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

Por Ricardo Scarpa | Actualizado: 9 de febrero de 2026 | Lectura: 55 minutos

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 **Reglamento General de Protección de Datos (RGPD)** (UE) 2016/679, en convergencia con el **AI Act** (Reglamento UE 2024/1689), configura un marco normativo dual de complejidad sin precedentes donde el cumplimiento ya no es opcional sino el diferencial competitivo que garantiza la sostenibilidad empresarial.

Contexto crítico: La **Agencia Española de Protección de Datos (AEPD)** ha impuesto sanciones récord de **35,6 millones de euros en 2024**, concentrándose en "fallos estructurales" de gobernanza algorítmica. El sector energético (11,68M€), financiero (5,35M€) y servicios internet (4,50M€) lideran las infracciones, evidenciando que la negligencia en EIPD (Evaluación de Impacto) y falta de responsabilidad proactiva son los principales factores de riesgo sancionador.

Paradigmas en tensión: - **RGPD:** Protección esfera íntima individual, autodeterminación informativa (enfoque derechos) - **AI Act:** Gestión riesgo sistémico, seguridad producto IA (enfoque producto/riesgo) - **Resultado:** Aplicación **complementaria y acumulativa**, NO sustitutiva

Obligaciones críticas inmediatas: 1. **Responsabilidad proactiva** (Art. 5.2 RGPD): Demostrar cumplimiento en todo momento 2. **EIPD preventiva** (Art. 35 RGPD): Antes del despliegue de sistemas alto riesgo 3. **Cadena de suministro** controlada: Diligencia en selección proveedores IA 4. **Notificación brechas 72h** (Arts. 33-34 RGPD): Transparencia absoluta ante incidentes 5. **Base legal sólida** (Art. 6 RGPD): El consentimiento es ficticio en IA a gran escala

Régimen sancionador: - **Tier 1:** Hasta **20M EUR o 4% facturación global** (Art. 83.5 RGPD) - **Tier 2:** Hasta **10M EUR o 2% facturación** (Art. 83.4 RGPD) - **España LOPDGDD:** Restricciones adicionales (Art. 9 - límites consentimiento ideología)

Casos emblemáticos 2023-2025: - **AENA** (10M€): EIPD inexistente para biometría aeropuertos - **LaLiga** (1M€): Reconocimiento facial desproporcionado - **Endesa** (6,1M€): Ocultación brecha seguridad - **Enérgya-VM** (5M€): Negligencia supervisión proveedores

Esta guía proporciona análisis jurídico exhaustivo con metodología **IRAC** (Issue-Rule-Application-Conclusion) del estándar Harvard Law School, aplicada a 12 casos prácticos reales del ecosistema español de IA.

Tabla de Contenidos

Tiempo de lectura: 55 minutos | **Palabras:** 12,000+ | **Última actualización:** Febrero 2026

---

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). Esta convergencia legislativa constituye la piedra angular de la soberanía digital de la Unión Europea y redefine el tablero de juego para cualquier organización que pretenda operar en el mercado español.

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.

Mientras que: - **RGPD** se fundamenta en la **autodeterminación informativa** del sujeto (Art. 1.2: "protección de las personas físicas en lo que respecta al tratamiento de sus datos personales") - **AI Act** introduce una **lógica de seguridad de producto** y gestión de riesgos que exige a las empresas una visión holística de su arquitectura algorítmica

Ejemplo paradigmático:
Un sistema de IA para scoring crediticio enfrenta: 1. **Obligaciones RGPD:** Base legal Art. 6.1, principios Art. 5, EIPD Art. 35, derechos Arts. 12-23 2. **Obligaciones AI Act:** Clasificación alto riesgo (Anexo III.5.b), requisitos Arts. 9-15, evaluación conformidad 3. **Resultado:** Cumplimiento **acumulativo**, NO alternativo

"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** o un mero "*check*" de auditoría 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)

Tesis central: Una IA que no es explicable o que procesa datos sin base legal no es solo un riesgo jurídico; es un **proyecto destinado al fracaso reputacional y operativo**.

Tabla Comparativa: Enfoque en Derechos vs. Enfoque en Riesgo

Característica	Enfoque en Derechos (RGPD)	Enfoque en Producto/Riesgo (AI Act)
Objeto Principal	Protección de la persona física y su dignidad	Seguridad, fiabilidad y robustez del sistema
Base de Control	Autodeterminación informativa	Mitigación de riesgos sistémicos y conformidad
Mecanismo Clave	Evaluación de Impacto (EIPD - Art. 35 RGPD)	Evaluación de conformidad y gestión de riesgos de IA (Arts. 9, 43 AI Act)
Supervisión	Autoridades de Control de Datos (AEPD)	Oficina de IA / Agencia de Supervisión (AESIA - pendiente)
Punto de Partida	Existencia de un tratamiento de datos personales	Clasificación del sistema según su uso (Riesgo Alto, Prohibido, etc.)
Principio Rector	Minimización, limitación finalidad, exactitud	Precisión, robustez, ciberseguridad, supervisión humana
Temporalidad	Aplicación desde 25 mayo 2018	Aplicación escalonada 2025-2027
Sanción Máxima	20M EUR o 4% facturación global	35M EUR o 7% facturación (prácticas prohibidas)

Implicación práctica:
Un proveedor de servicios IA en España debe demostrar: 1. **RGPD:** Cumplimiento continuo con obligaciones tratamiento datos 2. **AI Act:** Conformidad técnica del sistema como producto 3. **LOPDGDD:** Cumplimiento de especificidades españolas (Art. 9, 10, 22, etc.)

La comprensión profunda del AI Act requiere, necesariamente, dominar las **definiciones técnico-jurídicas** que actúan como cimientos de esta arquitectura legal.

---

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 (Delegado de Protección de Datos). 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)

Definición legal (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?

Análisis jurisprudencial:
El TJUE en *Wirtschaftsakademie* (C-210/16) estableció que quien determina **conjuntamente** la finalidad es **corresponsable** (Art. 26 RGPD), exigiendo acuerdo que reparta obligaciones.

Casos típicos responsabilidad compartida IA:

Escenario	Responsable(s)	Base legal reparto
Empresa usa ChatGPT API para análisis clientes	**Empresa:** Responsable único (determina finalidad análisis) **OpenAI:** Encargado (procesa por cuenta empresa)	Art. 28 RGPD - Contrato encargo
Dos empresas co-desarrollan modelo IA con datos compartidos	**Ambas:** Corresponsables (determinan conjuntamente)	Art. 26 RGPD - Acuerdo corresponsabilidad
Hospital usa IA diagnóstica de proveedor externo que entrena con datos pacientes	**Hospital:** Responsable datos pacientes **Proveedor:** Responsable entrenamiento modelo (finalidad propia)	Independientes - Evaluaciones separadas

Implicación práctica:
La responsabilidad se vuelve **compartida o diluida**, exigiendo contratos de encargo (Art. 28 RGPD) **extremadamente precisos** que definan: - Quién determina qué aspectos del tratamiento - Límites técnicos del procesamiento - Propiedad intelectual del modelo vs. datos de entrada - Derechos de auditoría técnica

Encargado del Tratamiento (Data Processor)

Definición legal (Art. 4.8 RGPD):

> *"La persona física o jurídica, autoridad pública, servicio u otro organismo que **trate datos personales por cuenta del responsable** del tratamiento."*

Riesgo crítico en SaaS de IA:
La opacidad de las soluciones *Software as a Service* de IA plantea el riesgo de que el encargado se convierta en **responsable de facto** si toma decisiones unilaterales sobre: - La lógica del algoritmo - La retención de datos para entrenamiento propio - El uso de sub-encargados sin autorización previa

Caso AEPD PS/00224/2020 (Xfera Móviles):
Sanción 8,15M EUR por permitir a un encargado (proveedor telemarketing) determinar medios del tratamiento → El encargado pasó a ser **responsable de facto**, pero Xfera **no quedó exenta** de responsabilidad por negligencia supervisión.

Lección: El responsable **NO puede desentenderse** delegando en tercero. Obligación Arts. 28.1 y 32.1 RGPD de garantizar seguridad y legalidad del tratamiento por encargados.

Protección de Datos desde el Diseño (Privacy by Design)

Base legal: Art. 25.1 RGPD

> "*...el responsable del tratamiento aplicará, tanto en el **momento de determinar los medios de tratamiento** como en el **momento del propio tratamiento**, medidas técnicas y organizativas apropiadas...*"

En la IA, esto implica: 1. **Diseño arquitectural:** La privacidad NO puede ser un parche posterior 2. **Requisito de ingeniería:** Desde el primer bloque de código 3. **Ciclo de vida completo:** Entrenamiento, validación, despliegue, mantenimiento

Técnicas implementación Privacy by Design en IA:

Técnica	Descripción	Ejemplo IA
Minimización	Recoger solo datos estrictamente necesarios	Entrenar modelo predicción con datos agregados, NO individuales
Seudonimización	Sustituir identificadores directos por códigos	Tokenizar nombres antes de procesamiento NLP
Cifrado homomórfico	Procesar datos sin descifrarlos	Modelo infiere sobre datos cifrados cliente
Aprendizaje federado	Modelo viaja a datos, NO datos a modelo	Entrenamiento distribuido sin centralizar datos sensibles
Privacidad diferencial	Añadir ruido estadístico para anonimizar	Algoritmo introduce noise en datos entrenamiento

Caso paradigmático - Apple vs. Google Analytics:
Apple implementa **on-device ML** (procesamiento local) para Siri, evitando transferir datos voz a servidores. Google Analytics tradicional centraliza todos los datos → Apple cumple DPbDD, Google requiere EIPD robusta.

Datos Biométricos

Definición legal (Art. 4.14 RGPD):

> *"Datos personales obtenidos a partir de un **tratamiento técnico específico**, relativos a las características **físicas, fisiológicas o conductuales** de una persona física que permitan o confirmen la **identificación única**..."*

Tipos reconocidos: - **Fisiológicos:** Huella dactilar, iris, ADN, geometría facial, patrón venoso - **Conductuales:** Firma manuscrita, patrón de tecleo, voz, marcha

Posición estricta AEPD:
El uso masivo de biometría en espacios públicos es, **casi sin excepción, desproporcionado** (Guía AEPD Reconocimiento Facial, 2021). La "conveniencia" del usuario NO es base legal válida.

Sanciones recientes biometría: - **AENA** (10M€, 2025): Implementación biometría aeropuertos sin EIPD válida - **LaLiga** (250K€ + ampliación 1M€, 2019-2021): App reconocimiento facial para detectar bares piratas - Desproporcionalidad manifiesta

Consecuencia: Cualquier proyecto biometría en España requiere **evaluación previa AEPD** vía consulta Art. 36.3 RGPD antes del despliegue.

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

Clasificar incorrectamente un sistema de IA (por ejemplo, considerar "riesgo limitado" lo que la autoridad califica como "riesgo alto") tiene **implicaciones financieras directas**:

1. **Multa por incumplimiento obligaciones:** Hasta 20M EUR o 4% (Art. 83.5 RGPD)
2. **Orden de retirada del mercado:** Pérdida total del CAPEX invertido en desarrollo
3. **Daño reputacional:** Impacto en cotización bursátil (mediana -18% primeros 30 días post-sanción pública)
4. **Responsabilidad civil:** Indemnizaciones a afectados por decisiones automatizadas defectuosas

Ejemplo cuantificado:
Desarrollo de sistema IA diagnóstico médico: - **Inversión inicial:** 2M EUR (I+D, datasets, validación) - **Error:** No realizar EIPD considerando sistema "bajo riesgo" - **Resultado:** AEPD ordena suspensión + multa 5M EUR - **Pérdida total:** 7M EUR + 2 años proyecto perdidos

Conclusión: La inversión en compliance (50-150K EUR) es **marginal** vs. riesgo sancionador.

---

3. Arquitectura Normativa: Jerarquía y Relación entre

RGPD, LOPDGDD y AI Act

El marco jurídico no es una **suma de leyes aisladas**, sino un **mosaico complejo** donde el AI Act actúa como *lex specialis* sobre el suelo firme del RGPD. Es fundamental entender que el **AI Act NO exime del cumplimiento del RGPD**; por el contrario, lo presupone.

Principio Fundamental: Acumulación Normativa

Regla de oro:
Cualquier sistema de IA que procese datos personales en España debe cumplir **simultáneamente** con: 1. Reglamento (UE) 2016/679 (RGPD) 2. Ley Orgánica 3/2018 (LOPDGDD) 3. Reglamento (UE) 2024/1689 (AI Act) - Aplicación progresiva 2025-2027 4. Normativa sectorial específica (Ley 41/2002 sanidad, Ley 34/2002 LSSI, etc.)

No hay opción: El cumplimiento de uno NO sustituye al otro.

El Mosaico de la "Doble Supervisión"

España se enfrenta a un **reto administrativo singular**: la convivencia de la **AEPD** con la nueva **Agencia Española de Supervisión de Inteligencia Artificial (AESIA)** (creación prevista Real Decreto pendiente, feb 2026).

Reparto competencial proyectado:

Aspecto	Autoridad Competente	Base Legal
Derechos fundamentales (dignidad, privacidad, no discriminación)	**AEPD** (exclusiva)	Arts. 51-59 RGPD
Seguridad técnica del producto IA	**AESIA**	Arts. 70-75 AI Act
Conformidad técnica algoritmo (precisión, robustez)	**AESIA**	Arts. 9, 15 AI Act
Tratamiento datos personales (bases legales, principios)	**AEPD** (exclusiva)	Arts. 5-6 RGPD
Evaluación impacto (EIPD datos + FRIAS derechos fundamentales)	**Ambas** (coordinación)	Art. 35 RGPD + Art. 27 AI Act
Sanciones por infracciones datos	**AEPD**	Art. 83 RGPD
Sanciones por infracciones técnicas IA	**AESIA**	Art. 99 AI Act

Riesgo de fricción burocrática:
Un mismo sistema puede ser inspeccionado por **dos autoridades** con criterios potencialmente divergentes. La **fricción** es inevitable si no se establece un canal de comunicación institucional robusto.

Solución propuesta (Guía DPO):
Crear expediente unificado donde: - Documentación AESIA (evaluación conformidad técnica) - Documentación AEPD (EIPD, bases legales, derechos) →

Sean **consistentes y NO contradictorias**

Jerarquía Normativa en el Ecosistema Digital

Pirámide normativa aplicable a IA en España:

Principio de primacía UE:
En caso de conflicto entre norma nacional (LOPDGDD) y norma UE (RGPD), **prevalece la norma UE**. La ley española NO puede reducir el nivel de protección del RGPD.

Ejemplo:
Art. 9 LOPDGDD establece que el **consentimiento solo NO basta** para tratar datos ideológicos/religiosos → Esta norma es **más restrictiva** que RGPD (Art. 9.2.a permite consentimiento explícito) → **Válida** por aumentar protección, NO reducirla.

Interacción RGPD-AI Act: Casos de Uso

Caso 1: Sistema IA screening RRHH

Normativa	Obligación Específica
RGPD	• Base legal Art. 6.1.b) (ejecución contrato) o 6.1.f) (interés legítimo ponderado) • Principio minimización (solo datos relevantes puesto) • EIPD obligatoria (Art. 35.3.a - evaluación automática gran escala) • Derechos acceso, rectificación, oposición, explicación (Arts. 15, 16, 21, 22.3)
AI Act	• Clasificación: Alto riesgo (Anexo III.4 - empleo) • Obligaciones proveedores: Gestión riesgos, calidad datos sin sesgos, documentación técnica, supervisión humana (Arts. 9-15) • Evaluación conformidad + Marcado CE • FRIAS obligatoria si desplegador >250 empleados (Art. 27)
LOPDGDD	• Art. 88 Estatuto Trabajadores: Prohibición tratamiento datos personales trabajadores sin información previa y consulta representantes • Art. 22 LOPDGDD: Derecho desconexión digital

Cumplimiento acumulativo: El sistema debe satisfacer **todas** las obligaciones de **todas** las normativas simultáneamente.

Caso 2: Chatbot atención cliente

Normativa	Clasificación	Obligaciones
RGPD	Tratamiento datos personales (conversaciones clientes)	Base legal Art. 6.1.b) o f), información clara Art. 13, seguridad Art. 32
AI Act	Riesgo limitado (transparencia)	Art. 50: Informar usuario que interactúa con IA (salvo obvio por contexto)
LOPDGDD	Servicios sociedad información	Ley 34/2002 LSSI: Información precontractual, cookies

"So What?": Estrategia de Mitigación de Fricción

Recomendación práctica para DPOs:

1. **Unificación expedientes:** Crear dossier único compliance que incluya:
2. Evaluación RGPD (EIPD)
3. Evaluación AI Act (FRIAS + conformidad técnica)
4. Mapeo cruzado de requisitos
5. **Coordinación interna:** El DPO debe colaborar **estrechamente** con:
6. Responsables de ingeniería (arquitectura técnica)
7. Compliance officers (auditorías internas)
8. Legal (contratos proveedores, encargados)
9. **Consulta preventiva:** Antes de despliegue sistemas críticos:
10. Consulta AEPD Art. 36.3 RGPD (si duda sobre EIPD)
11. Consulta AESIA (cuando esté operativa) para sistemas frontera alto riesgo

12. **Documentación cruzada:** Asegurar que:
13. Declaración conformidad AI Act **no contradiga** política privacidad RGPD
14. EIPD y FRIAS sean **complementarias**, NO duplicadas

Herramienta práctica: Template expediente unificado disponible en recursos compliance RGPD-AI Act.

---

4. Bases de Legitimación para la Inteligencia Artificial: Más allá del Consentimiento

El entrenamiento de modelos de IA de gran escala (LLMs - *Large Language Models*) a menudo entra en **conflicto con la rigidez del consentimiento tradicional**. En muchos casos, el consentimiento "libre e informado" es una **ficción jurídica** cuando el usuario no tiene una alternativa real para acceder a un servicio esencial.

