Las 15 claves del Reglamento Europeo de Inteligencia Artificial (Ai Act) (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).

Concepción CAMPOS ACUÑA
Experta en gestión pública
Codirectora de Red Localis y Prof. Asociada Derecho Administrativo (URV)
El Consultor de los Ayuntamientos, 15 de Julio de 2024, LA LEY
Complylaw, 17 de Julio de 2024, LA LEY
El Consultor Contratación Administrativa, 29 de Julio de 2024, LA LEY

LA LEY 13390/2024

La publicación en el Diario Oficial de la Unión Europea (DOUE) de 12 de julio del Reglamento de Inteligencia Artificial (RIA) ponía fin a un largo proceso legislativo para consensuar una norma sin precedentes, por su contenido y alcance, y activaba el cronómetro para una entrada en vigor en varias fases, dando inicio a un largo proceso de despliegue y cumplimiento con una clara finalidad: la protección de los derechos de las personas en un entorno de disrupción tecnológica sin limitar la apuesta por la innovación como senda de desarrollo económico y crecimiento del espacio europeo.

1 FINALIDAD

El 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 (RIA), también conocido como *AI Act,* enuncia sus objetivos de modo general en su Considerando I, y concretados en su artículo 1, que se pueden sintetizar en los siguientes:

— Mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular, para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial en la Unión.

— Promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, de conformidad con los valores y los principios de funcionamiento de la Unión.

— Asegurar un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea, incluidos la democracia, el Estado de Derecho y la protección del medio

ambiente, proteger frente a los efectos perjudiciales de los sistemas de IA en la Unión.

— Brindar apoyo a la innovación, en particular, a las pequeñas y medianas empresas (pymes), incluidas las empresas emergentes.

— Garantizar la libre circulación transfronteriza de mercancías y servicios basados en la IA, impidiendo así que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistemas de IA, a menos que el propio RIA lo autorice expresamente.

2 ÁMBITO DE APLICACIÓN

El Reglamento, marcado por el principio de extraterritorialidad, se aplicará, desde el punto **subjetivo**, a:

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 Unión, con independencia de si dichos proveedores están establecidos o ubicados en la Unión o en un tercer país.

b) Los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión.

c) Los proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión.

d) Los importadores y distribuidores de sistemas de IA.

e) Los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca.

f) Los representantes autorizados de los proveedores que no estén establecidos en la Unión.

g) Las personas afectadas que estén ubicadas en la Unión.

Desde el punto de vista del ámbito objetivo, se recogen una serie de **excepciones** materiales a su aplicación, entre la cuales destacan las competencias de los Estados en materia de seguridad nacional, aquellos supuestos de introducción en el mercado, puesta en servicio o uso de sistemas de IA con fines militares, de defensa o de seguridad nacional y específicamente con la investigación y el desarrollo científicos como única finalidad, así como los sistemas de IA desarrollados bajo licencias libres y de código abierto, salvo en el caso de que sean de alto riesgo.

Tampoco se aplicará a las obligaciones de 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.

3 ESTRUCTURA

El RIA se estructura en un total de **180 Considerandos, 113 artículos y 13 anexos,** con la siguiente asignación de contenidos materiales en Capítulos

CAPÍTULO I. Disposiciones generales

CAPÍTULO II. Prácticas de IA prohibidas

CAPÍTULO III. Sistemas de IA de alto riesgo

4 DEFINICIONES

El **artículo 2** RIA contempla una serie de definiciones con el propósito de fijar las premisas de partida, un total de 68, pero a los efectos de aquéllas que puedan resultar de mayor interés conviene destacar las siguientes:

- **«sistema de IA»**: 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;
- **«riesgo»:** la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio;
- **«proveedor»:** una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente.
- **«responsable del despliegue»**: una persona física o jurídica, o **autoridad pública**, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional
- **«evaluación de la conformidad»**: el proceso por el que se demuestra si se han cumplido los requisitos establecidos en el capítulo III, sección 2, en relación con un sistema de IA de alto riesgo
- **«datos biométricos»:** los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos;
- **«espacio de acceso público»:** cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad;
- **«modelo de IA de uso general»**: un modelo de IA, también uno 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.

