URÍA
MENÉNDEZ

Client briefing
PROTECCIÓN DE DATOS
17 de julio de 2024

Principales novedades del Reglamento (UE) de Inteligencia Artificial

Tras largas negociaciones entre las instituciones europeas, el Parlamento Europeo aprobó el 13 de marzo de 2024 el Reglamento de Inteligencia Artificial, cuyo texto final se ha publicado en el *Diario Oficial de la Unión Europea* el 12 de julio de 2024.

Al tratarse de la normativa de alcance más ambicioso aprobada sobre esta materia hasta la fecha en el mundo, el Reglamento de Inteligencia Artificial aspira a convertirse en un estándar normativo a escala global.

El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, de Inteligencia Artificial ("Reglamento IA") nace en el contexto de la Estrategia Europea de Inteligencia Artificial de la Comisión Europea, a través de la cual se pretende convertir a la UE en una región de referencia mundial para la inteligencia artificial ("IA"), garantizando que esta se centre en el ser humano y sea sostenible, segura, inclusiva y fiable, y que garantice el respeto a los derechos fundamentales, la democracia, el Estado de Derecho y la sostenibilidad medioambiental. Al mismo tiempo, el Reglamento IA tiene por objetivo impulsar la innovación y establecer a la UE como líder en el campo de la IA, actuando como un catalizador de la industria.

Los puntos principales del Reglamento IA se resumen a continuación.

1. DEFINICIÓN DE IA

Los principales conceptos que define el Reglamento IA son los siguientes:

***Sistema de IA**: un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de los datos de entrada que recibe, la manera de generar información de salida como predicciones, contenidos, recomendaciones o decisiones que puede influir en entornos físicos o virtuales.*

***Modelo de IA de uso general: un modelo de IA,** también uno entrenado con un gran volumen de datos utilizando la autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su comercialización.*

2. ÁMBITO DE APLICACIÓN DEL REGLAMENTO IA

El objetivo del Reglamento IA al fijar su ámbito subjetivo ha sido garantizar que las reglas que establece apliquen al impacto de sistemas de IA en la UE con independencia de la ubicación de estos sujetos

(aplicación extraterritorial).El Reglamento IA se aplica a los siguientes sujetos:

(A) los **proveedores** que introduzcan en el mercado o pongan en servicio sistemas de IA o que introduzcan en el mercado modelos de IA de uso general en la UE, con independencia de si dichos proveedores están establecidos o ubicados en la UE o en un tercer país;

(B) los **responsables del despliegue** de sistemas de IA que estén establecidos o ubicados en la UE;

(C) los **proveedores y responsables del despliegue** de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando la información de salida generada por el sistema de IA se utilice en la UE;

(D) los **importadores y distribuidores** de sistemas de IA en la UE;

(E) los **fabricantes** de productos que introduzcan en el mercado de la UE o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca comercial;

(F) los representantes autorizados de los proveedores que no estén establecidos en la UE; y

(G) las personas afectadas que estén ubicadas en la UE.

La UE pretende centrar el esfuerzo normativo en aquellos usos y sistemas de IA que generen un riesgo relevante en el mercado de la UE, con el fin de no obstaculizar el desarrollo de la IA o actividades de investigación y otros ámbitos con poco impacto como el uso doméstico.

Por ello, el Reglamento IA **no** será de aplicación a los siguientes sistemas y herramientas de IA:

(A) sistemas de IA que se utilicen exclusivamente con fines militares, de defensa o de seguridad nacional;

(B) las autoridades públicas de terceros países u organizaciones internacionales que utilicen sistemas de IA en el marco de acuerdos o de la cooperación internacionales con fines de aplicación de la ley y cooperación judicial con la UE o los Estados miembros, siempre que ofrezcan garantías suficientes respecto a la protección de los derechos y libertades fundamentales de las personas;

(C) los sistemas y modelos de IA desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad;

(D) actividad de investigación, prueba o desarrollo de sistemas o modelos de IA antes de su introducción en el mercado o puesta en servicio (pero sí se aplica a pruebas en condiciones reales);

(E) los responsables del despliegue que sean personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional; y

(F) algunos sistemas de IA liberados bajo licencias libres y de código abierto (p. ej., sí se aplica a sistemas de IA prohibidos o de alto riesgo).

