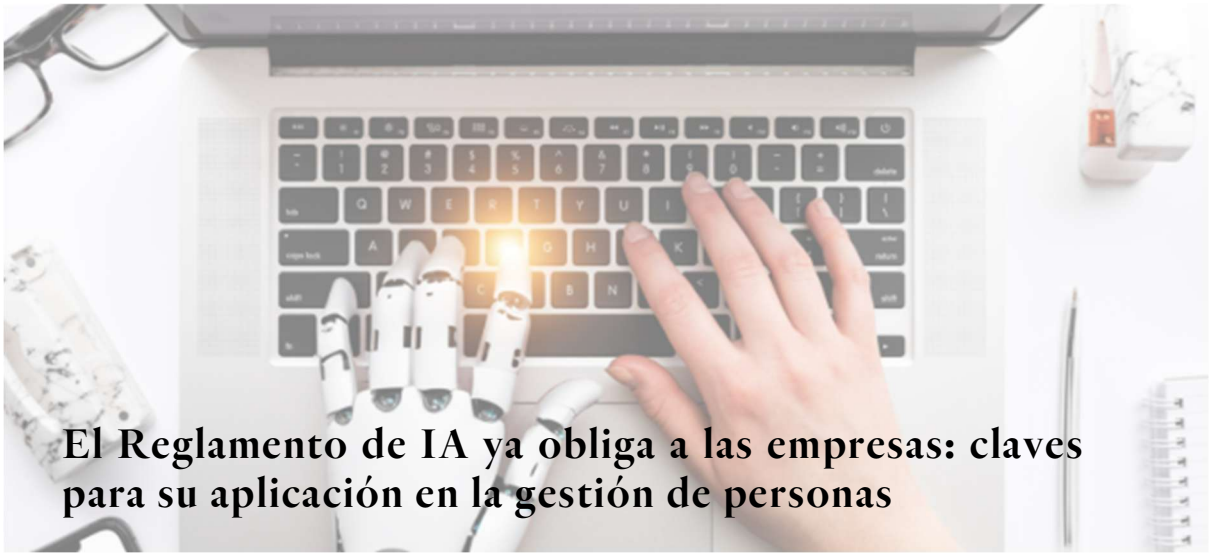
RocaJunyent Informa

Área de Derecho Laboral y
Protección de Datos y Nuevas Tecnologías



El Reglamento de IA ya obliga a las empresas: claves para su aplicación en la gestión de personas

El Reglamento IA ya está aquí

El Reglamento (UE) 2024/1689 de Inteligencia Artificial (en adelante, el "**Reglamento IA**" o "**RIA**")[1] no es una norma que afecte solo a empresas tecnológicas. Establece un marco jurídico vinculante para cualquier organización que utilice sistemas de IA, y aplica a toda la cadena de valor de IA, lo que supone, entre otros operadores: (i) los proveedores, que desarrollan o comercializan sistemas de IA; (ii) los responsables del despliegue, que utilizan sistemas de IA bajo su autoridad (categoría en la que se encuadra la mayoría de las empresas que emplean herramientas de IA en la gestión de personas); y (iii) los importadores y distribuidores, que introducen o ponen a disposición sistemas de IA en el mercado de la Unión.

[1]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 y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), accesible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079

> **La arquitectura regulatoria está suficientemente consolidada para actuar: si su empresa utiliza IA en la gestión de personas y aún no ha iniciado su proceso de cumplimiento, el momento es ahora.**

Calendario de aplicación del Reglamento de IA (RIA)

📍 **2 febrero 2025**
Prohibiciones absolutas (art. 5)
→ Entran en vigor las restricciones a determinadas prácticas de IA consideradas inaceptables.

📍 **2 agosto 2025**
Modelos de IA de uso general (Cap. V)
→ Se aplican las obligaciones para proveedores de modelos de propósito general.

📍 **2 agosto 2026**
Sistemas de alto riesgo (Anexo III, punto 4)
→ Son plenamente exigibles las obligaciones para sistemas de IA de alto riesgo, incluidos los del ámbito laboral.

Es importante tener en cuenta además que, dada la complejidad normativa y operativa del RIA, la propia Comisión Europea ha propuesto una extensión en los plazos y simplificación de obligaciones en el denominado Reglamento Ómnibus Digital de IA[2], actualmente en tramitación. De aprobarse – lo que se espera antes de Agosto de este año, se extendería el inicio de la entrada en aplicación de las obligaciones y el ajuste de las obligaciones de proporcionalidad a operadores de menor dimensión, lo que podría modificar parcialmente este calendario y las expectativas de los distintos agentes en el mercado.

