CUATRECASAS

Aspectos clave del Reglamento de Inteligencia Artificial

El Consejo de la Unión Europea dio ayer, 21 de mayo de 2024, su aprobación final al esperado Reglamento de Inteligencia Artificial (IA). Revisamos sus puntos principales.

Unión Europea - Legal Flash
22 de mayo de 2024

Aspectos Clave

- El Reglamento de IA busca promover la adopción de una **IA fiable** y **centrada en el ser humano**, y asegurar un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales frente a los riesgos potenciales de la IA.
- **Prohíbe determinados usos** de la IA que se consideran de riesgo inaceptable.
- Cataloga ciertos sistemas de IA como de **riesgo alto** y establece exigentes requisitos para estos sistemas, así como obligaciones para los participantes en la cadena de valor, incluidas las empresas que utilicen sistemas de IA.
- Regula la introducción en el mercado de **modelos de IA de uso general**.
- Impone **obligaciones de transparencia** en relación con determinados sistemas de IA, especialmente los destinados a interactuar con personas físicas y a la generación de contenidos.
- Construye un **sistema institucional** de gobernanza y supervisión y prevé elevadas **sanciones** por infracciones del Reglamento.

Introducción

El **Reglamento de Inteligencia Artificial (IA)** regula la **introducción en el mercado, la puesta en servicio y la utilización** de **sistemas de IA** en la Unión Europea. Su principal objetivo es fomentar el **desarrollo y la utilización de la IA** en la UE, así como **garantizar un alto nivel de protección de la salud, la seguridad y los derechos fundamentales**.

Adopta un **enfoque basado en el riesgo** que puede derivarse del uso de sistemas de IA, estableciendo requisitos y obligaciones a los diversos participantes en la cadena de valor. Las obligaciones no se limitan a los proveedores de sistemas de IA, sino que alcanzan también, entre otros, a **quienes utilizan sistemas de IA para fines profesionales**, que reciben el nombre de «**responsables del despliegue**».

El texto del Reglamento de IA es largo y complejo y en algunos puntos deberá ser desarrollado y aclarado mediante disposiciones y directrices de la Comisión Europea. En los apartados siguientes destacamos algunos de los **principales aspectos** del Reglamento.

La apuesta de la UE para regular la IA a través de este Reglamento se complementa con **otras iniciativas legislativas**, en particular dos propuestas de Directiva que se hallan actualmente en tramitación. Por una parte, la Propuesta de Directiva sobre responsabilidad civil en materia de IA, que establece normas procesales sobre prueba en relación con procedimientos de responsabilidad civil extracontractual por daños y perjuicios causados por sistemas de IA. Por otra parte, la Propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos, que derogará la anterior Directiva de 1985 y que aborda la responsabilidad derivada de sistemas de IA defectuosos que causen daños o pérdidas de datos, posibilitando reclamar una indemnización al proveedor de sistemas de IA o a cualquier fabricante que integre un sistema de IA en otro producto.

Por lo demás, el Reglamento de IA se entiende sin perjuicio del derecho de la UE en otras materias, algunas de ellas muy relacionadas, como la protección de datos, protección de los consumidores, derechos fundamentales, empleo, protección de los trabajadores o la seguridad de los productos. En particular, el Reglamento de IA no afecta a las obligaciones que impone el **Reglamento General de Protección de Datos** a los proveedores y responsables del despliegue en su papel de responsables o encargados del tratamiento cuando el desarrollo o la utilización de los sistemas de IA implique el tratamiento de datos personales.

Ámbito de aplicación

El Reglamento se aplica a:

- los **proveedores** que introduzcan en el mercado o pongan en servicio sistemas de IA, o introduzcan en el mercado *modelos* de IA de uso general, en la UE, con independencia de si están establecidos o ubicados en la UE o en un tercer país
- quienes utilicen un sistema de IA para fines profesionales ("**responsables del despliegue**") que estén establecidos o ubicados en la UE
- los proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados **fuera de la UE** si los resultados de salida del sistema se utilizan en la UE
- los **importadores y distribuidores** de sistemas de IA
- los **fabricantes de productos** que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y bajo su nombre o marca.
- los representantes autorizados de los proveedores no establecidos en la UE
- las personas afectadas que estén ubicadas en la UE

Se excluyen del ámbito del Reglamento ciertos sistemas, como los de uso exclusivamente militar, de defensa o seguridad nacional, o los destinados únicamente a la investigación y desarrollo científicos. Tampoco se aplica a las actividades de investigación, prueba o desarrollo de sistemas o modelos de IA antes de su introducción en el mercado o puesta en servicio. Queda también excluida su aplicación a personas físicas que utilicen sistemas de IA con **fines puramente personales**.