5 CLASIFICACIÓN Y GESTIÓN DE RIESGOS

Una de las señas de identidad del RIA es que está basado en un enfoque basado en el riesgo, siguiendo las técnicas de *Compliance,* fijando la siguiente clasificación:

1. Sistemas de IA de riesgo inaceptable

La identificación de una serie de usos prohibidos en el **artículo 5** RIA representa la identificación de las líneas rojas de la regulación europea, pues identifica una serie de sistemas que representan una amenaza directa a la seguridad pública, la privacidad y los derechos fundamentales. No obstante, se permiten una serie de excepciones, en relación con el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos recogidos en la norma.

2. Sistemas de IA de alto riesgo

Se identifican como de alto riesgo aquellos sistemas de IA que pueden tener impacto relevante en los derechos fundamentales de las personas. Algunos ejemplos son las infraestructuras críticas, la educación y la formación profesional, el empleo, los servicios públicos y privados esenciales (por ejemplo, la sanidad o la banca), determinados sistemas de las fuerzas de seguridad, la migración y la gestión aduanera, la justicia y los procesos democráticos (como influir en las elecciones). Se incluye el reconocimiento de emociones en el lugar de trabajo y en las escuelas, sistemas de puntuación ciudadana, la actuación policial predictiva (cuando se base únicamente en el perfil de una persona o en la evaluación de sus características) y la IA que manipule el comportamiento humano o explote las vulnerabilidades de las personas. Este tipo de sistemas se encuentran identificados en el **Anexo III** del RIA.

3. Sistemas de IA de riesgo limitado

En este caso nos encontramos ante los **sistemas de propósito general**, de riesgo limitado, asociado, por ejemplo, a situaciones de uso de sistemas de IA como *chatos*, en cuyo caso debe garantizarse a los usuarios la información de que están interactuando con una máquina para que puedan tomar una decisión informada de continuar o dar un paso atrás. Los proveedores también tendrán que asegurarse de que el contenido generado por IA sea identificable. Además, el texto generado por IA publicado con el propósito de informar al público sobre asuntos de interés público debe etiquetarse como generado artificialmente. Estas prevenciones también resultan de aplicación al contenido de audio y video que constituyen *deep fakes.*

4. Sistemas de IA de riesgo mínimo

No están regulados específicamente, pero se trata de aquellos supuestos en los que las personas pueden decidir de forma libre sobre su uso (por ejemplo, videojuegos con IA o filtros de spam).

El RIA contempla una secuencia de niveles de riesgo, y en función del diagnóstico, en cada caso aplica un sistema de gestión de esos riesgos, preservando las garantías jurídicas y el

buen funcionamiento de las instituciones. Evidentemente, a mayor riesgo, mayores obligaciones, llegando incluso a la prohibición en el caso de riesgos extremos para los derechos humanos, por ejemplo.

6 IA ÉTICA, ROBUSTA Y CONFIABLE: SUPERVISIÓN HUMANA

Una de las claves de la regulación europea, junto con el enfoque basado en riesgos, es la premisa básica de garantizar que los sistemas de IA sean éticos y confiables. El RIA recuerda en su **Considerando 27** la vigencia de las **Directrices éticas para una IA fiable** (2019) y, por tanto, de los **siete principios éticos** no vinculantes para la IA que tienen por objeto contribuir a garantizar la fiabilidad y el fundamento ético de la IA. Los siete principios son: acción y supervisión humanas; solidez técnica y seguridad; gestión de la privacidad y de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y ambiental, y rendición de cuentas. Sin perjuicio de los requisitos jurídicamente vinculantes del RIA y de cualquier otro acto aplicable del Derecho de la Unión, esas directrices contribuyen al diseño de una IA coherente, fiable y centrada en el ser humano, en consonancia con los valores en los que se fundamenta la Unión.

A tal fin será una herramienta fundamental el aseguramiento a través de las evaluaciones de impacto relativas a los derechos fundamentales para los sistemas de IA de alto riesgo (**artículo 27)** y la supervisión por la autoridad de vigilancia de mercado, sin perjuicio de la actuación de la Oficina de IA y Autoridades nacionales de supervisión.

La **supervisión humana** completa esta clave, al disponer el **artículo 14** RIA la obligación de que los sistemas de IA de alto riesgo se diseñen y desarrollen de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso. Esta supervisión tiene como objetivo será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de IA de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible, en particular cuando dichos riesgos persistan a pesar de la aplicación de otros requisitos.