En el ámbito laboral, el RIA tiene un impacto especialmente relevante en dos planos. En primer lugar, entre las prohibiciones absolutas ya vigentes, destaca la prohibición de utilizar sistemas de IA diseñados para inferir las emociones de personas físicas en el lugar de trabajo (artículo 5.1.f) RIA), así como los sistemas de categorización biométrica que deduzcan características especialmente protegidas como la raza, las opiniones políticas o la orientación sexual. En segundo lugar, el Anexo III, punto 4 del Reglamento clasifica como sistemas de alto riesgo todos aquellos utilizados en el empleo, la gestión de trabajadores y el acceso al trabajo por cuenta propia, distinguiendo dos categorías: (a) los sistemas destinados a la contratación o selección de personas físicas, en particular para publicar anuncios de empleo específicos, analizar y filtrar solicitudes de empleo y evaluar a los candidatos; y (b) los sistemas destinados a tomar decisiones que afecten a las condiciones de las relaciones laborales o a la promoción o rescisión de relaciones contractuales de índole laboral, a la asignación de tareas a partir de comportamientos individuales o rasgos o características personales, o a supervisar

[2] REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se modifican los Reglamentos (UE) 2024/1689 y (UE) 2018/1139 en lo que respecta a la simplificación de la aplicación de normas armonizadas en materia de inteligencia artificial (Reglamento ómnibus digital sobre IA), accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52025PC0836

y evaluar el rendimiento y el comportamiento de las personas en el marco de dichas relaciones. A pesar del calendario indicado, las empresas que quieran evaluar el uso de sistemas que puedan encontrarse en estas clasificaciones deben iniciar su estrategia de cumplimiento ahora.

La arquitectura regulatoria está suficientemente consolidada para actuar: si su empresa utiliza IA en la gestión de personas y aún no ha iniciado su proceso de cumplimiento, el momento es ahora.

Clasificación de las herramientas de RRHH como sistemas de alto riesgo

En la práctica, la clasificación de alto riesgo puede afectar a herramientas que su empresa ya tiene implantadas: el ATS de cribado de CVs, la plataforma de evaluación del desempeño, el sistema que asiste en decisiones de promoción o extinción, e incluso los módulos de IA integrados en el ERP o en el software de nóminas.

La clasificación como sistema de alto riesgo activa un conjunto de obligaciones para proveedores y responsables del despliegue. El Reglamento exige, entre otras, la implantación de un sistema de gestión de riesgos durante todo el ciclo de vida del sistema (artículo 9 RIA), el registro automático de eventos para garantizar la trazabilidad (artículo 12 RIA), la evaluación de conformidad previa al despliegue (artículos 43 y ss. RIA), obligaciones reforzadas de transparencia e información a las personas afectadas (artículo 13 RIA), la gobernanza de los datos de entrenamiento y el control de sesgos (artículo 10 RIA), y la supervisión humana efectiva de las decisiones del sistema (artículo 14 RIA). Para una información más detallada sobre el alcance y la aplicación práctica de estas obligaciones, pueden consultarse las guías publicadas por la Agencia Española de Supervisión de Inteligencia Artificial ("**AESIA**") en https://www.aesia.gob.es.

En la práctica, el cumplimiento de estas obligaciones supone una carga documental significativa y la necesidad de comprender con precisión los requisitos aplicables a cada sistema. El primer paso, y el más práctico y efectivo, es establecer un sistema interno de clasificación que permita: (i) identificar qué herramientas constituyen sistemas de IA a efectos del RIA y cuáles no; (ii) detectar cuáles de ellas incurren en alguna de las prohibiciones absolutas del artículo 5 RIA; (iii) determinar cuál es la categoría de riesgo (y si son sistemas de alto riesgo bajo el RIA); y (iv) mapear las obligaciones que pueden corresponder a cada categoría en esa clasificación. Sin este ejercicio previo, cualquier estrategia de cumplimiento resultará incompleta.

Aunque el sistema no sea de alto riesgo, hay obligaciones ya aplicables

No hay que olvidar, que el RIA no es la única norma a tener en cuenta. Una empresa puede cumplir formalmente el Reglamento IA y, aun así, estar expuesta a sanciones de la Inspección de Trabajo, nulidad de políticas internas y litigiosidad judicial. El ordenamiento español impone obligaciones propias, acumulativas al Reglamento IA, cuyo incumplimiento ya ha tenido consecuencias reales en los tribunales (entre otras, Ley Orgánica de Protección de Datos[3] ("**LOPDGDD**"), reformas del Estatuto de los Trabajadores[4] ("**ET**"), Ley de Trabajo a Distancia[5]). Algunas de las más relevantes son:

- **Art. 64.4.d) ET (transparencia algorítmica):** El comité de empresa tiene derecho a ser informado de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles. La norma nace vinculada al fenómeno de las plataformas digitales, pero su ámbito de aplicación es general: cualquier empresa que utilice sistemas algorítmicos con impacto en el empleo queda sujeta a este deber.

