de decisiones automatizadas sin adecuada supervisión humana en ámbitos sensibles. En esta línea, destacan iniciativas como la creación de registros de algoritmos utilizados en la gestión pública (lo que Barcelona ya contempla en su estrategia municipal para transparentar ante la ciudadanía qué sistemas de IA están en uso, con qué propósito y bajo qué garantías.

Otro deber específico para las AAPP usuarias es el de comunicar incidentes graves y cooperar con las autoridades de supervisión. Si, por ejemplo, un ministerio detecta que un sistema de IA empleado cometió un error que provocó un perjuicio importante (imaginemos, un algoritmo de reparto de recursos que dejó fuera indebidamente a colectivos vulnerables), tiene la carga de informar a AESIA u otra autoridad competente. Esto enlaza con posibles responsabilidades patrimoniales: si un ciudadano sufre un daño por funcionamiento anormal de un sistema de IA público, podría reclamar indemnización al amparo de la responsabilidad de la Administración. En tal caso, la Administración tendría que demostrar que actuó con la diligencia debida, escogiendo un sistema conforme y supervisándolo correctamente. La falta de esa diligencia (p.ej., no hacer la EIDF, no supervisar resultados) podría favorecer, sin duda, la posición del reclamante. Incluso, como indica la doctrina, aunque sancionar pecuniariamente a una Administración pública por infringir el Reglamento pudiera parecer contraintuitivo (sería el Estado sancionándose a sí mismo), nada impide que la autoridad de vigilancia –v.gr. AEPD o AESIA– declare la infracción y exija medidas correctivas obligatorias a la entidad infractora.

3. Riesgos jurídicos y responsabilidad en el uso de IA por poderes adjudicadores: Tal y

como se ha apuntado, los órganos de contratación encaran varios riesgos legales con la IA. Uno evidente (e importante) es el riesgo de impugnaciones y nulidad de decisiones. Si una adjudicación de contrato público o una concesión de subvención se basara en parte en la evaluación de una IA y esta tuviera sesgos o funcionara de forma opaca, los perjudicados podrían impugnar la decisión alegando vulneración de principios de igualdad, transparencia o motivación. Imaginemos un algoritmo que valore automáticamente ofertas en un concurso público: si un licitador no gana y sospecha que el algoritmo favoreció indebidamente a otros (quizá por un sesgo en los datos de entrenamiento), podría solicitar la revisión del proceso. Los tribunales exigirán que la Administración explique el funcionamiento del algoritmo y demuestre que no fue arbitrario. Esto conecta con precedentes internacionales: un tribunal neerlandés en 2020 anuló el sistema "SyRI" de detección de fraude social por considerarlo opaco y estigmatizante, violando el derecho a la vida privada y el principio de no discriminación[3]. En ese casó se determinó que incluso con fines legítimos (como puede ser combatir el fraude), si la IA pública es desproporcionada en sus impactos, es contraria a Derecho.

Otro riesgo es el de sanciones administrativas ya mencionado: la AESIA u otra autoridad podría incoar procedimiento sancionador contra un órgano de contratación que, por ejemplo, use un sistema de IA prohibido (imaginemos un Ayuntamiento implementando reconocimiento facial en sus cámaras urbanas sin autorización legal). Aunque la sanción pecuniaria en sí misma sería entre entes públicos (posible interés recíproco), el efecto reputacional y correctivo sería importante. El Anteproyecto habilita a que se dicte resolución declarativa de infracción incluso contra entes públicos, con medidas correctivas forzosas.

