RocaJunyent Informa

Departamento de Protección de Datos, Ciberseguridad y Tecnología

19 de julio de 2024

El pasado 12 de julio de 2024 se publicó el texto definitivo del nuevo Reglamento de Inteligencia Artificial ("**RIA**" o "**Reglamento**")[1] en el Diario Oficial de la Unión Europea. Analizamos sus puntos clave en esta alerta.

1. ¿Qué considera el RIA como Sistemas de Inteligencia Artificial?

El RIA está diseñado para supervisar y regular la implementación de la Inteligencia Artificial ("**IA**"), enfocándose particularmente en mitigar los riesgos asociados con su desarrollo y uso.

El Reglamento define los **Sistemas de IA** como sistemas basados en una máquina que está diseñada 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

[1] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

Asimismo, el RIA hace especial hincapié en los **Sistema de IA de Uso General**, definiéndolos como sistemas basados en un **Modelo de IA de Uso General**, que está entrenado con un gran volumen de datos utilizando 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 introducción en el mercado; los Sistemas de IA de Uso General puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA.

2. ¿Qué roles identifica el RIA?

El RIA identifica los siguientes roles en el ciclo de vida de los sistemas y modelos IA:

a) **Proveedor:** Persona física o jurídica, autoridad pública u organismo que desarrolla un sistema o modelo de IA y lo introduce en el mercado o pone en servicio bajo su propio nombre o marca, ya sea de forma gratuita o pagada.
b) **Responsable de despliegue:** Persona física o jurídica, o autoridad pública que utiliza un sistema de IA bajo su propia autoridad, excepto cuando el uso es de carácter personal y no profesional.
c) **Importador:** Persona física o jurídica ubicada en la Unión Europea que introduce en el mercado un sistema de IA que lleva el nombre o la marca de una entidad establecida fuera de la UE.
d) **Distribuidor:** Persona física o jurídica en la cadena de suministro, distinta del proveedor o importador, que comercializa un sistema de IA en la Unión Europea.
e) **Representante autorizado:** Persona física o jurídica en la Unión Europea que, mediante mandato escrito de un proveedor, asume las obligaciones y procedimientos establecidos en el reglamento en representación del proveedor.
f) **Fabricante del producto:** Fabricante según la definición de la legislación armonizada listada en el Anexo I del RIA.

Los seis roles se denominan conjuntamente “operador” y todos ellos pueden aplicarse al contexto de los sistemas de IA. Sin embargo, en el contexto de los modelos, sólo se pueden aplicar los roles de proveedor o representante autorizado. Es decir, no es posible ser responsable de despliegue, importador, distribuidor o fabricante del producto respecto a un modelo de IA

3. ¿Cuál es el ámbito de aplicación?

El ámbito de aplicación del Reglamento se extiende más allá de las organizaciones establecidas en la Unión Europea (“**UE**”), alcanzando también a aquellas que utilicen, desarrollen o intervengan como operadores en los sistemas y modelos de Inteligencia Artificial (“**IA**”) en el mercado europeo. Esto implica que, también deberán aplicarlo las numerosas multinacionales, con presencia o interacciones comerciales en la UE.

4. ¿A qué sistemas IA no se aplica el RIA?

El Reglamento de IA no se aplicará a los sistemas y herramientas de IA de dedicados a:

a) **Fines militares y de seguridad nacional:** Sistemas de IA utilizados exclusivamente para fines militares, de defensa o de seguridad nacional.
b) **Cooperación internacional:** Sistemas de IA utilizados por autoridades públicas de terceros países u organizaciones internacionales en el marco de acuerdos de cooperación internacional con la UE o sus Estados miembros, siempre que se garantice la protección de los derechos y libertades fundamentales.

c) **Investigación y desarrollo científico:** Sistemas y modelos de IA desarrollados y utilizados exclusivamente para la investigación y el desarrollo científicos.
d) **Pruebas y desarrollo precomercial:** Actividades de investigación, prueba o desarrollo de sistemas o modelos de IA antes de su introducción en el mercado o puesta en servicio (excepto pruebas en condiciones reales).
e) **Uso personal no profesional:** Sistemas de IA utilizados por personas físicas en actividades puramente personales y no profesionales.
f) **Licencias libres y código abierto:** Algunos sistemas de IA liberados bajo licencias libres y de código abierto, excepto aquellos que sean prohibidos o de alto riesgo.

5. ¿Cómo se categorizan los Sistemas IA?

Los Sistemas IA se categorizan según el riesgo que implican para los derechos fundamentales de las personas, existiendo Sistemas de Riesgo Inaceptable, de Alto Riesgo, de Riesgo Limitado y de Riesgo Mínimo.

