05/06/2026

# España da el paso: el Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia Artificial y lo que de verdad cambia para las empresas

**por Iván Martínez, CEO de Intedya**

Mientras buena parte del debate público sobre inteligencia artificial sigue oscilando entre el entusiasmo tecnológico y el alarmismo distópico, los

Estados miembros de la Unión Europea están haciendo lo que les corresponde: aterrizar el Reglamento (UE) 2024/1689, el llamado AI Act, a sus

ordenamientos jurídicos nacionales. España ha movido ficha con el **Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia**

**Artificial**, impulsado por el Ministerio para la Transformación Digital y de la Función Pública a través de la Secretaría de Estado de Digitalización e

Inteligencia Artificial. No es una ley menor. Tampoco es, pese a lo que algunos titulares sugieren, una "ley de IA española" que duplique el

en territorio español. Y trae novedades propias que conviene leer con calma.  Voy a tratar de ordenar lo que de verdad  importa, especialmente para

empresas, responsables de compliance, DPO y direcciones que están (o deberían estar) preparando su transición.

## Lo que la Ley es (y lo que no es)

El AI Act es un reglamento europeo de aplicación directa. Eso significa que ya obliga, sin necesidad de transposición. Pero el propio

Reglamento delega en los Estados miembros tres cuestiones críticas: el régimen sancionador, la designación de autoridades nacionales

competentes y el procedimiento administrativo para hacerlo efectivo. El Anteproyecto español hace exactamente eso, y añade algunos

elementos propios.

En términos prácticos, el texto:

-

Define el**régimen sancionador aplicable en España** por incumplimientos del Reglamento europeo.

- Regula el**régimen jurídico de autorización** para el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines policiales, uno de los puntos más sensibles del AI Act.

**Designa las autoridades de vigilancia del mercado** por sectores, con un modelo descentralizado que ya anticipa fricciones de coordinación.

- Crea el marco de gobernanza nacional, con la**Agencia Española de Supervisión de Inteligencia Artificial (AESIA)** como pieza central.

-

Introduce un nuevo derecho digital: el**derecho de desconexión o retirada** de sistemas de IA que hayan provocado incidentes graves.

No es, por tanto, una ley sobre qué se puede o no se puede hacer con IA (eso lo dice el Reglamento). Es la ley que dice**quién vigila, cómo sanciona y cuánto cuesta incumplir** en España.

## El régimen sancionador: cifras que no se pueden ignorar

Aquí está, sin ambages, la parte que va a captar la atención de los consejos de administración. El Anteproyecto clasifica las infracciones en tres niveles (muy graves, graves y leves) y establece horquillas sancionadoras que se alinean con el techo que marca el Reglamento europeo:

- **Infracciones muy graves por prácticas de IA prohibidas:** de 7.500.001 € a**35.000.000 €** o, si el infractor es una sociedad o grupo,**del 2% al 7% del volumen de negocios mundial** del ejercicio anterior, si esta cifra fuese mayor.
-

- **Infracciones muy graves en sistemas de alto riesgo:** de 7.500.001 € a 15.000.000 €, o del 2% al 3% del volumen de negocios mundial.
- **Infracciones graves:** de 500.001 € a 7.500.000 €, o del 1% al 2% del volumen de negocios mundial.
- **Infracciones leves:** de 6.000 € a 500.000 €, o del 0,5% al 1% del volumen de negocios mundial.

Una nota crítica para los grupos empresariales: el Anteproyecto establece expresamente que, cuando la sociedad infractora pertenezca a un grupo,**el cálculo del límite superior se hace sobre el volumen de negocios del grupo, no de la filial**. Es decir, se cierra de salida

del Reglamento europeo: la multa será**el porcentaje o el importe fijo, el que sea menor**. Y se introduce, además, un mecanismo de

**apercibimiento sin multa** para infracciones leves de pymes, condicionado a la adopción de medidas correctoras y, en su caso, a la

indemnización de los daños causados. Una vía de aterrizaje suave pensada para no asfixiar a la innovación, que conviene aprovechar

bien.