7 IMPACTO EN EL SECTOR PÚBLICO

El RIA afectará tanto al sector privado como al público, si bien es cierto que, con carácter general, en atención a los diferentes roles de cada uno de ellos. En el caso del sector público, el rol más frecuente será el de **«responsable del despliegue»**, entendiendo como tal una persona física o jurídica, o **autoridad pública**, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional.

En dicho sentido, las entidades del Sector Público, que en la actualidad están ya en un uso avanzado de sistemas de *chatbots* conversacionales, reconocimiento de voz, etc., deberán tener en consideración las obligaciones que impone el RIA, en especial cuando se trata de sistemas de IA de alto riesgo. El **artículo 26** RIA impone a los responsables de despliegue, específicamente, el deber de adoptar las medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas de conformidad con las instrucciones de uso que acompañan a los sistemas. Y, por otra parte, deberán asignar la supervisión humana a personas físicas que tengan la competencia, formación y autoridad necesarias, así como el apoyo necesario.

Dentro del papel que corresponde a los poderes públicos, es el de asumir uno de los grandes retos en el diseño e implantación de la IA, como es el relativo a los **sesgos y la discriminación** que puede producir en determinados colectivos y que se pueden

incorporar en los algoritmos de un modo consciente o inconsciente. Si bien el RIA se orienta de modo preventivo, garantizando la ética y fiabilidad desde el diseño, corresponde a los poderes públicos garantizar la debida protección, en especial respecto de aquellos colectivos más vulnerables. No debemos olvidar que el sector público no es solo administración tradicional burocrática, sino que afecta a ámbitos como la salud, la educación, la seguridad, donde la IA está teniendo ya un papel clave.

Pero, dadas las características e idiosincrasia del Sector Público, será la asimilación de los posibles usos de esta tecnología el verdadero desafío. A dicho fin, será clave la debida labor de alfabetización, y completar las correspondientes **transformaciones organizativas**, tanto a nivel de estructura general, como adecuación de plantillas y puestos de trabajo (incluyendo la creación de nuevos puestos y la adaptación de los existentes), reconfigurando las funciones y tareas, en atención al despliegue de los sistemas de IA en la gestión pública. En el ámbito privado se ha procedido ya a la creación de un nuevo puesto de trabajo con estas funciones, el conocido como **CAIO** (*Chief Artificial Intelligence Officer)* al que corresponderá, entre otras competencias, asesorar internamente en la implementación de soluciones basadas en IA o en el desarrollo de proyectos que incorporen tal tecnología, habrá que ver si se adopta esta figura en el sector público.

8 TRANSPARENCIA

Uno de los ejes de las obligaciones del RIA viene dado por el principio de transparencia. Se concreta en la obligación de que los sistemas de IA se desarrollen y utilicen de un modo que permita una **trazabilidad y explicabilidad** adecuadas, y que, al mismo tiempo, haga que las personas sean conscientes de que se comunican o interactúan con un sistema de IA, así como que se informe debidamente a los responsables del despliegue acerca de las capacidades y limitaciones de dicho sistema de IA y a las personas afectadas acerca de sus derechos.

Las obligaciones de transparencia aplicables a ciertos sistemas de IA se concretan en el **Capítulo IV** RIA, sin perjuicio de **las** obligaciones de transparencia y comunicación de información a los responsables del despliegue, establecidas en su **artículo 13**. En particular, los usuarios de **sistemas de categorización biométrica o de reconocimiento de emociones,** informarán a las personas sobre los que se use de tal realidad, con ciertas excepciones para la persecución del crimen. Los usuarios de sistemas de IA que produzcan imagen o sonido que parezcan de verdad personas, lugares, objetos, etc. (***deep fakes***), deberán informar de ello, con ciertas excepciones en la persecución del crimen o en contenidos evidentemente creativos, satíricos o ficticios. También afectará a los sistemas de IA de uso general que generen contenido sintético de audio, imagen, vídeo o texto; sistemas de reconocimiento de emociones o de un sistema de categorización biométrica o sistemas que generen o manipulen imágenes o contenidos de audio o vídeo que constituyan una ultra suplantación.

