

Desayuno-Coloquio  
IA, regulación y economía

# Claves del Reglamento IA

## Nuevas exigencias y cumplimiento

José Manuel Muñoz Vela

Abogado especialista Derecho Tecnológico e IA  
Doctor en Derecho  
Director Jurídico

ADEQLA

06 de marzo de 2025



## Ponente



**José Manuel Muñoz Vela**

Abogado especialista en Derecho Tecnológico e IA, con una trayectoria profesional de 25 años de experiencia de ejercicio de la abogacía a nivel nacional e internacional en las áreas indicadas. Socio y Director Jurídico de ADEQUA CORPORACIÓN.

Licenciado y Doctor en Derecho (Derecho de la Inteligencia Artificial) por la Universidad de Valencia, Premio Extraordinario de Doctorado, con amplia formación especializada en las áreas jurídica y tecnológica en entidades como la UV, el BI, el MIT o el Instituto de Empresa (IE). Ostenta distintos premios (Premio de investigación ISACA, Tomás y Valiente o García Goyena), reconocimientos y certificaciones internacionales como CISA, CISM, CGEIT, CRISC y CDPSE, así como las nacionales ACP o DPD.

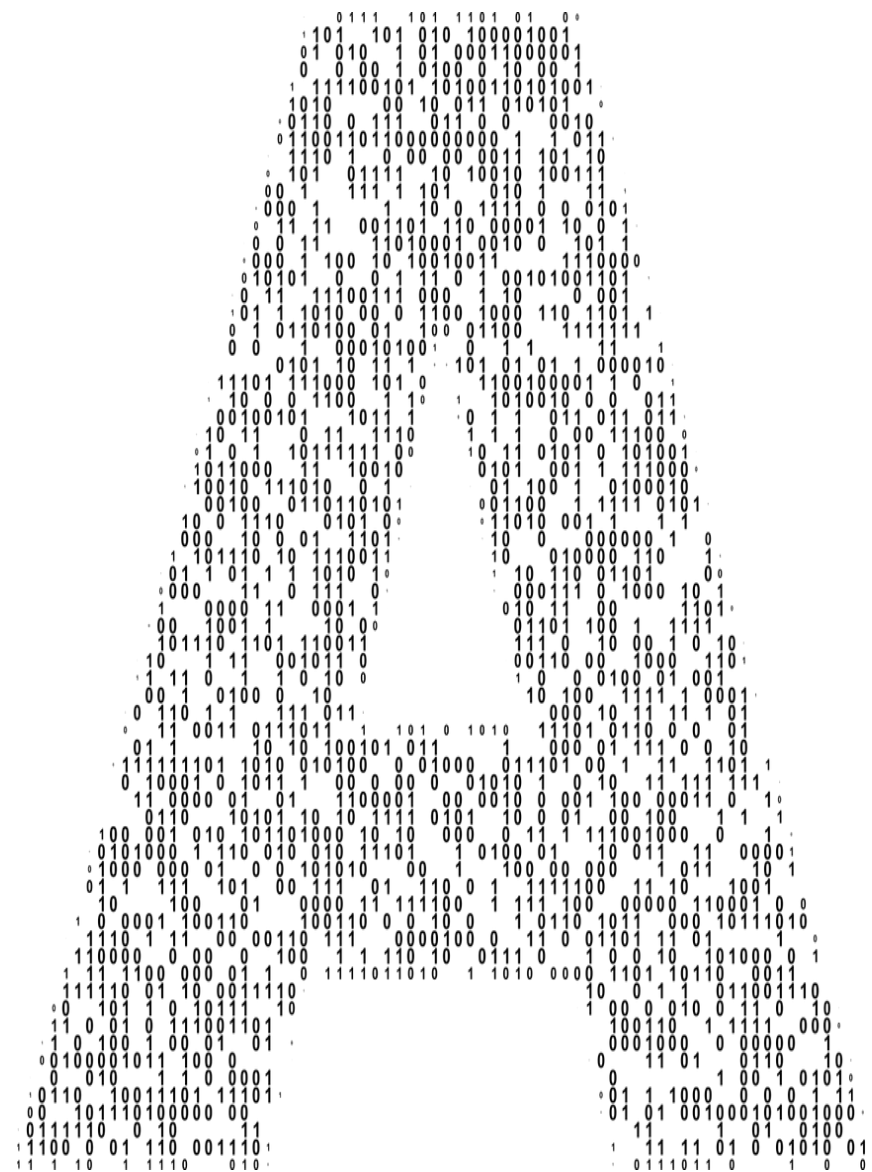
Es profesor en distintos programas y masters para distintas entidades y universidades en Derecho Digital e IA, así como ponente en congresos y jornadas. Es investigador en materia de Derecho de la Inteligencia Artificial y autor de múltiples artículos de investigación, monografías y otras publicaciones en materia de Derecho Digital e Inteligencia Artificial.