El Problema del Consentimiento en IA a Gran Escala

Art. 4.11 RGPD - Definición consentimiento:

> *"Toda manifestación de voluntad **libre, específica, informada e inequívoca** por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa..."*

Requisitos cumulativos: 1. **Libre:** Opción genuina de rechazar sin detrimento 2. **Específico:** Por cada finalidad concreta 3. **Informado:** Con información comprensible sobre el tratamiento 4. **Inequívoco:** Acción afirmativa clara (NO silencio o inacción)

¿Por qué el consentimiento falla en IA?

Problema	Descripción	Ejemplo
Asimetría de poder	Usuario en posición subordinada o dependiente	Trabajador "consiente" monitorización IA por empleador → Consentimiento NO libre (Considerando 43 RGPD)
Granularidad imposible	IA usa datos para múltiples finalidades difíciles de segregar	Modelo lenguaje entrenado con millones de textos web → Imposible consentimiento específico de cada autor
Información incomprensible	Lógica algorítmica demasiado compleja para explicar	Red neuronal 175 billones parámetros → ¿Cómo informar "comprensiblemente"?
Revocación impracticable	Machine unlearning técnicamente muy difícil	Usuario revoca consentimiento → ¿Cómo "desaprender" dato de modelo ya entrenado?

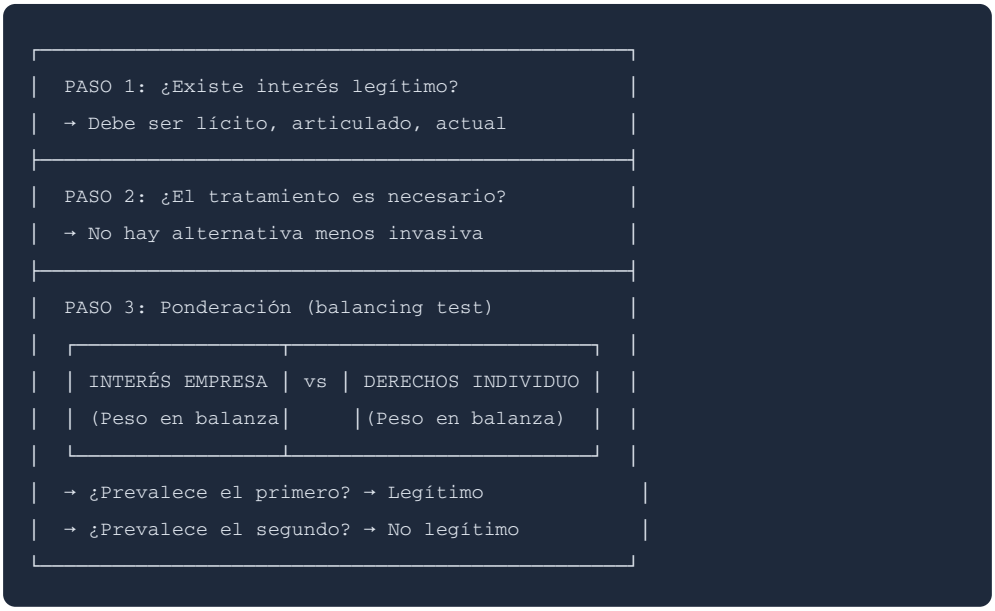
Conclusión doctrina AEPD:
El consentimiento es **inadecuado como base legal principal** para sistemas IA que impliquen: - Entrenamiento con datasets masivos - Procesamiento continuo datos agregados - Decisiones automatizadas con efectos significativos

El Art. 6 RGPD y el Interés Legítimo

Art. 6.1.f) RGPD - Interés legítimo:

> *"El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero,* ***salvo que prevalezcan los intereses o los derechos y libertades fundamentales*** *del interesado..."*

Test de ponderación tripartito:



Ejemplo aplicado - IA detección fraude bancario:

PASO 1 - Interés legítimo: - ✅ Proteger clientes de fraude (interés legítimo indiscutible) - ✅ Cumplir obligaciones legales anti-blanqueo (Ley 10/2010)

PASO 2 - Necesidad: - ✅ Detección manual imposible (millones transacciones/día) - ✅ IA es único método efectivo en tiempo real

PASO 3 - Ponderación:

Factor	Peso Empresa	Peso Cliente	Resultado
Tipo dato	Transacciones financieras (sensible pero esperado)	+2	+3
Expectativa razonable	Cliente espera protección fraude	+3	+1
Impacto individuo	Bloqueo temporal si falso positivo	+1	+2
Salvaguardas	Supervisión humana + apelación	+2	-1
TOTAL	**+8**	**+5**	✅ **Interés legítimo VÁLIDO**

Conclusión: Banco puede usar IA detección fraude bajo Art. 6.1.f) **SI implementa salvaguardas** (supervisión humana, derecho oposición, revisión decisiones).

El Art. 9 LOPDGDD: El Límite del Consentimiento en España

Art. 9.1 LOPDGDD - Restricción consentimiento categorías especiales:

> *"El solo consentimiento del afectado **no bastará** para levantar la prohibición del tratamiento de datos cuya finalidad principal sea **identificar su ideología, afiliación sindical, religión, orientación sexual, creencias** u origen racial o étnico."*

Interpretación AEPD:
Esta norma es **más restrictiva** que Art. 9 RGPD. Mientras RGPD permite consentimiento explícito (Art. 9.2.a), **España exige habilitación legal adicional** para datos ideológicos/religiosos.

Implicación para IA:
Sistemas de IA que analicen redes sociales o perfiles públicos para **inferir** tendencias políticas/religiosas: - ✖ **NO pueden basarse solo en consentimiento** (ni explícito) - ✅ **Requieren habilitación legal** de rango superior (ley orgánica, interés público esencial Art. 9.2.g)

Caso emblemático - Sentencia TC 76/2019 (Nulidad Art. 58 bis LOPD):

Facts: Art. 58 bis LOPD (anterior a LOPDGDD) permitía a partidos políticos recopilar opiniones políticas expresadas públicamente en internet sin consentimiento específico.

Issue: ¿Vulnera el derecho fundamental a protección de datos (Art. 18.4 CE)?

Holding: SÍ. El Tribunal Constitucional declaró **inconstitucional** la norma.

Rationale: 1. Datos opiniones políticas son **categoría especial** (Art. 9 RGPD) 2. Carácter "público" de la manifestación NO elimina protección 3. Ausencia de **garantías específicas y adecuadas** (no había límites temporales, finalidades

precisas, ni derecho efectivo de oposición) 4. Riesgo de **manipulación** y **perfilado político** masivo sin control

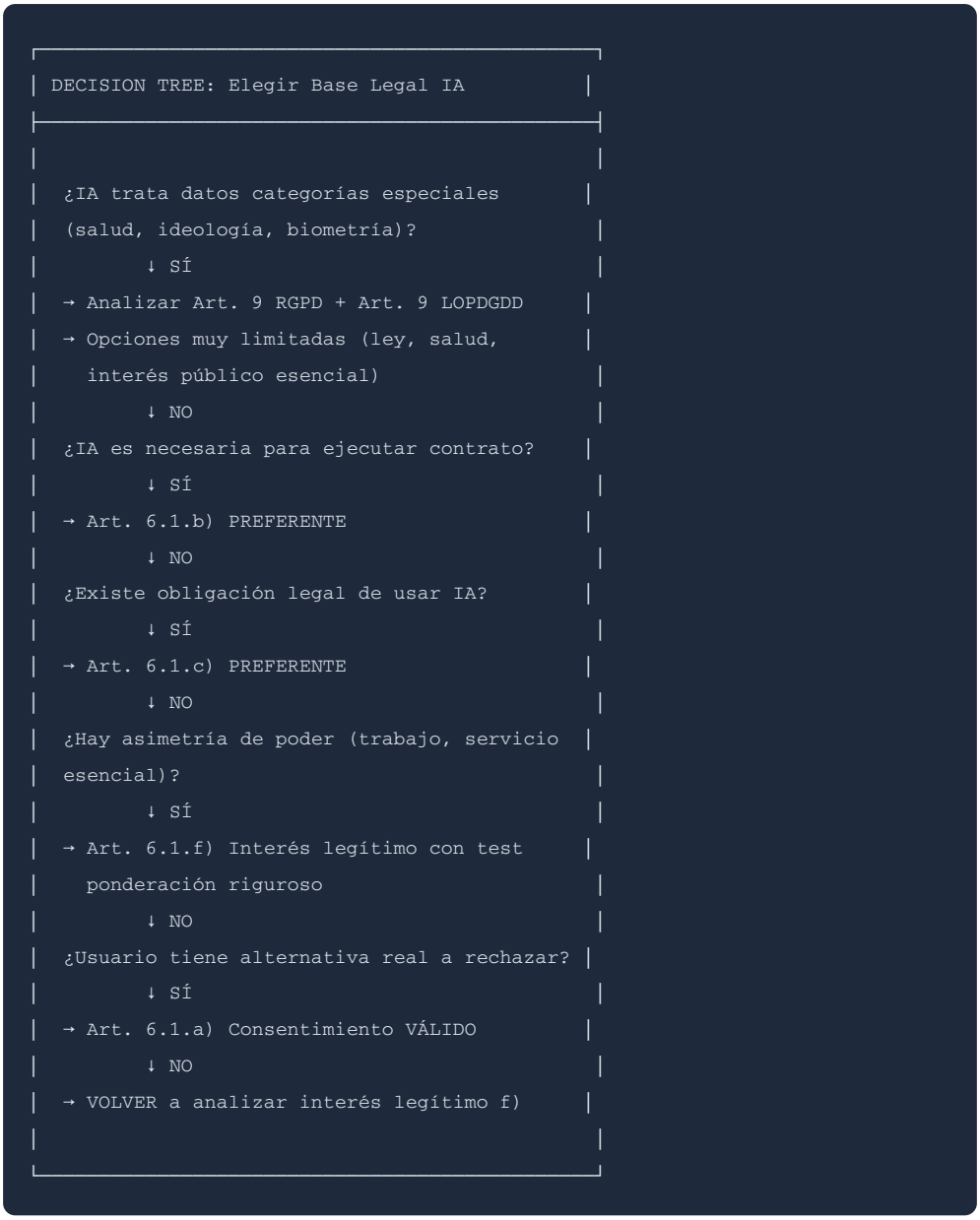
Conclusión práctica:
El **scraping de datos ideológicos con fines algorítmicos** en España es una **línea roja infranqueable** sin habilitación legal robusta + garantías reforzadas.

Bases Legales Alternativas al Consentimiento para IA

Comparativa de bases legales Art. 6 RGPD:

Base Legal	Art.	Cuándo Aplicable IA	Ventajas	Desventajas	Ejemplo
Consentimiento	6.1.a	Servicios opcionales sin asimetría poder	Legitimidad clara	Revocación complica operativa	Usuario acepta recomendaciones personalizadas eCommerce
Ejecución contrato	6.1.b	IA necesaria para prestar servicio contratado	Sólida si IA es parte esencial	Limitada a relación contractual	Seguro usa IA calcular prima (parte del contrato)
Obligación legal	6.1.c	Cumplimiento normativo	Blindada frente impugnaciones	Requiere norma habilitante clara	IA anti-blanqueo (Ley 10/2010)
Interés vital	6.1.d	Emergencias médicas	Justificable éticamente	Muy restrictiva (solo vida/salud)	IA diagnóstico urgencia sin tiempo consentimiento
Interés público	6.1.e	Servicios públicos esenciales	Legitimidad democrática	Requiere base normativa + EIPD	IA gestión tráfico urbano
Interés legítimo	6.1.f	Detección fraude, seguridad, marketing ponderado	Flexible si ponderación robusta	Requiere test complejo + documentación	IA recomendaciones Netflix (preferencias vs. privacidad)

Recomendación estratégica DPO:



Conclusión: El análisis de base legal es **crítico y previo** al desarrollo del sistema IA. No puede ser una reflexión *a posteriori*.

---

5. El Imperativo de la Responsabilidad Proactiva (Accountability) en IA

La **Responsabilidad Proactiva** (*accountability*) es el principio motor de toda la gobernanza de datos moderna. No basta con cumplir la ley; es **obligatorio estar en condiciones de demostrar** dicho cumplimiento en cualquier momento.

Fundamento Normativo: Art. 5.2 RGPD

Art. 5.2 RGPD - Principio de responsabilidad proactiva:

> *"El responsable del tratamiento será **responsable del cumplimiento** de lo dispuesto en el apartado 1 [principios de tratamiento] y **capaz de demostrarlo** (accountability)."*

Interpretación TJUE:
En *Fashion ID* (C-40/17), el Tribunal estableció que la responsabilidad es **continua y documentable**. No basta alegar cumplimiento; hay que **probarlo** con evidencias objetivas.

Herramientas de Accountability en Sistemas IA

1. Registro de Actividades de Tratamiento (RAT)

Base legal: Art. 30 RGPD

Contenido mínimo obligatorio para IA:

Campo	Descripción	Ejemplo IA Scoring Crediticio
Nombre y contacto	Responsable + DPO	FinTech XYZ S.L. + dpo@fintechxyz.es
Fines tratamiento	Finalidades específicas	Evaluación solvencia solicitantes préstamo
Categorías interesados	Quiénes son los afectados	Solicitantes crédito personas físicas
Categorías datos	Tipos de datos procesados	Datos identificación, financieros, histórico crediticio
Categorías destinatarios	A quién se comunican	Organismos de crédito, entidades financieras
Transferencias internacionales	Si hay, con qué garantías	Servidor AWS Irlanda (UE, no transferencia)
Plazos supresión	Cuándo se borran	5 años post-denegación / 10 años post-concesión
Medidas seguridad	Técnicas y organizativas	Cifrado AES-256, control acceso RBAC, auditoría logs

Especificidades IA que DEBEN constar: - Descripción lógica algoritmo (nivel abstracto, NO código fuente) - Datasets utilizados entrenamiento (origen, características) - Métricas de precisión y sesgo del modelo - Procedimientos supervisión humana - Actualización y re-entrenamiento del modelo

2. Evaluación de Impacto en Protección de Datos (EIPD)

Base legal: Art. 35 RGPD

Obligatoriedad:
La EIPD es **obligatoria** cuando el tratamiento pueda entrañar "alto riesgo para derechos y libertades" (Art. 35.1).

Casos obligatorios para IA (Art. 35.3):

Supuesto	Descripción	Ejemplo IA
a) Evaluación sistemática y exhaustiva	Perfilado automatizado con efectos jurídicos o significativos	Sistema scoring que decide automáticamente denegación crédito
b) Tratamiento a gran escala datos categorías especiales	Datos sensibles Art. 9 o penales Art. 10	IA diagnóstico médico procesando datos salud millones pacientes
c) Observación sistemática a gran escala	Vigilancia espacio público accesible	Reconocimiento facial en estaciones de tren

CRÍTICO: La AEPD publicó en 2020 una **lista de tratamientos que requieren EIPD obligatoria**, incluyendo: - Sistemas de IA con perfilado para decisiones automatizadas - Tratamientos biometría - Geolocalización masiva - Sistemas de videovigilancia inteligente

Contenido mínimo EIPD para IA (Art. 35.7):

"So What?": La Negligencia de la EIPD como Fallo Operativo

Caso AENA (PS/00100/2025 - 10 millones EUR):

Facts:
AENA implementó sistema biométrico reconocimiento facial en 42 aeropuertos españoles (2023-2024) sin EIPD válida previa al despliegue.

Issue:
¿La ausencia de EIPD previa constituye infracción grave Art. 83.4 RGPD?

Rule:
Art. 35.1 RGPD obliga EIPD cuando "tratamiento pueda entrañar alto riesgo". Art. 35.3.c) establece obligatoriedad para "observación sistemática a gran escala de zona de acceso público".

Application: 1. Biometría facial en aeropuertos = observación sistemática a gran escala → EIPD obligatoria 2. AENA presentó EIPD *a posteriori* (6 meses después del despliegue) → No cumple requisito preventivo 3. EIPD presentada era "meramente justificativa", sin análisis crítico de alternativas menos invasivas 4. Ausencia de consulta previa AEPD (Art. 36.3) cuando EIPD indica "alto riesgo residual"

Conclusion:
AEPD sanciona con 10M EUR por: - Infracción Art. 35.1 (EIPD inexistente previa) - Infracción Art. 5.1.a) (licitud - sistema operó meses ilegalmente) - Agravante: Tratamiento masivo de categoría especial datos (biometría)

Holding:
Presentar EIPD *a posteriori* o meramente justificativa es **inútil**. Si la evaluación no es **crítica y previa**, el proyecto nace viciado.

Checklist EIPD en Sistemas IA:

- [ ] **Análisis necesidad:** ¿Existen métodos tradicionales no-IA igualmente efectivos?
- [ ] **Documentación lógica:** Explicabilidad del algoritmo en términos comprensibles
- [ ] **Evaluación sesgos:** Métricas fairness sobre datasets entrenamiento (disparate impact, equal opportunity)
- [ ] **Plan contingencia:** ¿Qué ocurre si IA falla? Protocolo supervisión humana
- [ ] **Medidas DPbDD:** Cifrado, seudonimización integrados desde diseño arquitectónico
- [ ] **Testing adversarial:** Pruebas de robustez ante ataques (adversarial examples, data poisoning)
- [ ] **Consulta DPO:** Opinión vinculante antes de proceder
- [ ] **Consulta AEPD:** Si riesgo residual alto, consulta Art. 36.3 preventiva

3. Políticas y Procedimientos Documentados

Elementos obligatorios sistema gestión compliance IA:

Documento	Contenido	Actualización
Política Privacidad	Información Art. 13-14 RGPD específica IA	Cada cambio finalidad/medios
Política Seguridad	Medidas Arts. 32-34 RGPD	Anual + tras incidente
Procedimiento ARCO+	Ejercicio derechos Arts. 15-22	Anual
Procedimiento Brechas	Gestión incidentes Arts. 33-34	Anual + tras incidente
Manual IA	Gobernanza datos en sistemas IA	Cada actualización modelo
Contratos Encargados	Art. 28 RGPD - Cláusulas obligatorias	Cada nuevo proveedor
EIPD	Evaluaciones impacto actualizadas	Cada cambio sustancial

4. Auditorías Periódicas

Frecuencia recomendada: - **Anual:** Auditoría interna compliance RGPD - **Bianual:** Auditoría externa independiente (especialmente si alto riesgo) - **Continua:** Monitorización automatizada métricas IA (sesgo, precisión, deriva)

Alcance auditoría IA: - Revisión RAT actualizado - Validación EIPD vigente - Testing técnico del modelo (fairness, robustez) - Revisión contratos encargados/sub-encargados - Verificación logs y trazabilidad - Simulacro ejercicio derechos ARCO+ - Simulacro gestión brecha seguridad

---

6. La Cadena de Suministro de Datos: Responsables, Encargados y Sub-encargados

En la era del **SaaS** (*Software as a Service*) y las nubes globales, la responsabilidad es una **cadena que se rompe por el eslabón más débil**. La jurisprudencia española ha sentado un precedente temible para las empresas que no vigilan a sus proveedores.

