

Tema 1 Reglamento Europeo de IA: Implicaciones Básicas

Juan Aparicio &

Xavier Barber

(UMH)

Microcredencial Universitaria

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

GENERALITAT VALENCIANA

GVANEXT

Mark Zuckerberg, fundador de Facebook, comparece ante el Congreso de Estados Unidos por el escándalo de Cambridge Analytica

Redacción
BBC Mundo

10 abril 2018
Actualizado 10 abril 2018



Meta

La tensión entre el desarrollo tecnológico y su regulación

Históricamente ha existido un pulso constante entre el desarrollo tecnológico y su regulación, una contienda que la tecnología suele ganar, a pesar de los evidentes esfuerzos de los legisladores por marcar el ritmo.

Ni Perplexity ni OpenAI: Chrome se queda con Google

Un juez rechazó la propuesta del gobierno de EE.UU. de forzar a Google a vender Chrome. El navegador seguirá en manos de la tecnológica.

Google

Anthropic deberá pagar 1,500 millones de dólares a estos escritores por entrenar la IA con sus obras

Anthropic pagará al menos 3,000 dólares por cada obra que haya pirateado. La empresa descargó copias no autorizadas de libros en sus primeros esfuerzos por recopilar datos de entrenamiento para sus herramientas de IA.

🧠 Ley Europea de Inteligencia Artificial (AI Act)

🧩 **Enfoque basado en el riesgo.** Clasificación de aplicaciones de IA:

- **Riesgo inaceptable** → prohibidas (ej. scoring social, vigilancia biométrica en tiempo real).
- **Alto riesgo** → permitidas pero sujetas a supervisión estricta, evaluaciones de conformidad, gestión de riesgos, calidad de datos, transparencia y supervisión humana.
- **Riesgo limitado** → requisitos básicos de transparencia (ej. chatbots, deepfakes).
- **Mínimo riesgo** → prácticamente no reguladas (ej. filtros de spam, videojuegos).
- **IA de propósito general (GP-AI)** → transparencia en datos de entrenamiento, documentación técnica; GP-AI de alta capacidad con posible riesgo sistémico requiere evaluación adicional.

🧠 Ley Europea de Inteligencia Artificial (AI Act)

🧩 Enfoque basado en el riesgo

🛠️ Obligaciones clave

- **Proveedores de IA de alto riesgo**: gestión de riesgos, datos de calidad, documentación técnica, evaluación de impacto, auditorías externas .
- **Transparencia**: usuarios deben saber que interactúan con IA; GPT, ChatGPT, etc. deben divulgar datos de entrenamiento y licencias.
- **Sanciones**: multas de hasta el 7 % de la facturación global por incumplimiento.

🌍 Alcance extraterritorial y contexto global

- Aplica a cualquier empresa que opere o sirva al mercado europeo, incluso fuera de la UE.

🧠 Ley Europea de Inteligencia Artificial (AI Act)

🗓️ Estado y cronograma

- **Reglamento (UE) 2024/1689** aprobado: 13 marzo 2024; entró en vigor el 1 de agosto 2024
- Aplicación escalonada:

  Febrero 2025: entrada en vigor de primeras prohibiciones y restricciones con aplicación inmediata

  Agosto 2025: obligaciones sobre IA de propósito general (GP-AI)

  Agosto 2026–2027: cumplimiento completo para IA de alto riesgo .

Los tres principales modelos de gobernanza de la IA





Modelo estadounidense

1. Modelo estadounidense o “capitalismo de vigilancia”

- **Concentración de poder**

Un pequeño número de proveedores de servicios digitales disfruta de un poder de mercado preponderante y de ventajas informativas digitales, especialmente de control sobre los datos de los usuarios y sobre la publicidad.

- **Mercantilización de los datos**

Los datos personales se convierten en mercancía: se analizan y venden con fines comerciales.

🧠 Este modelo prioriza el beneficio económico sobre la privacidad, con una regulación laxa y un fuerte dominio de grandes plataformas tecnológicas.

Modelo chino

2. Modelo chino o “estado digital totalitario”

- **Control estatal total**

El Estado emplea tecnologías avanzadas como el reconocimiento facial, sensores y big data para vigilar masivamente a la población y controlar el comportamiento social.

- **Sistema de scoring social**

Se evalúan las acciones de los ciudadanos y empresas, asignando puntuaciones que determinan el acceso a servicios (créditos, viajes, empleos).

- **Tecnología al servicio de la estabilidad política**

La digitalización se usa como herramienta de control social, reforzando la autoridad del Partido Comunista.

🧠 Este modelo prioriza la seguridad y el orden público por encima de las libertades individuales, con una fuerte inversión estatal en tecnología y sin apenas regulación de privacidad.