Pertenece a distintas organizaciones y asociaciones nacionales e internacionales del sector tecnológico y digital, y ostenta distintos cargos y funciones en las mismas.



# ¿Inteligencia artificial?





Tecnología

Estratégica

Alto impacto

Potencial disruptivo

Potencial habilitador (TD)






*“La IA será más relevante y supondrá un cambio más profundo que el fuego, la electricidad o internet”.*

Sundar Pichai,  
CEO de Google



*“La IA será comparable a la revolución industrial”.*

Geoffrey Hinton  
Premio Nobel de Física 2024



*“Mitigar el riesgo de extinción de la IA debería ser una prioridad mundial junto con otros riesgos a escala social, como las pandemias y la guerra nuclear”.*

Center for AI Safety  
Mayo 2023





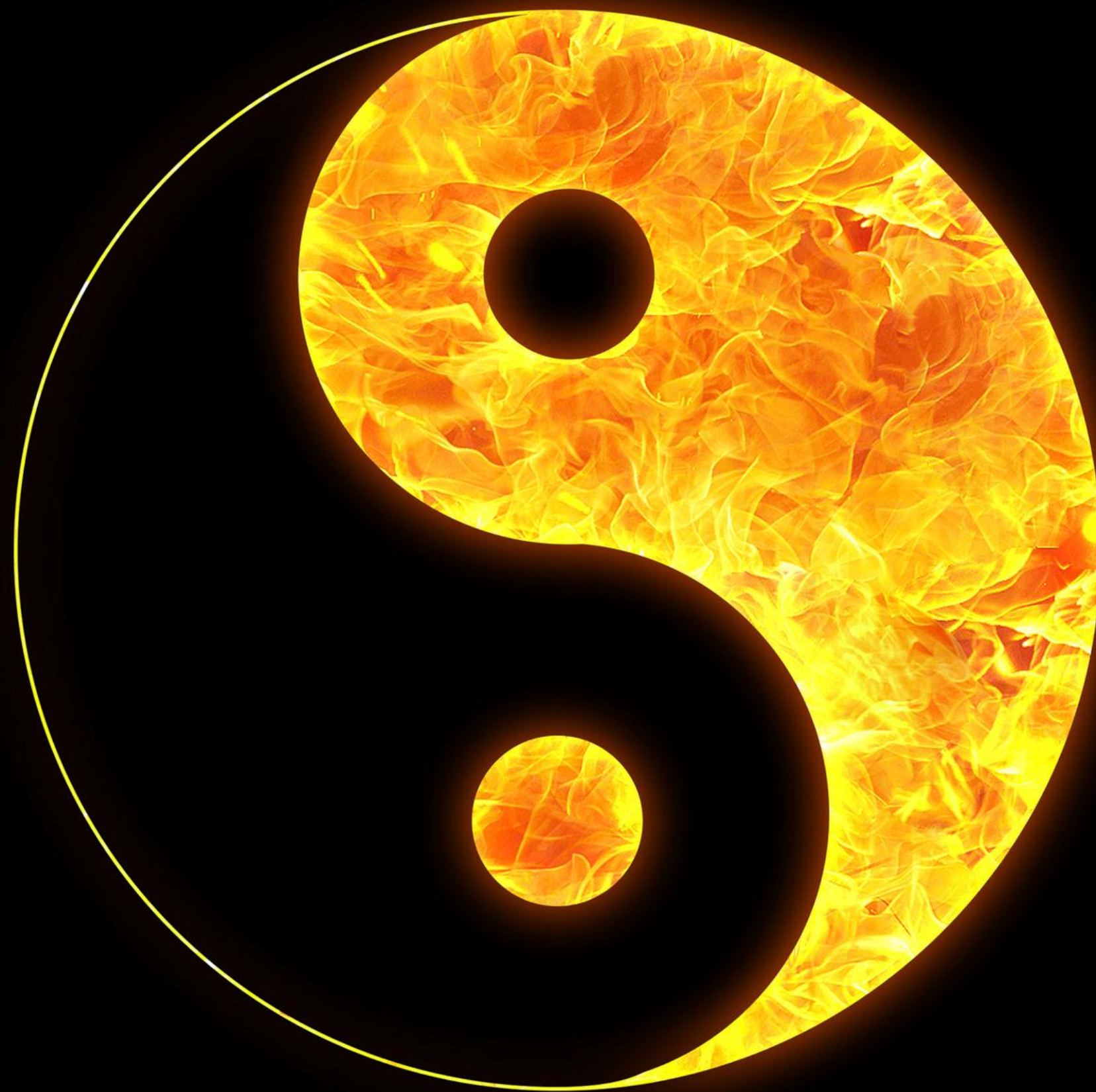
*“El riesgo de que una máquina pensante tome sus propias decisiones en contra de los seres humanos es real”.*

Geoffrey Hinton & John Hopfield  
2024

Fuente: La Vanguardia  
<https://envios.lavanguardia.com>



FEAR?