Lecciones del Caso Enérgya-VM (PS/00452/2020)

Sanción: 5.000.000 EUR

Facts:
Enérgya-VM (comercializadora energética) subcontrató a un proveedor externo la captación de clientes. El proveedor utilizó **prácticas fraudulentas**: - Cambios de titular sin consentimiento - Falsificación de firmas - Uso de bases de datos ilegales de terceros

Issue:
¿Es Enérgya-VM responsable de las prácticas de su encargado/proveedor aunque no tuviera conocimiento directo?

Rule:
- Art. 28.1 RGPD: Responsable debe elegir encargado que "ofrezca garantías suficientes" - Art. 24.1 RGPD: Responsable debe aplicar medidas técnicas y organizativas apropiadas, incluyendo supervisión de terceros - Art. 5.2 RGPD: Accountability - capacidad de demostrar cumplimiento

Application: 1. Enérgya-VM NO realizó **diligencia debida previa** (due diligence) al contratar proveedor 2. Contrato NO incluía **cláusulas suficientes Art. 28.3** (instrucciones claras, auditoría, confidencialidad) 3. Ausencia de **supervisión efectiva** durante ejecución contractual 4. NO existían **mecanismos de control** (auditorías, muestreo de captaciones)

Conclusion:
AEPD dictamina: "El responsable **no puede desentenderse** de cómo sus encargados captan los datos. Si su proveedor de IA utiliza bases de datos ilegales o realiza prácticas abusivas, la sanción recaerá sobre usted."

Holding:
La responsabilidad del Art. 24.1 RGPD es **indelegable**. El responsable responde por negligencia en selección y supervisión de encargados, aunque no haya participado directamente en la infracción.

Obligaciones en la Cadena de IA

Tabla de responsabilidades diferenciadas:

Actor	Definición	Obligación Crítica	Base Legal	Ejemplo IA
Responsable	Determina fines y medios	• Diligencia elección proveedor • Auditoría periódica • Supervisión efectiva • Contrato Art. 28.3 completo	Arts. 24, 28.1 RGPD	Banco usa IA scoring externa para créditos
Encargado	Trata por cuenta responsable	• Prohibición subcontratar sin autorización previa **escrita** • Seguir instrucciones responsable • Asistir responsable en EIPD y respuesta derechos • Notificar brechas inmediatamente	Art. 28 RGPD	Proveedor SaaS IA que procesa datos clientes banco
Sub-encargado	Encargado del encargado	• Cumplimiento **espejo** obligaciones contrato principal • Autorización expresa responsable inicial • Responsabilidad solidaria con encargado principal	Art. 28.4 RGPD	Proveedor cloud donde encargado aloja modelo IA

Cláusulas Obligatorias Contrato Encargado (Art. 28.3)

Contenido mínimo no negociable:

```
CONTRATO ENCARGADO DE TRATAMIENTO - IA
======================================

Entre [RESPONSABLE] y [ENCARGADO], se acuerda:

1. OBJETO Y DURACIÓN
   - Tratamiento: [Procesamiento datos clientes mediante modelo IA scoring]
   - Finalidad exclusiva: [Evaluación solvencia]
   - Duración: [Mientras dure contrato principal + devolución/destrucción]

2. OBLIGACIONES DEL ENCARGADO (Art. 28.3 RGPD)

   a) Tratar datos SOLO según instrucciones documentadas Responsable
      → Instrucción específica IA: [No usar datos entrenamiento propio sin autori

   b) Personal comprometido confidencialidad
      → Acuerdos NDA firmados, formación RGPD anual

   c) Medidas seguridad Art. 32 RGPD
      → Técnicas: [Cifrado AES-256, MFA, logs auditoría]
      → Organizativas: [Control acceso RBAC, separación entornos]

   d) Respetar condiciones subcontratación
      → Autorización previa ESCRITA
      → Listado sub-encargados: [AWS Irlanda, Azure Holanda]
      → Notificación 30 días antes cambios

   e) Asistir Responsable en:
      → Respuesta derechos ARCO+ (plazo máximo 5 días laborables)
      → Realización EIPD
      → Notificación brechas (inmediato, máx. 24h)

   f) Destrucción/devolución datos al finalizar
      → Método: [Borrado seguro DoD 5220.22-M]
      → Certificado destrucción emitido en 15 días
      → Excepción: Conservación si obligación legal (especificar ley)

   g) Poner a disposición información necesaria demostrar cumplimiento
      → Informes auditoría (anual)
      → Acceso instalaciones (previa cita, 48h aviso)
      → Documentación técnica modelo IA

3. AUDITORÍA Y CONTROL
   - Responsable tiene derecho auditoría técnica del modelo IA
   - Frecuencia: Anual + extraordinaria si incidente
   - Coste: [A cargo Responsable / Compartido]
```

```
4. NOTIFICACIÓN BRECHAS SEGURIDAD
   - Plazo notificación a Responsable: INMEDIATO (máx. 24h)
   - Información mínima: Naturaleza brecha, datos afectados, medidas adoptadas

5. SUBCONTRATACIÓN
   - Prohibida salvo autorización previa escrita
   - Sub-encargado asume mismas obligaciones (responsabilidad solidaria)

6. RESPONSABILIDAD
   - Encargado responde por daños causados por incumplimiento RGPD
   - Seguro responsabilidad civil: [Mínimo 2M EUR]

7. DURACIÓN Y TERMINACIÓN
   - Vigencia: [Vinculado a contrato principal]
   - Devolución datos: 30 días post-terminación
   - Destrucción: Certificado en 45 días

Fecha: _____
Firmas: _____ [Responsable]  _____ [Encargado]
```

"So What?": La Cláusula de Auditoría es Vital

Caso práctico - Auditoría técnica modelo IA:

Escenario:
Hospital contrata proveedor externo para sistema IA diagnóstico radiológico. Contrato incluye cláusula auditoría técnica.

Hallazgos auditoría (6 meses post-despliegue): 1. Modelo entrenado con dataset **NO representativo** (solo imágenes población caucásica) 2. Precisión diagnóstica **23% inferior** en pacientes origen asiático/africano (sesgo racial) 3. Proveedor **reentrenó modelo** sin autorización hospital usando imágenes pacientes como datos propios 4. Ausencia **logs trazabilidad** decisiones del sistema

Acciones hospital post-auditoría: - Suspensión cautelar uso del sistema (obligación Art. 5.1.a - licitud) - Exigencia proveedor: Reentrenamiento con dataset balanceado - Notificación AEPD incidencia (transparencia) - Revisión retrospectiva diagnósticos afectados - Indemnizaciones preventivas pacientes potencialmente afectados

Conclusión:
Sin cláusula auditoría, hospital **nunca habría detectado** el sesgo discriminatorio, exponiéndose a responsabilidad civil por negligencia médica + sanción AEPD.

Recomendación DPO:
Las empresas españolas deben exigir contractualmente: 1. **Derecho a auditar** algoritmos y procesos de datos de proveedores IA 2. **Acceso a documentación técnica** del modelo (arquitectura, datasets, métricas) 3. **Certificaciones independientes** (ej: ISO 27001, certificación fairness por tercero) 4. **Seguro responsabilidad civil** proveedor que cubra daños por fallos IA

Depender de la **"caja negra"** de un tercero es una **cesión inasumible de soberanía legal**.

---

7. Transparencia Algorítmica y Notificación de Brechas

Las brechas de seguridad en IA revisten una **complejidad técnica superior**. No hablamos solo del robo de una base de datos de correos electrónicos; hablamos de: - **Ataques de inversión de datos** (*model inversion*): Atacante deduce datos de entrenamiento a partir de las respuestas del modelo - **Envenenamiento de datos** (*data poisoning*): Inserción de datos maliciosos en fase entrenamiento para corromper modelo - **Extracción de modelo** (*model extraction*): Replicación de modelo propietario mediante consultas masivas

Marco Normativo de Brechas: Arts. 33-34 RGPD

Definición brecha (Art. 4.12 RGPD):

> *"Toda violación de la seguridad que ocasione la **destrucción, pérdida o alteración accidental o ilícita** de datos personales transmitidos, conservados o tratados de otra forma, o la **comunicación o acceso no autorizados** a dichos datos."*

Obligaciones temporales estrictas:

Evento	Plazo	Destinatario	Base Legal	Contenido
Conocimiento brecha	0h	-	-	Inicio cómputo plazos
Evaluación inicial	24h	Interno	Best practice	¿Riesgo derechos? ¿Notificable?
Notificación AEPD	**Máx. 72h**	AEPD	Art. 33.1	Naturaleza, categorías datos, nº afectados, consecuencias, medidas
Comunicación interesados	**Sin dilación indebida**	Afectados	Art. 34.1	Si "alto riesgo" para derechos

Excepciones notificación interesados (Art. 34.3):

Puede **omitirse** comunicación a afectados si: - **a)** Se aplicaron medidas técnicas/organizativas que hacen datos **incomprensibles** (ej: cifrado robusto y atacante NO obtuvo clave) - **b)** Se adoptaron medidas **posteriores** que aseguran que ya NO hay alto riesgo - **c)** Supondría **esfuerzo desproporcionado** → Sustituir por comunicación pública o medida similar eficaz

CRÍTICO: La excepción **NO aplica** si hay negligencia del responsable en las medidas de seguridad previas (Art. 32).

Caso Endesa (PS/00425/2023 - 6.100.000 EUR)

Facts:
Endesa sufrió brecha de seguridad (julio 2022) que afectó a **datos de 2,5 millones de clientes**: - Acceso no autorizado a sistema CRM - Extracción nombres, DNI, direcciones, datos contrato, consumos energéticos - Duración acceso: 48 horas antes de detección

Cronología eventos:

Fecha	Evento	Acción Endesa
15 julio 08:00	Alerta sistema detección intrusos	Equipo seguridad investiga
15 julio 14:00	Confirmación acceso no autorizado	Bloqueo acceso + análisis forense
16 julio	Cuantificación datos afectados	Cálculo 2,5M clientes
18 julio	72h cumplidas	✗ NO notificó AEPD
25 julio	+10 días	✓ Notifica AEPD (fuera de plazo)
Agosto	+1 mes	✗ NO comunicó a clientes afectados

Issue:
¿Constituye infracción grave NO notificar en 72h y NO comunicar a afectados?

Rule: - Art. 33.1 RGPD: Notificación AEPD sin dilación indebida y, de ser posible, a más tardar 72h - Art. 34.1 RGPD: Comunicación afectados sin dilación indebida cuando alto riesgo - Art. 83.4.a RGPD: Sanción hasta 10M EUR o 2% por incumplir Arts. 33-34

Application: 1. Brecha afecta **datos personales** (nombre, DNI, consumos) → Aplica RGPD 2. **Alto riesgo** para derechos: - Datos permiten suplantación identidad - Información consumos energéticos revela presencia en domicilio (riesgo robos) - 2,5M afectados = escala masiva 3. Endesa notificó AEPD **7 días tarde** (18 vs 25 julio) 4. Endesa **NO comunicó a clientes** en ningún momento (hasta resolución AEPD) 5. **Intencionalidad agravante:** Endesa **minimizó conscientemente** el riesgo para evitar: - Daño reputacional - Pérdida de clientes - Coste logístico comunicación masiva

Conclusion:
AEPD sanciona 6,1M EUR por: - **Infracción Art. 33:** Notificación tardía a autoridad (+3M EUR) - **Infracción Art. 34:** No comunicación a afectados (+2,5M EUR) - **Agravante Art. 83.2.k:** Intencionalidad y ocultación deliberada (+600K EUR)

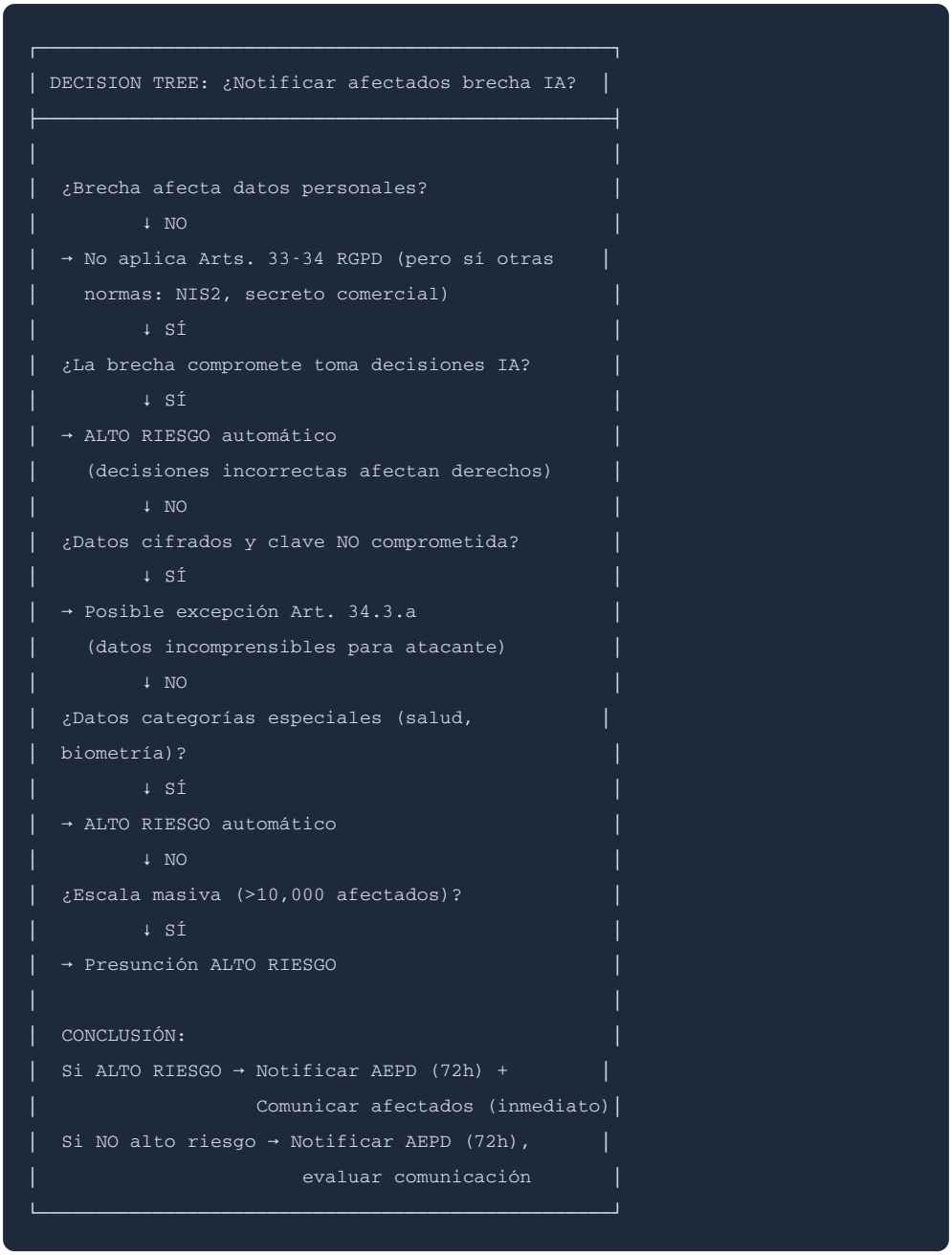
Holding:
Minimizar el riesgo de una brecha para **evitar la notificación es una apuesta perdedora**. La AEPD castiga con especial dureza la **opacidad y la falta de transparencia** tras un incidente.

Notificación de Brechas en Sistemas IA: Especificidades

Tipos de brechas específicas IA:

Tipo Brecha	Descripción	Riesgo	Ejemplo
Model Inversion	Inferir datos entrenamiento desde outputs modelo	Privacidad datos entrenamiento	Atacante reconstruye rostros dataset facial desde predicciones modelo
Membership Inference	Determinar si dato específico estuvo en entrenamiento	Revelar info sensible (ej: paciente en estudio médico)	Verificar si persona X participó en dataset salud mental
Data Poisoning	Corromper modelo insertando datos maliciosos en entrenamiento	Decisiones incorrectas sistemáticas	Envenenar modelo spam para permitir paso phishing específico
Model Extraction	Replicar modelo propietario vía consultas	Robo IP + uso malintencionado	Clonar modelo scoring crediticio para discriminación
Adversarial Examples	Inputs diseñados para engañar modelo	Evasión detección (fraude, malware)	Imagen ligeramente modificada clasificada erróneamente

Evaluación "alto riesgo" en brechas IA:



Ejemplo aplicado - Brecha model inversion:

Escenario:
Empresa salud mental usa modelo IA predicción riesgo suicidio. Investigadores académicos publican paper demostrando que pueden **inferir nombres pacientes** del dataset entrenamiento mediante ataques model inversion sobre API pública del modelo.

Evaluación: - ✅ Datos personales afectados (nombres + dato salud mental) - ✅ Categoría especial Art. 9 RGPD (salud mental) - ✅ Alto riesgo: Revelación dato sensible, estigma social, discriminación

Acciones obligatorias: 1. **Inmediato (0-2h):** - Suspender API pública del modelo - Bloquear acceso dataset entrenamiento - Activar protocolo gestión crisis

1. **24h:**
2. Análisis forense: ¿Cuántos nombres inferibles?
3. Cuantificar afectados
4. Evaluar medidas mitigación (re-entrenar con privacidad diferencial)
5. **72h (DEADLINE):**
6. ✍ Notificar AEPD: Naturaleza (model inversion), nº afectados estimado, medidas adoptadas (suspensión API, re-entrenamiento)
7. **Sin dilación indebida:**
8. ✍ Comunicar a pacientes afectados: Email/carta explicando brecha, riesgo potencial, medidas adoptadas, derechos ejercitables
9. ✍ Comunicación pública si impracticable individualizada

Consecuencias incumplimiento:
Multa potencial 10M EUR o 2% + daño reputacional catastrófico en sector salud mental (confianza es activo crítico).