Riesgo Inaceptable:

Los siguientes Sistemas IA son catalogados de Riesgo Inaceptable y, por tanto, están prohibidos por el RIA:

1. **Inferencia de características sensibles:** La categorización biométrica e individual para inferir características sensibles como la raza, orientación religiosa, ideológica o sexual, entre otras, al plantear serios riesgos para la privacidad y la discriminación.
2. **Reconocimiento biométrico en espacios públicos:** El uso de reconocimiento biométrico en remoto y en tiempo real en espacios accesibles al público con fines de prevención o investigación de delitos, sin cumplir ciertos requisitos de excepción (como tipos penales específicos y condiciones estrictas).
3. **Scraping de imágenes faciales:** El scraping generalizado de imágenes faciales de internet o CCTV para generar o ampliar bases de datos de reconocimiento facial.
4. **Reconocimiento de emociones en entornos sensibles**: El reconocimiento de emociones en entornos laborales y educativos, salvo con fines médicos o de seguridad,
5. **Scoring social:** Los sistemas de puntuación social que evalúan a personas o colectivos según su comportamiento social o características personales (conocidas, inferidas o predichas).
6. **Manipulación**: Los sistemas que utilizan técnicas subliminales, manipuladoras o engañosas para alterar el comportamiento de las personas, mermando su capacidad para tomar decisiones informadas y llevándolas a adoptar decisiones perjudiciales que de otro modo no hubieran tomado
7. **Explotación de vulnerabilidades**: Sistemas que exploten vulnerabilidades de las personas (edad, solvencia, discapacidad, etc.) o grupos de personas para influir en su comportamiento provocando perjuicios considerables.
8. **Predicción de riesgo delictivo**: Sistemas que evalúen y predigan el riesgo de comisión de delitos basándose únicamente en la elaboración del perfil de una persona física.

Alto Riesgo

Un sistema de IA es considerado de alto riesgo si cumple alguna de las siguientes condiciones:

1. Está destinado a ser un componente de seguridad de un producto regulado por la legislación armonizada de la UE (Anexo I), o es el propio producto.

2. El producto o el sistema de IA debe someterse a una evaluación de conformidad de terceros según la legislación armonizada de la UE (Anexo I).
3. Pertenece a alguno de los ocho sectores identificados en el Anexo III del RIA y pueden presentar un riesgo significativo para la salud, seguridad o derechos fundamentales, ni influyen sustancialmente en la toma de decisiones
   a. Biometria
   b. Infraestructuras Criticas
   c. Educación y Formación profesional
   d. Empleo, gestión de los trabajadores y acceso al autoempleo
   e. Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones
   f. Garantía del cumplimiento del derecho
   g. Migración, asilo y gestión del control fronterizo
   h. Administración de justicia y procesos democráticos

   Los Proveedores que consideren que un sistema perteneciente a los sectores descritos no es de alto riesgo debe documentar su evaluación antes de su comercialización y registrarla

6. ¿Cómo se categorizan los Modelos de IA uso general?

a) Riesgo Sistémico:

Un modelo de IA de uso general se considera de riesgo sistémico si cumple alguna de las siguientes condiciones:

1. Capacidades de gran impacto evaluadas mediante herramientas y metodologías técnicas adecuadas, utilizando indicadores y parámetros de referencia.
2. Decisión de la Comisión Europea en atención a criterios tasados:
   a. El número de parámetros del modelo;
   b. La calidad o el tamaño del conjunto de datos, por ejemplo medidos a través de criptofichas;
   c. La cantidad de cálculo utilizada para entrenar el modelo, medida en operaciones de coma flotante o indicada con una combinación de otras variables, como el coste estimado del entrenamiento, el tiempo estimado necesario o el consumo de energía estimado para el mismo;
   d. Las modalidades de entrada y salida del modelo, como la conversión de texto a texto (grandes modelos de lenguaje), la conversión de texto a imagen, la multimodalidad y los umbrales punteros para determinar las capacidades de gran impacto de cada modalidad, y el tipo concreto de entradas y salidas (por ejemplo, secuencias biológicas);
   e. Los parámetros de referencia y las evaluaciones de las capacidades del modelo, también teniendo en cuenta el número de tareas sin entrenamiento adicional, la adaptabilidad para aprender tareas nuevas distintas, su nivel de autonomía y capacidad de ampliación y las herramientas a las que tiene acceso;
   f. Si sus repercusiones para el mercado interior son importantes debido a su alcance, lo que se dará por supuesto cuando se haya puesto a disposición de al menos 10 000 usuarios profesionales registrados establecidos en la UE;
   g. El número de usuarios finales registrados.

b) Riesgos Ordinarios

   Todos los modelos no calificados como de riesgo sistémico.

7. ¿Qué son los espacios de prueba y cómo van a funcionar?