En cuanto a la responsabilidad patrimonial del Estado, conviene reiterar que la Administración actúa en este caso como usuaria y, a veces, como proveedora indirecta de un servicio potenciado por IA. Si una persona sufre un perjuicio antijurídico por un mal funcionamiento del sistema, la Administración responderá salvo que pruebe causas de exoneración. Por ejemplo, una víctima de un error diagnóstico cometido por una IA en un hospital público podría reclamar al servicio de salud público. La cuestión de si luego la Administración puede repercutir al proveedor privado del software (si hubo defecto) es otro nivel, pero de entrada el ciudadano verá a la Administración como responsable. Por ello, los contratos con proveedores privados de IA deben incluir cláusulas de indemnidad a favor de la Administración en caso de reclamaciones de terceros debidas a fallos del sistema, así como garantías y seguros adecuados por parte del contratista.

Para añadir algo más de leña al fuego, resulta evidente que para afrontar todo lo anterior los órganos de contratación deberán asumir nuevas responsabilidades organizativas. Sin ánimo de ser concluyente, entre ellas:

- Formación y capacitación del personal público: Resulta imprescindibles que los equipos jurídicos de las Administraciones comprendan conceptos técnicos de IA para poder regularlos adecuadamente; y los operadores técnicos necesitan formación jurídica básica para incorporar el "cumplimiento normativo" en el diseño y uso de IA. Equipos interdisciplinares (juristas, ingenieros, expertos en ética) deberán colaborar estrechamente. Cabe destacar que algunas Administraciones ya han creado órganos colegiados para ello: Por ejemplo, la Generalitat de Cataluña constituyó en 2024 la Comisión de Inteligencia Artificial, con altos cargos de todos los departamentos y expertos, cuya función es impulsar y supervisar la IA en servicios públicos, eva-

luar su impacto y velar por el cumplimiento normativo y ético, coordinando a los órganos. Esta Comisión está encargada de elaborar una estrategia de implantación de la IA en la Generalitat con principios de transparencia, equidad, seguridad y sostenibilidad.

- Elaboración de guías y protocolos internos: Al igual que Barcelona desarrolló su Protocolo de IA municipal integrando la IA en el ciclo de, cada organismo deberá dotarse de protocolos adaptados a su realidad. Estas guías deben basarse en el enfoque de riesgos: el protocolo de Barcelona aplica salvaguardas crecientes según si la IA es de riesgo limitado o alto, incluyendo asesoramiento externo para las de alto riesgo. También contempla la creación de un registro de algoritmos públicos accesible a la ciudadanía.
- Actualización de sistemas y auditorías periódicas: La IA no es estática; los modelos pueden degradarse con nuevos datos o contextos ("drift"). Las entidades usuarias tienen que establecer procedimientos de re-evaluación periódica de sus IA, en especial las de alto riesgo. Por ejemplo, si un ayuntamiento utiliza un algoritmo de asignación de becas, cada año debería auditar si los resultados presentaron sesgos inadvertidos, revisar si los datos de entrada siguen siendo válidos, y re-entrenar o ajustar el sistema si es necesario. Esta labor de monitorización continua es un desafío técnico y de recursos, pero es parte de las obligaciones de vigilancia activa.

En definitiva, las entidades del sector público en general (y los poderes adjudicadores, en concreto) se enfrentan a la necesidad de un cambio operativo significativo: integrar la gestión de riesgos de IA en su cultura organizativa. No se trata solo de cumplir formalmente la norma para evitar sanciones, sino de asumir una nueva responsabilidad institucional frente a la ciudadanía. La Administración debe mantener la confianza pública en la adopción de IA y eso implica demostrar que la IA se usa para mejorar servicios públicos sin socavar derechos, que siempre habrá un ser humano responsable y accesible detrás de una decisión automatizada, y que se promoverá la explicabilidad y corrección de errores. Como se ha señalado, la IA debe ser una herramienta para reducir la discrecionalidad arbitraria, no para aumentar la opacidad. Un uso adecuado podría incluso fortalecer la objetividad y coherencia de decisiones administrativas, pero un uso incontrolado podría degradar garantías.