En cualquier caso, el Reglamento IA no afecta y debe entenderse sin perjuicio de otra normativa aplicable a estos sistemas o herramientas, como la de protección de datos, derechos de los consumidores, seguridad de los productos o derecho laboral. Igualmente, el Reglamento IA no modifica la responsabilidad de los prestadores de servicios intermediarios establecida en el Reglamento (UE) 2065/2022 de Servicios Digitales (DSA).

3. ENFOQUE BASADO EN EL RIESGO

El Reglamento IA aborda la inteligencia artificial desde los riesgos que puede entrañar para las personas y procura adaptar el tipo y contenido de las obligaciones de conformidad con el alcance y gravedad de los riesgos que pueda suponer. Así, la apuesta de la UE ha sido optar en el Reglamento IA por un enfoque basado en riesgos de tal manera que el Reglamento IA adapta el tipo y contenido de sus normas a la intensidad y alcance de los riesgos que presentan los sistemas de IA sobre los que se aplica.

4. PRÁCTICAS DE LA IA PROHIBIDAS

El Reglamento IA considera que determinadas prácticas de IA tienen un riesgo inaceptable para la UE y, en concreto, el Reglamento de IA prohíbe las siguientes prácticas:

PRÁCTICAS DE IA PROHIBIDAS	
Técnicas subliminales, manipuladoras o engañosas	Utilización de técnicas subliminales que trasciendan la conciencia de una persona o deliberadamente manipuladoras o engañosas que tengan por objetivo o efecto alterar sustancialmente el comportamiento de las personas, mermando su capacidad de tomar decisiones informadas y haciendo que tome una decisión que de otro modo no habría tomado, tal que le provoque perjuicios considerables.

URÍA
MENÉNDEZ

PRÁCTICAS DE IA PROHIBIDAS	
Explotación de vulnerabilidades de las personas	Explotación de vulnerabilidades de las personas o grupos de personas (edad, discapacidad, situación social o económica) para alterar su comportamiento de un modo que pueda razonablemente provocar perjuicios considerables.
Clasificación de personas mediante puntuación ciudadana	Clasificación de personas o grupos de personas atendiendo a su comportamiento social o características personales conocidas, inferidas o predichas, tal que la puntuación ciudadana resultante provoque un trato perjudicial o desfavorable hacia determinadas personas o grupos de personas que sea injustificado o desproporcionado respecto a su comportamiento social o la gravedad de este, o en contextos sociales que no guarden relación con el contexto de obtención de los datos.
Predicción de potencial criminalidad	Evaluación del riesgo de una personas para evaluar o predecir la probabilidad de que pueda cometer una infracción penal basándose únicamente en la elaboración de perfiles o en la evaluación de rasgos y características de su personalidad.
Bases de datos mediante reconcomiendo facial masivo	Creación o ampliación de bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión.
Inferencia de emociones en centros educativos o de trabajo	Inferencia de las emociones de una persona en los lugares de trabajo y centros educativos, excepto cuando el sistema de IA esté destinado a su uso por motivos médicos o de seguridad.

PRÁCTICAS DE IA PROHIBIDAS	
Categorización biométrica para inferir datos de categorías especiales	Categorización biométrica para deducir o inferir de las personas su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual, excepto para el mero filtrado o etiquetado de conjuntos de datos o en el ámbito de aplicación de la ley.
Identificación biométrica remota en tiempo real en lugares públicos con fines policiales	Identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley, excepto que sea estrictamente necesario y conforme a una autorización judicial o administrativa preceptiva para: (i) la búsqueda de víctimas de secuestro, trata de personas o explotación sexual, o la búsqueda de personas desaparecidas; (ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad de las personas físicas o una amenaza real y actual o previsible de un atentado terrorista; (iii) localización o identificación de una persona sospechosa de haber cometido una infracción penal de especial gravedad (p. ej., terrorismo, tráfico de drogas, homicidio, pornografía infantil) tal y como se identifican en el Anexo II del Reglamento IA.