Noción de sistema de IA

El Reglamento define el concepto de "**sistema de IA"** como:

- «un sistema **basado en una máquina** que está diseñado para funcionar con **distintos niveles de autonomía** y que puede mostrar **capacidad de adaptación** tras el despliegue,
- y que, para **objetivos explícitos o implícitos**,
- **infiere** de la información de entrada que recibe
- la manera de generar **resultados de salida**, como predicciones, contenidos, recomendaciones o decisiones,
- que pueden influir en entornos físicos o virtuales»

Esta definición corresponde a la proporcionada por la OCDE[1], que el Reglamento adopta con el objetivo de facilitar la convergencia de nociones a escala internacional. Quedan fuera de la definición, y por tanto de la regulación, los sistemas de *software* de capacidades inferiores a las indicadas.

[1] Véase la *Recommendation of the Council on Artificial Intelligence*, OECD, 2019 (modificada en noviembre de 2023).

Sujetos afectados

Los principales sujetos contemplados en el Reglamento son los siguientes:

Denominación	Descripción
Proveedor	persona física o jurídica, autoridad u órgano público que desarrolla (o para quien se desarrolla) un sistema de IA, o un modelo de IA de uso general, y lo introduce en el mercado, o pone en servicio el sistema, bajo su nombre o marca
Importador	persona física o jurídica, ubicada o establecida en la UE que introduce en el mercado un sistema de IA de un proveedor establecido fuera de la UE
Distribuidor	persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor y del importador, que comercializa un sistema de IA en la UE
Responsable del despliegue	persona física o jurídica, autoridad u órgano público **que utilice un sistema de IA** bajo su propia autoridad, salvo si el uso se enmarca en una actividad personal no profesional.

Prácticas prohibidas

En coherencia con su perspectiva basada en el nivel de riesgo, el Reglamento de IA **prohíbe por completo** una serie de prácticas de IA que se consideran de riesgo inaceptable. Sintéticamente, y sin perjuicio de los variados matices y excepciones que establece el Reglamento, las prácticas prohibidas se refieren principalmente a:

- el empleo de **técnicas subliminales, manipuladoras o engañosas,** para alterar el comportamiento de una persona, o de un grupo, haciendo que tome una decisión que no habría tomado, con probables resultados perjudiciales

- la explotación de **vulnerabilidades** de una persona o de un colectivo, por su edad, discapacidad, o situación social o económica, para alterar su comportamiento, con probables resultados perjudiciales

- los sistemas para evaluar o clasificar personas físicas o colectivos durante un período de tiempo atendiendo a su comportamiento social o características (***social scoring***), dando lugar a un trato perjudicial o desfavorable que se produzca en contextos sociales no relacionados con aquellos en los que se obtuvieron los datos, o que resulte injustificado o desproporcionado

- los sistemas para valorar o **predecir** el riesgo de que una persona física cometa un delito, atendiendo únicamente a su perfil o a los rasgos de su personalidad
- la creación o ampliación de **bases de datos de reconocimiento facial** a partir de la extracción indiscriminada de imágenes de internet o de circuitos cerrados de televisión
- los sistemas de IA para **inferir emociones** de una persona física **en el lugar de trabajo** o en **centros educativos**, salvo por motivos médicos o de seguridad
- los sistemas que clasifiquen individualmente a personas físicas a partir en sus **datos biométricos** para inferir determinados **datos sensibles**
- los sistemas de **identificación biométrica remota en tiempo real en espacios de acceso público** con fines de garantía de cumplimiento del Derecho (*law enforcement*), salvo ciertas excepciones, sujetas a una serie de condiciones y garantías

Sistemas de IA de riesgo alto

El Reglamento de IA categoriza como de **riesgo alto** ciertos sistemas que suponen un peligro significativo de causar daños a la salud, la seguridad o los derechos fundamentales. A este respecto distingue dos grupos:

- los **sistemas vinculados a la legislación armonizada sobre seguridad de productos** incluida en el **Anexo I** del Reglamento: el sistema de IA será de alto riesgo cuando constituya un producto de los incluidos en esta regulación sectorial, o bien sea un componente de seguridad de estos productos; y siempre que, conforme a dicha legislación, el producto o el componente deba someterse a una evaluación de conformidad por parte de un organismo independiente.
- **sistemas incluidos en el Anexo III** del Reglamento: se trata de sistemas que, por el ámbito en que se emplean y el uso específico al que se destinan, presentan, en principio, un riesgo elevado.

