10 de octubre de 2024
Versión 1.0

GRUPO DE TRABAJO IA-REGIC
Categorías de IA en el Reglamento Europeo de Inteligencia Artificial (RIA)
Requisitos y obligaciones aplicables a cada categoría en investigación

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 ámbito regulatorio de la IA, actuando como un catalizador de la industria.

Desde REGIC, se ha formado un grupo de trabajo desde mayo de 2024 para analizar diferentes aspectos relacionados con la entrada en vigor del Reglamento de IA y cómo puede afectar a las Fundaciones y su actividad en los proyectos de investigación en los que participen.

Estas son las personas y entidades que han participado en la elaboración del presente documento:

Coordinadoras: Anna Boix. VHIR y Natalia Cal. IdiSNA.
Maribel Barros. FIBAO.
Amalia Díaz. IdISSC.
Miriam Carles. I3PT.
Lucas Espuig. IIS La Fe.
Fernando Ferragut. INCLIVA.
Alberto Labiano. IdiSNA.
Anna Moleras. IDIAP.
Belén Rodriguez. IISARAGON.
Andrea Vargas. IDIBELL.

Contenido

INTRODUCCIÓN.

Consideraciones previas y aspectos clave del RIA

El viernes 2 de febrero de 2024, los estados miembros de la UE votaron por unanimidad a favor de aceptar el Reglamento de IA (RIA). El texto final se publicó formalmente en julio de 2024, y se han establecido diferentes plazos de entrada en aplicación para determinados aspectos del RIA, el cual será totalmente aplicable en agosto de 2026, lo que significa que todos los que operen dentro de la UE deberán cumplir con todas las partes de este Reglamento.

Estamos ante un reglamento que utiliza un enfoque basado en el riesgo, que establece una categorización de los riesgos en función del daño que pueda ocasionar a las personas individuales o a la sociedad en su conjunto y, en función del tipo de riesgo (mínimo, limitado, alto o inaceptable) establece las reglas a tener en consideración y aplicar.

Así mismo, estamos ante una norma con amplia aplicación, es decir, no se centra únicamente en un tipo específico de negocio o tecnología, sino que abarca múltiples sectores de actividad. Esto garantiza que los principios fundamentales de la regulación de la IA, como la seguridad, la transparencia y la responsabilidad, se apliquen de manera uniforme a todos los sistemas de IA, sin importar dónde o cómo se utilice.

En lo que respecta a los sistemas de IA con los que se podrá trabajar en las Entidades Gestoras de Investigación implicarán la utilización de datos de categorías especiales como son los datos de salud, biométricos, etc. Ello implica trabajar con sistemas de alto riesgo que englobarán todas aquellas soluciones que pueden tener un impacto potencial en los derechos y toma de decisiones sobre las personas, como es el caso de un diagnóstico o tratamiento en el ámbito de la salud. En esta clasificación entrarían los dispositivos médicos (con certificación MDR) de clase-II-a o superior con inteligencia artificial y productos de diagnóstico *"in vitro"* (todos aquellos con certificación IVDR) que utilicen también esta tecnología. Así, por ejemplo, encontraríamos sistemas que incorporan la inteligencia artificial en el ámbito del software de interpretación de imágenes radiológicas, de electrocardiogramas, sistemas de monitorización a distancia de pacientes, de gestión del ritmo cardíaco, o de análisis de embriones en fecundación *"in vitro"* para evaluar y seleccionar embriones para la transferencia, entre otros. En la categoría de alto riesgo, también entrarían los sistemas que utilicen la inteligencia artificial como componente de seguridad, como puede ser el caso de la cirugía asistida por robot, los que incorporen la identificación biométrica, y determinadas soluciones de inteligencia artificial de asistencia

sanitaria, sean o no dispositivos médicos. En este caso se incluirían, por ejemplo, sistemas que podrían ser utilizados por autoridades públicas para evaluar la elegibilidad de las personas para los servicios públicos esenciales, soluciones para la evaluación y clasificación de llamadas de emergencia, sistemas para envío de servicios de primera intervención en emergencias médicas, o soluciones para el triaje de pacientes en urgencias con inteligencia artificial.

