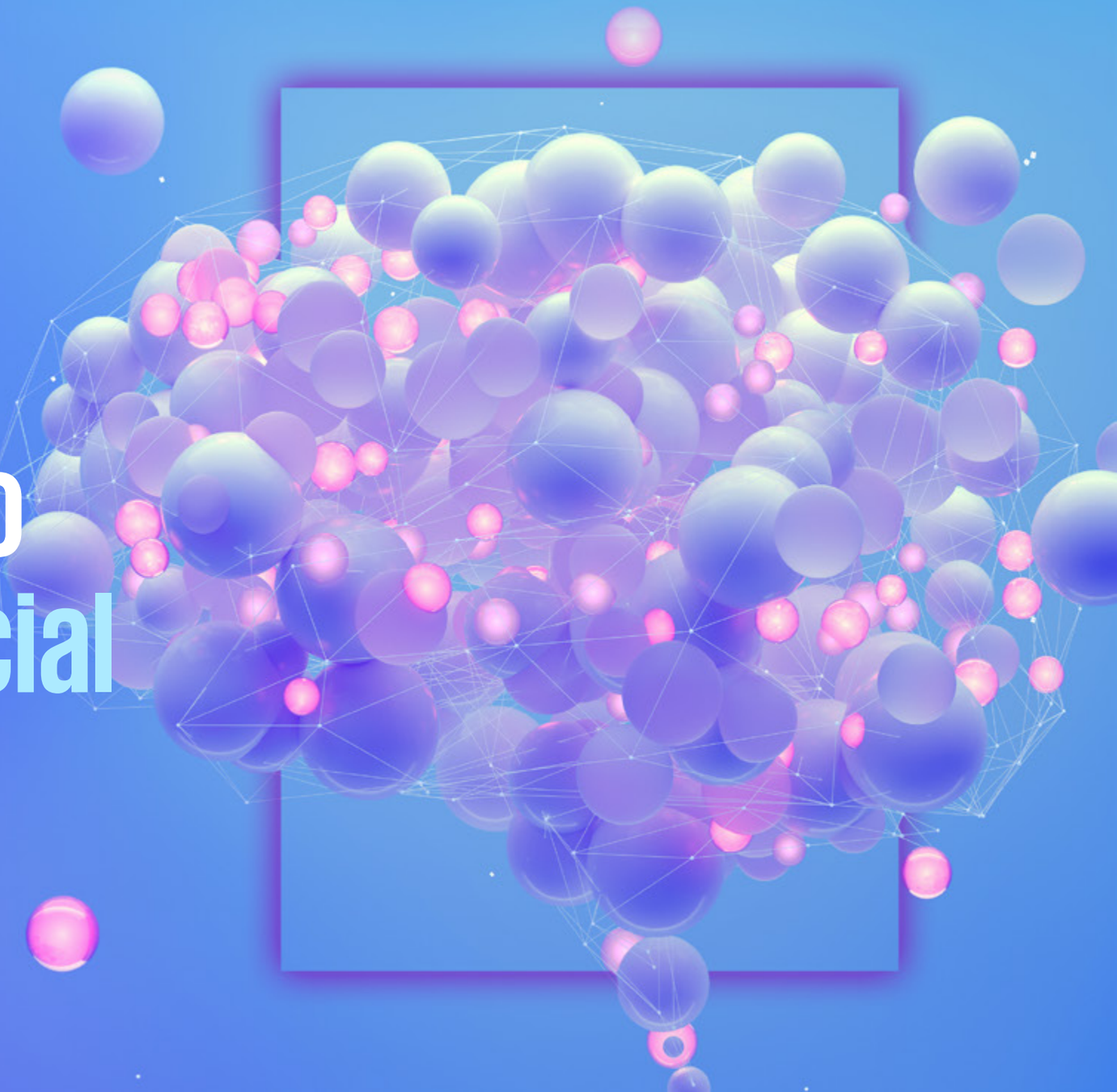
KPMG

Aspectos clave para entender la primera regulación del mundo de Inteligencia Artificial



KPMG. Make the Difference.

En diciembre de 2023, Europa se convertía en la primera jurisdicción en contar con una propuesta legislativa de tipo transversal en el mundo en materia de inteligencia artificial. Es el conocido 'Reglamento de Inteligencia Artificial', cuyo gran objetivo es proteger los derechos fundamentales ante la llegada de una tecnología que está llamada a cambiarlo todo (o casi todo).

Se trata de un reto mayúsculo para las empresas, ante el que surgen grandes interrogantes: ¿Qué preguntas deben hacerse las compañías para cumplir con el Reglamento de IA? ¿Qué obligaciones tienen en función del riesgo de cada sistema? ¿A qué sanciones se exponen por incumplirlas?

Descubre las respuestas a continuación.