*“La inteligencia artificial puede ser lo mejor o lo peor que nos ha sucedido a la humanidad”*

Stephen Hawking


# Retos y riesgos





**Riesgos para la privacidad**    **Infrautilización de la IA**    **Diversidad**  
**Uso o aplicación excesiva**    **Asimetría y asincronía**  
**Accesibilidad**    Incapacidad de la IA para representar una realidad social compleja  
**Privacidad**    **Seguridad**    **Riesgos para el mercado y los consumidores**  
**Equidad, discriminación, sesgo**    **Destrucción de empleo**  
**Explicabilidad**    Afectación otros derechos fundamentales    **Confidencialidad**  
Falta de calidad de los datos y conocimientos de entrada    **Veracidad**    **Hacking**  
**Inadecuada o negligente definición, configuración, funcionamiento o uso**    **Conectividad**  
**Responsabilidad**    **Transformación de las relaciones sociales**    **Error**  
**Erosión de sistemas democráticos**    **Interoperabilidad**    **Continuidad**  
**Resiliencia**    **Usos maliciosos y delictivos**    **Accountability**  
**Riesgos para la seguridad física y moral**    **Riesgos sobre bienes e instalaciones**  
**Riesgos asociados a su uso con fines de defensa**    **Desconexión**    **Riesgo de confusión**  
**Transparencia**    **(Des)información**    **Riesgos medioambientales**  
**PI**    **Sostenibilidad**    **Ausencia de normas éticas vinculantes**  
Ausencia de marcos reguladores específicos y falta de adecuación de los existentes





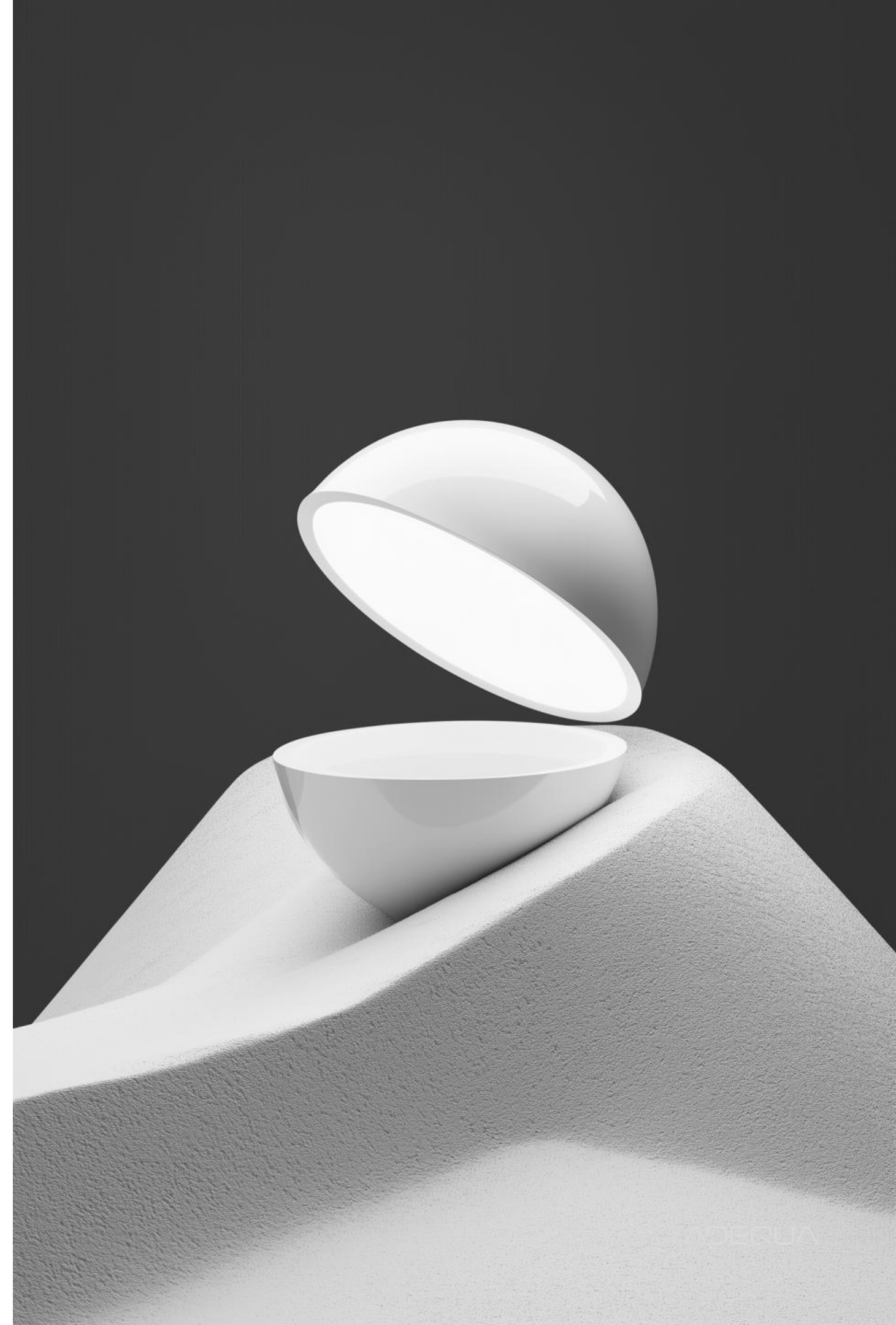
*“El mayor riesgo no es la tecnología sino el uso que se haga de ella, en atención especialmente a sus capacidades”*