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:

- P**roveedores** 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;
- **Responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la UE. Este sería el rol más cercano a las fundaciones en caso de que se pusiese en servicio un sistema de IA;**
- P**roveedores 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;
- I**mportadores y distribuidores** de sistemas de IA en la UE;
- F**abricantes** 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;
- Representantes autorizados de los proveedores que no estén establecidos en la UE;
- Personas afectadas que estén ubicadas en la UE.

Conceptos de interés a tener en consideración

Antes de entrar a analizar en detalle determinados aspectos que consideramos clave del RIA, es necesario tener presente varios conceptos que incluimos a continuación y que se contemplan en el artículo 3 y otros apartados del Reglamento.

Sistema de IA: 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.

Modelo de IA: aquel 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.

Prueba en condiciones reales: la prueba temporal de un sistema de IA para su finalidad prevista en condiciones reales, fuera de un laboratorio u otro entorno de simulación, con el fin de recabar datos sólidos y fiables y evaluar y comprobar la conformidad del sistema de IA con los requisitos del presente Reglamento; si se cumplen todas las condiciones establecidas en el artículo 57 o 60, no se considerará una introducción en el mercado o una puesta en servicio del sistema de IA en el sentido de lo dispuesto en el presente Reglamento

Introducción en el mercado: la primera comercialización en el mercado de la Unión de un sistema de IA o de un modelo de IA de uso general;

Puesta en servicio: el suministro de un sistema de IA para su primer uso directamente al responsable del despliegue o para uso propio en la Unión para su finalidad prevista;

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;

Identificación biométrica: reconocimiento automatizado de características humanas de tipo físico, fisiológico o conductual, como la cara, el movimiento ocular, la forma del cuerpo, la voz, la entonación, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor o las características de las pulsaciones de tecla, a fin de determinar la identidad de una persona comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos de referencia, independientemente de que la persona haya dado o no su consentimiento. Quedan excluidos los sistemas de IA destinados a la verificación biométrica, que comprende la autenticación, cuyo único propósito es confirmar que una persona física concreta es la persona que dice ser, así como la identidad de una persona física con la finalidad

exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga acceso de seguridad a un local.

Sistema de identificación biométrica en tiempo real: recogida de los datos biométricos, comparación e identificación que se producen de manera instantánea, casi instantánea o, en cualquier caso, sin una importante demora. En este sentido, no debe existir la posibilidad de eludir las normas contempladas en el presente Reglamento en relación con el uso «en tiempo real» de los sistemas de IA en cuestión generando demoras mínimas. Los sistemas «en tiempo real» implican el uso de materiales «en directo» o «casi en directo», como grabaciones de vídeo, generados por una cámara u otro dispositivo con funciones similares. En cambio, en los sistemas «en diferido» ya se han recabado los datos biométricos y la comparación e identificación se producen con una importante demora. A tal fin se utilizan materiales, como imágenes o grabaciones de vídeo captadas por cámaras de televisión en circuito cerrado o dispositivos privados, generados con anterioridad a la utilización del sistema en relación con las personas físicas en cuestión.

Autoridad notificante: autoridad nacional responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión. Características de autoridad notificante:

a. Cada Estado miembro nombrará o constituirá al menos una.
b. Responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión.
c. Cooperación entre las autoridades notificantes de todos los Estados miembros.
d. Imparcialidad, confidencialidad, objetividad y transparencia en el desarrollo de sus actividades.
e. Composición adecuada a las responsabilidades: “suficiente personal competente” especializado en tecnologías de la información, IA y Derecho.

Organismo notificado: organismo de evaluación de la conformidad notificado con arreglo al presente Reglamento y a otros actos pertinentes de la legislación de armonización de la Unión.

Organismo de evaluación de la conformidad: organismo que desempeña actividades de evaluación de la conformidad de terceros, como el ensayo, la certificación y la inspección. Este organismo deberá cumplir las siguientes características:

a. Ser notificados a la Comisión por las autoridades notificantes.
b. Cumplir los requisitos del artículo 31 y respetar las diferentes incompatibilidades establecidas en el Reglamento.
c. Imparcialidad, confidencialidad, objetividad y transparencia en el desarrollo de sus actividades.
d. Funcionamiento detallado en procedimientos documentales adecuados.
e. Personal cualificado suficiente para atender todas las actividades que se le requieran.
f. Certificaciones o evidencias documentales de cumplimiento de requisitos.