V. Perspectiva autonómica: el caso de Cataluña

El despliegue de la gobernanza de IA en el nivel autonómico añade otra capa de complejidad al asunto de referencia, dada la distribución competencial en el Estado español y la autonomía organizativa de las Comunidades Autónomas (CC.AA.) en la gestión ordinaria de sus competencias. Cataluña ofrece un ejemplo ilustrativo de cómo una administración territorial está abordando los retos normativos, institucionales y operativos que conlleva la implementación del nuevo marco de IA.

1. Competencias normativas y reto institucional: Como se ha visto, la regulación de la inteligencia artificial en cuanto a estándares técnicos y derechos fundamentales es competencia del Estado (al amparo de las competencias en bases y coordinación de la planificación económica general, legislación mercantil, y muy especialmente, de la normativa básica en materia de telecomunicaciones y sociedad de la información, así como la protección de datos de carácter personal que se armoniza a escala europea). El Anteproyecto de Ley de IA tiene carácter básico en

gran parte de su articulado, al emanar de un Reglamento de la UE y referirse a garantías de derechos fundamentales (art. 149.1.1ª CE) y regulación de condiciones básicas de igualdad. No obstante, las CC.AA. intervienen en varios aspectos: son sujetos obligados cuando actúan como operadores de IA, y a la vez pueden desarrollar normativa propia en ámbitos de su competencia siempre que respeten el marco básico. Por ejemplo, Cataluña podría legislar directrices adicionales sobre uso ético de IA en su administración, o crear órganos complementarios, en ejercicio de su competencia de autoorganización (art. 150 EAC) y de mejora de la calidad de sus servicios públicos. Un desafío potencial es la coordinación entre la Agencia estatal (AESIA) y entes autonómicos con misiones afines. En protección de datos, Cataluña tiene su Autoritat catalana de Protecció de Dades (APDCat) para el sector público catalán; sin embargo, el Anteproyecto no la menciona, asignando a la AEPD ciertas funciones sobre IA que podrían implicar actuaciones en Cataluña (por ejemplo, IA en seguridad pública). Será necesario clarificar estos aspectos (para precisamente evitar posibles conflictos competenciales entre AESIA y APDCat) así como duplicidades o lagunas de supervisión.

Otro aspecto es la capacidad institucional: Cataluña ha actuado de una manera proactiva creando órganos dedicados a la estrategia digital. En 2020 publicó su Estrategia de Inteligencia Artificial de Cataluña (Catalonia. AI), reconociendo la responsabilidad de los gobiernos de fomentar la IA extensamente pero siempre priorizando la ética, la seguridad, la sostenibilidad y la no discriminación. Sobre esa base, en 2022 constituyó el Observatorio de Ética en Inteligencia Artificial de Cataluña (impulsado con la colaboración de la Generalitat y Universidades) y en 2024, como ya se ha indicado, la Comisión de la Inteligencia Artificial dentro del Govern. Sus funciones incluyen, entre otras, definir actuaciones para impulsar y supervisar la IA en servicios públicos, evaluar el impacto de la IA en la Administración, velar por el cumplimiento de la normativa y las buenas prácticas éticas, y coordinar los órganos responsables. En la práctica, esto la convierte en una especie de "miniautoridad" interna de IA en la Generalitat.

2. Implementación operativa en la Administración de la Generalitat: Cataluña, al igual que otras comunidades, enfrenta retos prácticos similares a los del Estado, pero con algunas particularidades. Debe adaptar sus procedimientos administrativos sectoriales a las normas de IA. Por ejemplo, los Mossos d'Esquadra tendrán prohibido usar reconocimiento facial en tiempo real salvo orden judicial en supuestos de terrorismo o desapariciones; para hacerlo, Cataluña necesitaría base legal autonómica o aplicación directa de la estatal. En educación, si se emplean sistemas inteligentes para evaluaciones, la Generalitat deberá realizar EIDF y asegurar supervisión docente. Además, Cataluña es pionera en usar IA para mejorar la regulación y la simplificación normativa (proyecto *NormaLIS* con IA para resumir leyes en lenguaje claro, o en pruebas piloto como sentencias judiciales redactadas con ayuda de IA en su ámbito competencial.