Reglamento, de aplicación directa en la Unión Europea

Objetivos

1. Evitar heterogeneidad normativa
2. Abordar la IA con un enfoque basado en el riesgo, similar a RGPD
3. Impulsar una actitud proactiva en la gestión de IA
4. Favorecer el gobierno, responsabilidad y transparencia en su uso

¿Qué es una IA?

Un sistema de IA es un sistema basado en máquinas que, con objetivos explícitos o implícitos, **infiere, a partir de la entrada que recibe**, en cómo generar salidas tales como **predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales**. Los distintos sistemas de IA **varían en sus niveles de autonomía y capacidad de adaptación** tras su despliegue.

**La definición se ajusta a la de la OCDE, recientemente actualizada.*

Ejemplos:

Asistentes virtuales inteligentes (Siri, Alexa, Cortana…)

Sistemas de reconocimiento facial (FaceID de Apple)

Traductores simultáneos (Google Translate)

Sistemas de recomendación en plataformas de contenido

¿Cómo deben responder las organizaciones?

Pasos a seguir:

1

¿Tenemos un sistema IA?

2

¿Qué tipo de IA?

Es necesario categorizarlo:

RIESGO INACEPTABLE

En esta categoría se incluyen aquellos sistemas de IA que representan una amenaza directa a la seguridad pública, los derechos fundamentales o la privacidad. Su uso está estrictamente prohibido, salvo en situaciones muy excepcionales. Hablamos de sistemas caracterizados por:

- Manipular cognitivamente el comportamiento de personas.
- Manipular el comportamiento que aprovecha vulnerabilidades de personas o grupos concretos.
- Evaluar o puntuar socialmente.
- Identificar biométricamente en tiempo real en espacios públicos.

RIESGO ALTO !!

Aquí se incluyen los sistemas de IA que podrían tener un impacto considerable en los derechos fundamentales de los individuos por su relación con los servicios y procesos que afectan a la salud, seguridad, etc. Su uso está permitido siempre que se cumplan con ciertas salvaguardas adicionales y se monitorice su funcionamiento. Esta categoría engloba a sistemas que cumplen estas dos condiciones:

Condición 1

- Están destinados a utilizarse como componente de seguridad de un producto.
- Deben someterse a una evaluación de conformidad por terceros con vistas a la comercialización o puesta en servicio del producto.

Condición 2

O, por otra parte, sistemas que:

- Están destinados a utilizarse para la contratación o selección de personas físicas.
- Están destinados a tomar decisiones relativas a la promoción y resolución de relaciones contractuales de índoles laboral.

RIESGO LIMITADO

En este nivel se clasifican sistemas con algunas obligaciones concretas de transparencia:

- Sistemas de reconocimiento de emociones o que determinen la asociación a categorías sociales concretas a partir de datos biométricos.
- Sistemas que manipulan contenido (imagen, sonido, vídeo, …) que asemeje a personas, objetos, lugares e entidades y puedan inducir erróneamente a una persona a pensar que son auténticos o verídicos.

RIESGO BAJO

Son los sistemas que no se ajustan a las categorías anteriores. En esta clasificación prima la capacidad de decisión de los ciudadanos de forma libre, voluntaria e inequívoca para el uso de estas tecnologías.

3

Definir de marcos de gobernanza y de gestión de riesgos adecuados que permitan demostrar la existencia de marcos de **gestión confiable y responsable de la IA** a nivel corporativo.

4

RIESGO ALTO !!

En caso de tratarse de un sistema de riesgo alto, la compañía deberá **registrarlo**

En todo caso, es necesario crear una cultura en la que todas las partes involucradas (empleados, clientes, terceros externos) entiendan los riesgos asociados a los sistemas conforme a los marcos de gobernanza que se establezcan, impulsando la formación y la concienciación al respecto.

Obligaciones específicas para los sistemas de ALTO RIESGO !!

Implantación de un sistema de gestión de riesgos y calidad

Gobernanza de datos (por ejemplo, mitigación de sesgos, datos de formación representativos, etc.)

Transparencia (por ejemplo, instrucciones de uso, documentación técnica, etc.)

Supervisión humana (por ejemplo, explicabilidad, registros auditables, intervención humana, etc.).