En este **Anexo III** se delimitan **ocho ámbitos** y dentro de cada uno se identifican **casos concretos de uso**, que se consideran de alto riesgo (siempre que no resulten prohibidos). Recogemos a continuación estos ámbitos y destacamos algunos de los casos de uso comprendidos en cada uno de ellos, de forma sintética y sin entrar en el detalle:

- **biometría**: se incluyen sistemas de IA para identificación biométrica remota; categorización biométrica a partir de la inferencia de características sensibles o protegidas; reconocimiento de emociones, salvo los supuestos prohibidos
- **infraestructuras críticas**: sistemas que sean componentes de seguridad en la gestión y funcionamiento de infraestructuras digitales críticas, tráfico rodado, suministro de agua, gas, calefacción o electricidad

- **educación y formación profesional**: se incluyen sistemas para determinar la admisión a instituciones educativas o de formación profesional; evaluar resultados de aprendizaje; determinar el nivel educativo al que podrá acceder una persona; monitorizar y detectar comportamientos prohibidos de los estudiantes durante los exámenes

- **empleo, gestión de los trabajadores y acceso al autoempleo**: se incluyen aquí sistemas de IA para seleccionar o contratar personal, publicitar puestos de trabajo, analizar y filtrar solicitudes y evaluar candidatos; tomar decisiones sobre condiciones de trabajo o promoción o terminación de la relación laboral; asignar tareas a partir del comportamiento, rasgos o características de la persona; así como supervisar y evaluar el rendimiento y comportamiento de los trabajadores

- **servicios públicos y privados esenciales**: se incluyen sistemas para determinar acceso a prestaciones y servicios públicos esenciales de asistencia; calificación crediticia de personas físicas (salvo los sistemas para detectar fraude financiero); evaluación de riesgos y fijación de precios en seguros de vida y de salud; priorización de las respuestas en situaciones de emergencia, por ejemplo, policía, bomberos y asistencia médica; sistemas de triaje en asistencia sanitaria de urgencia

- **garantía de cumplimiento del Derecho**: comprende distintos sistemas relacionados con la prevención e investigación de delitos, incluyendo determinados sistemas predictivos, de perfilado de personas y de análisis de fiabilidad de pruebas

- **migración, asilo y gestión del control fronterizo**: se incluyen diversos sistemas de valoración de riesgos de seguridad, de migración irregular o de salud; examen de solicitudes de asilo; reconocimiento de personas en contexto de migración, asilo o control de fronteras

- **administración de justicia y procesos democráticos**: se incluyen sistemas de asistencia a la autoridad judicial en la investigación e interpretación de hechos y de la ley, así como sistemas para influir en el resultado de una elección o referéndum o en el comportamiento electoral de los votantes

Dentro de los ámbitos indicados, y siguiendo los criterios del Reglamento, la Comisión Europea podrá añadir, modificar o suprimir casos de uso considerados de alto riesgo.

A pesar de que un caso de uso esté incluido en el Anexo III, **no se considerará de alto riesgo** si no plantea un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales, incluyendo el caso de que no influya sustancialmente en la toma de decisiones. Para esta determinación, el Reglamento proporciona unas condiciones concretas, que la Comisión podrá modificar más adelante. Además, se encarga a la Comisión que elabore unas directrices específicas que incluyan "una lista exhaustiva de ejemplos prácticos de casos de uso de sistemas de IA que sean de alto riesgo y que no sean de alto riesgo". **En todo caso** se considerarán siempre de alto riesgo los sistemas incluidos en el Anexo III que elaboren **perfiles de personas físicas.**

Requisitos de los sistemas de IA de riesgo alto y obligaciones de los proveedores

El Reglamento establece **requisitos** muy exigentes que deben reunir los sistemas de alto riesgo, así como una serie de **obligaciones** para distintos sujetos.