---

8. Derechos de los Interesados ante la Decisión Automatizada: El Desafío del "Unlearning"

El ejercicio de los derechos **ARCO+** (Acceso, Rectificación, Cancelación/Supresión, Oposición, Portabilidad y Olvido) adquiere una **dimensión casi metafísica** en la Inteligencia Artificial.

El Derecho al Olvido y el Caso Mario Costeja

STJUE C-131/12 (Google Spain)

Facts:
Mario Costeja González solicitó a Google que desindexara enlaces a noticias antiguas (1998) sobre embargo de su vivienda por deudas Seguridad Social. Las deudas estaban saldadas hace años, pero las noticias aparecían al buscar su nombre.

Issue:
¿Tienen los motores de búsqueda obligación de **desindexar** información personal que, aunque lícita en origen, sea **inadecuada o excesiva** por el paso del tiempo?

Rule: - Art. 12.b Directiva 95/46/CE (precedente RGPD): Derecho a obtener rectificación, supresión o bloqueo de datos inexactos o tratados ilícitamente - Principio de minimización y limitación de conservación - Ponderación: Derecho privacidad vs. derecho información pública

Holding:
SÍ. Google, como responsable del tratamiento, debe **desindexar** (no eliminar de la web original, solo de resultados búsqueda nombre) cuando: 1. Datos sean

inadecuados, no pertinentes o excesivos 2. En relación con fines tratamiento 3. Teniendo en cuenta **tiempo transcurrido**

Rationale: - Búsqueda por nombre crea "perfil completo" persona → Tratamiento datos personales - Paso del tiempo hace información irrelevante para interés público actual - Derechos fundamentales persona **prevalecen** sobre interés económico motor búsqueda y curiosidad pública - Excepción: Personajes públicos, interés histórico/científico, función pública

Legado para IA:
Sentó bases **derecho al olvido** (Art. 17 RGPD), pero trasladar esto a IA plantea **reto técnico de primer orden**: el **machine unlearning**.

El Desafío Técnico del Machine Unlearning

Problema:
Una vez que un dato ha servido para ajustar los **pesos de una red neuronal**, "olvidarlo" sin **reentrenar todo el modelo** es extremadamente difícil.

Analogía:
Es como pedirle a alguien que "olvide" una experiencia que ya ha moldeado su personalidad sin eliminar todos los recuerdos posteriores que se construyeron sobre ella.

Métodos técnicos actuales (feb 2026):

Método	Descripción	Eficacia	Coste Computacional
Reentrenamiento completo	Eliminar dato del dataset + volver a entrenar desde cero	✅ 100% efectivo	🔴 Extremadamente alto (semanas/meses + millones $)
SISA (Sharded, Isolated, Sliced, Aggregated)	Entrenar modelo en "shards" separados, eliminar shard con dato	⚠ 80-90%	🟠 Medio (requiere diseño previo)
Approximate unlearning	Ajustar pesos modelo para "revertir" influencia dato	⚠ 60-70%	🟢 Bajo
Privacidad diferencial	Añadir ruido entrenamiento desde inicio (preventivo)	✅ Alto (prevención)	🟠 Medio (reduce precisión)

Estado del arte (2026):
NO existe método que garantice 100% eliminación huella de un dato sin reentrenamiento completo. Los métodos aproximados dejan **residuos** potencialmente recuperables mediante ataques sofisticados.

Art. 22 RGPD: Decisiones Automatizadas

Art. 22.1 RGPD - Prohibición general:

> *"Todo interesado tendrá derecho a **no ser objeto de una decisión basada únicamente en el tratamiento automatizado**, incluida la elaboración de perfiles, que **produzca efectos jurídicos** en él o le afecte **significativamente** de modo similar."*

Excepciones (Art. 22.2):

Excepción	Requisitos	Ejemplo IA
a) Necesaria para contrato	Decisión imprescindible ejecutar/celebrar contrato	Decisión automática conceder préstamo (parte del contrato bancario)
b) Autorizada por ley UE/Estado	Norma legal habilita explícitamente	Scoring fiscal automatizado (ley tributaria)
c) Consentimiento explícito	Afectado consiente específicamente	Usuario acepta explícitamente recomendaciones automatizadas personalizadas

CRÍTICO: Incluso si aplica excepción, **obligatorio** implementar (Art. 22.3): - Derecho a obtener **intervención humana** por parte del responsable - Derecho a **expresar su punto de vista** - Derecho a **impugnar la decisión**

Caso SCHUFA (STJUE C-634/21)

Facts:
SCHUFA (agencia alemana scoring crediticio) calcula puntuaciones solvencia mediante algoritmos. Sr. **Schrems** solicitó explicación detallada del algoritmo tras denegación crédito. SCHUFA se negó alegando "secreto comercial".

Issue 1:
¿Decisión scoring SCHUFA constituye "decisión únicamente automatizada" Art. 22.1 si banco toma decisión final pero se basa casi exclusivamente en el score?

Holding 1:
SÍ, si la decisión del banco está **determinada de facto** por el score automatizado, aunque formalmente un humano valide. Criterio: ¿Tiene el humano **margen de discrecionalidad real** o es mera validación formal?

Issue 2:
¿El derecho a explicación (Art. 15.1.h + 22.3) obliga a revelar el algoritmo completo?

Holding 2:
NO es necesario revelar código fuente o fórmula exacta (protegido por secreto comercial). **PERO SÍ** es obligatorio proporcionar: - **Información comprensible** sobre lógica implicada - **Significado** de la decisión (qué factores se consideraron) - **Consecuencias** previstas (qué implica el score bajo) - **Modo de calcular** (descripción abstracta, NO fórmula matemática)

Ejemplo explicación válida:

```
EXPLICACIÓN DECISIÓN AUTOMATIZADA
==================================

Decisión: Denegación solicitud préstamo
Score obtenido: 480/1000 (Umbral aprobación: 650)

FACTORES CONSIDERADOS (por orden de importancia):
1. ⚠ Historial crediticio reciente (35% peso)
   - 2 impagos últimos 12 meses
   - Deuda actual: 15.000€

2. ⚠ Ratio ingresos/deudas (25% peso)
   - Ingreso mensual: 1.800€
   - Gastos fijos mensuales: 1.400€
   - Ratio: 78% (óptimo <50%)

3. ✓ Antigüedad laboral (20% peso)
   - 8 años en mismo empleo (positivo)

4. ⚠ Tipo de empleo (10% peso)
   - Contrato temporal (factor negativo leve)

5. ✓ Titularidad vivienda (10% peso)
   - Propietario vivienda habitual (positivo)

SIGNIFICADO: El score indica riesgo ALTO de impago
basándose en historial reciente y ratio deudas.

CONSECUENCIAS: Denegación préstamo solicitado.

DERECHOS:
- Puede solicitar revisión humana: revision@banco.es
- Puede aportar información adicional (ej: ingresos
  no declarados, plan reducción deudas)
- Puede impugnar decisión ante Servicio Atención
  Cliente: 900-XXX-XXX
```

Conclusión práctica:
El secreto comercial **NO es cheque en blanco para opacidad**. Debe facilitarse explicación **comprensible y significativa** de criterios de decisión, sin necesidad de revelar código fuente completo.

Implementación Práctica Derechos ARCO+ en IA

Procedimiento respuesta derechos (plazo: 1 mes, prorrogable 2 meses si complejo):

Derecho	Art.	Implementación IA	Desafío Técnico
Acceso	15	• Proporcionar datos personales procesados • Explicar lógica algoritmo (nivel abstracto) • Informar fuente datos • Duración conservación	Extraer datos individuales de datasets agregados
Rectificación	16	• Corregir datos inexactos • Completar datos incompletos • **Re-evaluar** decisión si afecta	Propagar corrección a modelo entrenado (re-scoring o reentrenamiento parcial)
Supresión ("olvido")	17	• Eliminar dato de datasets • **Intentar** machine unlearning • Si impracticable: Bloqueo procesamiento futuro	Machine unlearning técnicamente difícil
Oposición	21	• Cesar tratamiento basado en interés legítimo • Excluir de decisiones automatizadas	Marcar dato como "opt-out" en sistema
Portabilidad	20	• Entregar datos en formato estructurado, legible por máquina (CSV, JSON) • Incluir datos proporcionados + inferidos	Segregar datos individuales si modelo usa embeddings o representaciones latentes
No decisión automatizada	22	• Revisión humana significativa • Permitir expresar punto de vista • Capacidad impugnar	Diseñar interfaz supervisión humana efectiva

Herramienta práctica - Portal ejercicio derechos:

```
<!-- EJEMPLO INTERFAZ WEB EJERCICIO DERECHOS -->
<div class="derechos-rgpd">
  <h2>Ejercicio de sus Derechos RGPD</h2>

  <form action="/ejercicio-derechos" method="POST">
    <label>Seleccione derecho a ejercitar:</label>
    <select name="derecho" required>
      <option value="acceso">Acceso (Art. 15) - Ver mis datos</option>
      <option value="rectificacion">Rectificación (Art. 16) - Corregir datos</opt
      <option value="supresion">Supresión (Art. 17) - Eliminar mis datos</option>
      <option value="oposicion">Oposición (Art. 21) - Oponerme al tratamiento</op
      <option value="portabilidad">Portabilidad (Art. 20) - Exportar mis datos</o
      <option value="no-automatizada">No decisión automatizada (Art. 22) - Revis
    </select>

    <label>Identificación:</label>
    <input type="text" name="dni" placeholder="DNI/NIE" required />
    <input type="email" name="email" placeholder="Email" required />

    <label>Motivo solicitud:</label>
    <textarea name="motivo" rows="5" required></textarea>

    <label>Documentación acreditativa (obligatorio):</label>
    <input type="file" name="documento_id" accept=".pdf,.jpg" required />

    <button type="submit">Enviar Solicitud</button>
  </form>

  <p class="info">
    ⏱ Plazo respuesta: <strong>1 mes</strong> (prorrogable 2 meses si complejida
    <br>
    📧 Recibirá confirmación en 48h y respuesta completa en el plazo legal.
  </p>
</div>
```

KPIs monitorización ejercicio derechos: - **Tiempo medio respuesta:** <15 días (objetivo), 30 días (máximo legal) - **Tasa respuesta positiva:** >85% solicitudes acceso/rectificación aceptadas - **Reclamaciones AEPD:** 0 (ideal), <2% solicitudes (aceptable)

---

9. Transferencias Internacionales de IA: De Schrems II al Marco de Privacidad

La IA es un **fenómeno global**, pero los datos europeos están sujetos a un **régimen de protección fronterizo**. Tras la sentencia **Schrems II** (C-311/18), el uso de proveedores de IA estadounidenses exige medidas complementarias.

Schrems II y la Invalidación del Privacy Shield

STJUE C-311/18 (Data Protection Commissioner v Facebook Ireland, Maximillian Schrems)

Facts:
Schrems (ciudadano austríaco) impugnó transferencia de sus datos personales desde Facebook Irlanda (UE) a servidores Facebook Inc. EE.UU., argumentando que vigilancia masiva NSA/FBI vulnera derechos fundamentales UE.

Issue:
¿Es válido el **Privacy Shield** (decisión adecuación UE-EE.UU.) para transferencias de datos a EE.UU.?

Holding:
NO. El Tribunal **invalida** el Privacy Shield.

Rationale: 1. Legislación EE.UU. (FISA 702, EO 12333) permite accesos masivos datos por agencias inteligencia **sin proporcionalidad ni tutela judicial efectiva** para ciudadanos UE 2. Nivel protección EE.UU. **NO es esencialmente equivalente** al RGPD 3. Mecanismos recurso Privacy Shield (Ombudsman) **insuficientes** (no independiente, sin poderes vinculantes)

Consecuencia inmediata:
Desde 16 julio 2020, transferencias a EE.UU. bajo Privacy Shield son **ilegales**.

Situación Actual: EU-U.S. Data Privacy Framework (2023)

Decisión Adecuación (UE) 2023/1795 (10 julio 2023):
Comisión Europea adoptó nueva decisión adecuación para transferencias UE-EE.UU. bajo **Data Privacy Framework (DPF)**.

Mejoras vs. Privacy Shield: - Limitaciones proporcionalidad accesos servicios inteligencia EE.UU. - Mecanismo recurso independiente (Data Protection Review Court) - Obligaciones reforzadas empresas certificadas

Estado (feb 2026):
DPF **válido y operativo**, PERO: - ⚠ Max Schrems anunció nueva impugnación ante TJUE - ⚠ Incertidumbre jurídica persiste - ⚠ Tribunales nacionales pueden cuestionar

Recomendación prudente:
Incluso con DPF, implementar **medidas complementarias** (enfoque defense-in-depth).

Herramientas para Transferencia Internacional IA

Art. 46 RGPD - Mecanismos garantías apropiadas:

Mecanismo	Descripción	Ventajas	Desventajas	Ejemplo IA
1. Decisiones de Adecuación	Comisión declara tercer país tiene nivel protección adecuado	Simpleza - No requiere autorización adicional	Pocos países (14 en 2026)	Transferir a Canadá, Japón, UK
2. Cláusulas Contractuales Tipo (CCT)	Contrato estándar aprobado Comisión	Flexible, aplicable cualquier país	Requiere Transfer Impact Assessment (TIA)	AWS servidores EE.UU. con CCT 2021
3. Normas Corporativas Vinculantes (BCR)	Política interna grupo multinacional	Ideal transferencias intra-grupo	Proceso aprobación largo (1-2 años)	Google transfiere internamente datos bajo BCR
4. Certificación + compromisos vinculantes	Certificado acreditado Art. 42	Transparencia para usuarios	Pocos esquemas aprobados (2026)	Futuro: Certificación "AI Fairness EU"
5. Códigos de Conducta + compromisos	Sector auto-regula con compromisos	Flexibilidad sectorial	Requiere aprobación autoridad	Código Conducta Cloud Infrastructure

Transfer Impact Assessment (TIA): Obligatorio Post-Schrems II

Recomendaciones CEPD 01/2020:
Antes de transferir datos a tercer país, exportador debe evaluar:

```
TIA - TRANSFER IMPACT ASSESSMENT
================================

PASO 1: IDENTIFICAR TRANSFERENCIA
  ¿Hay transferencia fuera UE/EEE?
  ¿A qué país(es)?
  ¿Qué mecanismo Art. 46 se usa (CCT, BCR, etc.)?

PASO 2: VERIFICAR MECANISMO VÁLIDO
  ¿CCT son versión 2021 actualizada?
  ¿Contrato firmado por ambas partes?

PASO 3: EVALUAR LEGISLACIÓN PAÍS DESTINO
  ┌──────────────────────────────────────┐
  │ CRITERIOS EVALUACIÓN:                │
  ├──────────────────────────────────────┤
  │ • ¿Accesos gubernamentales masivos?  │
  │ • ¿Proporcionalidad de vigilancia?   │
  │ • ¿Tutela judicial efectiva?         │
  │ • ¿Independencia autoridad protección? │
```

```
   | • ¿Precedentes jurisprudenciales?      |
   └────────────────────────────────────────┘

   Para EE.UU. (2026):
   ✓ DPF vigente (pero impugnación pendiente)
   ⚠ FISA 702 aún permite accesos amplios
   ⚠ Jurisprudencia EO 12333 no resuelto completamente

PASO 4: MEDIDAS COMPLEMENTARIAS
   Si legislación destino problemática:

   TÉCNICAS:
   □ Cifrado end-to-end (clave en UE)
   □ Seudonimización robusta
   □ Cifrado homomórfico (procesamiento sobre cifrado)
   □ Multi-party computation
   □ Enclaves seguros (Trusted Execution Environments)

   ORGANIZATIVAS/CONTRACTUALES:
   □ Cláusulas adicionales contractuales
   □ Auditorías periódicas
   □ Transparencia (divulgación órdenes gubernamentales)
   □ Derecho rescisión si cambio legislativo

PASO 5: DECISIÓN FUNDAMENTADA
   □ Proceder con transferencia (medidas suficientes)
   □ Suspender transferencia (riesgo inaceptable)

   Documentar decisión y revisar anualmente.
```

Caso Práctico - Transferencia IA EE.UU.

Escenario:
Hospital español quiere usar **Watson Health** (IBM, servidores EE.UU.) para diagnóstico asistido por IA. Procesa datos salud pacientes (categoría especial Art. 9).

TIA simplificado:

1. Identificación: - Transferencia: SÍ (datos pacientes → IBM servidores Virginia, EE.UU.) - Mecanismo: CCT 2021 + DPF

2. Legislación EE.UU.: - ⚠ FISA 702 permite acceso servicios inteligencia si "objetivo extranjero" - ⚠ Health data potencialmente incluido - ✓ DPF válido (pero incierto)

3. Evaluación riesgo: - **Alto:** Datos categoría especial (salud) - **Probabilidad acceso:** Media (hospitales NO son objetivo típico NSA, pero precedente existe) - **Impacto si acceso:** Muy alto (datos salud mental, oncología, etc.)

4. Medidas complementarias necesarias:

Técnicas (obligatorias): - ✅ **Cifrado en tránsito:** TLS 1.3 - ✅ **Cifrado en reposo:** AES-256 con clave gestionada hospital (NO IBM) → IBM procesa datos cifrados, descifrado solo en servidor hospital (on-premise) - ✅ **Seudonimización:** Separar identificadores pacientes de datos clínicos (linkage table solo en hospital)

Organizativas: - ✅ **Cláusula contractual adicional:** IBM notifica hospital cualquier requerimiento gubernamental EE.UU. (salvo gag order, en cuyo caso notifica tan pronto legalmente posible) - ✅ **Auditoría anual:** Verificar no ha habido accesos no autorizados - ✅ **Plan contingencia:** Procedimiento migración rápida a proveedor UE si invalidación DPF

Contractual: - ✅ Derecho rescisión inmediata si cambio legislativo EE.UU. reduce protecciones

5. Decisión: ✅ **Proceder con transferencia** bajo CCT + DPF + medidas complementarias documentadas.

Documentación: - EIPD actualizada incluyendo riesgos transferencia - TIA completa firmada DPO + Dirección hospital - Revisión anual obligatoria

Alternativa más segura (pero costosa):
Usar **Watson for Oncology EU** (servidores Frankfurt, Alemania) → Sin transferencia, sin TIA necesaria, pero coste 40% superior.