Transparencia que se materializa ya desde el diseño, al extenderse en relación con los **datos utilizados en el entrenamiento previo y el entrenamiento de los modelos de IA de uso general**, incluidos los textos y los datos protegidos por el Derecho en materia de derechos de autor, al exigir que los proveedores de dichos modelos elaboren y pongan a disposición del público un resumen suficientemente detallado de los contenidos utilizados para el entrenamiento del modelo de IA de uso general. Todo ello sin perjuicio de otras obligaciones de transparencia aplicables a los responsables del despliegue de sistemas de IA establecidas en el Derecho de la Unión o nacional.

Para garantizar el debido cumplimiento de las obligaciones de transparencia, la Comisión podrá también fomentar y facilitar la elaboración de **códigos de buenas prácticas a escala de la Unión,** a fin de facilitar la aplicación eficaz de las obligaciones en materia de detección y etiquetado de contenidos generados o manipulados de manera artificial.

9 INNOVACIÓN

Una de las objeciones comunes al RIA es la de que supondrá una barrera a la innovación. Su filosofía no es ésa, sino la de apoyar la innovación, respetar la libertad de ciencia y no socavar la actividad de investigación y desarrollo, y de ahí la exclusión en su aplicación (**Considerando 25 y Artículo 3**).

Apoyando dicha línea regulatoria, se fomentan los **espacios comunes europeos de datos europeos,** entre otros los de salud, que se configuran así como una herramienta clave para ofrecer un acceso fiable, responsable y no discriminatorio a datos de alta calidad con los que entrenar, validar y probar los sistemas de IA, ofreciendo así una ventaja competitiva a los operadores de mercado, pues el acceso a los datos y la capacidad de utilizarlos son fundamentales para la innovación y el crecimiento.

El **Capítulo VI** del RIA, se refiere específicamente a las **medidas de apoyo a la innovación,** disponiendo que los Estados miembros velarán por que sus autoridades competentes establezcan al menos un espacio controlado de pruebas para la IA a escala nacional, que estará operativo a más tardar el 2 de agosto de 2026, los conocidos como ***sandbox* regulatorio,** para desarrollar, entrenar, probar y validar sistemas IA bajo su guía, supervisión y soporte

En España, se daba cumplimiento temprano a esta previsión con el **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. Esta iniciativa del Gobierno de España, con la colaboración de la Comisión Europea, pretende obtener, como resultado de esta experiencia, unas guías basadas en la evidencia y la experimentación que faciliten a las entidades, especialmente las pequeñas y medianas empresas, y a la sociedad en general, el alineamiento con el RIA.

10 OBLIGACIONES DE ALFABETIZACIÓN

El correcto despliegue e implantación de la IA requerirá de la dotación y despliegue de las correspondientes **competencias profesionales** por parte de los distintos actores implicados en el proceso, necesidad que se hace extensiva tanto al sector público como al privado y que se enmarca en una fase más del proceso de transformación digital ya iniciado hace unas décadas, pero todavía inconcluso.

Según las definiciones del RIA entendemos por **«alfabetización en materia de IA»**: las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y demás personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto de la norma europea, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar.

A dichos efectos, el **artículo 4** RIA impone a proveedores y responsables del despliegue de sistemas de IA la adopción de las medidas precisas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA. Este proceso se realizará teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas.

En España, se ha aprobado un Plan de competencias digitales de ámbito general, y también

un marco específico para el Sector Público, **Competencias digitales de las empleadas y empleados públicos**, aprobado por el INAP, que contempla una competencia específica sobre el uso ético y responsable de la IA, que abarca aspectos como la privacidad, la transparencia, la equidad y la rendición de cuentas. Esta competencia es transversal a todas las demás y permite a los empleados públicos aplicar criterios éticos en el diseño, la implementación y la evaluación de soluciones basadas en IA.

11 CÓDIGOS DE CONDUCTA

En consonancia con la obligación de garantizar un despliegue ético y confiable de la IA, el RIA apuesta por las herramientas de *soft law,* códigos de conducta (de aplicación voluntaria) como elementos de autorregulación. Para ello la Oficina de IA y los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta, con los correspondientes mecanismos de gobernanza, destinados a fomentar la aplicación voluntaria de alguno o de todos los requisitos establecidos en el capítulo III, sección 2, a los **sistemas de IA que no sean de alto riesgo,** teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector que permitan la aplicación de dichos requisitos (**artículo 95**).

La idea es que esta técnica se extienda también a los **responsables del despliegue**, elaborando códigos de conducta con requisitos específicos para todos los sistemas de IA, sobre la base de objetivos claros e indicadores clave de resultados para medir la consecución de dichos objetivos.

