



Nota informativa

## Aplicación de determinados preceptos del Reglamento de Inteligencia Artificial (RIA)

En la presente Nota se analiza el nuevo **Reglamento de Inteligencia Artificial (RIA)** de la Unión Europea, aprobado en junio de 2024. Se incluye el repaso del calendario de implementación, detallando las distintas fases de entrada en vigor hasta 2027. Se examinan en profundidad las prácticas de IA que quedarán expresamente prohibidas a partir de febrero de 2025, y se proporciona una guía práctica con las medidas y controles que deberán adoptar empresas y entidades públicas para adecuarse a esta nueva normativa. Finalmente, se abordan las consecuencias del incumplimiento, incluyendo el régimen sancionador previsto en el reglamento.

### Contexto y objetivos

---

En un contexto de creciente desarrollo y uso de la Inteligencia Artificial (IA), el Parlamento Europeo aprobó 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 (en adelante, "Reglamento de Inteligencia Artificial" o "RIA").

#### Objetivos

El RIA tiene como objetivo principal **unificar el marco normativo en los Estados Miembros** para abordar el impacto social, económico y ético, garantizando que su desarrollo sea compatible con los valores y derechos y libertades establecidos en la Unión Europea.

Además, el Reglamento establece sanciones significativas para asegurar el cumplimiento de la normativa, así como para fomentar la confianza en la IA y asegurar su desarrollo ético y respetuoso con los derechos fundamentales.

**Importante:** la aplicación del Reglamento de la IA deberá ser en todo caso compatible y coordinada con la legislación vigente de la UE en materia de Protección de datos y de Propiedad Intelectual.

## Calendario de aplicación de la RIA

---



## Sistemas de IA prohibidos conforme al RIA

---

Con ello, a partir del 2 de febrero de 2025 del corriente quedan expresamente prohibidas las siguientes prácticas de uso de IA, las cuales analizaremos a continuación:

- ✗ **Uso de técnicas subliminales, manipuladoras o engañosas** con el objetivo de alterar sustancialmente el comportamiento de una persona o colectivo, reduciendo su capacidad de decisión y llevándolos a tomar decisiones que no habrían tomado en circunstancias normales, causando perjuicios considerables.
- ✗ **Explotación de vulnerabilidades** de personas físicas o colectivos debido a su edad, discapacidad o situación social o económica, cuando ello altere significativamente su comportamiento y provoque perjuicios significativos.
- ✗ **Evaluación o clasificación de personas** según su comportamiento social o características personales, cuando la puntuación resultante implique un trato perjudicial o desfavorable en contextos no relacionados o un trato injustificado o desproporcionado.
- ✗ **Realización de evaluaciones o predicciones sobre el riesgo de comisión de delitos** basadas únicamente en perfiles, rasgos o características de su personalidad.
- ✗ **Creación o ampliación de bases de datos de reconocimiento facial** mediante la recopilación masiva y no selectiva de imágenes de internet o circuitos cerrados de televisión.
- ✗ **Inferencia de emociones de una persona** en entornos laborales y educativos, salvo para fines médicos o de seguridad.
- ✗ **Sistemas de categorización biométrica** que clasifiquen personas según sus datos biométricos para deducir información sensible como opiniones políticas, afiliaciones sindicales, creencias religiosas o filosóficas, entre otras.
- ✗ **Uso de sistemas de identificación biométrica remota en tiempo real en espacios públicos** con fines de aplicación de la ley, salvo en casos estrictamente necesarios para objetivos específicos como la búsqueda de personas desaparecidas, la prevención de amenazas graves para la seguridad o la localización de sospechosos en investigaciones penales.

## Plan de acción para la adecuación al RIA

---

Ante este escenario de aplicación progresiva del RIA resulta **necesario** que las empresas y entidades públicas que pretendan comercializar, desarrollar, proveer, usar sistemas de IA o que se encuentren en alguno de los eslabones de la cadena de los sistemas de IA, se

adecuen a este marco legal y supervisen de forma recurrente que en su organización no se están usando sistemas de IA prohibidos por el RIA.

Algunos de los **controles generales a implantar** por los distintos participantes serían los siguientes:

- Identificar aquellos sistemas de IA prohibidos en sus procesos y aquellos permitidos.
- Listado de los controles a aplicar y recogida de evidencias para evidenciar que sus sistemas de IA son seguros.
- Elaborar un inventario/registro sistemas IA que se estén usando o planificando por cada área.
- Formar a las personas trabajadoras sobre los riesgos y evitar el uso de sistemas de IA prohibidos en su actividad.
- Elaborar un registro proveedores IA y contratos suscritos.
- Establecer procedimientos para la auditoría de proveedores IA.
- Análisis de riesgos y evaluación de impacto en materia de protección de datos y riesgos específicos IA.
- Auditoría de cumplimiento normativo (RGPD, seguridad de la información, IP, futuro Reglamento IA).
- Listado de medidas preventivas para reducir los riesgos de la IA.
- Reportar a las autoridades competentes cualquier uso indebido de IA que detecten.

Las anteriores acciones **son esenciales** ante el escenario sancionador del Reglamento de Inteligencia Artificial, atendiendo que las **multas pueden alcanzar hasta 35 millones de euros** o el **7% del volumen de negocio** anual global de la empresa, lo que sea mayor.

## Contacto



**Carme Setó**  
Socia | IP&IT y protección  
de datos  
[cseto@duransindreu.com](mailto:cseto@duransindreu.com)  
93 602 52 22