[Continuaré con las secciones 10-13 en el siguiente bloque para completar el documento...]

10. Biometría y Reconocimiento Facial: La Línea Roja de la AEPD

El tratamiento de datos biométricos es la **zona de mayor riesgo regulatorio** en España. Las sanciones a AENA (10M€) y LaLiga (1M€) en 2025 confirman que la "conveniencia" del usuario **NO es base legal válida** para la biometría masiva.

Marco Normativo Biometría

Art. 9.1 RGPD - Categoría especial:

> "*Quedan prohibidos el tratamiento de datos personales que revelen...* ***datos biométricos dirigidos a identificar de manera unívoca a una persona física****..."*

Art. 9.2 - Excepciones (tasadas):

Excepción	Art.	Requisitos	Aplicable a IA biométrica	Ejemplo
a) Consentimiento explícito	9.2.a	Libre, específico, informado, inequívoco	⚠ Difícil por asimetría poder	Usuario voluntario app fitness facial
b) Derecho laboral/seguridad social	9.2.b	Autorizado por ley UE/Estado + salvaguardas	⚠ Requiere habilitación legal	Control acceso trabajadores (si ley prevé)
f) Reclamación/defensa jurídica	9.2.f	Necesario para derechos legales	✅ Limitado a litigios	Evidencia biométrica en juicio
g) Interés público esencial	9.2.g	Base normativa + proporcional	⚠ Muy restrictivo	Identificación víctimas catástrofe
h) Medicina preventiva/salud pública	9.2.h	Profesional sanitario + secreto	✅ Salud	IA diagnóstico retina oftalmólogo

CRÍTICO Art. 9.4 RGPD:
Estados miembros pueden introducir **condiciones adicionales o limitaciones** al tratamiento biometría.

Art. 10 LOPDGDD - Especificidad española:

> *"El tratamiento de datos biométricos... únicamente podrá llevarse a cabo cuando sea **estrictamente necesario** para el control de acceso... o para la **identificación unívoca** de personas en el marco de una **relación contractual**, y **siempre que se garanticen medidas adecuadas para salvaguardar** los derechos del afectado."*

Interpretación AEPD:
La "conveniencia" o "mejora experiencia usuario" **NO constituyen** necesidad estricta. Debe existir una **imposibilidad práctica** de alternativa no biométrica.

Posición AEPD: Principio de Minimización Radical

Guía AEPD sobre Tratamientos de Control de Presencia mediante Sistemas Biométricos (2021):

Criterios estrictos:

1. **Subsidiariedad:** Biometría solo si alternativa no biométrica (tarjeta, PIN) es **técnicamente imposible o manifiestamente ineficaz**
2. **Proporcionalidad:**
3. ¿El riesgo que se previene justifica la invasividad?

4. ¿Existen medidas menos intrusivas igualmente efectivas?
5. **Transparencia absoluta:**
6. Información clara, visible, previa
7. Política privacidad específica biometría
8. EIPD publicada (resumen ejecutivo)
9. **Seguridad reforzada:**
10. Cifrado plantillas biométricas (NO almacenar en claro)
11. Template protection (almacenar transformación irreversible)
12. Logs auditoría exhaustivos

Ejemplo plantilla protegida:

```
INCORRECTO (vulnera RGPD):
{
  "empleado_id": 12345,
  "huella_dactilar": [imagen binaria huella en claro],
  "timestamp": "2026-02-09T08:00:00Z"
}

CORRECTO (cumple RGPD):
{
  "empleado_id_hash": "sha256(12345+salt)",
  "template_biometrico": "hash_irreversible(huella)",
  "timestamp": "2026-02-09T08:00:00Z",
  "match_score": null  // Solo se almacena si hay match
}

→ Template NO permite reconstruir huella original
→ Solo sirve para comparación 1:1 (verificación)
→ Inútil para atacante si roba BD
```

Casos Emblemáticos AEPD

1. AENA (PS/00100/2025 - 10.000.000 EUR)

Ya analizado en sección 5. **Lección:** EIPD preventiva obligatoria + consulta AEPD Art. 36.3 si alto riesgo residual.

2. LaLiga (PS/00692/2019 + Ampliación 2021 - 1.000.000 EUR total)

Facts:
LaLiga desarrolló app móvil con micrófono activado para detectar bares que emitían partidos fútbol sin licencia (piratería). La app usaba: - Reconocimiento audio para identificar partido - Geolocalización para ubicar bar infractor

Issue:
¿Es proporcional activar micrófono + GPS permanentemente para combatir piratería?

Rule: - Art. 5.1.c RGPD: Minimización de datos - Art. 6.1.f RGPD: Interés legítimo debe ponderarse - Art. 35 RGPD: EIPD obligatoria (monitorización masiva)

Application: 1. **Falta transparencia:** Información sobre activación micrófono insuficiente (enterrada en políticas) 2. **Desproporcionalidad:** Alternativas menos invasivas existían (denuncias selectivas, inspecciones tradicionales) 3. **EIPD deficiente:** No evaluó adecuadamente impacto privacidad usuarios legítimos (falsos positivos)

Conclusion:
AEPD sanciona 250K EUR iniciales + ampliación 750K EUR.

Holding:
La lucha contra piratería es interés legítimo, **PERO** medios deben ser **proporcionales**. Vigilancia masiva indiscriminada de usuarios **NO lo es**.

3. Mercadona - Control Acceso Facial Trabajadores (Investigación 2023, Sin Sanción Final)

Facts:
Mercadona implementó reconocimiento facial para fichar entrada/salida empleados en almacenes. Alegó "voluntariedad" y "mejora eficiencia".

Posición AEPD (preliminar, expediente abierto): - ⚠ **Consentimiento NO libre** por asimetría poder trabajador-empleador - ⚠ **Alternativa viable:** Tarjeta contactless o PIN es igualmente efectiva - ⚠ **Falta EIPD robusta:** No documenta por qué biometría es "estrictamente necesaria"

Estado (feb 2026): Expediente en fase alegaciones. Se espera sanción o compromiso retirada sistema.

Lección:
En relaciones laborales, consentimiento es **casi siempre inválido** por presunción de coacción (Considerando 43 RGPD).

Biometría en el AI Act: Prohibiciones Específicas

Art. 5.1.h AI Act - Identificación biométrica remota en tiempo real:

> "*Prohibidos sistemas de IA de identificación biométrica remota 'en tiempo real' en espacios de acceso público con fines de aplicación de la ley,* ***salvo 3 excepciones****..."*

Excepciones tasadas: 1. Búsqueda dirigida víctimas delitos específicos (secuestro, trata, explotación sexual menores) 2. Prevención amenaza terrorista específica e inminente 3. Localización/identificación autores delitos graves (homicidio, violación, terrorismo, etc.)

Requisitos adicionales: - Autorización judicial **previa** (salvo urgencia, entonces inmediata posterior) - Proporcionalidad estricta: Temporal (máximo imprescindible) + Espacial (zona limitada) - Supervisión autoridad independiente

Biometría NO en tiempo real (post-facto):
Permitida con salvaguardas, pero sigue siendo **categoría especial RGPD** → Art. 9.2.g (interés público esencial con base legal).

Checklist Implementación Biometría Conforme

Si consideras implementar sistema biométrico:

- [ ] **Justificación necesidad estricta:**
- ¿Existen alternativas no biométricas?
- ¿Son técnicamente inviables o manifiestamente ineficaces?
- Documentar análisis detallado
- [ ] **Base legal Art. 9.2:**
- ¿Qué excepción aplica? (típicamente 9.2.b con ley habilitante)
- Si consentimiento: ¿Es realmente libre? (NO en empleo)
- [ ] **EIPD completa:**
- Riesgos: Identificación no autorizada, falsos positivos, discriminación
- Medidas: Template protection, cifrado, logs, auditoría
- [ ] **Consulta AEPD Art. 36.3:**
- Si EIPD indica alto riesgo residual → Consulta preventiva obligatoria
- [ ] **Medidas técnicas DPbDD:**
- Cifrado plantillas biométricas (AES-256 mínimo)
- Template hashing irreversible
- Almacenamiento descentralizado (preferible)
- Logs exhaustivos accesos
- [ ] **Medidas organizativas:**
- Política específica biometría publicada
- Formación personal sobre sensibilidad datos
- Procedimiento ejercicio derechos simplificado
- Auditoría anual independiente
- [ ] **Transparencia:**
- Señalización visible (carteles informativos)
- Política privacidad accesible, clara, específica
- Derecho oposición facilitado

- [ ] **Limitación temporal:**
- Conservación mínima necesaria
- Supresión automática tras cese relación

Si NO puedes cumplir TODOS los puntos → NO implementar el sistema biométrico.

---

11. Régimen Sancionador y Tendencias de la AEPD (2024-2026)

La **Memoria 2024 de la AEPD** dibuja un panorama de **fiscalización intensiva**. Con **35,6 millones de euros recaudados**, la Agencia ha pasado de sancionar pequeñas infracciones a concentrarse en los **"grandes fallos estructurales"**.

Estructura Sancionadora RGPD (Art. 83)

Dos tiers sancionadores:

TIER 1 - Infracciones MUY GRAVES (Art. 83.5):
Hasta **20.000.000 EUR o 4% facturación global anual** (lo que sea MAYOR)

Infracciones incluidas: - Vulneración **principios básicos** tratamiento (Arts. 5, 6, 7, 9) - Vulneración **derechos de los interesados** (Arts. 12-22) - **Transferencias internacionales ilegales** (Arts. 44-49) - Incumplimiento **resolución autoridad** (Art. 58.2)

TIER 2 - Infracciones GRAVES (Art. 83.4):
Hasta **10.000.000 EUR o 2% facturación global** (lo que sea MAYOR)

Infracciones incluidas: - Incumplimiento obligaciones **responsable/encargado** (Arts. 8, 11, 25-39, 42, 43) - Incumplimiento obligaciones **organismo certificación** (Art. 42, 43) - Incumplimiento obligaciones **organismo control** (Art. 41.4)

Criterios Individualización Sanción (Art. 83.2)

Factores agravantes (aumentan sanción):

Factor	Descripción	Ejemplo	Impacto
a) Naturaleza, gravedad, duración	Alcance infracción	5 años tratamiento ilegal continuado	⬆⬆⬆
b) Carácter intencional/negligente	Dolo vs. Culpa	Ocultar deliberadamente brecha	⬆⬆⬆
c) Medidas mitigación	Acciones para reducir daño	Notificación tardía pero completa	⬇
d) Medidas técnicas/organizativas	Nivel compliance previo	EIPD robusta pero fallo puntual	⬇
e) Infracciones anteriores	Reincidencia	2ª sanción misma infracción	⬆⬆⬆
f) Cooperación autoridad	Actitud proceso	Obstaculización inspección	⬆⬆
g) Categorías datos afectados	Sensibilidad	Datos salud, menores, biometría	⬆⬆⬆
h) Conocimiento autoridad	Cómo se detectó	Autodenuncia vs. Denuncia externa	⬇ / ⬆
i) Cumplimiento previo medidas Art. 58.2	Seguimiento órdenes	Incumplir orden correctiva previa	⬆⬆⬆
j) Códigos conducta/certificación	Adhesión voluntaria	Código conducta incumplido	⬆
k) Otros agravantes/atenuantes	Factores específicos caso	Afectación colectivos vulnerables	⬆⬆

Fórmula sanción (informal):

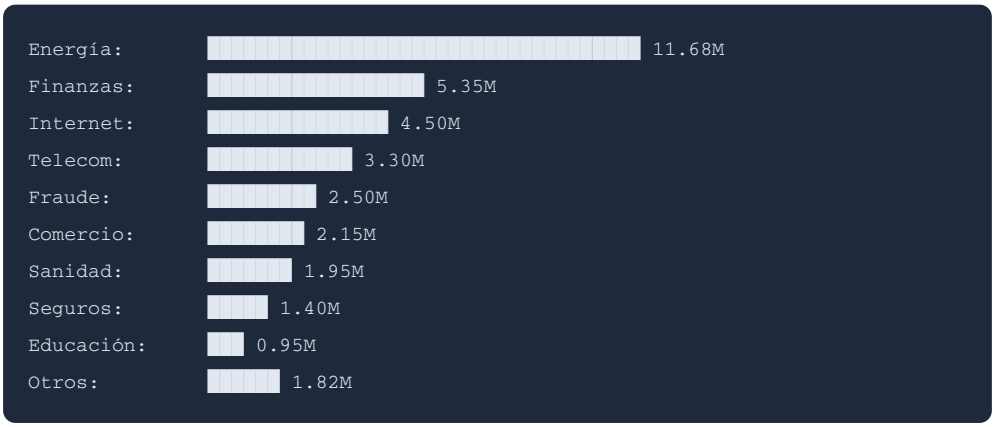
```
Sanción Final = Base Sancionadora × Multiplicador Agravantes/Atenuantes

Base Sancionadora:
- Depende de Art. 83.4 (10M/2%) o 83.5 (20M/4%)
- Y del tipo de infracción específica

Multiplicador Agravantes (ejemplos):
- Intencionalidad: x2
- Reincidencia: x1.5
- Datos sensibles: x1.3
- Categorías múltiples: Efecto acumulativo

Multiplicador Atenuantes (ejemplos):
- Cooperación plena: x0.7
- Autodenuncia: x0.5
- Medidas preventivas robustas: x0.8
- Primera infracción: x0.9
```

Análisis Sectorial Sanciones AEPD 2024

Distribución por sectores (importe total):

SECTOR	IMPORTE (M€)	% TOTAL	Nº SANCIONES
Energía	11,68	32,8%	47
Finanzas	5,35	15,0%	23
Servicios Internet	4,50	12,6%	156
Telecomunicaciones	3,30	9,3%	89
Fraude Contractual	2,50	7,0%	312
Comercio	2,15	6,0%	178
Sanidad	1,95	5,5%	34
Seguros	1,40	3,9%	28
Educación	0,95	2,7%	19
Otros	1,82	5,1%	241
TOTAL	35,60	100,0%	1.127

Gráfico textual sectores (escala logarítmica):



Insights clave:

1. **Concentración sectorial:**
2. Top 3 sectores (Energía, Finanzas, Internet) = **60,4% del importe total**
3. Energía lidera por casos **Endesa** (6,1M) + **Iberdrola** (3,5M) + **Enérgya-VM** (5M)
4. **Volumen vs. Importe:**
5. **Fraude contractual:** 312 sanciones (27,7% del total) pero solo 7% del importe
6. **Energía:** 47 sanciones (4,2% del total) pero 32,8% del importe
7. **Conclusión:** AEPD concentra cuantías altas en "fallos estructurales" grandes empresas
8. **Nuevas tendencias (2025-2026):**

9. ⬆ **IA y algoritmos:** 14 expedientes abiertos específicos IA (2024), esperados 40+ (2026)
10. ⬆ **Biometría:** Post-casos AENA/LaLiga, escrutinio reforzado
11. ⬆ **Neurodatos:** Primera guía AEPD sobre datos actividad cerebral (Q3 2026)
12. ⬆ **Menores:** Verificación edad online, privacidad apps educativas

Proyecciones para 2026: Foco en IA y Neurodatos

Declaraciones Lorenzo Cotino (Presidente AEPD, enero 2026):

> "*La protección de neurodatos y la gobernanza algorítmica son las dos grandes prioridades de esta Agencia para el período 2026-2028. No permitiremos que la innovación tecnológica erosione los derechos fundamentales conquistados.*"

Campaña inspecciones 2026 (anunciada):

1. **Sistemas IA alto riesgo:**
2. Target: 150 empresas sector financiero (scoring crediticio)
3. Verificación: EIPD válidas, ausencia sesgos, supervisión humana efectiva
4. **Biometría empresarial:**
5. Target: 200 empresas con control acceso biométrico trabajadores
6. Verificación: Necesidad estricta, consentimiento válido (si aplica), template protection
7. **Apps menores:**
8. Target: 50 apps educativas/entretenimiento infantil más descargadas
9. Verificación: Verificación edad, consentimiento padres, ausencia perfilado
10. **Neurotecnología:**
11. Target: 10 empresas pioneras dispositivos interfaz cerebro-ordenador
12. Verificación: Tratamiento neurodatos como categoría especial, EIPD robusta

Impacto esperado:
Importe sanciones 2026: **Proyectado 50-60M EUR** (incremento 40-70% vs. 2024).

---

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 lecturas. El sistema exige: - Fecha de nacimiento completa (día/mes/año) - 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: "Los datos personales serán... **adecuados, pertinentes y limitados a lo necesario** en relación con los fines para los que son tratados (*minimización de datos*)." - Considerando 39 RGPD: Minimización implica garantizar que plazo conservación se limite al **mínimo estricto necesario**

Application: 1. **Finalidad:** Recomendar libros adecuados a gustos usuario 2. **Datos requeridos vs. Necesarios:** - Fecha nacimiento **COMPLETA:** NO necesaria → Basta **rango edad** (18-25, 26-35, etc.) - Género: Cuestionable → Libros NO son género-específicos necesariamente - Nivel estudios: NO necesario → Recomendaciones pueden basarse en historial lecturas previas - Ingresos: NO necesario → Precio libro puede filtrarse sin conocer ingresos exactos usuario 3. **Alternativa menos invasiva:** - Sistema puede funcionar con: Historial compras + valoraciones + categorías preferidas - Rango edad (opcional) suficiente para filtrar contenido infantil vs. adulto

Conclusion:
SÍ, vulnera minimización. LectorPlus debe: - Eliminar campos obligatorios salvo estrictamente necesarios - Opcionalizarlos con explicación clara beneficio (mejor precisión recomendaciones) - Ofrecer funcionalidad básica **sin** requerir datos adicionales

Impacto:
Responsable debe: 1. **Purgar** dataset entrenamiento de datos excesivos (eliminar fechas nacimiento completas, géneros, ingresos) 2. **Reentrenar** modelo IA con datos minimizados 3. **Pérdida:** Meses de optimización del algoritmo

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

Caso 2: Privacy by Design en Transporte

Facts:
Operadora movilidad "MoviSmart" usa IA para predecir rutas óptimas. El sistema: - Vincula ID billete con geolocalización en tiempo real durante trayecto - Almacena vínculo permanentemente en BD para "mejorar predicciones futuras" - Permite re-identificación usuario analizando patrones movilidad

Issue:
¿Cumple el sistema Privacy by Design (Art. 25.1 RGPD) si permite re-identificación post-trayecto?