Los códigos de conducta podrán ser elaborados por proveedores o responsables del despliegue de sistemas de IA particulares, por las organizaciones que los representen o por ambos, también con la participación de cualquier parte interesada y sus organizaciones representativas, como, por ejemplo, las organizaciones de la sociedad civil y el mundo académico. Los códigos de conducta podrán comprender uno o varios sistemas de IA en función de la similitud de la finalidad prevista de los distintos sistemas.

No obstante, a efectos de evitar mayores cargas y obstáculos en el uso y despliegue de los sistemas de la IA, la Oficina de IA y los Estados miembros tendrán en cuenta los intereses y necesidades específicos de las **pymes**, incluidas las empresas emergentes, a la hora de fomentar y facilitar la elaboración de códigos de conducta.

En el compromiso de un adecuado seguimiento, el RIA dispone que cada **cuatro años**, la Comisión evaluará la efectividad de los códigos de conducta.

12 GOBERNANZA

El despliegue de las previsiones del RIA requerirá de un adecuado modelo de gobernanza, que se estructura a través del **Comité Europeo de IA**, con un representante de cada Estado Miembro. El Supervisor Europeo de Protección de Datos será observador y la Comisión participará sin voto. Este órgano contará con la asesoría de un grupo permanente de representación de interesados, que incluirá proveedores, usuarios, entidades notificadas, organizaciones civiles, etc. Cada EEMM designará una autoridad notificadora y al menos una autoridad de supervisión de mercado en relación con el RIA.

De conformidad con el apartado de definiciones corresponde a la **«Oficina de IA»,** contribuir a la implantación, el seguimiento y la supervisión de los sistemas de IA y modelos de IA de uso general, y a la gobernanza de la IA prevista por la Decisión de la Comisión de 24 de enero de 2024 (DOUE-Z-2024-70007).

La Oficina tiene por objeto permitir el desarrollo, el despliegue y el uso futuros de la IA de un modo que fomente los beneficios sociales y económicos y la innovación, mitigando al

mismo tiempo los riesgos. Igualmente, trabajará para fomentar la investigación y la innovación en IA fiable, robusta.

En el ámbito de los respectivos EEMM la **«autoridad nacional de supervisión»** que se encargue de supervisar la aplicación y ejecución de lo dispuesto en la mencionada Ley de Inteligencia Artificial, así como de coordinar las actividades encomendadas a dichos Estados miembros, actuar como el punto de contacto único para la Comisión, y representar al Estado miembro en cuestión ante el Comité Europeo de IA.

En España se ha dado cumplimiento a esta obligación con la creación de la **Agencia Española de Supervisión de Inteligencia Artificial** (AESIA), por el Real Decreto 729/2023, de 22 de agosto. La Agencia ejerce las funciones de inspección, comprobación, y sanción de conformidad con el Reglamento de IA. En definitiva, será la principal autoridad supervisora nacional.

Con fecha máxima de **2 de agosto de 2028**, la Comisión evaluará el funcionamiento de la Oficina de IA, si se le han otorgado poderes y competencias suficientes para desempeñar sus funciones, y si sería pertinente y necesario para la correcta aplicación y ejecución del RIA, mejorar la Oficina de IA y sus competencias de ejecución, así como aumentar sus recursos. La Comisión presentará un informe sobre su evaluación al Parlamento Europeo y al Consejo.

13 RÉGIMEN SANCIONADOR

En el marco regulatorio el RIA se reconoce a los EEMM la **potestad sancionadora**, disponiendo que establecerán el régimen de sanciones y otras medidas de ejecución, como advertencias o medidas no pecuniarias, aplicable a las infracciones de la propia norma que cometan los operadores y adoptarán todas las medidas necesarias para garantizar que se aplican de forma adecuada y efectiva. Las sanciones serán efectivas, proporcionadas y disuasorias, en especial, deberán tener en cuenta los intereses de las pymes, incluidas las empresas emergentes, así como su viabilidad económica.

La determinación de la **cuantía de las sanciones (artículo 99)** se realiza mediante la fijación de un porcentaje del volumen de negocios anual global de la empresa infractora en el ejercicio financiero anterior o un importe predeterminado, si este fuera superior. Las sanciones económicas pueden alcanzar la cifra de 35 millones de euros o el 7 % del volumen de negocios anual total a escala mundial del infractor durante el ejercicio financiero anterior, cuándo el importe fuera superior. En el caso de las pymes, incluidas las empresas emergentes, la multa será por el menor de los importes y porcentajes anteriores.