*La regulación de la inteligencia artificial. Reto y oportunidad desde una perspectiva global e internacional*

José Manuel Muñoz Vela

Editorial Aranzadi. Octubre 2024

# Soluciones





1. Políticas

2. Éticas

3. Jurídicas (Legales, contractuales y corporativas)

4. Judiciales

5. Normalización y Estandarización

6. Agencia internacional

7. Otras



# Jurídicas \_ Legales






## Regulación legal

☐ SI

☐ NO

☐ NS/NC



*“Hay más regulaciones para las tiendas de sándwiches que para las empresas de inteligencia artificial”*

Stuart Russell

UE



Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre la Inteligencia Artificial -**Artificial Intelligence Act**- + **Legislación de armonización**.

Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024 sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo

Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la **adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial** (Directiva sobre la responsabilidad de la IA). COM(2022) 496 final. 2022/0303 (COD). [Nueva evaluación de impacto complementaria de septiembre de 2024 y exclusión del Programa de Trabajo 2025]

Reglamento sobre los **requisitos de ciberseguridad para los productos con componentes digitales** (Cyber Resilience Act). Propuesta. 15.9.2022. COM(2022) 454 final

**Convenio del Consejo de Europa** sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho

**Código de conducta UE-EEUU** sobre inteligencia artificial

Otros instrumentos: **Código de Buenas Prácticas** para la IA de propósito general



# Reglamento IA de la UE

## Claves

1. **Objetivo:** Establecer un marco jurídico uniforme para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la UE, de conformidad con los valores de la Unión, que a su vez promueva la adopción de una IA centrada el ser humano y fiable que garantice un alto nivel de protección de la salud, la seguridad y los derechos fundamentales, que proporcione protección frente a sus efectos perjudiciales en la UE y que apoye la innovación, mejorando el funcionamiento del mercado interior
2. **Definición:** OCDE
3. **Estructura:** 180 considerandos, 13 capítulos, 113 artículos y 13 anexos
4. **Principales rasgos:** Primera norma en el mundo que pretendía regular la IA de manera global y horizontal desde un enfoque de riesgos. Norma de primera generación de pretendida eficacia universal intensa.

## 5. Clasificación de los sistemas (enfoque de riesgos):

- Sistemas de IA de riesgo inadmisibles: Prohibidos
- Sistemas de IA de alto riesgo
- Sistema de IA de riesgo medio o limitado
- Sistema de IA de riesgo bajo o mínimo
- Modelos de IA de uso general con/sin riesgo sistémico
- Sistema de IA no clasificado

No se aplica: Sistemas de IA con fines militares, de defensa o de seguridad nacional (con matices), sistemas o modelos de IA (incluyendo sus resultados de salida), exclusivamente desarrollados y puestos en servicio con fines de investigación y desarrollo científico, ni tampoco a actividades de investigación, prueba o desarrollo relativa a sistemas o modelos de IA antes de su introducción en el mercado o puesta en servicio, a sistemas de IA divulgados con arreglo a licencias libres y de código abierto salvo excepciones, ni a los responsables del despliegue (usuarios) que sean personas físicas que los usen en el ámbito doméstico (actividad no profesional ni empresarial)