De modo muy sintético, los sistemas de IA de riesgo alto deben cumplir, entre otros, los **requisitos siguientes**:

- implantar y mantener un **sistema de gestión de riesgos** durante todo el ciclo de vida del sistema de IA
- asegurar **la calidad de los conjuntos de datos** de entrenamiento, validación y prueba mediante prácticas de gobernanza y gestión de datos adecuadas
- elaborar la **documentación técnica** del sistema y mantenerla actualizada
- permitir el **registro automático de eventos**
- proporcionar **instrucciones de uso comprensibles a los responsables del despliegue**
- permitir la **supervisión humana** efectiva durante su uso
- cumplir niveles adecuados de **precisión, solidez y ciberseguridad**

La demostración del cumplimiento de estos requisitos se facilita con determinadas presunciones, y en especial con la presunción de que se cumplen cuando el sistema se ajusta a los correspondientes estándares elaborados por organizaciones europeas de normalización y cuyas referencias se publiquen en el Diario Oficial de la UE, o cuando se ajusten a especificaciones comunes que establezca la Comisión Europea.

El Reglamento establece obligaciones para los proveedores, para los responsables del despliegue, así como para otros sujetos afectados.

Las principales **obligaciones de los proveedores** de sistemas de IA de alto riesgo son las siguientes:

- asegurar que sus sistemas cumplan los **requisitos** anteriores y demostrar dicho cumplimiento a solicitud motivada de la autoridad competente
- contar con un sistema de **gestión de la calidad**
- conservar la **documentación** sobre el sistema a disposición de las autoridades, así como los **archivos de registro** que estén bajo su control
- asegurar que el sistema se somete al procedimiento **de evaluación de la conformidad**; elaborar una **declaración UE de conformidad;** y colocar el **marcado CE** en el sistema
- registrar el sistema en la **base de datos** de la UE de sistemas de alto riesgo
- adoptar las **medidas correctoras** oportunas, incluida la retirada o la desactivación, cuando consideren que el sistema no es conforme con el Reglamento

En determinados casos, un distribuidor, importador, responsable del despliegue o tercero **será considerado proveedor** y estará sujeto a anteriores obligaciones. Se trata de ciertos

supuestos en que la persona en cuestión **pone su nombre o marca** en el sistema de IA previamente introducido en el mercado, o lo **modifica sustancialmente**.

¿Qué obligaciones se imponen a las empresas que utilizan sistemas de IA de alto riesgo?

Las personas físicas o jurídicas que utilicen sistemas de IA de alto riesgo para fines profesionales reciben la denominación de "responsables del despliegue" (*deployers*) y están sujetas a diversas obligaciones, entre las que destacan las siguientes:

- adoptar las **medidas técnicas y organizativas** para garantizar que usan los sistemas de acuerdo con las instrucciones de uso
- encomendar la **supervisión humana** a personas adecuadas
- asegurar que los **datos de entrada** sean **pertinentes y representativos** para la finalidad del sistema, en la medida en que ejerzan el control sobre esos datos
- **vigilar el funcionamiento** del sistema e **informar de riesgos e incidentes** al proveedor, importador o distribuidor y a la autoridad de vigilancia del mercado
- conservar los **archivos de registro** que generen si están bajo su control
- **informar a los trabajadores y a sus representantes legales** antes de implementar un sistema de IA de alto riesgo en el lugar de trabajo
- cuando empleen sistemas para tomar o ayudar a tomar decisiones, **informar** a las personas físicas afectadas por esas decisiones
- **cooperar** con las autoridades competentes
- garantizar la **alfabetización** suficiente en materia de IA de su personal y demás personas que se encarguen en su nombre del funcionamiento y utilización de los sistemas de IA

En determinados supuestos, los responsables del despliegue deberán llevar a cabo una **evaluación de impacto** en materia de derechos fundamentales.