Precisión, solidez y ciberseguridad (por ejemplo, pruebas y supervisión)

Evaluación de impacto sobre los derechos fundamentales y evaluación de conformidad

Ejemplos:

Sistemas de verificación de la autenticidad de los documentos de viaje

Dispositivo médico: un robot de cirugía supervisada por una IA

Sistemas que arrojen una puntuación de crédito que impide la obtención de un préstamo

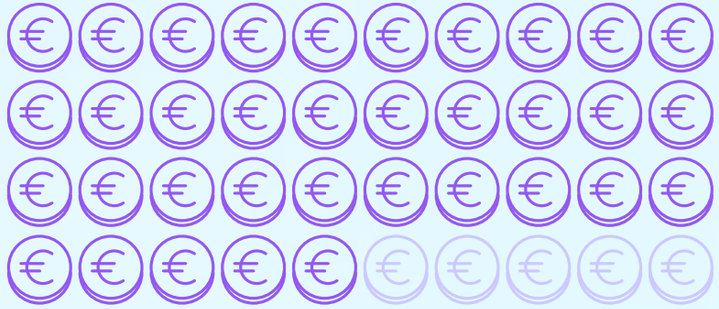
Sistemas de selección de personal

Sanciones en caso de incumplimiento

RIESGO ALTO

Hasta el **7%** **de la facturación anual global**

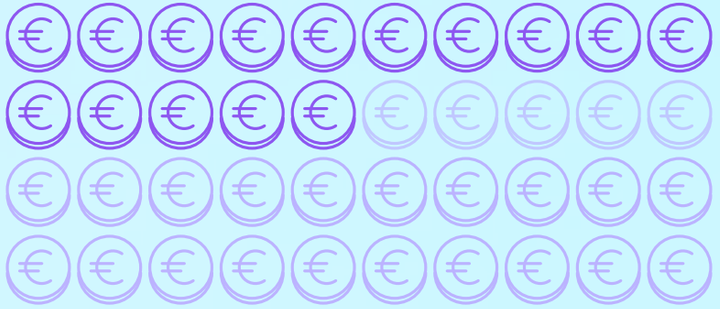
o



35 **millones de euros en caso de sistemas de IA prohibidos**

Hasta el **3%** **de la facturación anual global**

o



15 **millones de euros para la mayoría de las demás infracciones**

Hasta el **1,5%** **de la facturación anual global**

o

7,5 **millones de euros por suministrar información incorrecta**

Próximos pasos

El texto completo del acuerdo aún no se encuentra disponible, es un pacto político que deberá recibir la aprobación formal tanto del Parlamento Europeo como del Consejo. Se espera que esta aprobación ocurra a principios del 2024.

Una vez que el texto definitivo sea aprobado, entrará en vigor 20 días tras la publicación en DOUE, siendo de aplicación 2 años después, con algunas excepciones.

Mientras tanto…

- La Comisión iniciará trabajos para lograr un Pacto sobre la IA, que busca obtener el compromiso voluntario de la industria.
- La UE continuará colaborando en plataformas internacionales como el G7, la OCDE, el Consejo de Europa, el G20 y la ONU.

Cómo puede ayudarte KPMG

Para abordar y cumplir con la nueva regulación, compartimos nuestros principios, pilares éticos y aproximación al gobierno en materia de Inteligencia Artificial.

KPMG Trusted AI es nuestro enfoque estratégico y marco para diseñar, construir, desplegar y utilizar soluciones de IA de manera responsable y ética, con el objetivo de acelerar la creación de valor con confianza.

Las capacidades de la IA están evolucionando rápidamente y por tanto, también nuestro enfoque con especial atención a las obligaciones específicas asociadas a IA Generativa (GenAI).

A medida que los avances tecnológicos y los estándares legales, éticos, y de riesgos maduren, KPMG continuará revisando y evolucionando nuestro marco de Trusted AI y servicios asociados como sea necesario.

La transformación nunca para. Nosotros tampoco.

En KPMG creemos que la transformación es una oportunidad que no se puede dejar pasar. Integrando la mejor tecnología, con los procesos adecuados y las capacidades y visión necesarias, la transformación será un éxito. Por esa razón, hemos trabajado durante décadas en el corazón de las empresas, ayudando a nuestros clientes a maximizar el potencial de sus personas y de su tecnología, trabajando junto para alcanzar resultados reales. Porque cuando personas y tecnologías se unen, el resultado es insuperable.

Construyendo un mundo diferente:

Los profesionales de KPMG marcan la diferencia en la transformación tecnológica de tu organización. Juntos, te ayudamos a orientar tu negocio al cliente, optimizar funciones para afrontar nuevos retos, gestionar los riesgos y la regulación, alcanzar nuevas cotas de generación de valor y crear un entorno para adaptarse a los cambios.

KPMG. Make the Difference.

Contactos

Javier Aznar
Socio de Technology Risk de KPMG en España
E: jaznar@kpmg.es
T: +34 699 35 00 29

Noemí Brito
Socia responsable del área de 'Legal Operations & Transformation Services' (LOTS) y de IP & IT de KPMG Abogados
E: noemibrito@kpmg.es
T: +34 689 38 57 98

Eva García
Socia responsable de Análisis de Datos e Inteligencia Artificial de KPMG en España
E: evagarcia1@kpmg.es
T: +34 685 94 88 10

Te ayudamos a sacar el máximo partido al despliegue de la inteligencia artificial generativa en tu organización

Descubre cómo

kpmg.es