## 6. Sistemas prohibidos

### Art. 5

- a) Sistemas o aplicaciones de IA que tengan como objetivo o comporten manipular subliminalmente el comportamiento humano de forma que se cause un daño a sí mismo o a terceros;
- b) Sistemas diseñados o que se aprovechen de la vulnerabilidad de una persona o colectivo por razones de edad, discapacidad, situación social o económica específica, que tengan como objetivo o conlleven la manipulación sustancial de su comportamiento causando un perjuicio o siendo probable que se cause;
- c) Sistemas que permiten la evaluación o clasificación de personas o colectivos (puntuación o *scoring* social) con fines públicos o privados y que comporten determinados perjuicios;
- d) Sistemas para la evaluación o predicción del riesgo de comisión de delitos por parte de una persona basados exclusivamente en la elaboración de su perfil o de los rasgos y características de su personalidad (salvo para apoyar valoración humana de la implicación de una persona en una actividad delictiva);
- e) Sistemas de categorización biométrica que clasifiquen individualmente a personas físicas basándose en sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual (con excepciones)
- f) Sistemas de identificación biométrica remota en tiempo real y en espacios de acceso público con fines de garantía de aplicación del Derecho (con excepciones)
- g) Sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante el *scraping* no selectivo de imágenes faciales de Internet o de grabaciones de CCTV;
- h) Sistemas de IA para inferir emociones de una persona física en el lugar de trabajo y en los centros educativos (excepto por razones médicas o de seguridad).
- i) Otros que infrinjan cualquier otra Disposición del Derecho de la UE

## 7. Sistemas de alto riesgo

Art. 6, 7, Anexo III y disposiciones concordantes

7.1. Sistemas de IA destinados a ser utilizados como componente de seguridad en productos sujetos a la legislación armonizada de seguridad de los productos de la UE del Anexo I (Juguetes, aviación, automóviles, dispositivos médicos o ascensores) o sean el producto en sí mismo (si debe someterse a evaluación de conformidad de terceros).

7.2. Sistemas expresamente clasificados de alto riesgo para la salud y la seguridad o los derechos fundamentales (Revisables, ampliables y con excepciones) contemplados en el Anexo III:

- a) Sistemas de identificación biométrica remota (con excepciones);
- b) Sistemas de IA destinados a ser utilizados para la categorización biométrica en función de atributos o características sensibles o protegidos basada en la inferencia de dichos atributos o características;
- c) sistemas de IA destinados a ser utilizados para el reconocimiento de emociones;
- d) sistemas destinados a ser utilizados como componentes de seguridad en la gestión y funcionamiento de infraestructuras digitales críticas, de tráfico rodado o del suministro de agua, gas, calefacción o electricidad;
- e) sistemas a ser utilizados en educación y formación profesional con determinadas finalidades;
- f) sistemas a ser utilizados en materia de empleo, gestión de los trabajadores y acceso al autoempleo con determinadas finalidades;
- g) sistemas a ser utilizados para determinadas finalidades en ámbito del acceso y utilización de servicios privados y públicos esenciales o prestaciones públicas esenciales (incluye asistencia sanitaria, calificación crediticia o evaluación de riesgos y tarificación en el sector de los seguros);
- h) sistemas a ser utilizados con determinadas finalidades por las autoridades garantes del cumplimiento del Derecho o entidades, órganos u organismos en apoyo de éstas;
- i) sistemas a ser utilizados para la gestión de migración, asilo y control de fronteras con determinadas finalidades (siempre que su uso esté permitido por el Derecho de la UE o nacional aplicable);
- j) sistemas a ser utilizados en el ámbito de la Administración de justicia y en procesos democráticos con concretas finalidades.



## 8. Requisitos y obligaciones esenciales para sistemas de alto riesgo

- Requisitos legislación de armonización
- Sistema de análisis y gestión de riesgos
- Medidas de mitigación y control
- Información y formación a responsables del despliegue
- Gobernanza y gestión de datos (Datos de entrenamiento, validación y prueba)
- Documentación técnica y actualización
- Registro automático de eventos durante su ciclo de vida: Trazabilidad.
- Transparencia y suministro de información a los usuarios
- Vigilancia y control humano durante su funcionamiento
- Precisión, solidez y ciberseguridad
- Gestión de la calidad
- Conservación de información y registros
- Evaluación de conformidad (declaración) antes de su comercialización o puesta en servicio
- Registro
- Certificaciones, declaración UE de conformidad y marcado CE de conformidad
- Vigilancia poscomercialización
- Accesibilidad
- Cooperación y prueba de conformidad a requerimiento de autoridad
- Evaluaciones de impacto en derechos fundamentales (EIDF)

## 9. Sujetos obligados

Art. 2

Operadores... Proveedores, fabricantes de productos, responsables del despliegue, representantes autorizados, importadores o distribuidores, personas afectadas ubicadas en la UE. También proveedores y responsables del despliegue de sistemas de IA que estén en un tercer país cuando los resultados de salida generados por el sistema de IA se utilicen en la UE.