g. Verificarán la conformidad de los sistemas de IA de alto riesgo siguiendo los procedimientos de evaluación de la conformidad establecidos en el artículo 43.
h. Evitarán cargas innecesarias para los proveedores cuando desempeñen sus actividades, y tendrán debidamente en cuenta el tamaño del proveedor, el sector en que opera, su estructura y el grado de complejidad del sistema de IA de alto riesgo de que se trate, en particular con vistas a reducir al mínimo las cargas administrativas y los costes del cumplimiento para las microempresas y pequeñas empresas
i. Respetará, sin embargo, el grado de rigor y el nivel de protección requeridos para que el sistema de IA de alto riesgo cumpla los requisitos del presente Reglamento.
j. Pondrán a disposición de la autoridad notificante mencionada en el artículo 28, y le presentarán cuando se les pida, toda la documentación pertinente, incluida la documentación de los proveedores, a fin de que dicha autoridad pueda llevar a cabo sus actividades de evaluación, designación, notificación y supervisión, y de facilitar la evaluación descrita en la presente sección.

Autoridad nacional competente: autoridad notificante o autoridad de vigilancia del mercado; en lo que respecta a sistemas de IA puestos en servicio o utilizados por instituciones, órganos y organismos de la Unión, las referencias hechas en el presente Reglamento a autoridades nacionales competentes o a autoridades de vigilancia del mercado se interpretarán como referencias al Supervisor Europeo de Protección de Datos.

Autoridad de vigilancia del mercado: autoridad nacional que lleva a cabo las actividades y adopta las medidas previstas en el Reglamento (UE) 2019/1020.

Oficina de IA: entidad encargada de la función de la Comisión consistente en 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; las referencias hechas en el presente Reglamento a la Oficina de IA se entenderán hechas a la Comisión. Trabajará por la implementación de la nueva normativa y la elaboración de códigos de conducta, y promoverá el desarrollo y el uso de la inteligencia artificial fiable y la cooperación internacional.

Espacio controlado de pruebas: La nueva ley exige a las autoridades nacionales que desarrollen al menos un espacio controlado de pruebas (sandbox) en condiciones similares al mundo real para que los desarrolladores de soluciones de inteligencia artificial, especialmente los provenientes de la pequeña y mediana empresa, puedan tener oportunidad de desarrollar, entrenar y validar los modelos, durante un período limitado antes de su lanzamiento al público general. Sin embargo, habrá que ver cómo se articulará este entorno de pruebas y cómo se desplegará la nueva responsabilidad de las autoridades de evaluar los sistemas de alto riesgo en España. Sobre el entorno de pruebas, la legislación española ya contempló en el Real Decreto 817/2023, de 8 de noviembre, el establecimiento de un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta del Reglamento Europeo por el que se establecen normas armonizadas en materia de inteligencia artificial.

Art. 2 Reglamento UE 2017/745 sobre los Productos Sanitarios (MDR). Producto sanitario: todo instrumento, dispositivo, equipo, programa informático, implante, reactivo, material u otro artículo destinado por el fabricante a ser utilizado en personas, por separado o en combinación, con alguno de los siguientes fines médicos específicos:

- diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad,
- diagnóstico, seguimiento, tratamiento, alivio o compensación de una lesión o de una discapacidad,
- investigación, sustitución o modificación de la anatomía o de un proceso o estado fisiológico o patológico,
- obtención de información mediante el examen in vitro de muestras procedentes del cuerpo humano, incluyendo
- donaciones de órganos, sangre y tejidos,

Regla 11. Los programas informáticos destinados a proporcionar información que se utiliza para tomar decisiones con fines terapéuticos o de diagnóstico se clasifican en la clase IIa, salvo si estas decisiones tienen un impacto que pueda causar:

- la muerte o un deterioro irreversible del estado de salud de una persona, en cuyo caso se clasifican en la clase III, o
- un deterioro grave del estado de salud de una persona o una intervención quirúrgica, en cuyo caso se clasifican en la clase IIb.

Los programas informáticos destinados a observar procesos fisiológicos se clasifican en la clase IIa, salvo si se destinan a observar parámetros fisiológicos vitales, cuando la índole de las variaciones de dichos parámetros sea tal que pudiera dar lugar a un peligro inmediato para el paciente, en cuyo caso se clasifican en la clase IIb. Todos los demás programas informáticos se clasifican en la clase I.