## Una gobernanza descentralizada: oportunidad y riesgo

Quizás el aspecto más estructural del Anteproyecto, y el que más impacto tendrá en el día a día de las empresas, es el**modelo de**

**autoridades de vigilancia del mercado**. España opta por un esquema descentralizado por sectores:

- **AESIA** como punto de contacto único y autoridad para sistemas de IA prohibidos (en general), sistemas de alto riesgo del Anexo III en biometría, infraestructuras críticas, educación y formación, empleo, servicios esenciales, y sistemas no clasificados como prohibidos o de alto riesgo cuando incumplan obligaciones de transparencia.
-

**Agencia Española de Protección de Datos (AEPD) y autoridades autonómicas de protección de datos** para sistemas de IA en biometría con fines policiales o de gestión de fronteras, garantía del cumplimiento del Derecho y migración/asilo.

- **Banco de España y CNMV** para sistemas de evaluación de solvencia y calificación crediticia.

-

**Dirección General de Seguros y Fondos de Pensiones** para sistemas usados en evaluación de riesgos y fijación de precios en seguros de vida y salud.

- **CGPJ y Junta Electoral Central** para los ámbitos de administración de justicia y procesos democráticos.

-

Las**autoridades sectoriales designadas bajo los actos armonizados** del Anexo I del Reglamento, para los sistemas de IA integrados en productos regulados.

Esto tiene una lectura positiva (cada sector lo supervisa quien conoce el negocio) y otra preocupante: el riesgo de aplicación heterogénea. Una conducta similar podría recibir respuestas distintas de autoridades distintas. El Anteproyecto es consciente del problema y crea la **Comisión mixta de coordinación de autoridades de vigilancia del mercado**, presidida y gestionada por AESIA, que será la pieza llamada a evitar interpretaciones divergentes. Habrá que ver cómo se articula en la práctica. Para las empresas con sistemas de IA transversales (pensemos en una entidad financiera que use IA para scoring crediticio, gestión de RR.HH. y atención al cliente al mismo tiempo) el mapa de interlocutores supervisores puede volverse complejo. Identificar quién es la autoridad competente sobre cada sistema dejará de ser una cuestión teórica.

**El nuevo derecho de desconexión: España vuelve a innovar en derechos digitales**

Uno de los elementos más originales del Anteproyecto es la introducción de un nuevo**derecho digital de desconexión o retirada del**

**mercado** de sistemas de IA que hayan provocado incidentes graves. La exposición de motivos lo compara, no sin cierta vocación

histórica, con el reconocimiento en su día del "derecho al olvido" por el TJUE. ¿Qué implica? Que cualquier persona física o jurídica

podrá denunciar, incluso de forma anónima a través de un buzón externo gestionado por AESIA, hechos que pudieran constituir

infracción, y que la autoridad competente podrá adoptar medidas cautelares incluyendo**la retirada del producto o la desconexión o**

**prohibición del sistema de IA** en su ámbito territorial cuando la continuidad del sistema implique un riesgo inaceptable.

Esto, leído con calma, es una herramienta poderosísima. Para el ciudadano, supone un mecanismo real de reacción frente a perjuicios graves causados por IA (el texto cita expresamente el supuesto de fallecimiento de un familiar). Para las empresas, supone un cambio de paradigma: ya no basta con cumplir formalmente;**un incidente grave puede traducirse en la desconexión cautelar del sistema antes incluso de que el expediente sancionador esté resuelto**.

La obligación de notificar incidentes graves, tipificada como infracción**muy grave** si se omite, deja de ser un trámite burocrático. Pasa a ser el eje sobre el que pivota la respuesta del sistema sancionador.