El reto operativo principal es la falta de recursos especializados. Implementar todo lo anterior exige inversión en tecnología, talento y cambio cultural. Cataluña, con su estrategia AI, ha invertido en hubs de investigación y programas de capacitación, pero la administración pública en sentido estricto requiere formación específica. A tal fin, se podrían aprovechar sinergias: la Escuela de Administración Pública de Cataluña puede introducir módulos de IA para funcionarios; la APDCat ha lanzado guías sobre decisiones automatizadas y podría crearse una red interdepartamental de responsables de IA en cada Consejería, que intercambien buenas prácticas.

3. Coordinación multinivel y posibles tensiones competenciales: Si bien hasta ahora las acciones del Govern de la Generalitat se han llevado a cabo en consonancia con el marco jurídico europeo y estatal, podría haber espacios para normativa propia. Por ejemplo, Cataluña podría dictar una ley autonómica de algoritmos en la Administración catalana, desarrollando las obligaciones de transparencia del art. 13 Ley 40/2015 e incluso yendo más allá (por ejemplo, creando un registro público de algoritmos autonómico obligatorio por ley, algo que de momento Barcelona ha hecho a nivel local voluntario). Mientras no contravenga ni rebaje las exigencias estatales, esa normativa sería posible al amparo de la competencia de organización y procedimientos administrativos propios (dentro de la legislación básica estatal). Otra posible tensión es la atribución de sanción a entes locales o autonómicos: si la AESIA detecta infracción en un ayuntamiento catalán, ¿podría Cataluña argumentar que la tutela del administrado frente a esa entidad debería corresponder a un órgano catalán? Dado que es ejecución de legislación básica europea, probablemente no: prevalece el esquema centralizado. Pero en la práctica, la AESIA probablemente actuará de forma coordinada, notificando a la Generalitat para que internamente corrija.

VI. Conclusiones

La irrupción de un marco jurídico específico para la inteligencia artificial, compuesto por el Reglamento (UE) 2024/1689 y su desarrollo a través de la futura Ley española de Buen Uso y Gobernanza de la IA, marca un hito en el Derecho Administrativo contemporáneo equiparable a la entrada en vigor del RGPD en materia de datos personales. Su impacto en el sector público, en particular en los órganos de contratación y poderes adjudicadores, será profundo y multidimensional:

En primer lugar, se establece con claridad que ningún actor –público ni privado– queda al margen de las obligaciones cuando interviene en el ciclo de vida de los sistemas de IA. Todos los participantes tienen deberes proporcionados a su papel, desde el desarrollador que debe incorporar la ética del diseño (*ethics by design*) y la gestión de riesgos, hasta la Administración usuaria que debe garantizar la supervisión humana y la transparencia ante el ciudadano. Esta red de obligaciones compartidas refuerza la responsabilidad integral en la adopción de IA, fomentando una cultura de cumplimiento similar a la consolidada en materia de protección de datos: la IA deja de ser un terreno exento para pasar a estar fuertemente regulada bajo principios de precaución y centrado en la defensa de los derechos fundamentales.

En segundo lugar, los órganos de contratación se erigen en una pieza clave de la gobernanza de IA. Por un lado, la contratación pública actúa como puerta de entrada: las Administraciones solo deberían adquirir soluciones de IA que cumplan los estándares europeos, convirtiendo sus pliegos en un instrumento para elevar la exigencia de mercado (las empresas deberán llegar con sus "deberes hechos" de conformidad normativa si quieren contratar con el sector público). Por otro lado, esas mismas Administraciones, al utilizar IA para prestar servicios o tomar decisiones, se encuentran bajo el escrutinio de legalidad y posibles responsabilidades. La IA no les exime de sus principios medulares (legalidad, igualdad, objetividad, motivación), al contrario, las obliga a redoblar esfuerzos de control interno. La experiencia internacional demuestra que la sociedad y los tribunales no tolerarán "cajas negras" que decidan sobre derechos sin posibilidad de explicación o corrección. España, con sus reformas legales pioneras en 2021, ya sentó bases importantes al consagrar el