EXCEPCIONES DE APLICACIÓN DEL RIA: ÁMBITO DE INVESTIGACIÓN

Introducción.

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.

Artículo 2.6 RIA.- El presente Reglamento **no se aplicará a los sistemas o modelos** de IA, incluidos sus resultados de salida, desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad.

Artículo 2.6 8 RIA.- El presente Reglamento **no se aplicará a ninguna actividad** de **investigación, prueba o desarrollo** relativa a sistemas de IA o modelos de IA antes de su introducción en el mercado o puesta en servicio. Estas actividades se llevarán a cabo de conformidad con el Derecho de la Unión aplicable. Las pruebas en condiciones reales no estarán cubiertas por esa exclusión.

No obstante, es muy importante tener presente que cuando en el desarrollo de una investigación se den las circunstancias establecidas en el **artículo 6** (con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b), un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican en el apartado 1.a y 1.b del artículo) o el **artículo 60** (pruebas en condiciones reales fuera de los espacios controlados de pruebas para la IA), no será de aplicación las excepciones antes mencionadas.

Obligaciones.

En primer lugar, basándonos en las consideraciones dadas por el **Considerando 25 RIA**, tenemos que es necesario garantizar que el presente Reglamento no afecte de otro modo a la actividad de investigación y desarrollo científicos sobre sistemas o modelos de IA antes de su introducción en el mercado o su puesta en servicio. Por lo que se refiere a la actividad de investigación, prueba y desarrollo orientada a productos en relación con sistemas o modelos de IA, las disposiciones del presente Reglamento tampoco deben aplicarse antes de que dichos sistemas y modelos se pongan en servicio o se introduzcan en el mercado.

Sin embargo, esta no deja de ser una cuestión controvertida sin solución aparente durante la primera fase de aplicación del RIA. De este modo, pasamos a valorar que la excepción en la aplicación del RIA en materia científica y de investigación no debe pasar en primera instancia por una valoración global del concepto de “excepción” y de “investigación”, sino que se debe acudir a la definición concreta del proyecto o ensayo, así como la finalidad de la herramienta de

IA que se vaya a implementar dentro del mismo y hasta donde, dentro del marco de investigación, el equipo va a actuar.

De este modo, respetando la literalidad del artículo 2, dejamos a salvo los conceptos de "puesta en servicio" y de "introducción en el mercado", además de la exención de "pruebas en condiciones reales" que no estarán cubiertas por la excepción del art. 2.8. Sin el papel y la transparencia del investigador a cargo del proyecto y de la definición de cómo va a funcionar la IA en la investigación no podemos avanzar ni adoptar de forma plena la excepción ni marcar los límites. Así por ejemplo, encontraríamos que el desarrollo de algoritmos, o la creación y prueba de los mismos algoritmos de IA en un entorno de investigación controlado; la realización de estudios experimentales que no impliquen la implementación del sistema en aplicaciones prácticas fuera del entorno de investigación; o el trabajo en la investigación teórica de conceptos y métodos de IA, son algunos de los casos que, sin lugar a dudas y cumpliendo con la aplicación legislativa (de antemano) quedarían bajo las facilidades que ofrece el art. 2 en pos de la innovación científica, y por lo tanto, incluidas en la excepción.

Si bien no se pretende entrar en las cuestiones derivadas de la comercialización, sí que debemos abordar la puesta en servicio y las pruebas en condiciones reales para saber a qué límites (normativos) debemos atenernos.

La **"puesta en servicio"** de un sistema de IA es un concepto clave en el Reglamento (UE) 2024/1689 y se refiere al momento en que un sistema de IA se utiliza por primera vez en condiciones reales para su propósito previsto. Para los sistemas de IA desarrollados en un contexto de investigación, la puesta en servicio implica el uso del sistema fuera del entorno de investigación controlado, ya sea para aplicaciones comerciales o en situaciones prácticas.

Durante la fase de investigación, el sistema de IA está exento del reglamento siempre que se utilice exclusivamente para actividades de investigación científica y no se ponga en servicio en condiciones reales. Los resultados y el sistema de IA no deben ser utilizados para desarrollar o comercializar productos o servicios. Una vez que el sistema de IA se pone en servicio, es decir, se utiliza fuera del entorno de investigación para aplicaciones prácticas o comerciales, debe cumplir con todos los requisitos del reglamento. El sistema debe pasar por un proceso de evaluación de conformidad para asegurar que cumple con las normas de seguridad, ética, transparencia y demás obligaciones establecidas en el Reglamento.