Con el objetivo de reforzar la competitividad europea en el ámbito de la IA, se habilita un espacio controlado de pruebas ("**Sandbox**") orientado a ofrecer un entorno controlado para desarrollar, probar, y

validar sistemas de IA innovadores en condiciones reales. Con el Reglamento, se busca establecer normas comunes para la creación de un Sandbox y un marco para la cooperación entre las autoridades de supervisión implicadas. No obstante, serán las autoridades de supervisión locales quienes determinarán los requisitos concretos para el acceso a los Sandbox. En España, el Real Decreto 817/2023, de 8 de noviembre, tiene como objeto la creación del primer entorno controlado de para ensayar la aplicación de ciertos requisitos previstos en el Reglamento

8. ¿Qué son los códigos de conducta que se mencionan en el Reglamento de IA?

Los códigos de conducta son herramientas para promover la ética, la transparencia y la responsabilidad en el desarrollo y uso de la IA. La Oficina de IA y los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta, diseñados para ser aplicados de manera voluntaria por los proveedores de sistemas de IA. Estos códigos están destinados a fomentar la aplicación voluntaria de los requisitos establecidos en el capítulo III, sección 2, a los sistemas de IA que no sean de alto riesgo. Estos deberán incluir, entre otros, mecanismos de gobernanza, las mejores prácticas del sector y la adopción de soluciones técnicas.

9. ¿Cuándo será de aplicación?

El RIA será de aplicación de forma paulatina:

1º) **1 de agosto de 2024:** Entrada en vigor del RIA
2º) **2 de febrero de 2025:** Entrada en aplicación de las prohibiciones de uso, seis meses después de la entrada en vigor del reglamento.
3º) **2 de mayo de 2025:** Concluye el plazo para la finalización de los códigos de buenas prácticas, nueve meses después de la entrada en vigor del reglamento.
4º) **2 de agosto de 2025:** Entrada en aplicación de las disposiciones dirigidas a modelos de IA, doce meses después de la entrada en vigor del reglamento.
5º) **2 de agosto de 2026:** Entrada en aplicación del resto de la norma, veinticuatro meses después de la entrada en vigor del reglamento.
6º) **2 de agosto de 2027:** Entrada en aplicación del artículo 6.1 y del anexo I del RIA para calificar sistemas de Alto Riesgo, treinta y seis meses después de la entrada en vigor del reglamento.

A los 5 años se deberá realizar una revisión del Reglamento de IA.

10. ¿Cuáles son las entidades de supervisión?

En España, la autoridad de supervisión competente para el Reglamento de Inteligencia Artificial es la AESIA (Agencia Española de Supervisión de la Inteligencia Artificial). A nivel europeo, se establecerá un Comité Europeo de Inteligencia Artificial con un representante de cada Estado miembro, encargado de orientar la implementación del reglamento, elaborar guías y establecer reglas para sandboxes. La Oficina Europea de IA desempeña un papel crucial en supervisar el cumplimiento del reglamento en los Estados miembros, asegurando una aplicación uniforme y efectiva en todos los sectores que utilizan sistemas de IA. Trabaja en colaboración con las autoridades nacionales para coordinar actividades de control y formación, garantizando el respeto a los estándares establecidos. A nivel internacional, la Oficina participa en foros y acuerdos globales para promover una gobernanza global de IA y compartir estrategias regulatorias comunes.

11. ¿Cuáles son los incumplimientos y las sanciones?

Las multas por infracción del RIA se fijaron como un porcentaje del volumen de negocios anual global de la empresa infractora en el ejercicio financiero anterior o una cantidad predeterminada, la que fuera más alta. Como máximo representaría el 7% del volumen de negocio global. Las medidas punitivas

están diseñadas para garantizar el cumplimiento del RIA y fomentar un uso ético y responsable de la inteligencia artificial. Algunas de las sanciones que podrían aplicarse son las siguientes:

En Modelos de IA, hasta 15M de euros o el 3% por el volumen de negocio para el incumplimiento de las obligaciones

En los Sistemas de IA:

- Hasta 35M de €, o 7% del volumen anual de negocio para empresas por incumplir las prohibiciones del Reglamento.
- Hasta 15M de €, o 3% del volumen anual de negocio por incumplir las obligaciones del Reglamento a proveedores, importadores, distribuidores, usuarios.
- Hasta 7,5M de €, o 1% del volumen anual de negocio por suministrar información incorrecta a entidades notificadas o autoridades nacionales competentes

Además de las sanciones económicas, las empresas pueden enfrentarse a una serie de consecuencias derivadas de las infracciones del RIA. Prohibición de uso. En casos graves de incumplimiento, las autoridades competentes pueden imponer la prohibición del uso de ciertos sistemas de inteligencia artificial o de toda la actividad relacionada con la IA a la empresa infractora. Retirada de certificaciones y licencias. Si una empresa ha obtenido certificaciones o licencias para el uso de sistemas de inteligencia artificial y se descubre que ha incumplido las regulaciones del RIA, estas certificaciones o licencias pueden ser revocadas. Responsabilidad civil y penal. Además de las sanciones administrativas, las empresas y personas responsables del desarrollo o uso indebido de sistemas de IA pueden enfrentarse a acciones legales civiles y penales por daños causados a terceros o por violaciones de derechos fundamentales