5. SISTEMAS IA DE ALTO RIESGO

En línea con el enfoque al riesgo, el Reglamento IA establece disposiciones específicas sobre sistemas IA clasificados como de alto riesgo, a los que se les imponen obligaciones reforzadas. El Reglamento clasifica como sistema de IA de alto riesgo (con criterios actualizables por la Comisión Europea):

Productos regulados	Aquellos que estén destinados a utilizarse como componente de seguridad en determinados productos regulados o el propio sistema de IA sea un producto regulado (p. ej., juguetes, automóviles, aviones, embarcaciones, productos sanitarios) tal y como se identifican en el Anexo I del Reglamento IA.
Ámbitos de especial relevancia o sensibles	Aquellos identificados como de especial relevancia o sensibles en el Anexo III del Reglamento IA, que incluye **determinados usos** de IA en ámbitos tales como la biometría, centros educativos o laborales, servicios financieros, infraestructuras críticas, acceso a servicios esenciales –p. ej., servicios sanitarios, financieros, de emergencias–, policía, migración y asilo, administración de justicia o procesos electorales, salvo que no planteen riesgos importante de perjuicio a los derechos fundamentales de las personas físicas (p. ej., si tienen por objeto realizar una tarea de procedimiento limitada, mejorar el resultado de una actividad humana previamente realizada o detectar pautas o desviaciones de las pautas de toma de decisiones sin la finalidad de sustituir o influir en la evaluación humana, y siempre que no impliquen perfilado).

5.1 REQUISITOS DE LOS SISTEMAS DE ALTO RIESGO

El Reglamento IA establece los siguientes requisitos para los sistemas de IA considerados de alto riesgo:

(A) **Establecimiento de un sistema de gestión de riesgos** para la identificación y análisis de los riesgos conocidos y razonablemente previsibles, así como para la adopción de medidas adecuadas frente a tales riesgos.

(B) **Sujeción a prácticas de gobernanza y gestión de datos** que incluyan prácticas adecuadas para la finalidad prevista **en relación con** los conjuntos de datos de entrenamiento, validación y prueba (teniendo en cuenta, entre otros, posibles sesgos o contextos de uso).

(C) **Elaboración de documentación técnica** antes de su introducción en el mercado o puesta en servicio, debiéndose mantener actualizada y elaborada de forma que demuestre que el sistema de IA cumple con los requisitos exigidos por el Reglamento IA.

(D) **Conservación de registros** con medidas que permitan técnicamente el registro automático de eventos (archivos de registros) a lo largo de toda la vida del sistema de IA.

(E) **Comunicación de información a los responsables del despliegue de forma transparente** tal que los responsables del despliegue puedan utilizar e interpretar correctamente la información de salida del sistema de IA (p. ej., mediante unas instrucciones de uso que expliquen las características, capacidades y limitaciones del funcionamiento del sistema de IA).

(F) **Inclusión de vigilancia humana** con el fin de prevenir o reducir riesgos que puedan surgir en el uso del sistema de IA, dotando al sistema de IA de herramientas de interfaz humano-máquina adecuadas.

(G) Desarrollo **con niveles adecuados de precisión, solidez y ciberseguridad** y que funcionen de manera uniforme en estos sentidos a lo largo de todo su ciclo de vida (p. ej., mediante el establecimiento de meditas técnicas y organizativas frente a errores, fallos, sesgos o violaciones de seguridad).

5.2 PRINCIPALES OBLIGACIONES RELATIVAS A LOS SISTEMAS DE ALTO RIESGO

SUJETOS	OBLIGACIONES
Proveedores	Velar por que el sistema de IA de alto riesgo cumpla con los requisitos establecidos en el Reglamento IA.
	Identificarse por nombre comercial y dirección de contacto y colocar el marcado "CE" en el sistema de IA o, si no fuera posible, en la documentación que lo acompañe.
	Asegurar que el sistema de IA de alto riesgo se ha sometido a un procedimiento de evaluación de conformidad de acuerdo con el Reglamento IA, previo a su introducción en el mercado o puesta en servicio.
	Registrar el sistema de IA de alto riesgo y registrarse como proveedor de sistema de IA de alto riesgo en la base de datos regulada en el Reglamento IA.
	Establecer un sistema de gestión de la calidad que garantice el cumplimento de las obligaciones del Reglamento IA (p. ej., procedimientos, políticas, evaluaciones, controles) tal que su cumplimiento quede debidamente documentado y pueda demostrarse a las autoridades competentes.
	Conservar toda la documentación relativa al cumplimiento del Reglamento IA (incluyendo, entre otros, la declaración UE de conformidad) por un plazo de diez años desde la introducción en el mercado o puesta en servicio del sistema de IA de alto riesgo

SUJETOS	OBLIGACIONES
	Conservar los archivos de registro generados automáticamente por el sistema de IA por un tiempo adecuado según su finalidad (por regla general, el plazo no será inferior a seis meses).
	Adoptar inmediatamente las medidas correctoras necesarias cuando consideren que un sistema de IA no es conforme al Reglamento de IA e informar de ello a distribuidores, responsables del despliegue y otros sujetos afectados (p. ej., importadores).
	Cooperar con las autoridades competentes, proporcionando información y documentación y demostrando conformidad con el Reglamento IA.
	Nombrar un representante autorizado en la UE si el proveedor está establecido fuera de la UE, el cual tendrá, en su caso, las obligaciones anteriores.