## 10. Medidas de apoyo a la innovación

Art. 57 y ss.

Espacios controlados de pruebas (*sandboxes*)

Medidas de apoyo a pymes y startups (acceso prioritario a sandbox, sensibilización y formación específicas, canales de comunicación y respuesta específicos, fomento de su participación en la normalización, reducción de tasas o simplificación de sistemas)

## **11. Gobernanza de la IA**

Art. 64 y ss

Oficina de IA (Decisión 24.01.2024)

Consejo Europeo de IA

Foro consultivo

Grupo de expertos científicos (independientes)

Autoridades nacionales estados miembros (España > AESIA)

## **12. Instrumentos de acompañamiento y desarrollo**

Art. 95, siguientes y concordantes

Actos delegados y de ejecución, códigos de conducta, directrices de la Comisión para su aplicación práctica, etc.

## **13. Normalización y estandarización**

Art. 40 y ss

Decisión de Ejecución de la Comisión de 22.5.2023

Comité Europeo de Normalización (CEN), Comité Europeo de Normalización Electrotécnica (CENELEC) e Instituto Europeo de Normas de Telecomunicación (ETSI)

Objeto: terminología, marcos de referencia, sistemas de gestión de riesgos, gobernanza y calidad de los conjuntos de datos utilizados, registro automático de eventos (trazabilidad), transparencia e información para los usuarios, supervisión humana, especificaciones de precisión, robustez, ciberseguridad, sistema de gestión de la calidad para proveedores y evaluaciones de la conformidad

Normalización internacional ISO/IEC. Comité de Normalización ISO/IEC JTC 1 SC 42



## **14. Evaluación y revisión**

Art. 112

Distintos mecanismos. Ejemplo: Revisión anual del listado de sistemas de alto riesgo del Anexo III y sistemas prohibidos (Art. 5).

## **15. Régimen sancionador**

Art. 99 a 101

Incorpora las bases de los regímenes sancionadores que deberán establecer los Estados miembros, como instrumento conminatorio para el cumplimiento de las obligaciones previstas en el mismo.

Las sanciones previstas pueden ascender hasta 35.000.000€ o el 7 % del volumen de negocios mundial, total y anual de la empresa infractora correspondiente al ejercicio anterior, si esta cifra es superior.

## 16. Modificación de otros instrumentos normativos

Art. 102 a 110

Modificación del Reglamento (CE) nº 300/2008, el Reglamento (UE) nº 168/2013, la Directiva 2014/90/UE, la Directiva (UE) 2016/797, el Reglamento (UE) 2018/858, el Reglamento (UE) 2018/1139, el Reglamento (UE) 2019/2144 y la Directiva (UE) 2020/1828

## 17. Entrada en vigor y aplicación


Art. 113

Publicado DOUE el 12.07.2024 y en vigor a los 20 días, esto es, desde 1 de agosto. No aplicable hasta dentro de dos (2) años, con excepciones:

- Los capítulos I y II (Disp. Gen. y prohibidos) aplicables a partir del 2 de febrero de 2025
- El capítulo III, sección 4 (Autoridad notificante y organismos notificados), el capítulo V (Modelos IA uso general), el capítulo VII (Gobernanza), el capítulo XII (Sanciones) y el artículo 78 (Confidencialidad) serán aplicables a partir del 2 de agosto de 2025 (a excepción del artículo 101-Multas a proveedores de modelos de IA de uso general)
- El artículo 6, apartado 1, y las obligaciones reguladas en el Reglamento serán aplicables y exigibles a partir de 2 de agosto de 2027.



# España



Real Decreto-ley 9/2021 (“Ley Riders”)

Ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la CV. Art. 16.

Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación. Art. 23.

Ley 28/2022, de 21 de diciembre, de fomento del ecosistema de las empresas emergentes. Disposición Adicional Séptima. Agencia Española de Supervisión de Inteligencia Artificial

Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la IA en Extremadura

Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial. 16.10.2023

Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial

Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial

Orden TDF/619/2024, de 18 de junio de 2024, ha creado y regulado el Consejo Asesor Internacional en Inteligencia Artificial



The background features a light gray, textured surface resembling torn paper or a topographical map. In the bottom left corner, there is a network diagram consisting of five white spheres of varying sizes connected by thin white lines. A small orange vertical bar is located in the top left corner.

# Internacional

**EE.UU.:** ~~Executive Order 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence 30.10.2023. AI Civil Rights Act 24.09.2024.~~ A nivel estatal: California (Proyecto de Ley 1047 del Senado de California), Connecticut, Florida, Luisiana, Minnesota, Montana, Texas, Virginia, Illinois, Alabama, Washington, Nueva York, Vermont, Tennessee o Colorado. A nivel local, Boston, Miami, Nueva York, San José (California) y Seattle.