Antes de la puesta en servicio, es crucial mantener el sistema de IA dentro del entorno de investigación. Se deben documentar todas las actividades de investigación y asegurarse de cumplir con las normas éticas y de integridad científica. Además, es importante garantizar que el uso del sistema no implique condiciones reales o comerciales.

En la preparación para la puesta en servicio, se debe realizar una evaluación de riesgos del sistema de IA. También es necesario desarrollar la documentación técnica requerida y establecer mecanismos de supervisión humana y transparencia. En última instancia, el sistema debe pasar por el proceso de evaluación de conformidad requerido por el reglamento (definición 20 del artículo 3 RIA).

Por otro lado, la relación entre la puesta en servicio y las **pruebas en condiciones reales** es fundamental en el contexto de proyectos de investigación que desarrollan sistemas de inteligencia artificial. Es crucial entender cómo el RIA maneja esta transición para asegurarse de que el cumplimiento normativo se mantenga durante todas las fases del proyecto. Las pruebas en condiciones reales implican evaluar y verificar el desempeño del sistema de IA en un entorno que simula su uso final, pero dentro del contexto de investigación. El reglamento permite ciertas pruebas en condiciones reales siempre que estas pruebas sean parte del proceso de investigación científica y no impliquen una comercialización o un uso prolongado como producto final. El objetivo es validar la funcionalidad, seguridad y efectividad del sistema antes de su despliegue final.

La puesta en servicio se refiere al uso del sistema de IA en condiciones reales para su propósito final, fuera del entorno controlado de investigación, lo que incluye cualquier forma de comercialización o uso práctico continuo. Una vez que se pone en servicio, el sistema de IA debe cumplir plenamente con el Reglamento, incluyendo evaluaciones de conformidad, transparencia y supervisión humana.

Es fundamental mantener una documentación exhaustiva sobre las pruebas, incluyendo objetivos, metodologías y resultados y asegurar que estas pruebas se realicen bajo supervisión ética y con consentimiento informado si involucran sujetos humanos (a este respecto el propio RIA deriva a la aplicación normativa del RGPD). Las pruebas deben ser seguras y que cualquier riesgo esté controlado limitando la duración y el alcance de estas para que permanezcan claramente dentro del contexto de investigación y no se consideren puesta en servicio.

En el caso de que consideremos una puesta en servicio, la preparación para la misma debe establecer realizar una evaluación exhaustiva para garantizar que el sistema cumpla con todos los requisitos del reglamento antes de su despliegue final. A este respecto, debe ser fundamental que se complete toda la documentación técnica necesaria, detallando los aspectos de diseño, desarrollo, pruebas y resultados. Hay que asegurar que todos los aspectos del sistema sean transparentes y estén bien documentados para los usuarios finales y autoridades reguladoras y establecer canales claros para la retroalimentación y mejora continua del sistema.

Documentación, cumplimiento normativo y certificaciones.

El Reglamento europeo de inteligencia artificial debe cumplirse en el momento en que el sistema de IA desarrollado en el marco de un proyecto de investigación se destine a fines comerciales o se ponga a disposición del público. En este caso, aunque el Reglamento (UE) 2024/1689 excluye a los sistemas de inteligencia artificial utilizados exclusivamente para actividades de investigación científica de su aplicación, es importante gestionar estos sistemas de manera responsable y ética y considerar una serie de obligaciones y recomendaciones que indicamos a continuación:

- Obtener la aprobación de los comités de ética correspondientes si la investigación implica el uso de datos sensibles o el potencial impacto en sujetos humanos.