Los proveedores que entienda que su sistema de IA no es de alto riesgo antes de introducirlo en el mercado deberán realizar y documentar una evaluación al respecto. Esta evaluación podrá ser requerida por las autoridades competentes.

SUJETOS	OBLIGACIONES
Importadores	Verificar que el proveedor ha cumplido con sus obligaciones derivadas del Reglamento IA antes de introducirlo en el mercado.
	No introducir en el mercado un sistema de IA de alto riesgo cuando consideren que no es conforme al Reglamento IA e informar de ello al proveedor, representantes autorizados y a las autoridades de vigilancia de mercado.
	Identificarse por nombre comercial y dirección de contacto en el sistema de IA o, si no fuera posible, en la documentación que lo acompañe, así como asegurar que lleva el marcado “CE”.
	Asegurar que las condiciones de almacenamiento o transporte del sistema de IA de alto riesgo no comprometen el cumplimiento con el Reglamento IA.
	Conservar la documentación relativa al cumplimiento del Reglamento IA por un plazo de diez años desde la introducción en el mercado o puesta en servicio del sistema de IA de alto riesgo.
	Cooperar con las autoridades competentes, proporcionando información y documentación y demostrando conformidad con el Reglamento IA.

SUJETOS	OBLIGACIONES
Distribuidores	Verificar que el importador y proveedor han cumplido con sus obligaciones derivadas del Reglamento IA y asegurar que el sistema de IA de alto riesgo lleva el marcado "CE".
	No comercializar un sistema de alto riesgo cuando consideren que no es conforme al Reglamento IA e informar de ello al proveedor o importador.
	Velar por que se adopten las medidas correctoras necesarias cuando consideren que un sistema de IA no es conforme al Reglamento IA e informar de ello al proveedor, importador u otros operadores pertinentes (p. ej., autoridad competente), así como, en su caso, informarles de las medidas correctoras adoptadas al respecto.
	Asegurar que las condiciones de almacenamiento o transporte del sistema de IA de alto riesgo no comprometen el cumplimiento con el Reglamento IA.
	Cooperar con las autoridades competentes, proporcionando información y documentación y demostrando conformidad con el Reglamento IA.
Responsable del despliegue	Establecer medidas técnicas y organizativas adecuadas para garantizar el correcto y normal desarrollo de los sistemas de IA, de conformidad con las instrucciones de los proveedores y con la normativa aplicable.
	Encomendar la supervisión humana de los sistemas de IA a personas cualificadas que puedan intervenir y controlar su funcionamiento, así como garantizar el respeto de los derechos fundamentales y la seguridad de las personas.
	Asegurar que los datos de entrada utilizados para el propósito previsto del sistema de IA sean pertinentes y representativos y que se actualicen, controlen y revisen periódicamente.
	Vigilar el funcionamiento del sistema de IA de alto riesgo basándose en sus instrucciones de uso y, cuando proceda, informar a los proveedores con arreglo a las obligaciones de vigilancia poscomercialización y el plan de poscomercialización, así como comunicar al proveedor y a la autoridad de vigilancia del mercado competente cualquier riesgo o incidente grave que se detecte, e incluso suspender el uso del sistema si es necesario para evitar o mitigar los daños.

SUJETOS	OBLIGACIONES
	Conservar los archivos de registro generados automáticamente por el sistema de IA durante un periodo de tiempo adecuado para la finalidad prevista del sistema (al menos seis meses o lo que disponga la legislación vigente) y facilitar su acceso al proveedor, a la autoridad de vigilancia del mercado y a los organismos notificados cuando lo soliciten.
	Informar a los representantes de los trabajadores y a los trabajadores afectados de si estarán expuestos a la utilización de un sistema de IA de alto riesgo.
	Realizar una evaluación de impacto sobre los derechos fundamentales en relación con el uso específico del sistema de IA, potenciales riesgos, mecanismos de supervisión humana y demás medidas oportunas para prevenir riesgos en la implementación de dichos sistemas de IA.[1]
	Informar a las personas expuestas al uso del sistema de IA de que están interactuando con una herramienta de IA, de su propósito y de las implicaciones para sus derechos y obligaciones, salvo que sea evidente o no sea razonable hacerlo.
	Cooperar con las autoridades competentes en la implementación del Reglamento IA, facilitando la documentación y la información necesarias y cumpliendo con las medidas correctivas o sancionadoras que se adopten.

