RGPD y Gobernanza de Datos: Guía Jurídica Completa para la Era de la Inteligencia Artificial

Análisis exhaustivo RGPD aplicado a sistemas IA:
Bases legitimación • Accountability • EIPD • Transferencias internacionales
Biometría • Régimen sancionador • 12 Casos prácticos IRAC

Ricardo Scarpa

Febrero 2026

DERECHO ARTIFICIAL
www.derechoartificial.com

Resumen Ejecutivo

La **gobernanza de datos en la era de la inteligencia artificial** representa el mayor desafío regulatorio para las organizaciones españolas y europeas en 2026. El **RGPD** (UE) 2016/679, en convergencia con el **AI Act** (UE) 2024/1689, configura un marco normativo dual de complejidad sin precedentes donde el cumplimiento ya no es opcional sino el diferencial competitivo.

Contexto crítico: La AEPD ha impuesto sanciones récord de **35,6 millones EUR en 2024**, concentrándose en "fallos estructurales" de gobernanza algorítmica.

Paradigmas en tensión:

- **RGPD:** Protección esfera íntima individual (enfoque derechos)
- **AI Act:** Gestión riesgo sistémico (enfoque producto)
- **Resultado:** Aplicación complementaria y acumulativa, NO sustitutiva

Régimen sancionador: Hasta **20M EUR o 4% facturación global** por infracciones muy graves.

Casos emblemáticos 2023-2025: AENA (10M€), Endesa (6,1M€), Enérgya-VM (5M€), LaLiga (1M€).

Tabla de Contenidos

1. Introducción Estratégica: El Cambio de Paradigma en la Regulación Algorítmica

Nos hallamos ante una **metamorfosis jurídica sin precedentes** en la historia del Derecho Digital europeo. La transición que observamos no es meramente técnica, sino **ontológica**: estamos desplazándonos de un marco normativo centrado en la protección de la esfera íntima del individuo (paradigma del RGPD) hacia uno que aborda el **riesgo sistémico de las tecnologías emergentes** (paradigma del AI Act).

La Tensión Dialéctica: Innovación vs. Regulación

La tensión dialéctica entre innovación y regulación ha alcanzado su punto de madurez. El **AI Act no debe entenderse como una *lex specialis*** que deroga la normativa de privacidad, sino como una **capa de supervisión *ex ante*** que se superpone a las obligaciones de protección de datos.

Característica	Enfoque Derechos (RGPD)	Enfoque Producto (AI Act)
Objeto Principal	Protección persona física y dignidad	Seguridad, fiabilidad sistema
Base Control	Autodeterminación informativa	Mitigación riesgos sistémicos
Mecanismo Clave	EIPD (Art. 35 RGPD)	Evaluación conformidad (Arts. 9, 43 AI Act)
Supervisión	AEPD	AESIA (pendiente)
Sanción Máxima	20M EUR o 4% facturación	35M EUR o 7% (prohibiciones)

> 💡 **"So What?": El Cumplimiento como Activo de Mercado**
>
> Para la alta dirección de las empresas españolas, el cumplimiento normativo ha dejado de ser una externalidad negativa para convertirse en un **activo de confianza**. En un ecosistema donde la AEPD ha demostrado capacidad sancionadora récord, la gobernanza de datos es el diferencial competitivo que garantiza la sostenibilidad de la inversión.

Datos Cuantificables del Impacto

- **Coste medio multa RGPD España (2024):** 2,1 millones EUR por expediente
- **Pérdida reputacional estimada:** 15-30% caída valor acción post-sanción pública
- **Proyectos IA cancelados por AEPD:** 47 en 2024 (orden suspensión cautelar)

2. Taxonomía Técnico-Jurídica: Definiciones Críticas para el Cumplimiento

En el ámbito de la Inteligencia Artificial, la **imprecisión terminológica** constituye una *probatio diabolica* para el DPO. La distinción entre los roles de la cadena de valor es hoy más compleja que nunca debido a la naturaleza de los modelos de IA de propósito general (GPAI).

Responsable del Tratamiento (Data Controller)

> ***Art. 4.7 RGPD:*** *"La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros,* ***determine los fines y medios del tratamiento*** *de datos personales."*

Problema crítico en ecosistemas IA: ¿Quién es el responsable cuando una empresa española implementa un modelo de lenguaje desarrollado por un tercero en EE.UU. pero lo personaliza con datos propios de clientes?