[3] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf
[4] Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430
[5] Ley 10/2021, de 9 de julio, de trabajo a distancia. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2021-11472

- **Arts. 87.3, 89 y 90 LOPDGDD y RDL 9/2021:** Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador. Este puede acceder a los contenidos únicamente para controlar el cumplimiento de las obligaciones laborales, pero debe establecer previamente criterios de utilización que respeten los estándares mínimos de protección de la intimidad —con participación de los representantes de los trabajadores en su elaboración— e informar a los trabajadores de dichos criterios.

- **RGPD, Ley 31/1995 y LO 3/2007:** El tratamiento de datos en la evaluación del rendimiento activa evaluaciones de impacto, y los algoritmos que reproducen sesgos de género, edad u origen étnico generan responsabilidad bajo la normativa de igualdad y prevención de riesgos psicosociales.

> **No basta con cumplir el Reglamento IA de forma aislada: un enfoque compartimentado genera lagunas de cumplimiento y multiplica la exposición jurídica.**

La consecuencia práctica es clara: no basta con cumplir el Reglamento IA de forma aislada. Un enfoque compartimentado, que aborde el Reglamento IA sin considerar el Estatuto de los Trabajadores, o que revise la protección de datos sin evaluar el impacto en la negociación colectiva, genera lagunas de cumplimiento y multiplica la exposición jurídica. La gestión de personas mediante IA exige un asesoramiento que integre todas las disciplinas desde el primer momento.

El Tribunal Supremo ya ha confirmado la nulidad de políticas de control digital elaboradas sin participación de la representación legal de los trabajadores (art. 87.3 LOPDGDD), con la consecuencia añadida de que las pruebas obtenidas a su amparo pueden ser declaradas ilícitas.

Las zonas grises son las que concentran un riesgo práctico más elevado: es en los sistemas que formalmente no alcanzan el umbral de alto riesgo del Reglamento IA, pero que generan una exposición jurídica real bajo la normativa laboral y de protección de datos, donde las empresas pueden cometer errores de valoración en la medición de los riesgos. Estos sistemas están extendidos con carácter general en el día a día empresarial, pensemos por ejemplo en sistemas de videovigilancia y monitorización (el control del rendimiento mediante cámaras, capturas de pantalla automáticas o análisis de actividad en pantalla puede ser técnicamente un sistema de IA que no alcanza el umbral de alto riesgo, pero puede vulnerar el artículo 20 bis del Estatuto de los Trabajadores y el RGPD y la LOPDGDD); o los algoritmos de asignación de turnos y cargas de trabajo (distribuyen automáticamente turnos y pueden no ser alto riesgo si no adopta decisiones vinculantes sobre condiciones esenciales, pero si afecta a la conciliación, salud o equidad, puede rozar las obligaciones de negociación colectiva, las normas de prevención de riesgos laborales y la igualdad de trato, entre otras).

Medidas inmediatas para el cumplimiento en materia de IA

Estos son los pasos inmediatos que cualquier empresa puede dar desde hoy para crear su estrategia de IA:

1. **Inventario de sistemas de IA.** Identifique y clasifique los sistemas de IA empleados en la gestión de personas: ATS, evaluación del rendimiento, módulos de IA en el ERP, nóminas o comunicación interna. Sin inventario no hay cumplimiento posible.

2. **Verificación de prohibiciones absolutas y de alto riesgo.** Revise su inventario a la luz de las prohibiciones del RIA. Si alguna herramienta encaja en estas categorías, debe desactivarse de inmediato. Identifique los sistemas de alto riesgo para saber qué obligaciones se tiene.
3. **Información al comité de empresa.** Valore en qué medida ha de cumplir con la obligación de transparencia algorítmica del artículo 64.4.d) ET. Esta obligación está en vigor desde 2021, con independencia del Reglamento IA.
4. **Supervisión humana real.** La supervisión humana debe ser efectiva, no solo formal. Valore un proceso que permita ejercerla en los términos que pide la norma.
5. **Auditoría de la política de control digital basada en IA.** Si su política de monitorización digital no fue elaborada con participación de la representación legal de los trabajadores, podría ser declarada nula en caso de impugnación (art. 87.3 LOPDGDD). Si no se informa de sistemas IA, puede estar incompleta.
6. **Revisión de los contratos con sus proveedores.** Verifique que incluyen cláusulas de cumplimiento del Reglamento IA, datos personales y garantías de que los datos de sus trabajadores no se utilizan para entrenar modelos de terceros.
7. **Formación en IA.** El artículo 4 RIA exige que el personal que opere sistemas de IA tenga conocimiento suficiente en la materia.
8. **Aprobar una política de uso de IA.** Una política que guíe a sus trabajadores y regule el uso de IA, los criterios de supervisión humana y los límites del control tecnológico reduce significativamente el riesgo de conflicto y refuerza la posición de la empresa ante los tribunales.