derecho a conocer y revisar los algoritmos administrativos, y ahora con este Anteproyecto añade la capacidad sancionadora para casos de incumplimiento. Así, se completa un marco de accountability pública en el uso de IA: las Administraciones responderán ante los ciudadanos, ante las autoridades de supervisión y ante los jueces por la forma en que integren la IA en sus funciones.

En tercer lugar, se observa que el desafío principal será operativo. El cumplimiento efectivo de estas obligaciones requerirá invertir en formación de empleados públicos, actualización de procesos de contratación y auditoría, y adopción de metodologías nuevas (evaluaciones de impacto algorítmico, registros de algoritmos, entre otros). Organizaciones grandes quizás puedan dotarse de unidades especializadas o contratar asesoramiento externo, mientras que las más pequeñas probablemente necesitarán guías y apoyo centralizado (rol que AESIA podría desempeñar emitiendo guías prácticas y ofreciendo asistencia técnica a entes locales). Sería conveniente elaborar herramientas comunes, por ejemplo, plantillas de evaluación de impacto que puedan reutilizarse, o incluso considerar soluciones cooperativas interadministrativas (como consorcios para auditar algoritmos compartidos, por ejemplo). Todo ello, sin perder de vista que la IA evoluciona rápidamente: la normativa tiene vocación flexible, pero las Administraciones deberán mantener una actitud de mejora continua y actualización de sus controles a medida que surjan nuevas tecnologías.

En cuarto lugar, la perspectiva autonómica añade complejidad, pero también oportunidades de innovación. Cataluña muestra que, respetando el marco común, se pueden impulsar iniciativas locales valiosas que luego sirvan de referencia a nivel nacional (como el protocolo de Barcelona o la metodología de APDCat). La clave estará en articular sinergias: que las comunidades autónomas y el Estado compartan experiencias, quizá en el seno del futuro Comité Europeo de IA donde habrá representantes de cada Estado (y, por ejemplo, España podría llevar aportaciones de sus regiones). Es previsible que se genere jurisprudencia y doctrina administrativa en distintos territorios, lo que enriquecerá la comprensión del Derecho de IA. Habrá que velar, no obstante, por la coherencia: al ser un Reglamento de aplicación directa, no debería haber discrepancias notables en su ejecución entre comunidades, so pena de fragmentar el mercado interior, algo que precisamente esta regulación busca evitar.

En conclusión, estamos ante un cambio de paradigma en la actuación de los poderes públicos: la introducción de la IA bajo condiciones de gobernanza estricta. Lejos de promover una inhibición en el uso de estas tecnologías (nadie propone renunciar a sus beneficios), el marco legal persigue un equilibrio: incentivar la innovación y la digitalización de lo público, pero "domando" la IA para que sirva al interés general sin poner en jaque los valores democráticos ni los derechos de los ciudadanos. La IA debe ser un medio para mejorar la eficiencia y la calidad de las políticas públicas, pero nunca un fin en sí misma ni un pretexto para recortar garantías. La última palabra en decisiones que afecten a personas la seguirá teniendo un humano responsable, y las Administraciones deberán estar preparadas para dar la cara y explicar "qué hizo su algoritmo y por qué". Como principio rector, la transparencia emerge una vez más como la mejor aliada: no solo la transparencia hacia las autoridades supervisoras, sino sobre todo hacia la ciudadanía, fomentando la confianza. Esto requerirá incluso un esfuerzo pedagógico para que los ciudadanos entiendan cómo y por qué se usa IA en el sector público, qué ventajas tiene y qué controles existen para evitar abusos.