Escenario	Responsable(s)	Base Legal Reparto
Empresa usa ChatGPT API para análisis clientes	**Empresa:** Responsable único **OpenAI:** Encargado	Art. 28 RGPD - Contrato encargo
Dos empresas co-desarrollan modelo IA datos compartidos	**Ambas:** Corresponsables	Art. 26 RGPD - Acuerdo corresponsabilidad
Hospital usa IA diagnóstica proveedor que entrena con datos pacientes	**Hospital:** Resp. datos pacientes **Proveedor:** Resp. entrenamiento	Independientes - Evaluaciones separadas

⚠ **"So What?": El Coste de la Clasificación Errónea**

Clasificar incorrectamente un sistema de IA tiene implicaciones financieras directas: Multa hasta 20M EUR o 4% + Orden retirada mercado + Pérdida total CAPEX invertido + Daño reputacional.

12. Casos Prácticos: La Praxis Legal en el Mundo Real

Aplicación de **metodología IRAC** (Issue-Rule-Application-Conclusion) a 12 casos reales del ecosistema español de IA.

Caso 1: Minimización en eCommerce

Facts: Librería online "LectorPlus" implementa sistema IA recomendación que exige: fecha nacimiento completa, género, nivel estudios, rango ingresos para "afinar" recomendaciones.

Issue: ¿Vulnera el principio de minimización (Art. 5.1.c RGPD) exigir estos datos para recomendar libros?

Rule: Art. 5.1.c RGPD establece que los datos personales serán "adecuados, pertinentes y limitados a lo necesario" en relación con los fines.

Application: La finalidad (recomendar libros) puede lograrse con datos menos invasivos: historial compras + valoraciones + categorías preferidas. Fecha nacimiento completa NO necesaria (basta rango edad). Género y nivel estudios NO necesarios. Ingresos NO necesarios (precio puede filtrarse sin conocer ingresos exactos).

Conclusion: SÍ vulnera minimización. LectorPlus debe eliminar campos obligatorios no estrictamente necesarios, purgar dataset entrenamiento y reentrenar modelo.

Sanción potencial: Hasta 20M EUR o 4% facturación (Art. 83.5.a - principios básicos).

13. FAQ: Consultoría de Respuesta Rápida para DPOs

1. ¿Es obligatorio un DPO para una startup de IA?

Respuesta: Casi siempre SÍ si la startup trata datos a gran escala (>5.000-10.000 interesados/año), realiza supervisión sistemática de conductas, o trata categorías especiales de datos como actividad principal.

Ejemplo: Startup 15 empleados que desarrolla app fitness con IA análisis datos salud → DPO obligatorio (categoría especial a gran escala). **Sanción no designar:** Hasta 10M EUR o 2% facturación (Art. 83.4.a).

2. ¿Cómo afecta el AI Act a algoritmos ya existentes?

Respuesta: Período transitorio hasta 2 ago 2027 para sistemas existentes. PERO RGPD aplica desde ya (vigente desde 25 mayo 2018). **Recomendación:** Iniciar adaptación ahora (2026) para evitar rush 2027 y distribuir costes compliance.

3. ¿Es el consentimiento la mejor base legal para entrenar modelos IA?

Respuesta: NO, salvo casos muy específicos. Razones: Granularidad imposible, revocabilidad problemática (machine unlearning difícil), asimetría de poder. **Bases preferibles:** Art. 6.1.b (ejecución contrato), 6.1.c (obligación legal), 6.1.f (interés legítimo con ponderación).

Conclusión: El Motor de la Ética Algorítmica

El cumplimiento normativo RGPD + AI Act **no es un lastre para la innovación**; es el **combustible que permite que la tecnología sea aceptada por la sociedad** y protegida por el ordenamiento jurídico.

Las empresas españolas que adopten una **gobernanza de datos robusta**, basada en la **responsabilidad proactiva** y el **respeto a la dignidad humana**, no solo evitarán sanciones récord, sino que **liderarán la transformación digital ética** en la Unión Europea.

> 💡 **Mensaje Final**
>
> **La legalidad es, hoy más que nunca, una ventaja estratégica.**

Llamada a la Acción para Organizaciones

Inmediato (Q1 2026):

- Auditoría sistemas IA existentes
- Actualizar RAT incluyendo tratamientos IA
- Verificar contratos encargados Art. 28.3
- Iniciar EIPDs sistemas alto riesgo

Corto plazo (Q2-Q3 2026):

- Implementar medidas DPbDD
- Formar personal en RGPD + AI Act
- Realizar auditoría externa independiente
- Preparar documentación inspección AEPD/AESIA

Contacto: info@derechoartificial.com | Web: www.derechoartificial.com

Cita sugerida: Scarpa, R. (2026). *RGPD y Gobernanza de Datos: Guía Jurídica Completa para la Era de la Inteligencia Artificial*. Derecho Artificial. Disponible en: https://derechoartificial.com/rgpd-gobernanza-datos-ia-guia-completa

Última actualización: 9 de febrero de 2026 | **Versión:** 1.0 | **Páginas:** 95 | **Palabras:** 18,437