Obligaciones de transparencia para ciertos sistemas

El Reglamento impone, además, ciertas obligaciones de transparencia en relación con determinados sistemas de IA, con independencia de si son sistemas de alto riesgo o si no lo son. Se trata de los casos siguientes:

- Sistemas destinados a **interactuar directamente con personas físicas**: el **proveedor** deberá diseñar el sistema de modo que las personas afectadas estén informadas de que interactúan con un sistema de IA

- Sistemas que generen contenido **sintético de audio, imagen, vídeo o texto**: el **proveedor** velará porque los resultados de salida estén marcados y sea posible detectar que han sido generados o manipulados artificialmente

- Sistemas de **reconocimiento de emociones** y de **categorización biométrica**: el **responsable del despliegue** deberá informar del funcionamiento del sistema a las personas físicas expuestas a él

- Sistemas que generen o manipulen imágenes, audio o video que constituyan una **ultrasuplantación (*deep fake*)**, así como texto para informar sobre asuntos de interés público: el **responsable del despliegue** hará público que se trata de contenidos generados o manipulados artificialmente

Modelos de IA de uso general

Además de sistemas de IA, el Reglamento contempla también determinados **modelos** de IA. Los modelos de IA se integran en sistemas, pero no constituyen en sí mismos un sistema. El Reglamento ha considerado como **modelos de IA de uso general** aquellos que presentan un grado de generalidad considerable, capaces de realizar una gran variedad de tareas y que pueden integrarse en diversos sistemas o aplicaciones.

Los **proveedores** de estos modelos están sujetos a una serie de obligaciones, que incluyen:

- documentar el proceso de entrenamiento, así como los resultados de su evaluación
- informar sobre sus características y requisitos legales a los proveedores de sistemas de IA que tengan intención de integrar en ellos el modelo
- establecer directrices asegurar el respeto de la normativa de propiedad intelectual, en particular en materia de minería de texto y datos
- publicar un resumen detallado del contenido usado para el entrenamiento del modelo de uso general

Por sus elevadas capacidades de gran impacto, ciertos modelos de uso general se consideran de **riesgo sistémico**, y se imponen obligaciones más estrictas a sus proveedores para mitigar los riesgos.

Régimen sancionador

Los Estados miembros de la UE deberán establecer el régimen de sanciones aplicable a las infracciones.

- La realización de **prácticas prohibidas** por el Reglamento IA estará sujeta a multas de **hasta 35 millones de euros o el 7 % de la facturación anual mundial**, aplicando el importe que sea de mayor cuantía.

- El incumplimiento de las principales obligaciones de los proveedores, representantes autorizados, importadores, distribuidores y responsables del despliegue estará sujeto a multas de **hasta 15 millones de euros o el 3 % de la facturación anual mundial**, aplicando el importe que sea de mayor cuantía.

- El **suministro de información incorrecta, incompleta o engañosa** a los organismos notificados y a las autoridades nacionales competentes en respuesta a una solicitud estará sujeto a multas de **hasta 7,5 millones de euros o hasta el 1 % de la facturación anual mundial**, aplicando el importe que sea de mayor cuantía.

Cuando se trate de pymes, incluidas las empresas emergentes, se podrá aplicar la cuantía que resulte menor entre el importe o el porcentaje máximos señalados.

Próximos pasos

El Reglamento entrará en vigor a los 20 días de su publicación oficial, y será aplicable con carácter general al cabo de 24 meses. Sin embargo, se establecen plazos distintos para determinados artículos, que oscilan entre los 6 meses para las prácticas prohibidas, los 12 meses para ciertas normas de gobernanza, y los 36 meses para las reglas sobre sistemas de riesgo alto vinculados a la legislación armonizada sobre seguridad de productos.

Para obtener información adicional sobre el contenido de este documento puede enviar un mensaje a nuestro equipo del *Área de Conocimiento e Innovación* o dirigirse a su contacto habitual en Cuatrecasas.

©2024 CUATRECASAS

Todos los derechos reservados.
Este documento es una recopilación de información jurídica elaborado por Cuatrecasas. La información o comentarios que se incluyen en el mismo no constituyen asesoramiento jurídico alguno.
Los derechos de propiedad intelectual sobre este documento son titularidad de Cuatrecasas. Queda prohibida la reproducción en cualquier medio, la distribución, la cesión y cualquier otro tipo de utilización de este documento, ya sea en su totalidad, ya sea en forma extractada, sin la previa autorización de Cuatrecasas.

bsi. ISO/IEC 27001 Information Security Management
IS 713573