**Canadá:** Ley de Datos e Inteligencia Artificial (AIDA)

**UK:** *A pro-innovation approach to AI regulation 29.03.2023.* Proyecto de Ley de Protección de Datos e Información Digital.

**China:** *Internet Information Service Algorithmic Recommendation Management Provisions (2022), Shenzhen AI Regulation aims to promote the AI industry (2022) y Shanghai Regulations on Promoting the Development of the AI Industry. Medidas Administrativas para los Servicios de IA generativa 15.08.2023.*

**Canadá, Brasil, Colombia, Chile, Argentina, México, Perú, Turquía, Kenia, Nigeria, Egipto, Emiratos Árabes Unidos, India, Rusia, Japón, Corea del Sur, Singapur, Vietnam, Israel.....**



## **Reglamento IA de la UE**

Prohibiciones, requerimientos y obligaciones exigibles desde el 2 de febrero de 2025

- Sistemas prohibidos (artículo 5)
- Alfabetización (artículo 4)



## Sistemas prohibidos

Directrices sobre prácticas de inteligencia artificial prohibidas  
Comisión Europea 04.02.2025

### Acceso

[https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act?pk\\_source=ec\\_newsroom&pk\\_medium=email&pk\\_campaign=Shaping%20Europe%27s%20Digital%20Future%20website%20updates](https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act?pk_source=ec_newsroom&pk_medium=email&pk_campaign=Shaping%20Europe%27s%20Digital%20Future%20website%20updates)



## Ejemplo

### Scraping:

- La noción de “no selectiva” significa sin un enfoque específico en un individuo o grupo de individuos determinados. Si se le ordena a una herramienta de *scraping* que recopile imágenes o vídeos que contengan solo rostros humanos de individuos específicos o de un grupo predefinido de personas, entonces el *scraping* se convierte en selectivo o dirigido. Por ejemplo, el que se usa para buscar a un delincuente en concreto, no está bajo la prohibición.
- La combinación de *scraping* selectivo con no selectivo entraría dentro de la prohibición.
- El *scraping* debe realizarse en internet o en CCTV. La publicación de una imagen en redes, evidentemente, no equivale a consentimiento.
- Cuando un sistema de IA recibe una fotografía de una persona y busca coincidencias del rostro en Internet, es decir, "motores de búsqueda de imágenes de ingeniería inversa", esto se considerará extracción selectiva.

No aplica, por ejemplo, cuando se extraen datos biométricos distintos de los faciales, cuando no se usa IA o la base de datos no se utiliza para reconocimiento de personas (Ej. Para entrenar modelos de IA).

Sin perjuicio de que sea contrario al RGPD.

## Alfabetización

Todas las empresas que operen en la UE como proveedoras o entidades usuarias (responsable del despliegue del sector público o privado) de cualquier sistema inteligente deben garantizar que su personal involucrado en el funcionamiento y uso del mismo, posea conocimientos suficientes y adecuados a su perfil sobre IA. Esto incluye desde ingenieros hasta equipos de RRHH que utilicen herramientas de reclutamiento asistidas por IA.

Prácticas para el fomento del aprendizaje y el intercambio sobre alfabetización en IA, exigida por el artículo 4 del Reglamento IA de la UE. Oficina Europea IA 04.02.2025

### Acceso

[https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy?pk\\_source=ec\\_newsroom&pk\\_medium=email&pk\\_campaign=Shaping%20Europe%27s%20Digital%20Future%20website%20updates](https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy?pk_source=ec_newsroom&pk_medium=email&pk_campaign=Shaping%20Europe%27s%20Digital%20Future%20website%20updates)

# Recomendaciones

- ❑ Identificar y catalogar los sistemas y modelos de IA que utilicen o pretenden utilizar/desarrollar, licencias y usos
- ❑ Identificar si utilizan tecnologías prohibidas, como el reconocimiento de emociones en entornos laborales o educativos
- ❑ Definir políticas y normas de uso adecuado
- ❑ Implementar programas de formación, capacitando a empleados en materia de IA, riesgos, normas éticas y corporativas de uso, y requisitos legales.

Pero también:

- ❑ Revisar los procesos/procedimientos de selección y contratación de modelos, sistemas y proveedores
- ❑ Definir políticas y requerimientos de adquisición, desarrollo, integración y despliegue (Ej. AAPP – Transparencia, explicabilidad, no discriminación, responsabilidad...)
- ❑ Revisar los licencias, pliegos y contratos con proveedores, con la finalidad de asegurar que los modelos y sistemas de IA de terceros cumplan con requisitos legales y obligaciones exigidas a sistemas, modelos, proveedores y usuarios (Ej. La transparencia exigida tanto en el ámbito privado como público)
- ❑ Y, en función del contexto de la entidad usuaria y sistemas implicados, crear un comité de gobernanza de IA o CAIO (Chief AI officer), designando responsables de supervisar el cumplimiento y gestionar los riesgos asociados a la IA.