Modelo europeo

3. Modelo europeo o “humanista”

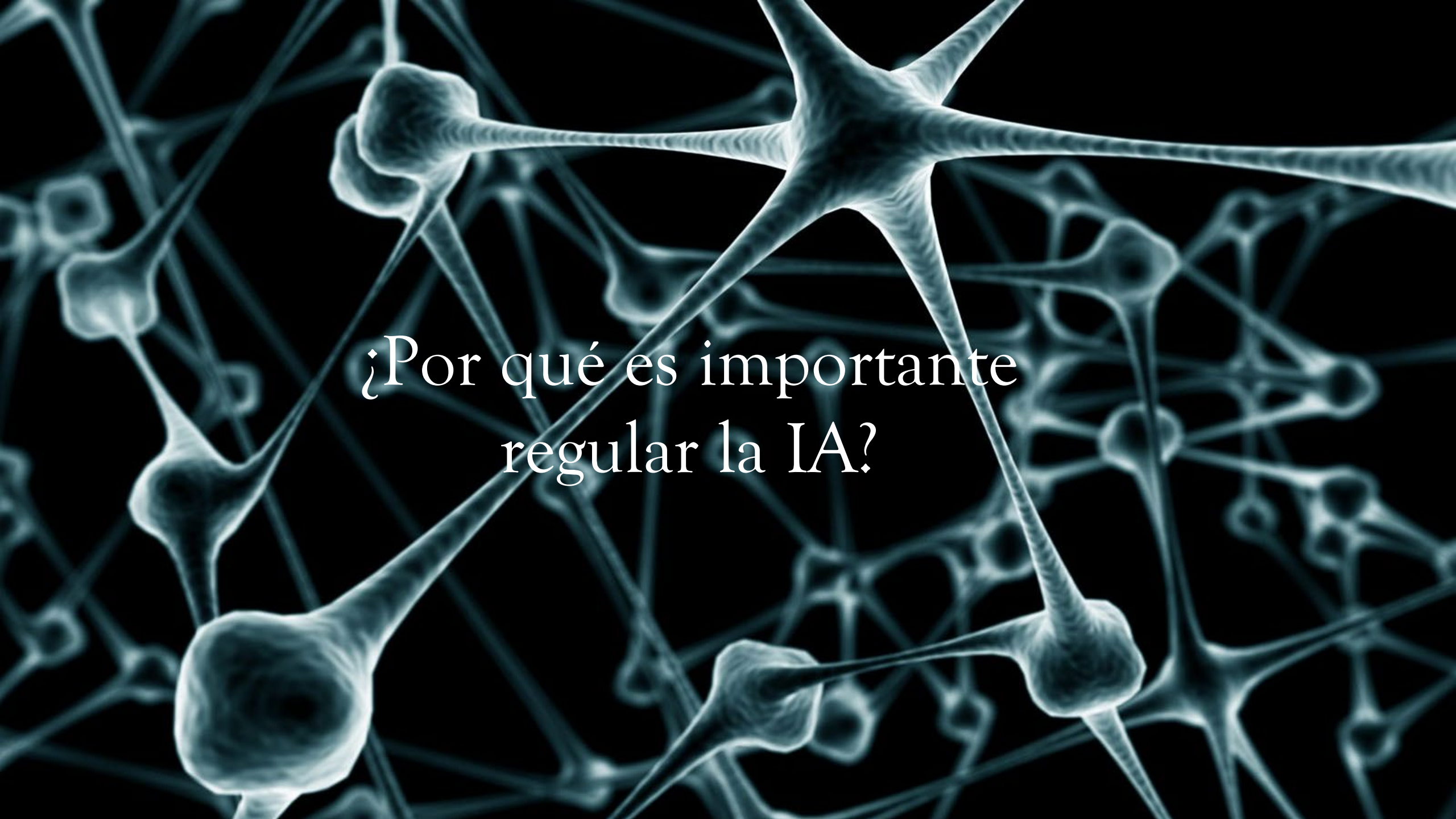
- **Regulación centrada en derechos fundamentales**

Los proveedores de servicios digitales están limitados por normas estrictas de la Unión Europea, que prioriza la **protección de los valores democráticos y la privacidad** de los usuarios.

- **IA regulada con enfoque ético**

La propuesta de **regulación europea sobre la Inteligencia Artificial** (AI Act) busca asegurar un uso confiable, transparente y seguro de estas tecnologías, siendo una de las regulaciones más exigentes a nivel global.

🧠 Este modelo promueve una digitalización al servicio del ciudadano, defendiendo la dignidad humana frente al beneficio comercial o al control estatal.


¿Por qué es importante
regular la IA?