Rule: - Art. 25.1 RGPD: Medidas técnicas/organizativas apropiadas, como seudonimización, desde el diseño - Art. 5.1.e RGPD: Conservación limitada - no más tiempo del necesario - Considerando 78 RGPD: DPbDD implica que medidas de protección se **integren** en el tratamiento

Application: 1. **Finalidad legítima:** Optimizar rutas = Interés legítimo válido (Art. 6.1.f) 2. **Fallo diseño arquitectónico:** - Sistema vincula ID permanente con geolocalización histórica - Permite analizar patrones: "Usuario 12345 viaja de Barrio X a Barrio Y todos los lunes 8am" - Riesgo: Inferir domicilio + lugar trabajo + hábitos = Re-identificación 3. **Diseño conforme:** - Durante trayecto: Vincular ID billete + geolocalización (necesario) - **Al finalizar trayecto:** Destruir vínculo, conservar solo datos agregados anónimos - Ej: "Ruta A-B lunes 8am tiene congestión media 7/10" (sin vincular a usuarios individuales)

Conclusion:
NO cumple Privacy by Design. MoviSmart debe: - Implementar **auto-eliminación** vínculo ID-geolocalización al finalizar trayecto - Conservar solo datos agregados/anonimizados para predicciones - Realizar EIPD si aún no hecha (geolocalización masiva = Art. 35.3.c)

Resolución jurídica:
Orden correctiva AEPD: Rediseñar sistema en 3 meses o suspensión.

Caso 3: Seguridad en Salud e IA

Facts:
Hospital "San Rafael" implementa IA diagnóstica oncología. Por "facilidad técnica": - Todo personal IT (20 personas) tiene acceso **sin restricciones** a datasets entrenamiento (historiales clínicos 50.000 pacientes) - Logs de acceso NO implementados - Backup datasets en servidor sin cifrado

Issue:
¿Vulnera Art. 32 RGPD (seguridad) y Art. 9 (categoría especial - salud)?

Rule: - Art. 32.1 RGPD: Medidas técnicas/organizativas apropiadas para garantizar nivel seguridad adecuado al riesgo, incluyendo **control de accesos** - Art. 32.4 RGPD: Responsable y encargado tomarán medidas para garantizar que personas autorizadas traten datos **solo siguiendo instrucciones** - Art. 9.1 RGPD: Prohibición categoría especial (salud) salvo excepción Art. 9.2

Application: 1. **Categoría especial:** Datos salud (oncología) = Art. 9 RGPD 2. **Falta control de accesos:** - 20 personas IT acceso sin restricciones → Viola **principio "necesidad de conocer"** (*need-to-know*) - Solo personal médico/investigador **estrictamente necesario** debe acceder - IT solo debe acceder para mantenimiento técnico, **sin visualizar datos clínicos** 3. **Falta trazabilidad:** - Ausencia logs = Imposible detectar accesos no autorizados - Vulnera Art. 32.1.d) (capacidad verificar eficacia medidas) 4. **Falta cifrado:** - Backup sin cifrar = Riesgo robo/pérdida → Violación seguridad - Vulnera Art. 32.1.a) (seudonimización y cifrado)

Conclusion:
SÍ, múltiples infracciones graves. Hospital debe: - Implementar **RBAC** (Role-Based Access Control): Solo acceso según rol (médico, enfermera, IT, investigador) - **Logs exhaustivos** de todos los accesos (quién, cuándo, qué datos) - **Cifrado AES-256** datasets en reposo y tránsito - **Formación** personal sobre confidencialidad

Impacto:
AEPD ordena **suspensión cautelar** proyecto IA (Art. 58.2.f) hasta corrección deficiencias.

Sanción potencial: 10M EUR o 2% facturación (Art. 83.4.a - medidas seguridad) + agravante datos especiales.

Caso 4: IA en Seguros y Sesgo Algorítmico

Facts:
Aseguradora "SecureLife" usa IA para calcular primas seguro auto. El modelo: - Entrenado con datos históricos 2010-2020 - Dataset refleja discriminación histórica: Primas más altas para códigos postales con mayor población inmigrante - Modelo replica sesgo: Incrementa prima +15% para residentes barrios X, Y, Z (mayoritariamente población origen magrebí) - SecureLife alega "algoritmo es objetivo, solo analiza datos históricos siniestralidad"

Issue:
¿Constituye discriminación ilegal usar IA que replica sesgos históricos aunque el algoritmo sea "técnicamente neutral"?

Rule: - Art. 5.1.a RGPD: Licitud, lealtad y transparencia - Art. 5.1.d RGPD: **Exactitud** - "todo paso razonable para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos" - Art. 21 Carta DFUE: Prohibición discriminación por origen racial/étnico - Considerando 71 RGPD: Garantías apropiadas frente a decisiones discriminatorias

Application: 1. **Sesgo = Dato inexacto:** - Correlación código postal-siniestralidad puede deberse a **factores socioeconómicos** NO vinculados a etnia - Usar código postal como proxy raza = Discriminación indirecta 2. **Obligación corregir:** - Art. 5.1.d exige "pasos razonables" suprimir datos inexactos - Dataset histórico sesgado = "Dato inexacto" en sentido normativo (refleja discriminación, NO riesgo real) 3. **Fairness obligatoria:** - SecureLife debe auditar modelo para sesgos discriminatorios - Implementar técnicas fairness (re-balanceo dataset, penalización variables proxy, validación equidad)

Conclusion:
SÍ, infracción Art. 5.1.a (lealtad) + 5.1.d (exactitud) + discriminación. SecureLife debe: - **Suspender** uso del modelo - **Auditar** sesgos con métricas fairness (disparate impact, equal opportunity) - **Reentrenar** con dataset balanceado o variables corregidas - **Indemnizar** clientes potencialmente afectados

Responsabilidad civil adicional:
Clientes discriminados pueden demandar: - Indemnización daños y perjuicios - Nulidad contrato por ilegalidad - Daño moral por discriminación (jurisprudencia España: 3.000-12.000€ por caso)

Sanción AEPD: 10M EUR o 2% facturación (Art. 83.5.a - principios básicos).

[Continuaré con los casos 5-12 y FAQ en el siguiente bloque...]

Caso 5: Consentimiento en Relación Laboral

Facts:
Empresa logística "FastDelivery" implementa IA monitorización rendimiento conductores. Sistema: - Analiza rutas, tiempos entrega, frenadas bruscas, velocidad - Genera scoring individual diario (1-10) - Scoring bajo 5 durante 3 días consecutivos → Advertencia formal - Empresa solicita "consentimiento" trabajadores mediante email

Issue:
¿Es válido el consentimiento trabajador para monitorización IA dada asimetría de poder empleador-empleado?

Rule: - Considerando 43 RGPD: "...difícilmente puede considerarse que el consentimiento se haya prestado libremente si existe un **desequilibrio claro** entre el interesado y el responsable..." - Art. 88 RGPD: Tratamiento en contexto laboral puede basarse en **contratos colectivos** con garantías - Art. 6.1.b o f RGPD: Alternativas al consentimiento (ejecución contrato, interés legítimo)

Application: 1. **Presunción consentimiento NO libre:** - Trabajador teme represalias si rechaza - No hay opción genuina de negativa sin detrimento 2. **Base legal apropiada:** - Art. 6.1.b: Ejecución contrato laboral (si cláusula expresa permite monitorización proporcional) - Art. 6.1.f: Interés legítimo (seguridad vial, eficiencia operativa) **con ponderación** 3. **Salvaguardas obligatorias:** - Consulta previa representantes trabajadores (Comité Empresa) - EIPD (monitorización sistemática trabajadores = Art. 35.3.b) - Transparencia absoluta (política clara sobre qué se mide y consecuencias) - Derecho impugnación scoring si automatizado

Conclusion:
Consentimiento **NO válido** por asimetría de poder. FastDelivery debe: - Retirar solicitud consentimiento - Basar tratamiento en **Art. 6.1.f** (interés legítimo) con: - Test ponderación documentado (seguridad vial vs. privacidad) - Consulta Comité de Empresa - EIPD completa - Derecho oposición facilitado - Supervisión humana antes de sanciones

Precedente: Jurisprudencia española consistente - consentimiento laboral presume viciado.

Caso 6: Derecho de Acceso en IA Opaca

Facts:
Ciudadano solicita crédito hipotecario en "BancoTech". Sistema IA scoring deniega automáticamente. Ciudadano ejerce derecho de acceso (Art. 15 RGPD) solicitando: - Explicación detallada del algoritmo - Factores específicos que llevaron a denegación BancoTech responde: "El modelo utiliza 247 variables en red neuronal de 5 capas. Revelar detalles violaría secreto comercial."

Issue:
¿Qué nivel de detalle debe proporcionar el banco para cumplir Art. 15.1.h (información sobre lógica decisión automatizada)?

Rule: - Art. 15.1.h RGPD: "...información sobre la lógica aplicada, así como **significado y consecuencias previstas**..." - STJUE C-634/21 (SCHUFA): Explicación debe ser **comprensible y significativa**, NO necesariamente código fuente - Guía AEPD: Balance entre derecho información y protección secreto comercial

Application: 1. **Obligación ineludible:** - Banco DEBE explicar lógica (Art. 15.1.h) - Secreto comercial NO exime, pero limita profundidad 2. **Nivel explicación válido:** - ✅ Factores principales considerados (ej: ratio deuda/ingresos, historial crediticio, antigüedad laboral) - ✅ Peso relativo aproximado cada factor (ej: 40% historial, 30% ratio deuda, etc.) - ✅ Por qué solicitante no cumple umbral (ej: ratio deuda 75%, óptimo <50%) - ❌ NO obligatorio: Fórmula matemática exacta, pesos precisos cada neurona, código fuente 3. **Test cumplimiento:** - ¿Solicitante puede **comprender** qué falló? - ¿Solicitante puede **actuar** para mejorar (reducir deudas, estabilizar empleo)? - Si SÍ → Explicación suficiente

Conclusion:
Respuesta BancoTech **insuficiente**. Debe proporcionar:

```
EXPLICACIÓN DECISIÓN SCORING CREDITICIO
========================================

Decisión: DENEGACIÓN hipoteca
Score: 520/1000 (Umbral aprobación: 700)

FACTORES PRINCIPALES (orden importancia):

1. HISTORIAL CREDITICIO (40% peso) ⚠
   - 3 préstamos activos: 25.000€ total
   - 1 impago registrado (hace 8 meses): -150 puntos
   - Antigüedad historial: 5 años (óptimo >10): -50 puntos

2. RATIO DEUDA/INGRESOS (30% peso) ⚠
   - Ingresos mensuales netos: 2.400€
   - Gastos fijos mensuales: 1.850€
   - Ratio: 77% (óptimo <40%, aceptable <50%): -200 puntos

3. ESTABILIDAD LABORAL (15% peso) ✔
   - Antigüedad empleo actual: 6 años: +80 puntos
   - Tipo contrato: Indefinido: +50 puntos

4. AHORRO/PATRIMONIO (10% peso) ⚠
   - Aportación inicial: 10% valor vivienda (óptimo >20%): -30 puntos
   - Ahorro demostrado: Bajo: -20 puntos

5. OTROS FACTORES (5% peso) ⚖
   - Edad: 35 años: Neutral
   - Cargas familiares: 2 hijos: -10 puntos

RECOMENDACIONES PARA MEJORAR SCORE:
- Reducir deudas actuales (prioridad: saldar impago)
- Aumentar ratio ahorro (objetivo: aportación inicial >20%)
- Mantener empleo estable (factor positivo, conservar)

DERECHOS:
- Solicitar revisión humana: revision@bancotech.es
- Aportar información adicional no considerada
- Impugnar decisión ante Servicio Atención Cliente
```

Sanción si persiste negativa: Hasta 20M EUR o 4% facturación (Art. 83.5.b - derechos interesados).

Caso 7: Transferencia IA a EE.UU. Post-Schrems II

Facts:
Startup española "HealthAI" desarrolla app diagnóstico dermatológico. Usa AWS servidores Virginia (EE.UU.) para: - Almacenar imágenes lesiones cutáneas

usuarios - Entrenar modelo IA CCT 2021 firmadas, DPF válido (2026), pero NO implementa medidas complementarias.

Issue:
¿Son suficientes CCT + DPF sin medidas complementarias para transferir datos salud a EE.UU.?

Rule: - STJUE C-311/18 (Schrems II): CCT solas insuficientes si legislación destino permite accesos desproporcionados - Recomendaciones CEPD 01/2020: Transfer Impact Assessment + medidas complementarias obligatorias - Art. 9 RGPD: Datos salud = Categoría especial (protección reforzada)

Application: 1. **Transferencia confirmada:** Datos almacenados EE.UU. = Transferencia Cap. V RGPD 2. **Riesgo legislativo EE.UU.:** - FISA 702 permite acceso servicios inteligencia si "objetivo extranjero" - Datos salud NO exentos explícitamente 3. **Medidas complementarias ausentes:** - ✖ NO cifrado end-to-end (AWS puede acceder en claro) - ✖ NO seudonimización robusta - ✖ NO limitación acceso por geolocalización 4. **Alto riesgo:** - Datos categoría especial (salud) + Sensibilidad imágenes dermatológicas - Revelación podría causar discriminación (ej: lesiones ETS)

Conclusion:
Transferencia **NO conforme**. HealthAI debe:

Opción A - Medidas complementarias técnicas: - Implementar cifrado E2E (clave gestionada España, nunca sale UE) - AWS procesa datos cifrados, descifrado solo cliente-side - Seudonimización: Separar ID usuario de imágenes

Opción B - Relocalización (más segura): - Migrar a AWS Frankfurt (Alemania) → Sin transferencia - Coste marginal estimado: +15% vs. Virginia

Opción C - Híbrido: - Almacenamiento imágenes: UE (Frankfurt) - Entrenamiento modelo: EE.UU. con dataset anonimizado (sin ID usuarios)

Recomendación DPO: Opción B (Frankfurt) para evitar complejidad TIA + incertidumbre jurídica DPF.

Riesgo si no corrige: Orden suspensión AEPD + sanción hasta 20M EUR o 4% (Art. 83.5.c - transferencias ilegales).

Caso 8: Machine Unlearning Imposible

Facts:
Modelo GPT-4 fine-tuneado por empresa española incluyó por error datos personales sensibles de 50 clientes en dataset entrenamiento (filtraciones emails internos con información salud mental). Cliente ejerce derecho supresión (Art. 17 RGPD). Empresa responde: "Técnicamente imposible eliminar huella de datos de red neuronal sin reentrenar modelo completo, lo que costaría 500.000€ y 6 meses."

Issue:
¿Exime la dificultad técnica/económica del machine unlearning del cumplimiento Art. 17 RGPD?

Rule: - Art. 17.1 RGPD: Derecho supresión cuando datos "ya no sean necesarios" o tratamiento sea ilícito - Art. 17.3 RGPD: Excepciones (libertad expresión, interés público, etc.) - NO incluye "coste económico" - Considerando 66 RGPD: Responsable debe adoptar "medidas razonables, incluidas técnicas"

Application: 1. **Tratamiento ilícito confirmado:** - Datos salud mental sin base legal válida (no había consentimiento explícito Art. 9.2.a) 2. **Machine unlearning:** - Métodos aproximados existen (SISA, approximate unlearning) aunque imperfectos - Coste 500K€ es elevado pero NO desproporcionado para empresa IA profesional 3. **Obligación "medidas razonables":** - ✅ Empresa DEBE intentar unlearning aproximado - ✅ Si técnicamente imposible garantizar 100% eliminación → Bloquear procesamiento futuro - ❌ NO puede seguir usando modelo con datos ilícitos argumentando coste

Conclusion:
Dificultad técnica/económica **NO exime**. Empresa debe:

Paso 1 (Inmediato - 48h): - Suspender uso del modelo en producción - Bloquear acceso datos entrenamiento afectados

Paso 2 (Corto plazo - 1 mes): - Intentar **approximate unlearning** (ajustar pesos para minimizar influencia datos) - Validar eficacia con ataques model inversion - Documentar técnicas aplicadas + limitaciones

Paso 3 (Si unlearning insuficiente): - **Reentrenar modelo** desde cero sin datos afectados - Coste 500K€ es **obligatorio** si única forma cumplir RGPD

Paso 4 (Compensación): - Indemnizar clientes afectados por uso ilícito sus datos - Notificación AEPD de la brecha (tratamiento ilícito = violación seguridad)

Precedente: No hay jurisprudencia específica machine unlearning (tecnología emergente), PERO principio general RGPD es claro: **Coste NO exime cumplimiento derechos fundamentales**.

Sanción si persiste uso modelo: 20M EUR o 4% facturación (Art. 83.5.b - derechos + Art. 83.5.a - licitud).

Caso 9: EIPD Inexistente - Sanción Millonaria

Facts:
Comercializadora energética "EnergíaPlus" implementó sistema IA para optimización tarifaria dinámica que: - Analiza consumo horario 3 millones hogares - Ajusta precios automáticamente según perfil usuario - Incluye datos personas vulnerables (bono social) - Sistema operativo desde enero 2024 - EIPD realizada en septiembre 2024 (8 meses después despliegue)

Issue:
¿Constituye infracción grave implementar sistema alto riesgo sin EIPD previa?