[1] Cuando el sistema de IA implique el tratamiento de datos personales, podrá ser necesario también realizar una evaluación de impacto relativa a la protección de datos de conformidad con el Reglamento (UE) 679/2016 General de Protección de Datos. Ambas evaluaciones de impacto son compatibles, aunque no excluyentes, y podrán ser complementarias entre sí.

6. OBLIGACIONES DE TRANSPARENCIA PARA DETERMINADOS SISTEMAS DE IA

El Reglamento IA establece también obligaciones de transparencia para los **proveedores** y **responsables del despliegue** de determinados sistemas de IA, que han de cumplirse en la primera interacción o exposición:

SISTEMAS DE IA	SUJETO	OBLIGACIONES
Sistemas de IA destinados a interactuar con personas (p. ej., chatbots o asistentes virtuales)	Proveedores y responsables del despliegue	Garantizar que las personas expuestas al uso del sistema de IA estén informadas de que están interactuando con un sistema de IA, salvo que ello sea evidente teniendo en cuenta las circunstancias y el contexto de utilización.
Sistemas de IA que generen contenido sintético de audio, vídeo o texto.	Proveedores	Velar por que los resultados de salida estén marcados en un formato legible por máquina y sea posible detectar que han sido generados o manipulados artificialmente.
Sistemas de IA que generen contenido sintético de audio, vídeo o texto.	Responsables del despliegue	Hacer público que un contenido que constituya una ultrafalsificación ha sido generado o manipulado artificialmente.

7. MODELOS DE IA DE USO GENERAL

Un modelo de IA de uso general se clasificará como modelo de IA de uso general con riesgo sistémico si tiene capacidades de gran impacto o si tiene capacidades determinadas. Se presumirá que el sistema de IA tiene capacidades de gran impacto cuando acumule determinada cantidad de cálculo utilizada para su entrenamiento (en concreto, cuando la cantidad acumulada de cálculo medida en operaciones de coma flotante sea superior a $10^{\wedge 25}$).

Se establecen diversas obligaciones de los proveedores de modelos de IA de uso general:

(A) elaborar y mantener actualizada la documentación técnica del modelo de IA de uso general exigida por el Reglamento IA;

(B) poner a disposición de los proveedores información de los sistemas de IA que tengan intención de integrar en un modelo de IA de uso general;

(C) evaluar los modelos de conformidad con protocolos y herramientas que reflejen el estado de la técnica y evaluar y reducir los posibles riesgos sistémicos que puedan derivarse del desarrollo;

(D) vigilar, documentar y comunicar a la Oficina de IA o a las autoridades nacionales competentes la información sobre incidentes graves y velar por que se establezca un nivel adecuado de protección de la ciberseguridad

8. OTRAS DISPOSICIONES DEL REGLAMENTO

(A) **Espacios de pruebas:** El Reglamento IA permite que los datos personales legalmente recabados con otros fines puedan tratarse en un espacio controlado de pruebas para la IA únicamente con el objetivo de desarrollar, entrenar y probar determinados sistemas de IA en el espacio de pruebas cuando se cumplan determinadas condiciones.

(B) **Autoridades nacionales competentes:** El Reglamento IA exige a los Estados miembros designar una autoridad notificadora y una autoridad de supervisión de mercado en el ámbito de la inteligencia artificial. Además, se dota a las autoridades nacionales de capacidad de investigación y de sanción, y se establece la obligación de incorporar un punto de contacto único oficial en cada Estado miembro de la UE.

En España, la autoridad de vigilancia del mercado competente es la Agencia Española de Supervisión de la IA (AESIA), que está adscrita al Ministerio para la Transformación Digital y de la Función Pública y tiene sede en A Coruña.