### Identificación biométrica remota «en tiempo real»: el equilibrio fino

El Capítulo III del Anteproyecto regula uno de los puntos más debatidos del AI Act: el uso excepcional de**identificación biométrica remota en tiempo real en espacios públicos con fines policiales**. España opta por un modelo de**autorización judicial previa** otorgada por los Juzgados de lo Contencioso-administrativo, con resolución motivada en 48 horas y silencio desestimatorio. Los

tráfico de armas, homicidio, violación, sabotaje, entre otros).

El régimen, con su exigencia de proporcionalidad, motivación y limitaciones temporales, geográficas y personales, está bien diseñado. La cuestión será su aplicación efectiva y, sobre todo, la capacidad de los juzgados para responder con la celeridad y el rigor técnico que exige un control judicial real sobre el uso policial de IA biométrica.

### Calendario: lo que está en vigor y lo que viene

El Anteproyecto contempla una entrada en vigor escalonada que sigue el calendario del AI Act:

- **2 de agosto de 2025:** régimen sancionador aplicable a sistemas de IA prohibidos y a organismos notificados.
- **2 de agosto de 2026:** régimen sancionador aplicable a operadores de sistemas de IA de alto riesgo del Anexo III.
-

**2 de agosto de 2027:** régimen sancionador aplicable a operadores de sistemas de IA de alto riesgo del Anexo I (los integrados en productos sujetos a la legislación armonizada de la Unión).

Esta gradación es importante.**Quien hoy esté operando un sistema clasificable como de alto riesgo bajo el Anexo III tiene**

**exactamente la ventana que va de aquí a agosto de 2026 para alinearse.** No es mucho tiempo si se considera lo que implica: gestión

de calidad, documentación técnica, sistema de gestión de riesgos, vigilancia poscomercialización, evaluación de conformidad, marcado

CE, registro en la base de datos europea y, para entidades del sector público y prestadores de servicios públicos, evaluación de impacto

en derechos fundamentales.

## Lo que las empresas deberían estar haciendo ya

Desde la perspectiva de un responsable de compliance, hay un puñado de acciones que no admiten más dilación.

-

Primero, inventario. No se puede gobernar lo que no se conoce. Identificar todos los sistemas de IA en uso (propios, embebidos en productos de terceros, en pruebas piloto) y clasificarlos conforme a las categorías del Reglamento (prohibido, alto riesgo, riesgo limitado, riesgo mínimo).

-

Segundo, análisis de rol. Determinar para cada sistema si la organización actúa como proveedor, responsable del despliegue, importador, distribuidor o representante autorizado. Las obligaciones, y por tanto las infracciones, cambian sustancialmente según el rol.

-

Tercero, gap analysis. Comparar el estado actual frente a las exigencias del Reglamento y del Anteproyecto. Especial atención a documentación técnica, sistema de gestión de calidad, vigilancia poscomercialización, transparencia hacia personas físicas, y obligaciones específicas en entornos laborales (informar a representantes de los trabajadores).

-

Cuarto, plan de transición. Hoja de ruta hasta agosto de 2026 con responsables, plazos, presupuestos y métricas. Si el cumplimiento de RGPD enseñó algo, es que las transiciones regulatorias no se improvisan en los seis meses previos a la fecha de aplicación.

-

Quinto, articulación con marcos existentes. El AI Act no opera en vacío: se solapa con el RGPD, con la normativa de seguridad de productos, con regulación sectorial específica. Las organizaciones que ya tienen sistemas de gestión maduros (ISO 27001, ISO 37301, ISO 42001) parten con ventaja y deben aprovecharla.

España no inventa nada con este Anteproyecto: ejecuta una obligación que le impone el Derecho de la Unión. Pero lo hace con elementos propios (el derecho de desconexión, el régimen específico para pymes, el canal anónimo de denuncia, la atribución a juzgados contencioso-administrativos de la autorización del uso biométrico policial) que merecen reconocimiento. La pregunta de fondo,

cuando se trata, y desde 2026 lo será sin discusión, de un asunto de gobierno corporativo y de cumplimiento normativo con sanciones equiparables, o superiores, a las del RGPD.