En definitiva, el Anteproyecto de Ley para el Buen Uso y la Gobernanza de la IA, junto con

el Reglamento europeo, dibujan un horizonte en que la Administración Digital Inteligente deberá ser sinónimo de Administración Íntegra y Abierta. España tiene la oportunidad de situarse a la vanguardia de la implementación de una IA confiable en el sector público. El éxito dependerá de la efectiva colaboración entre legisladores, administraciones (en todos sus niveles), sector privado y sociedad civil para materializar los principios en prácticas concretas. Si se logra, la IA podrá desplegar todo su potencial transformador, incrementando la capacidad de nuestras instituciones para servir al ciudadano de manera más eficiente y personalizada, sin renunciar al Estado de Derecho ni a los valores que nos definen como sociedad.

VII. Bibliografía

Documentos normativos y fuentes oficiales

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. (Pendiente de publicación DOUE; texto provisional aprobado por Consejo y PE).

Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial (España, 2025). Texto aprobado en Consejo de ministros de 11 de marzo de 2025.

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (modificada por Ley 11/2021, de 9 de julio, en materia de administración digital).

Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común (modificada por Ley 11/2021 en materia de actuación automatizada).

Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos (artículos 13 y 14 sobre actuación automatizada).

Comunicación ministro de Transformación Digital (Gobierno de España) de 11 de marzo de 2025: *El Gobierno da luz verde al anteproyecto de ley para un uso ético, inclusivo y beneficioso de la Inteligencia Artificial*

Nota de prensa AESIA (Agencia Española de Supervisión de IA): *Garantizando una IA ética y responsable*. AESIA, 2023.

Doctrina y comentarios especializados

Silvia Pascua Vicente: *España: El Gobierno aprueba el anteproyecto de ley para el buen uso y la gobernanza de la inteligencia artificial*. Instituto Autor, Actualidad, 20 Mar 2025.

Pedro Padilla Ruiz: *Informe jurídico sobre el Anteproyecto de Ley para el Buen Uso y la Gobernanza de la IA en España* (realizado con IA). Blog pedropadillaruiz.es, 2025.

Guillem Alsina Gonzàlez: *Estas son las claves del Anteproyecto de Ley de Buen Uso y Gobernanza de la IA*. Digital Inside, 24 Mar 2025.

José Luis Piñar Mañas (Dir.): *Administraciones Públicas e inteligencia artificial: ¿más o menos discrecionalidad?*. La Administración al Día (INAP), 2023

Xavier Ribas: *Reglamento de IA de la UE – Obligaciones de transparencia de proveedores y usuarios*.

Observatorio de Ética en IA de Cataluña: *Manifiesto para avanzar en una IA fiable*, Generalitat de Catalunya, 2023.

Informes y otros:

OCDE: *Principios de IA* (2019, actualizados 2024)

High-Level Expert Group on AI (EU): *Ethics Guidelines for Trustworthy AI* (2019).

APDCat: Presentación herramienta *Algoritmos seguros y libres de sesgo*, Parlament de Catalunya, 28/1/2025

Ajuntament de Barcelona: *Protocolo para la implementación de sistemas algorítmicos en el ámbito municipal* (2021)

Generalitat de Catalunya: *Constitución de la Comisión de la Inteligencia Artificial*. Nota de prensa Consorci AOC, 30 abril 2024.

El País (Cataluña): *Cataluña busca humanizar la inteligencia artificial*, 29 Ene 2025.

[1] La AESIA se crea por la disposición adicional séptima de la Ley 28/2022, de 21de diciembre, de fomento del ecosistema de las empresas emergentes, conforme a la exigencia prevista en el artículo 91, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. El estatuto de la AESIA fue aprobado por Real Decreto 729/2023, de 22 de agosto.

[2] Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

[3] Vid. Sentencia SyRI – System Risk Indication, del Tribunal del Distrito de la Haya de 5 de febrero de 2020, Caso C/09/550982.