(C) **Estándares normalizados de los requisitos de cumplimiento:** La Comisión Europea o las autoridades europeas de normalización podrá establecer estándares normalizados de especificaciones comunes para los requisitos de cumplimiento del Reglamento IA a fin de facilitar que los sistemas de IA evidencien su adecuación al Reglamento IA.

(D) **Comité Europeo de Inteligencia Artificial:** Se establece un sistema revisado de gobernanza a nivel europeo, esto es, el Comité Europeo de Inteligencia Artificial, unidad independiente de la Comisión Europea, con un representante de cada Estado miembro, con competencias de ejecución a escala de la UE. La tarea del Comité es supervisar los modelos fundacionales y los sistemas de alto riesgo, y será asesorado por un grupo permanente de representación de grupos de interés, tales como proveedores, usuarios u organizaciones civiles.

(E) **Vigilancia, supervisión y controles:** Las autoridades de vigilancia del mercado deben informar anualmente a la Comisión Europea y a las autoridades nacionales de competencia de cualquier información recabada en el transcurso de las actividades de vigilancia del mercado, así como acerca del recurso a prácticas prohibidas que se hayan producido durante el año. Además, las autoridades de vigilancia del mercado y la Comisión Europea podrán proponer actividades conjuntas de investigación.

(F) **Confidencialidad:** La Comisión Europea, las autoridades de vigilancia del mercado, los organismos notificados y cualquier otra persona física o jurídica que participe en la aplicación de Reglamento IA deben respetar la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades.

(G) **Códigos de conducta:** La Oficina de IA fomentará y facilitará la elaboración de Códigos de práctica a escala de la UE, como elemento para contribuir a la correcta aplicación del Reglamento IA. Asimismo, la Comisión Europea y los Estados miembros apoyarán la redacción de Códigos de conducta con el objetivo de impulsar la aplicación voluntaria de algunos de los requisitos del Reglamento IA en determinados sistemas de IA.

(H) **Sanciones:** Corresponde a los Estados miembros establecer el régimen sancionatorio, incluyendo medidas de apercibimiento u otras medidas de ejecución no pecuniarias, así como la aplicabilidad del régimen sancionador a autoridades y organismos públicos. El Reglamento IA también establece que el régimen sancionador tendrá en cuenta los intereses de las pymes, incluidas las empresa emergentes así como su viabilidad económica.

Se fijan multas por infracciones del Reglamento IA.

Infracción	**Multa**
No respeto de la prohibición de las prácticas de IA	Multas de hasta **35 millones de euros** o, si el infractor es una empresa, de hasta el **7 % del volumen de negocios** mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.
Incumplimiento de las obligaciones impuestas por el Reglamento IA	Multas de hasta **15 millones de euros** o, si el infractor es una empresa, de hasta el **3 % del volumen de negocios** mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.
Presentación de información inexacta, incompleta o engañosa a las autoridades competentes en respuesta a una solicitud	Multas de hasta **7,5 millones de euros** o, si el infractor es una empresa, de hasta el **1 % del volumen de negocios** total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.

9. ENTRADA EN VIGOR

El Reglamento IA tendrá efecto y aplicación directa en todos los países de la UE y entra en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*, es decir, el 2 de agosto de 2024.

No obstante, el Reglamento IA no será aplicable hasta pasados los dos años desde su publicación, es decir, hasta el 2 de agosto de 2026, salvo determinados preceptos:

- las disposiciones generales del Reglamento IA y las prácticas de IA prohibidas serán aplicables a partir de los **seis meses** después de la entrada en vigor, es decir, el 2 de febrero de 2025.
- las disposiciones relativas a las autoridades notificantes y organismos notificados, a los modelos de IA de uso general, a la estructura de gobernanza (oficina de IA, creación y estructura del Comité Europeo de IA, funciones del Comité, foro consultivo, etc.) y a las sanciones serán aplicables a partir de los **doce meses** después de la entrada en vigor, es decir, el 2 de agosto de 2025.
- las disposiciones relativas a los sistemas de IA clasificados como sistemas de alto riesgo y las obligaciones correspondientes serán aplicables a los **tres años** después de la entrada en vigor, es decir, el 2 de agosto de 2027.

10. ABOGADOS DE CONTACTO

Leticia López-Lapuente
+34 91 586 0131
leticia.lopez-lapuente
@uria.com

Ignacio Esteban Avendaño
+34 91 586 0644
ignacio.esteban@uria.com

Mirian Goitia
+34 91 587 0887
mirian.goitia@uria.com