Régimen sancionador que no excluye los **«efectos colaterales»**, es decir, que además de las sanciones que puedan aplicarse por el incumplimiento del RIA, las infracciones pueden implicar la aplicación del establecido en otros ámbitos materiales de actuación, como en el caso de **protección de datos, propiedad intelectual, ciberseguridad, confidencialidad, competencia, consumidores y usuarios, laboral, administrativo, penal, laboral, e**tc.

14 DELEGACIÓN DE PODERES

El RIA recoge el otorgamiento a la **Comisión** los poderes para adoptar actos delegados en las condiciones establecidas en el **artículo 97**, previa consulta a los expertos designados por cada Estado miembro.

La Comisión tiene delegados los poderes de:

- Enmendar la lista de tipos de sistema que se consideran HRAIS en el Anexo III.

- Asegurar que la documentación exigida sea suficiente para asegurar la conformidad de los sistemas con el Reglamento, a la vista del progreso técnico.
- Enmendar el Anexo VI (valoración de conformidad mediante control interno) y el Anexo VII (valoración de conformidad mediante valoración del sistema de control de calidad y la documentación) para adecuarlos al progreso técnico.
- Requerir que ciertos HRAIS para los que el Reglamento autoriza demostrar conformidad mediante control interno, se vean sujetos a pruebas de conformidad por entidad notificada.
- Enmendar el Anexo V (contenidos de la declaración de conformidad) para adecuarlo al progreso técnico.

Con posterioridad a su adopción lo notificará simultáneamente al Parlamento Europeo y al Consejo.

15 ENTRADA EN VIGOR

El **artículo 113 RIA** contempla el plazo de entrada en vigor, estableciendo un proceso de aplicación en diferentes fases, sin perjuicio de otras obligaciones temporales que ya hemos ido desgranando y que se recogen en el **artículo 112 RIA, Evaluación y revisión.**

Entrada en vigor general

La entrada en vigor del RIA se produce a los 20 días de su publicación en el DOUE, es decir, el 1 de agosto de 2024 y será de aplicación a los dos años, es decir, el 1 de agosto de 2026.

Al lado de este plazo de vigencia y aplicación general la se recogen una serie de **Reglas especiales de aplicación:**

- **2 de febrero de 2025.**
  - Capítulo I.- Disposiciones generales
  - Capítulo II.- Sistemas prohibidos
- **2 de agosto de 2025**
  - Capítulo V.- Modelos de IA de uso general
  - Capítulo VII.- Gobernanza
  - Artículo 78.- Confidencialidad
  - Capítulo XIII.- Sanciones (excepto multas a proveedores de modelos de IA de uso general, artículo 101)
- **2 de agosto de 2027**
  - Artículo 6.1.- Reglas de clasificación de los sistemas de IA de alto riesgo y obligaciones derivadas

Entre las obligaciones de evaluación y revisión, destacar que la Comisión evaluará la necesidad de modificar la lista del **anexo III** y la lista de prácticas de IA prohibidas previstas en el artículo 5 una vez al año a partir de la entrada en vigor del RIA y hasta el final del período de delegación de poderes.

Cada cuatro años, la Comisión, informará al Parlamento y el Consejo sobre la aplicación del RIA, valorando recursos técnicos y humanos disponibles y sanciones aplicadas.

(1) Este trabajo se enmarca en sendos proyectos de investigación concedidos para el período comprendido entre el 01/09/2022 al 31/08/2025 y de los que son investigadoras principales las profesoras Juana Morcillo y Susana de la Sierra:

a) Proyecto nacional; Proyecto PID2021-*124967OB-I00* (*«Protección jurídica y oportunidades de los colectivos vulnerables ante la digitalización y la inteligencia artificial»-PRODIGIA*), financiado por MICIU/AEI /10.13039/501100011033 y por FEDER, UE.

b) Proyecto regional *«Digitalización y colectivos vulnerables: protección, garantías y propuestas para su implantación en Castilla-La Mancha» (PRODIGITAL: SBPLY/21/180501/000089)*, financiado por JCCM/FEDER, UE.