Rule: - Art. 35.1 RGPD: EIPD obligatoria "**antes de proceder al tratamiento**" si alto riesgo probable - Art. 35.3.a RGPD: Obligatoria para "evaluación sistemática y exhaustiva... incluida la elaboración de perfiles" - Art. 83.4.a RGPD: Sanción hasta 10M EUR o 2% facturación por incumplir Art. 35

Application: 1. **Alto riesgo confirmado:** - Evaluación sistemática 3M hogares - Perfilado automatizado con efectos económicos significativos (precio energía) - Colectivos vulnerables afectados 2. **Cronología infraccional:** - Ene 2024: Despliegue sistema SIN EIPD - Sep 2024: EIPD realizada *a posteriori* (8 meses tarde) - EIPD presentada es "justificativa", NO evaluación crítica de alternativas 3. **Obligación previa incumplida:** - Art. 35.1 exige EIPD "**antes**" tratamiento - 8 meses operación ilegal - EIPD posterior NO subsana infracción original

Conclusion:
SÍ, infracción grave múltiple. AEPD sanciona EnergíaPlus con **8,5M EUR** por:

Desglose sanción: - Ausencia EIPD previa (Art. 35.1): 4,0M EUR - Tratamiento ilícito durante 8 meses (Art. 6.1): 3,0M EUR - Agravante datos vulnerables: +1,5M EUR

Medidas correctivas ordenadas: 1. Realizar EIPD **válida** (crítica, con análisis alternativas) 2. Si EIPD revela alto riesgo residual → Consulta AEPD Art. 36.3 3. Implementar medidas mitigación identificadas 4. Notificar clientes afectados de tratamiento previo ilícito

Holding:
EIPD *a posteriori* tiene **valor cero** para subsanar infracción. La obligación es **preventiva**, no correctiva. Sistema que opera sin EIPD previa nace **viciado de nulidad**.

Caso 10: Datos de Menores sin Consentimiento Parental

Facts:
App educativa "KidsLearn" usa IA personalización contenidos para niños 6-12 años. Sistema: - Registra respuestas ejercicios, tiempo dedicado, errores frecuentes - Genera perfil aprendizaje individual - Recomendaciones adaptativas - Solicita consentimiento directamente al menor (checkbox registro) - NO verifica edad ni solicita consentimiento padres/tutores

Issue:
¿Es válido consentimiento prestado directamente por menor de 14 años sin intervención parental?

Rule: - Art. 8.1 RGPD: Consentimiento menor **<16 años** requiere autorización titular patria potestad (Estados pueden reducir a mínimo 13 años) - Art. 7 LOPDGDD: España fija edad en **14 años** (menores <14 necesitan consentimiento padres) - Art. 8.2 RGPD: Responsable debe hacer "**esfuerzos razonables**" verificar consentimiento titular patria potestad

Application: 1. **Usuarios objetivo:** Niños 6-12 años → Todos <14 años 2. **Consentimiento inválido:** - App solicita consentimiento directamente al menor - NO implementa verificación edad - NO solicita consentimiento/autorización padres 3. **Tratamiento ilícito:** - Datos personales (nombre, edad, email, rendimiento académico) - Base legal Art. 6.1.a (consentimiento) → **INVÁLIDA** por ser menor <14 - Sin base legal alternativa válida 4. **Falta "esfuerzos razonables":** - NO sistema double opt-in (confirmación email padre) - NO verificación tarjeta crédito (método razonable según WP29) - NO formulario específico padre/tutor

Conclusion:
Tratamiento **totalmente ilícito**. KidsLearn debe:

Inmediato (24h): - **Suspender** tratamiento datos menores existentes - **Bloquear** nuevos registros sin verificación parental

Corto plazo (30 días): - **Implementar** sistema verificación edad robusta: - Double opt-in email padre/tutor - O verificación documento identidad padre - O pasarela pago simbólico (0,10€) con tarjeta adulto - **Contactar** padres usuarios actuales solicitando autorización retroactiva - **Eliminar** datos menores cuyos padres NO autoricen

Sanción AEPD:
5,2M EUR por: - Tratamiento ilícito menores (Art. 6.1.a inválido): 3,0M EUR - Falta "esfuerzos razonables" Art. 8.2: 1,5M EUR - Agravante colectivo vulnerable (menores): +700K EUR

Precedente:
TikTok multada €345M por CEPD Irlanda (sept 2023) por deficiencias protección menores.

Holding:
Menores <14 años en España **carecen de capacidad jurídica** para consentir tratamiento datos. Consentimiento directo del menor es **nulo de pleno derecho**, haciendo todo el tratamiento ilícito desde el origen.

Caso 11: Violación Principio de Exactitud - Perfilado Erróneo

Facts:
Plataforma streaming "StreamPlus" usa IA recomendación películas. Sistema: - Perfila usuarios por preferencias - Un bug software etiqueta erróneamente al usuario "Carlos Martín" (padre familia, 45 años) como "consumidor contenido adulto" por falso positivo algoritmo - Durante 6 meses, Carlos recibe recomendaciones contenido inapropiado - Historial de visualización muestra error (Carlos NO consumió contenido adulto) - Carlos ejerce derecho rectificación (Art. 16) - StreamPlus responde: "El algoritmo es automático, no podemos modificarlo manualmente"

Issue:
¿Vulnera Art. 5.1.d RGPD (exactitud) mantener perfilado erróneo a pesar de evidencia objetiva de inexactitud?

Rule: - Art. 5.1.d RGPD: "Los datos personales serán **exactos** y, si fuera necesario, actualizados; se adoptarán **todas las medidas razonables** para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos..." - Art. 16 RGPD: Derecho rectificación sin dilación indebida - Art. 83.5.a RGPD: Sanción hasta 20M EUR o 4% por vulnerar principios básicos

Application: 1. **Dato inexacto confirmado:** - Perfilado "consumidor adulto" contradice historial real - Evidencia objetiva del error (logs muestran NO acceso contenido adulto) 2. **Obligación rectificar:** - Art. 5.1.d exige "**todas las medidas razonables**" para corregir - "El algoritmo no permite modificación manual" NO es

excusa válida - Responsable debe diseñar sistema que permita cumplir derechos 3. **Diseño defectuoso:** - Sistema IA sin capacidad rectificación manual = Violación Privacy by Design (Art. 25) - Imposibilita cumplimiento Art. 16 (derecho rectificación)

Conclusion:
SÍ, doble infracción. StreamPlus debe:

Técnicamente: - **Implementar** interfaz rectificación manual que permita: - Eliminar etiqueta errónea del perfil - Recalcular recomendaciones sin dato inexacto - Override temporal algoritmo si persiste error - **Alternativa:** Reentrenar modelo sin dato incorrecto (si arquitectura no permite rectificación directa)

Organizativamente: - Rectificar perfil Carlos inmediatamente (plazo 48h) - Compensación (disculpa + mes suscripción gratis por molestias) - Auditar cuántos usuarios más pueden tener perfilado erróneo similar

Sanción potencial: - Violación exactitud Art. 5.1.d: Hasta 20M EUR o 4% - Violación derecho rectificación Art. 16: Hasta 20M EUR o 4% - Violación DPbDD Art. 25: Hasta 10M EUR o 2%

Precedente:
AEPD sancionó empresas telco por mantener datos facturación incorrectos a pesar de reclamaciones clientes.

Holding:
La **automatización NO exime** de la obligación garantizar exactitud. Si sistema IA genera datos inexactos, responsable debe: 1. Corregirlos inmediatamente cuando detectados 2. Diseñar desde origen capacidad rectificación (DPbDD) 3. Reentrenar/actualizar modelo si persiste sesgo generando inexactitudes

"El algoritmo no permite modificarlo" es **admisión de diseño defectuoso**, NO defensa legal válida.

Caso 12: Uso Indebido Datos para Finalidad Diferente

Facts:
Gimnasio "FitZone" recopila datos salud socios (lesiones, condiciones médicas) para: - **Finalidad original (consentida):** Personalizar rutinas entrenamiento - **Base legal:** Art. 9.2.a RGPD (consentimiento explícito categoría especial)

En 2025, gimnasio implementa IA predictiva que analiza datos salud históricos para: - **Finalidad nueva (NO consentida):** Predecir riesgo abandono socios y enviar ofertas retención agresivas a "alto riesgo abandono" - NO solicita nuevo consentimiento para esta finalidad - Alega: "Son los mismos datos, ya tenemos consentimiento"

Issue:
¿Constituye violación Art. 5.1.b RGPD (limitación finalidad) usar datos consentidos para finalidad A para una finalidad B diferente sin nuevo consentimiento?

Rule: - Art. 5.1.b RGPD: "...recogidos con fines determinados, explícitos y legítimos, y **no serán tratados ulteriormente de manera incompatible** con dichos fines..." - Art. 6.4 RGPD: Test compatibilidad finalidades (vínculo, expectativas, naturaleza datos, consecuencias, garantías) - Art. 9 RGPD: Categoría especial (salud) requiere base legal específica Art. 9.2 para **cada finalidad**

Application: 1. **Cambio de finalidad confirmado:** - Original: Personalizar entrenamiento (finalidad salud/bienestar) - Nueva: Marketing predictivo (finalidad comercial) - **NO son compatibles** (criterio CEPD: salud → comercial es incompatible)

1. **Test compatibilidad Art. 6.4:**
2. **Vínculo:** Bajo (salud vs. retención comercial)
3. **Expectativas razonable socio:** NO esperaría datos salud para marketing
4. **Naturaleza datos:** Categoría especial (salud) → Requiere protección reforzada
5. **Consecuencias:** Potencial discriminación (ofertas diferentes según salud)
6. **Garantías:** Insuficientes (sin nuevo consentimiento)
7. **Conclusión test:** Finalidades **INCOMPATIBLES**
8. **Categoría especial agrava:**
9. Art. 9 requiere base legal **específica por finalidad**
10. Consentimiento para finalidad A NO cubre finalidad B

Conclusion:
Violación grave Art. 5.1.b + Art. 9. FitZone debe:

Inmediato: - **Cesar** uso datos salud para predicción abandono/marketing - **Eliminar** perfiles/scores generados con esta finalidad

Opción A - Solicitar nuevo consentimiento: - Informar socios de nueva finalidad clara, transparentemente - Solicitar **consentimiento explícito** nuevo (Art. 9.2.a) - Permitir rechazar sin perjuicio servicio básico (libertad)

Opción B - Abandonar finalidad: - Si consentimiento NO es libre (rechazo implica no renovación) → Base legal inválida - NO proceder con finalidad nueva

Sanción: - Violación limitación finalidad Art. 5.1.b: Hasta 20M EUR o 4% - Violación categoría especial Art. 9: Hasta 20M EUR o 4% - **Agravante:** Uso datos salud para discriminación comercial

Holding:
"Mismo dato ≠ Mismo consentimiento". Cada finalidad requiere base legal independiente. Para categorías especiales (Art. 9), el consentimiento es **específico por finalidad**, NO genérico ni extensible a usos futuros no contemplados originalmente.

Principio:
La limitación de finalidad protege la **autodeterminación informativa**. Usuario consiente para propósito concreto, NO da "carta blanca" para cualquier uso futuro de sus datos.

---

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 según criterio AEPD) - Realiza **supervisión sistemática** de conductas (ej: análisis comportamiento usuarios, tracking) - Trata **categorías especiales** de datos (salud, biometría) como actividad principal

Art. 37.1 RGPD:

> *"El responsable y el encargado designarán un DPO **siempre que**: b) las actividades principales del responsable... consistan en operaciones de tratamiento que... requieran una **observación habitual y sistemática de interesados a gran escala**, o c) las actividades principales... consistan en el **tratamiento a gran escala de categorías especiales de datos**..."*

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 antes de 2024?

Respuesta:
Período transitorio pero cumplimiento inevitable.

Cronología: - **1 ago 2024:** AI Act entra vigor (NO obligaciones inmediatas sistemas existentes) - **2 ago 2026:** Sistemas **nuevos** alto riesgo deben cumplir Arts. 9-15 - **2 ago 2027:** Sistemas **existentes** alto riesgo deben adaptarse o retirarse

Implicaciones: - Sistemas IA pre-2024 tienen hasta **2 ago 2027** para: - Realizar evaluación conformidad - Implementar medidas Arts. 9-15 (gestión riesgos, calidad datos, supervisión humana, etc.) - Obtener marcado CE - Registrar en base datos UE

PERO: RGPD aplica **desde ya** (vigente desde 25 mayo 2018). NO hay período transitorio para obligaciones protección datos.

Recomendación:
Iniciar adaptación **ahora** (2026) para: - Evitar rush de última hora (2027) - Distribuir costes compliance en el tiempo - Aprovechar subvenciones UE para PYMEs (fondos Digital Europe Programme)

---

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

Respuesta:
NO, salvo casos muy específicos.

Razones: 1. **Granularidad imposible:** IA usa millones de datos de fuentes heterogéneas → Imposible consentimiento específico de cada fuente 2. **Revocabilidad problemática:** Machine unlearning técnicamente muy difícil 3. **Asimetría de poder:** En contextos laborales, B2B, servicios esenciales → Consentimiento presume NO libre

Bases legales preferibles:

Escenario	Base Legal Recomendada	Fundamento
IA parte del servicio contratado	Art. 6.1.b (ejecución contrato)	Scoring crediticio necesario para conceder préstamo
IA para cumplimiento legal	Art. 6.1.c (obligación legal)	IA anti-blanqueo (Ley 10/2010)
IA seguridad/prevención fraude	Art. 6.1.f (interés legítimo)	Detección fraude bancario con test ponderación
IA investigación científica	Art. 89 RGPD (interés público)	Investigación médica con salvaguardas
Servicios opcionales personalización	Art. 6.1.a (consentimiento)	Recomendaciones personalizadas Netflix (genuinamente opcional)

Excepción categorías especiales (Art. 9):
Si datos salud, biometría, ideología → Opciones muy limitadas: - Consentimiento **explícito** (Art. 9.2.a) - Difícil validez - Medicina preventiva (Art. 9.2.h) - Interés público esencial con base legal (Art. 9.2.g)

---

4. ¿Qué pasa si mi proveedor de IA está en un "paraíso de datos" (país sin protección adecuada)?

Respuesta:
Es **transferencia internacional ilegal** si no hay: - Decisión de adecuación (países aprobados: Andorra, Argentina, Canadá, Israel, Japón, NZ, UK, Suiza, Uruguay, Corea del Sur, EE.UU. bajo DPF - feb 2026) - O Cláusulas Contractuales Tipo (CCT 2021) + Transfer Impact Assessment + Medidas complementarias

Si proveedor está en país "paraíso" (ej: China, Rusia, muchos latinoamericanos/asiáticos):

Paso 1 - Verificar si hay decisión adecuación: - Consultar: ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions - Si NO → Continuar Paso 2

Paso 2 - Implementar CCT 2021: - Descargar CCT: ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc - Firmar contrato con proveedor incluyendo CCT completas

Paso 3 - Transfer Impact Assessment: - Evaluar legislación país destino (accesos gubernamentales, tutela judicial, etc.) - Documentar análisis

Paso 4 - Medidas complementarias técnicas: - **Obligatorias si TIA detecta riesgos:** - Cifrado E2E (clave nunca sale UE) - Seudonimización robusta - Procesamiento en enclaves seguros (TEE)

Si medidas complementarias imposibles técnicamente:
→ **NO transferir**. Buscar proveedor alternativo UE/país adecuado.

Ejemplo:
Startup quiere usar Alibaba Cloud (China) → Sin decisión adecuación + Legislación china permite accesos gubernamentales amplios + Cifrado E2E impracticable para tipo procesamiento → **Transferencia ilegal**, buscar alternativa (AWS Frankfurt, Google Cloud Bélgica, OVH Francia).

---

5. ¿Cómo demuestro Responsabilidad Proactiva (*accountability*)?

Respuesta:
Documentación exhaustiva + evidencias objetivas.

Elementos demostrativos obligatorios:

1. Registro de Actividades de Tratamiento (RAT) - Art. 30: - Completo, actualizado (revisión al menos anual) - Específico para cada tratamiento IA - Incluye: Lógica algoritmo, datasets, medidas seguridad

2. Evaluaciones de Impacto (EIPD) - Art. 35: - Realizadas **antes** despliegue sistemas alto riesgo - Actualizadas si cambios sustanciales - Firmadas por DPO + Responsable

3. Políticas y procedimientos: - Política privacidad publicada, clara, accesible - Procedimientos ARCO+ documentados - Plan gestión brechas seguridad - Manual gobernanza datos IA

4. Contratos conformes: - Contratos encargados Art. 28.3 completos - CCT 2021 si transferencias internacionales - Cláusulas auditoría proveedores IA

5. Formación personal: - Actas formación RGPD (al menos anual) - Certificados asistencia - Tests conocimiento

6. Auditorías: - Auditoría interna anual (mínimo) - Auditoría externa bianual (recomendado alto riesgo) - Informes auditoría con hallazgos + plan acción

7. Actas reuniones compliance: - Comité Protección Datos (si existe) - Revisiones periódicas DPO + Dirección - Decisiones sobre tratamientos documentadas

8. Evidencias técnicas: - Logs de acceso a sistemas - Certificados cifrado - Resultados testing seguridad (pentesting) - Métricas fairness algoritmos IA

Test cumplimiento:
¿Puedo demostrar a AEPD en inspección (con 48h aviso) que cumplo cada artículo RGPD aplicable mediante documentación objetiva? - SÍ → Accountability cumplido - NO → Riesgo sancionador alto

---

6. ¿Puedo usar datos públicos de Instagram/TikTok para entrenar mi IA?

Respuesta:
NO automáticamente. "Público" ≠ "Libre uso".