Esto es solo el inicio. En agosto de 2025 serán exigibles las disposiciones para modelos de IA de propósito general (como GPT-4), y el resto sucesivamente. Prepararse hoy no es una opción, sino una necesidad

# Referencias bibliográficas:



MUÑOZ VELA, J.M. (Octubre 2024). *La regulación de la inteligencia artificial. Reto y oportunidad desde una perspectiva global e internacional*. Editorial Aranzadi.



MUÑOZ VELA, J.M. y Otros (Octubre 2024). *Comentarios al Reglamento Europeo de Inteligencia Artificial*. Editorial Aranzadi La Ley.

Otras referencias bibliográficas personales: MUÑOZ VELA, J.M. (2024). “Retos, riesgos y responsabilidad de la inteligencia artificial”, en GIMÉNEZ, I. (Cor) (2024) *Inteligencia Artificial. Retos y oportunidades*. Editorial Fundación de Estudios Bursátiles y Financieros; MUÑOZ VELA, J.M. (2023). “IA y responsabilidad civil. Comentarios a las propuestas europeas en materia de derechos de daños por productos defectuosos y adaptación de las normas de responsabilidad civil extracontractual”. Revista Aranzadi de derecho y nuevas tecnologías. Nº. 61. Editorial Aranzadi (Thomson Reuters); MUÑOZ VELA, J.M. (2023). “Inteligencia artificial generativa. Desafíos para la propiedad intelectual”. (1º Premio Nacional de artículos de investigación García Goyena). Revista de Derecho UNED. 2024; MUÑOZ VELA, J.M. (2023) “Inteligencia artificial y derecho de autor. Creaciones artificiales y su protección jurídica”, en Martínez Velencoso, L.M. y Plaza Penadés, J. (Dir.) (2023), *Retos normativos del mercado único digital europeo*. Tirant Lo Blanch; MUÑOZ VELA, J.M. (2022). “Avanzando en la regulación de la IA. Hacia un equilibrio entre ética, protección de los derechos fundamentales, seguridad, confianza, innovación, desarrollo y competitividad”. Derecho Digital e Innovación. Núm. 14. Octubre-Diciembre. 2022. Ed. Wolters Kluwer; MUÑOZ VELA, J.M. (2022). Retos, riesgos, responsabilidad y regulación de la inteligencia artificial. Un enfoque de seguridad física, lógica, moral y jurídica. Editorial Aranzadi (Thomson Reuters); MUÑOZ VELA, J.M. (2022). “Avanzando en la regulación de la IA. Hacia un equilibrio entre ética, protección de los derechos fundamentales, seguridad, confianza, innovación, desarrollo y competitividad”. *Derecho Digital e Innovación*. Núm. 14. Octubre-Diciembre. 2022. Ed. Wolters Kluwer; MUÑOZ VELA, J.M. (2022). “Inteligencia artificial y Cuestiones de propiedad intelectual e industrial”. *Revista Aranzadi de derecho y nuevas tecnologías*. Nº. 59. 2022. Editorial Aranzadi (Thomson Reuters); MUÑOZ VELA, J.M. (2022). “Inteligencia artificial y responsabilidad penal”. Derecho Digital e Innovación. Núm. 11. Enero-Marzo 2022. Ed. Wolters Kluwer; MUÑOZ VELA, J.M. (2021). *Cuestiones éticas de la Inteligencia Artificial y repercusiones jurídicas. De lo dispositivo a lo imperativo*. Thomson Reuters Aranzadi





# Gracias por su atención

[josemanuel@adequa.eu](mailto:josemanuel@adequa.eu)

Advertencia legal: Esta presentación puede contener materiales, imágenes u otros contenidos protegidos por leyes y tratados nacionales e internacionales en materia de Propiedad Intelectual e Industrial. Los derechos sobre los mismos quedan reservados para sus respectivos titulares, especialmente respecto de noticias publicadas en medios de comunicación en su versión pública digital, sin perjuicio de su inclusión a efectos meramente ilustrativos o ejemplificativos. Se halla prohibido su uso comercial, su reproducción total o parcial, su uso para entrenamiento de modelos o sistemas inteligentes, así como su tratamiento informático, copia, divulgación, comunicación a terceros, transmisión, distribución, préstamo o cualquier otra forma de cesión o comunicación de la misma a terceros sin autorización. Agradecimiento especial a Pixabay como fuente de distintos contenidos gráficos ilustrativos (fotos) y a sus autores.