Riesgos éticos

La IA puede tomar decisiones que afectan directamente a las personas. Por ello, es fundamental que su desarrollo y uso sigan **principios éticos** que garanticen un funcionamiento **justo, seguro y responsable**, evitando **daños** y **discriminación injusta**.

🧩 **Riesgos éticos comunes:**

🔸 **Discriminación algorítmica**

Los sistemas de IA pueden generar sesgos injustos en decisiones clave (empleo, créditos, justicia), perpetuando desigualdades por género, raza u origen.

🔸 **Generación de contenido nocivo**

Los modelos generativos pueden difundir información falsa, dañina o difamatoria, comprometiendo la **integridad** y la **veracidad** de los contenidos **(Deepfakes)**.

Protección de datos y privacidad en la IA

La inteligencia artificial maneja grandes volúmenes de datos personales, lo que genera **riesgos importantes para la privacidad y la seguridad** de la información. Las regulaciones buscan asegurar que estos datos se traten de forma **segura y respetuosa** con los derechos fundamentales.

⚠️ **Riesgos clave:**

🔸 **Brechas de seguridad**

Los sistemas de IA pueden ser vulnerables a ciberataques, exponiendo datos personales y sensibles.

🔸 **Vigilancia invasiva**

El uso de tecnologías como el reconocimiento facial o de voz para el seguimiento constante puede **afectar gravemente la privacidad y la autonomía** individual.



Reglamento de IA en Europa

Reglamento de IA en Europa

🛡️ Seguridad en los sistemas de IA

La **seguridad** es una prioridad clave en la regulación europea de la inteligencia artificial. El Reglamento busca garantizar que los sistemas de IA sean **seguros para las personas y las organizaciones**, minimizando riesgos y consecuencias negativas.

🔍 ¿Qué implica?



Prevención de **fallos técnicos** o de diseño

Evitar el **uso indebido** o malintencionado

Protección frente a riesgos para la **vida, salud y bienestar**

🚗 **Ejemplo:** IA aplicada a **vehículos autónomos**, donde un fallo puede tener consecuencias críticas.

Reglamento de IA en Europa



🔍 Transparencia en la inteligencia artificial

La regulación europea promueve la **divulgación clara de cómo funcionan los sistemas de IA**, para que usuarios y partes interesadas puedan **comprender su lógica de decisión** y actuar con mayor conocimiento.

🎯 Objetivo:

Fomentar la **confianza** y la **toma de decisiones informadas** por parte de usuarios, desarrolladores y autoridades.

💡 Ejemplo:

IA utilizada en **análisis de crédito**, donde es crucial entender los criterios que afectan la aprobación o denegación.

Reglamento de IA en Europa



🔁 Trazabilidad y no discriminación en la IA

La **trazabilidad** implica que debe ser posible **rastrear cómo se tomó una decisión** automatizada, lo cual es esencial para **detectar errores o sesgos** y garantizar sistemas auditables.

Además, la regulación prohíbe cualquier forma de **discriminación algorítmica**, asegurando que las decisiones no se vean afectadas por **origen étnico, género u otros factores protegidos**.

🧪 Ejemplo:

IA utilizada en **procesos de selección de personal** (filtros automáticos de CV).

Reglamento de IA en Europa



🧍 Supervisión humana en la inteligencia artificial

Aunque los sistemas de IA pueden realizar tareas complejas, es esencial que **las decisiones significativas sean supervisadas por personas**. Esta intervención humana garantiza un control adecuado y **previene consecuencias negativas** derivadas de errores o automatismos inadecuados.

🩺 Ejemplo:

IA aplicada al **diagnóstico médico**, donde el juicio profesional sigue siendo indispensable.

Sistemas de IA prohibidos

🧠 **Manipulación cognitiva:** Están prohibidos los sistemas de IA que manipulen el comportamiento de personas, **especialmente si pertenecen a grupos vulnerables**.

⚠️ **Ejemplos:**

- **Juguetes activados por voz** que promuevan conductas peligrosas en menores.
- **Explotación de vulnerabilidades** relacionadas con la edad, discapacidad u otras condiciones.

Sistemas de IA prohibidos

📊 **Puntuación social**

Está prohibida la utilización de IA para la **clasificación de personas** en función de: su comportamiento, su estatus socioeconómico, o sus características personales.

🧬 **Identificación biométrica y detección emocional**

Queda prohibido el uso de:

🔹 **Sistemas de identificación biométrica** en tiempo real y a distancia, como el **reconocimiento facial** en **espacios públicos**, debido a su carácter invasivo y su riesgo para los derechos fundamentales.

🔹 **Inferencia de emociones** en contextos sensibles como: gestión de fronteras, lugares de trabajo y centros educativos.