



## Nuevo paradigma normativo

El Reglamento de Inteligencia Artificial 2024/1689 (de ahora en adelante, RIA), aprobado el 13 de junio de 2024, establece un marco jurídico vinculante para el desarrollo, comercialización y uso de la IA en la Unión Europea. Su finalidad es armonizar la innovación tecnológica con la protección de los derechos fundamentales, garantizando que los sistemas de IA sean seguros, transparentes y acordes a la normativa.

El RIA no únicamente afecta a empresas que pertenezcan al Espacio Económico Europeo (EEE), sino también a proveedores y operadores ubicados en terceros países cuyos sistemas de IA sean comercializados o utilizados en el mercado comunitario.

## Entrada en vigor y aplicación

**A tenor del artículo 113 RIA, el Reglamento será aplicable, con carácter general, a partir del 2 de agosto de 2026, pero prevé que con anterioridad a esa fecha ya se empiecen a aplicar algunos de sus preceptos, concretamente, a partir del 2 de febrero de 2025 debe cumplirse con lo dispuesto en los Capítulos I y II, que incluyen:**

- Artículo 4. Obligación de alfabetización en IA.
- Artículo 5. Prácticas de IA estrictamente prohibidas.

## Sujetos obligados

Según el artículo 2 RIA la normativa se aplica a:

- **Proveedores de IA.** Empresas o entidades que desarrollen, comercialicen o pongan en servicio sistemas de IA o modelos de uso general en la UE, sin importar si su sede se encuentra fuera o dentro de la UE.
- **Responsables del despliegue de sistemas IA.** Entidades que utilicen IA en sus operaciones y dispongan de sede o actividad en la UE.
- **Proveedores y responsables del despliegue de sistemas IA de fuera de la UE.** Empresas de terceros países cuyos productos de IA se utilicen en el territorio de la UE.
- **Importadores y distribuidores de IA.** Empresas que introduzcan sistemas de IA en el mercado europeo, asegurando su conformidad con la normativa.
- **Fabricantes de productos con IA integrada.** Empresas que incorporen IA en sus productos y los comercialicen bajo su propia marca.
- **Representantes autorizados.** Entidades que actúan en nombre de proveedores no establecidos en la UE, asegurando su conformidad con el Reglamento.
- **Personas afectadas en la UE.** Ciudadanos y residentes europeos que puedan verse impactados por sistemas de IA.

Por otro lado, debe tenerse en cuenta que el Reglamento **no aplica** en determinados supuestos, entre otros, la seguridad nacional, defensa y operaciones militares, las actividades de investigación, prueba o desarrollo relativa a sistemas de IA o modelos de IA antes de su introducción en el mercado o puesta en servicio, o a las personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de

carácter no profesional, los citados supuestos y otros, así como las condiciones de no aplicabilidad se regulan en diversos apartados del artículo 2 RIA.

Además, el citado artículo 2, también regula de qué modo afecta el RIA a la aplicación de otras normas, como por ejemplo, el Reglamento (UE) 2016/679 (RGPD) o el Reglamento de Servicios Digitales (2022/2065) en relación a los prestadores de servicios intermediarios.

## Obligaciones

### Alfabetización en IA: artículo 4

La alfabetización en materia de IA, definida en el artículo 3 RIA, tiene como objetivo garantizar que los proveedores y **responsables del despliegue** de sistemas de IA adopten las medidas necesarias para garantizar que las **personas involucradas en introducir en el mercado sistemas de IA, o en su puesta en marcha y uso, dispongan de los conocimientos, habilidades y comprensión necesarias para utilizarlos de manera responsable y conforme a la normativa**. De esta manera, el artículo 4 RIA, establece obligaciones relativas a requisitos de formación y capacitación para su personal, en relación con el funcionamiento, los riesgos y las limitaciones de la IA.

Esta disposición implica un impacto transversal en los operadores económicos que desarrollen, comercialicen, desplieguen o supervisen sistemas de IA en sus procesos, con el objetivo de garantizar que su personal disponga de los conocimientos adecuados sobre esta tecnología.

La formación debe estar adaptada a:

- Su nivel técnico.
- El uso específico de la IA.
- Las personas potencialmente afectadas por el uso de la IA.

### Prácticas prohibidas

El artículo 5 RIA prohíbe una serie de **prácticas que se consideran inaceptables** debido a su potencial riesgo para la sociedad y los derechos fundamentales. Estas prohibiciones son de cumplimiento obligatorio y no admiten excepciones, salvo en circunstancias expresamente reguladas.

Estas prácticas prohibidas son:

1. **Manipulación subliminal y engañosa.** Sistemas de IA que utilicen técnicas subliminales, manipuladoras o engañosas que escapen de la conciencia de la persona para influir en su comportamiento causando un daño significativo.
2. **Explotación de vulnerabilidades.** Sistemas de IA diseñados para aprovecharse de personas en situación de especial vulnerabilidad debido a su edad, discapacidad o circunstancias socioeconómicas, con el objetivo de influir en su comportamiento y generarles un perjuicio.
3. **Puntuación social y clasificación discriminatoria.** Uso de IA para evaluar o clasificar a personas en función de su comportamiento social o características personales, cuando esto derive en (i) trato desfavorable en contextos distintos a la recopilación de datos o (ii) trato discriminatorio o desproporcionado.