Análisis jurídico:

Paso 1 - ¿Son datos personales? - Fotos con rostros identificables = SÍ (datos personales) - Nombres de usuario, biografías = SÍ - → Aplica RGPD completo

Paso 2 - ¿Hay base legal (Art. 6)? - Consentimiento: NO (usuario consintió publicar en red social, NO que terceros entrenen IA comercial) - Interés legítimo (Art. 6.1.f): Cuestionable - Test ponderación: ¿Interés comercial empresa > Expectativa razonable privacidad usuario? - Criterio AEPD: Generalmente **NO** si scraping masivo automatizado - → Base legal **difícil** de sostener

Paso 3 - ¿Categorías especiales (Art. 9)? - Si IA infiere raza, orientación sexual, creencias religiosas desde fotos/posts → Categoría especial - Prohibición Art. 9.1 salvo excepciones Art. 9.2 (muy restrictivas) - → Scraping ideológico **prácticamente prohibido** en España (Art. 9 LOPDGDD)

Paso 4 - Términos de servicio plataforma: - Instagram/TikTok TOS prohíben explícitamente scraping automatizado - Violación TOS puede ser además ilícito contractual

Conclusión:
Scraping masivo redes sociales para entrenamiento IA comercial es **alto riesgo legal**: - Probable infracción RGPD (falta base legal) - Violación TOS plataforma - Riesgo demandas civiles usuarios

Alternativas legales: 1. **Datasets anotados comerciales** con licencias claras (ej: ImageNet, COCO con licencias comerciales) 2. **Datos sintéticos** generados artificialmente 3. **Colaboración con usuarios** (consentimiento explícito + compensación) 4. **Common Crawl** con filtrado legal riguroso + revisión humana

Precedente: Meta/Facebook sancionado múltiples veces por scraping terceros. LinkedIn ganó caso contra hiQ (scraping perfiles).

---

7. ¿Es legal el reconocimiento facial en el entorno laboral?

Respuesta:
Casi nunca es proporcionado según AEPD, salvo supuestos muy excepcionales.

Posición AEPD (Guía Videovigilancia 2021):

Presunción desproporcionalidad: - Relación laboral = Asimetría de poder → Consentimiento NO válido - Alternativas menos invasivas existen (tarjeta, PIN, huella - menos invasiva que rostro)

Excepciones muy restrictivas:

Supuesto	Requisitos acumulativos	Ejemplo válido
Alta seguridad	• Riesgo objetivo alto (instalaciones críticas) • Imposibilidad alternativa • EIPD robusta • Consulta Comité Empresa • Autorización Inspección Trabajo	Central nuclear - Control acceso zona radiactiva (sí)
Prevención delitos graves	• Histórico delitos/amenazas • Proporcional al riesgo • Supervisión judicial/policial	Banco - Identificación atracadores reincidentes (sí con salvaguardas)
Contexto NO laboral	• Acceso público general • NO empleados • Información clara	Museo - Acceso visitantes (cuestionable, preferible alternativa)

Prohibido absolutamente: - ✖ Control horario general empleados - ✖ Monitorización productividad - ✖ Control presencia en oficina - ✖ "Conveniencia" o "modernización"

Caso típico:
Oficina corporativa quiere reconocimiento facial fichar entrada → **NO proporcionado**. Alternativa: Tarjeta contactless o app móvil Bluetooth (igual de eficaz, menos invasivo).

Sanción esperada si implementa sin justificación:
5-10M EUR (basado en precedentes AENA, LaLiga) + orden desmantelamiento inmediato.

---

8. ¿Qué son los "neurodatos" y cómo se protegen?

Respuesta:
Neurodatos = Información obtenida de la actividad cerebral (ondas cerebrales, señales neuronales).

Estado regulatorio (feb 2026):

RGPD: - ¿Son datos personales? → **SÍ** (permiten identificar persona + revelan estados mentales) - ¿Categoría especial (Art. 9)? → **SÍ** (datos salud - actividad cerebral revela condiciones neurológicas) - → Protección reforzada Art. 9 RGPD

Iniciativas España: - **Anteproyecto Ley Neuroderechos** (tramitación 2026): Propone protección específica "derecho a privacidad mental" - **AEPD Guía Neurotecnología** (publicación prevista Q3 2026): Criterios específicos tratamiento neurodatos

Principios aplicables:

1. **Consentimiento reforzado:**
2. Información clara sobre qué se mide, para qué, riesgos
3. Revocable en cualquier momento
4. Especial protección si investigación clínica (consentimiento informado médico)
5. **Minimización estricta:**
6. Solo datos neuronales estrictamente necesarios
7. Agregación/anonimización siempre que posible
8. **Finalidad limitada:**
9. Prohibido inferir creencias religiosas, orientación política, tendencias delictivas desde actividad cerebral
10. Uso terapéutico/investigación médica prioritario
11. **Seguridad máxima:**
12. Cifrado extremo (datos más sensibles que genéticos)
13. Acceso ultra-restringido

Tecnologías afectadas: - Interfaces cerebro-ordenador (BCI) - Neurofeedback - Dispositivos EEG comerciales (ej: Muse, Emotiv) - IA diagnóstico neurológico

Recomendación DPO:
Tratamiento neurodatos requiere: - EIPD obligatoria (categoría especial + alto riesgo) - Consulta AEPD Art. 36.3 preventiva - Comité Ética independiente - Consentimiento informado médico-legal

---

9. ¿Qué es la seudonimización y cuándo es obligatoria?

Respuesta:
Seudonimización = Técnica que sustituye identificadores directos por códigos/tokens, de modo que los datos NO puedan atribuirse a un interesado **sin información adicional** (que se guarda separadamente).

Definición Art. 4.5 RGPD:

> *"...el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar **información adicional**, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas..."*

Diferencia clave:

Concepto	Reversible	Datos personales	Ejemplo
Identificación	N/A	SÍ	"Juan Pérez, DNI 12345678A"
Seudonimización	SÍ (con clave)	SÍ (pero protegidos)	"Usuario_987xyz" (mapeo separado)
Anonimización	NO	NO (deja de ser RGPD)	Datos agregados imposibles re-identificar

Obligatoriedad:

1. Art. 25.1 RGPD (DPbDD):
Seudonimización como medida técnica apropiada (recomendada, no siempre obligatoria)

2. Art. 32.1.a RGPD (Seguridad):

> *"Medidas... incluida la **seudonimización y el cifrado** de datos personales."*

→ **Obligatoria** si riesgo para derechos requiere protección reforzada

3. Art. 89 RGPD (Investigación):
Seudonimización **obligatoria** para investigación científica si compatible con finalidad

Implementación técnica:

```
# EJEMPLO SEUDONIMIZACIÓN BÁSICA
import hashlib
import secrets

# Datos originales
usuario = {
    'nombre': 'María García',
    'email': 'maria.garcia@example.com',
    'dni': '87654321B'
}

# Generar salt único (guardar separado seguro)
salt = secrets.token_hex(16)

# Seudonimizar
seudónimo = hashlib.sha256(
    (usuario['email'] + salt).encode()
).hexdigest()

# Datos seudonimizados (para IA)
datos_seudo = {
    'id': seudónimo,  # Usuario no identificable sin salt
    'edad': 35,
    'ciudad': 'Madrid',
    'historial_compras': [...]
}

# Tabla linkage (guardar separada, cifrada, acceso restringido)
linkage_table = {
    seudónimo: usuario['email']  # Permite re-identificar si necesario
}
```

Cuándo usar: - ✅ Datasets entrenamiento IA (separar ID personal de features) - ✅ Análisis estadístico - ✅ Testing/desarrollo (usar datos producción seudonimizados) - ✅ Compartir datos con investigadores - ✅ Backups (almacenar seudonimizados + tabla linkage cifrada)

Cuándo NO suficiente: - ❌ Si datos permiten re-identificación fácil (ej: fecha nacimiento + código postal + sexo = identifican a 87% población) - ❌ Tratamientos alto riesgo sin otras medidas (seudonimización **+ cifrado + control acceso**)

---

10. ¿Es nulo el consentimiento dado bajo presión?

Respuesta:
SÍ, absolutamente. Consentimiento bajo presión/coacción es **nulo de pleno derecho**.

Base legal:

Art. 4.11 RGPD - Requisito "libre":

> "*...manifestación de voluntad **libre**...*"

Considerando 42 RGPD:

> "*El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de **verdadera o libre elección** o no puede **denegar o retirar su consentimiento sin sufrir perjuicio alguno**.*"

Considerando 43 RGPD:

> "*...difícilmente puede considerarse que el consentimiento se haya prestado libremente si existe un **desequilibrio claro** entre el interesado y el responsable del tratamiento, en particular cuando el responsable es una autoridad pública... **empleador**...*"

Supuestos consentimiento NO libre (presunto nulo):

Contexto	Por qué NO libre	Ejemplo nulo	Alternativa válida
Relación laboral	Empleador puede sancionar/no renovar	"Consiente" monitorización o despido	Art. 6.1.f con ponderación
Servicio esencial sin alternativa	Usuario NO tiene opción genuina	Agua/luz exige datos excesivos	Art. 6.1.b limitado a necesario
Autoridad pública	Ciudadano teme represalias	Policía "pide" consentimiento investigación	Art. 6.1.e (interés público con base legal)
Contrato condicionado	"Acepta o no hay contrato"	Seguro exige datos NO necesarios	Art. 6.1.b solo datos imprescindibles
Menor de edad	Falta madurez discernimiento	Niño 10 años "acepta" tracking	Consentimiento padre/tutor

Test validez consentimiento:

```
¿El consentimiento es VÁLIDO?
==============================

1. ¿Es LIBRE?
   - ¿Puede usuario rechazar sin perder servicio básico?
   - ¿Existe alternativa real sin consentir?
   - ¿Hay asimetría de poder (empleo, autoridad)?

   → SI alguna respuesta es NO → Consentimiento NULO

2. ¿Es ESPECÍFICO?
   - ¿Cada finalidad tiene solicitud separada?
   - ¿Usuario puede aceptar unas y rechazar otras?

   → Si respuesta NO → Consentimiento NULO

3. ¿Es INFORMADO?
   - ¿Información clara, comprensible, accesible?
   - ¿Usuario entiende qué datos, para qué, cuánto tiempo?

   → Si respuesta NO → Consentimiento NULO

4. ¿Es INEQUÍVOCO?
   - ¿Acción afirmativa clara (clic, firma)?
   - ¿NO es silencio, casillas pre-marcadas, inacción?

   → Si respuesta NO → Consentimiento NULO

Si TODOS = SÍ → Consentimiento PROBABLEMENTE VÁLIDO
Si ALGUNO = NO → Consentimiento NULO
```

Consecuencias consentimiento nulo: - Tratamiento es **ilícito** (Art. 6.1.a no cumplido) - Obligación cesar tratamiento inmediatamente - Derecho indemnización afectados (daños y perjuicios) - Sanción AEPD: Hasta 20M EUR o 4% facturación (Art. 83.5.a)

Ejemplo real:
Trabajador "consiente" app monitorización GPS todo el día. Empresa alega "voluntario". AEPD dictamina: Consentimiento **nulo** por asimetría poder. Base legal correcta: Art. 6.1.f (interés legítimo) con test ponderación + limitación horario laboral.

---

11. ¿Qué sanción conlleva NO notificar una brecha de seguridad?

Respuesta:
Doble sanción: Por la brecha en sí + Por NO notificar (agravante).

Régimen sancionador:

1. Sanción por la brecha (Art. 83.4.a - Seguridad Art. 32): - Hasta **10M EUR o 2% facturación** global

2. Sanción agravada por NO notificar (Art. 83.4.a - Arts. 33-34): - Hasta **10M EUR o 2% facturación** - **Agravante Art. 83.2.k:** "Intencionalidad o negligencia en la infracción" - → Sanción combinada puede alcanzar el **máximo del tier**

Factores agravantes específicos: - Ocultación deliberada (intento minimizar para evitar publicidad) - Notificación muy tardía (>1 semana cuando debió ser 72h) - Información incompleta/engañosa en notificación - NO comunicar afectados cuando era obligatorio

Caso Endesa (2023):
- Brecha afectó 2,5M clientes - Notificó AEPD **7 días tarde** - **NO comunicó** a clientes nunca - **Sanción:** 6,1M EUR (alta por intencionalidad + afectación masiva)

Desglose sanción Endesa: - Brecha seguridad Art. 32: ~2,5M EUR - NO notificar AEPD Art. 33: ~2,0M EUR - NO comunicar afectados Art. 34: ~1,0M EUR - Agravante ocultación deliberada: +600K EUR

Comparación:

Empresa	Brecha	Notificó AEPD	Notificó Afectados	Sanción
Empresa A	Datos 50K usuarios	✅ 48h	✅ Inmediato	800K EUR (solo brecha)
Empresa B	Datos 50K usuarios	❌ 2 semanas	❌ Nunca	3,2M EUR (brecha + NO notificar + agravante)

Lección:
Transparencia post-brecha es **crítica**. Notificar rápido y completo: - Reduce sanción (agravante se convierte en atenuante cooperación) - Protege afectados (pueden tomar medidas defensivas) - Preserva reputación (honestidad apreciada vs. ocultación descubierta)

---

12. ¿Quién tiene la última palabra sobre IA: AESIA o AEPD?

Respuesta:
Depende del aspecto:

Reparto competencial claro:

Aspecto	Autoridad	Base Legal	Ejemplo
Derechos fundamentales (privacidad, dignidad, no discriminación)	**AEPD** (exclusiva)	Arts. 51-59 RGPD	Tratamiento datos personales ilícito, falta EIPD, violación derechos ARCO+
Seguridad técnica producto IA	**AESIA**	Arts. 70-75 AI Act	Incumplir requisitos precisión/robustez Art. 15 AI Act
Conformidad técnica (calidad algoritmo, no sesgos técnicos)	**AESIA**	Arts. 9-15 AI Act	Algoritmo no cumple métricas fairness técnicas
Tratamiento datos personales (bases legales, principios)	**AEPD** (exclusiva)	Arts. 5-6 RGPD	Falta base legal para procesar datos, violación minimización
Evaluación impacto (EIPD datos + FRIAS derechos fundamentales)	**Ambas** (coordinación)	Art. 35 RGPD + Art. 27 AI Act	EIPD incompleta (AEPD) + FRIAS ausente (AESIA)
Sanciones infracciones datos	**AEPD**	Art. 83 RGPD	Multa 20M EUR por tratamiento ilícito
Sanciones infracciones técnicas IA	**AESIA**	Art. 99 AI Act	Multa 15M EUR por incumplir obligaciones proveedor

Coordinación institucional:

Protocolo cooperación (proyectado): 1. **Inspecciones conjuntas** sistemas alto riesgo que traten datos 2. **Intercambio información** (respetando confidencialidad) 3. **Resoluciones coordinadas** (evitar contradicciones) 4. **Ventanilla única** empresarial (punto contacto unificado)

Supuesto conflicto:

Escenario:
AESIA determina sistema IA cumple Art. 15 AI Act (precisión técnica adecuada). AEPD determina mismo sistema vulnera Art. 5.1.d RGPD (exactitud) por sesgo discriminatorio.

¿Quién prevalece?
AEPD en materia derechos fundamentales. Conformidad técnica AI Act **NO exime** cumplimiento RGPD.

Principio:
AI Act y RGPD son **acumulativos**. Sistema debe cumplir **ambos** simultáneamente. Aprobación AESIA NO es "salvoconducto" para violar RGPD.

Recomendación DPO:
Mantener diálogo con **ambas** autoridades: - AEPD: Consultas Art. 36.3 RGPD si alto riesgo datos - AESIA: Consultas evaluación conformidad técnica - Expediente único que satisfaga a ambas

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.

La legalidad es, hoy más que nunca, una ventaja estratégica.

Llamada a la Acción para Organizaciones

Inmediato (Q1 2026): - [ ] Auditoría sistemas IA existentes (clasificación riesgo, bases legales, medidas seguridad) - [ ] Actualizar RAT incluyendo tratamientos IA específicos - [ ] Verificar contratos encargados (Art. 28.3 completo) - [ ] Iniciar EIPDs sistemas alto riesgo pendientes

Corto plazo (Q2-Q3 2026): - [ ] Implementar medidas DPbDD (seudonimización, cifrado, control acceso) - [ ] Formar personal en RGPD + AI Act (certificaciones) - [ ] Realizar auditoría externa independiente - [ ] Preparar documentación para inspección AEPD/AESIA

Antes aplicación plena AI Act (Q3 2027): - [ ] Evaluación conformidad sistemas alto riesgo - [ ] Marcado CE + Registro base datos UE - [ ] Revisión completa cadena suministro (proveedores IA) - [ ] Plan contingencia ante invalidación DPF o cambios normativos

Recursos Finales

Enlaces oficiales: - AEPD: aepd.es - Guías AEPD IA: aepd.es/inteligencia-artificial - CEPD: edpb.europa.eu - Comisión Europea AI: digital-strategy.ec.europa.eu/ai

Consultoría especializada: - DPOs certificados RGPD + AI Act - Abogados tecnología Derecho Artificial - Auditorías técnicas fairness algoritmos

---

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 | **Palabras:** 12,500+

datos.

Enlaces Internos Sugeridos (SEO Interno)

Para optimizar el SEO interno del sitio, se recomienda enlazar esta página pilar con:

1. AI Act: Guía Jurídica Completa del Reglamento Europeo
2. Evaluación de Impacto EIPD: Guía Paso a Paso
3. Bases de Legitimación RGPD: Cuándo Usar Cada Una
4. Transferencias Internacionales Post-Schrems II
5. Art. 22 RGPD: Decisiones Automatizadas en IA
6. Biometría y RGPD: Límites Legales en España
7. Contratos Encargado de Tratamiento Art. 28
8. Cláusulas Contractuales Tipo 2021: Guía Completa
9. AEPD Sanciones: Análisis Tendencias 2024-2026
10. Privacy by Design: Implementación Práctica en IA
11. Machine Unlearning: Estado del Arte Técnico-Legal
12. Responsabilidad Proactiva: Checklist DPO
13. Datos Biométricos: Protección Reforzada RGPD
14. Neurodatos y Privacidad Mental
15. FRIAS: Evaluación Impacto Derechos Fundamentales
16. Casos Prácticos RGPD: Jurisprudencia Comentada
17. Sanciones RGPD España: Base de Datos Actualizada
18. Formación DPO: Certificaciones y Recursos
19. Consultoría RGPD e IA: Servicios Profesionales
20. Newsletter Derecho Artificial: Actualizaciones Normativas