4. **Evaluaciones de riesgo delictivo sin base objetiva.** Sistemas de IA utilizados para predecir la probabilidad de que una persona cometa un delito, cuando se basen exclusivamente en su perfil o en la evaluación de la personalidad, sin hechos objetivos verificables con la actividad delictiva.
5. **Creación o ampliación de bases de datos de reconocimiento facial sin consentimiento.** Uso de IA para recopilar imágenes faciales de internet o grabaciones CCTV sin autorización, con el fin de construir bases de datos de reconocimiento facial.
6. **Inferencia de emociones en el entorno laboral y educativo.** Uso de IA para interpretar las emociones de las personas en entornos laborales o educativos, salvo en casos justificados por razones médicas o de seguridad.
7. **Categorización biométrica con fines sensibles.** Sistemas que utilicen datos biométricos para inferir información como raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida u orientación sexuales, salvo en casos de obtención de datos biométricos adquiridos legalmente.
8. **Identificación biométrica en tiempo real en espacios públicos.** Uso de IA para identificar personas en tiempo real en lugares públicos con fines policiales, salvo en situaciones excepcionales y bajo condiciones estrictas (como búsqueda de víctimas de delitos graves, prevención de amenazas terroristas inminentes e identificación de sospechosos en investigaciones de delitos graves).

## Régimen sancionador a partir del 2 de agosto de 2025

El incumplimiento del RIA puede suponer:

Tipo de infracción	Multa máxima	Aplicabilidad
<b>Infracciones por prácticas de IA prohibidas</b>	35 millones de euros o 7% del volumen total de negocio	Quienes comercialicen, desarrollen o <b>usen sistemas IA prohibidos</b> .
<b>Infracciones por incumplimiento de obligaciones del Reglamento</b>	15 millones de euros o 3% del volumen del negocio global	Proveedores, importadores, distribuidores y <b>responsables de despliegue</b> que no cumplan con requisitos como:  (i) Garantizar la alfabetización en la IA (ii) Incumplir requisitos de transparencia y documentación. (iii) No seguir las obligaciones de importadores y distribuidores de IA.
<b>Infracciones por información incorrecta o engañosa</b>	7,5 millones de euros o 1% del volumen de negocio global	Quienes suministren información falsa, incompleta o engañosa a los organismos reguladores o a las autoridades de supervisión.
<b>Sanciones reducidas a PYMEs y Startups</b>	Según viabilidad económica	-

## Recomendaciones para los responsables del despliegue de sistemas de IA

El RIA dispone que las entidades que desarrollen, comercialicen o **utilicen sistemas de IA en la Unión Europea**, deben adoptar medidas para garantizar el cumplimiento normativo. En este sentido, los responsables del despliegue de IA, deben centrarse en dos aspectos clave a partir del 2 de febrero de 2025:

### 1. Garantizar la alfabetización en IA

- a. Elaborar y aprobar políticas internas de uso de la IA
- b. Implementar programas de formación para el personal involucrado en el desarrollo, comercialización o uso de sistemas de IA.
- c. Adaptar la capacitación a los distintos niveles técnicos y funciones dentro de la organización.
- d. Asegurar que los equipos responsables comprendan los riesgos, limitaciones y requisitos - legales - aplicables a la IA.
- e. Verificar que los proveedores y socios comerciales cumplan con los requisitos de alfabetización en IA.

### 2. Verificar que no se usen sistemas de IA prohibidos

- a. Realizar auditorías o verificaciones internas sobre el uso de IA en la organización para identificar posibles prácticas prohibidas.
- b. Examinar cualquier sistema de IA adquirido o implementado, asegurándose de que no incurra en:
  - i. Manipulación subliminal o engañosa.
  - ii. Explotación de vulnerabilidades de personas en situación de riesgo.
  - iii. Puntuación social o clasificación discriminatoria.
  - iv. Evaluaciones de riesgo delictivo sin base legal objetiva.
  - v. Creación o ampliación de bases de datos de reconocimiento facial sin consentimiento.
  - vi. Interferencia de emociones en entornos laborales o educativos.
  - vii. Identificación biométrica en tiempo real sin autorización regulatoria.
- c. En el caso de que se confirme que se está usando un sistema de IA prohibido, la organización deberá adoptar las medidas necesarias para cesar en su uso, teniendo en cuenta el impacto que ello pueda tener en su actividad.

El cumplimiento de estas obligaciones es fundamental para evitar sanciones y garantizar que el uso de la IA se realice de forma ética, transparente, segura y conforme a la normativa vigente.

Debe tenerse en cuenta que **estas obligaciones aplican a cualquier sistema de IA que sea usado en el marco de las actividades de negocio de las empresas**, incluyendo tanto a sofisticados sistemas dedicados al análisis de datos, o la ayuda a la toma de decisiones, como a sistemas que ya se consideran de uso común, como las aplicaciones de chatbot de inteligencia artificial ("ChatGPT" o similares), por tanto, **se recomienda a los responsables del despliegue de IA que adopten un enfoque proactivo en la supervisión de tales sistemas y que aprovechen la aplicación gradual del Reglamento de IA** para ir adecuándose de manera paulatina a la regulación.

---

**Departamento de Privacidad, Compliance, Ciberseguridad y Sostenibilidad**

**Ecija Barcelona**

T +34 933 808 255

[info@ecijalegal.com](mailto:info@ecijalegal.com)

[www.ecija.com](http://www.ecija.com)

# ECIJA

**Ecija Barcelona**

T +34 933 808 255

[info@ecijalegal.com](mailto:info@ecijalegal.com)

[www.ecija.com](http://www.ecija.com)



Most recognized Spanish firm in LATAM and Best European TMT Firm



34 practices globally recognized in 10 jurisdictions



Best Technology Firm



Amongst most innovative European Firms

**THE LAWYER**

Best European TMT Firm



Most innovative project. Best Digital Economy Firm