- Cumplir con las normativas de protección de datos, como el Reglamento General de Protección de Datos (RGPD) de la UE. Siempre que sea posible, anonimizar los datos y almacenarlos de manera segura. Según el proyecto, deberemos considerar obtener el consentimiento informado debidamente explicado y cumplimentado.
- Designar a responsables de la supervisión del uso de la IA en el proyecto. Estas personas deben tener la competencia, formación y autoridad necesarias para gestionar los sistemas de IA de manera adecuada.
- Implementar un sistema de monitoreo continuo para detectar y corregir cualquier uso indebido o impacto negativo de los sistemas de IA.
- Mantener una documentación detallada del desarrollo y uso del sistema de IA. Esto incluye los datos de entrenamiento, los algoritmos utilizados, y los resultados obtenidos. Es igualmente importante documentar claramente los objetivos de la investigación y los métodos empleados para asegurar la reproducibilidad y la transparencia.
- Considerar y documentar un análisis de riesgos éticos, técnicos y de sesgo en los datos, así como implementar las medidas para mitigar estos riesgos y asegurarse de que los resultados de la investigación no se utilicen para fines no previstos. Así como una evaluación de impacto en privacidad y/o en derechos fundamentales si fuese necesario.
- Plan de pruebas en condiciones reales.
- Plan de Transición a Puesta en Servicio o Uso Comercial (evaluación de conformidad) sólo según el avance del proyecto.

SISTEMAS DE IA PROHIBIDOS

Introducción

El Reglamento, en su artículo 5, establece una lista de IA prohibidas que abarca todos los sistemas de IA cuyo uso se considera inaceptable por ser contrario a los valores de la Unión, por ejemplo, porque violan derechos fundamentales.

Las prohibiciones engloban aquellas prácticas que tienen un gran potencial para manipular a las personas mediante técnicas subliminales que trasciendan su consciencia o que aprovechan las vulnerabilidades de grupos vulnerables concretos, como los menores o las personas con discapacidad, para alterar de manera sustancial su comportamiento de un modo que es probable que les provoque perjuicios físicos o psicológicos a ellos o a otras personas.

Prácticas prohibidas

Introducción en el mercado, puesta en servicio o la utilización de un sistema de IA.

Manipulación. (Art.5.1.a)).
Técnicas subliminales, técnicas deliberadamente manipuladoras o engañosas, que alteren de forma sustancial el comportamiento de una persona o grupo de personas y que afecten a su capacidad de toma de decisiones, provocando (o pudiendo provocar) a dicha persona o grupo de personas perjuicios considerables.

Personas vulnerables. (Art.5.1.b)).
Explotación de vulnerabilidades de una persona o grupo específico de personas derivadas de:
- su edad o discapacidad,
- su situación social o económica especifica

Con el objetivo o el efecto de alterar de manera sustancial el comportamiento de dichas personas, provocándoles o, pudiendo razonablemente provocar, unos perjuicios considerables a esa persona, o a otra.

Evaluación o clasificación de personas. (Art.5.1.c)).
Esta práctica prohíbe la evaluación o clasificación de personas o grupo de personas durante un periodo determinado de tiempo, atendiendo a su comportamiento social o a características personales o en su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante, que provoque un trato perjudicial hacia determinadas personas físicas o grupos de personas:
- en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;
- que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este.

Introducción en el mercado, la puesta en servicio para un fin específico, o el uso de un sistema de IA

Realización de evaluaciones de riesgo de personas físicas, con el fin de evaluar o predecir la probabilidad de que una persona física cometa una infracción penal. (Art.5.1.d)).
Esta evaluación o predicción se basa únicamente en la elaboración del perfil de una persona física, de sus rasgos o características de su personalidad.

Excepción: Esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la evaluación humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva

Extracción no selectiva de imágenes. (Art.5.1.e)).
Creación o ampliación bases de datos de reconocimiento facial, mediante la extracción no selectiva de imágenes faciales de internet, o de circuitos cerrados de televisión.

Inferencia en emociones de personas físicas en los lugares de trabajo y centros educativos. (Art.5.1.f)).
Excepción: cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad, no aplicará esta prohibición.

Introducción en el mercado, la puesta en servicio para un fin específico, o el uso de un sistema de categorización biométrica

Clasificación individual de personas. (Art.5.1.g)).
Sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual (datos especialmente sensibles).

Excepción: esta prohibición no abarca el etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la aplicación de la ley.

Uso de sistemas de identificación biométrica remota

Identificación biométrica en tiempo real. (Art.5.1.h)).
Uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley.

Excepción: esta prohibición no aplica en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

- Búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas;

- la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista;
- la localización o identificación de una persona sospechosa de haber cometido una infracción penal a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

El párrafo primero, letra h), se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 en lo que respecta al tratamiento de datos biométricos con fines distintos de la aplicación de la ley.

El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público conforme a los objetivos establecidos (5.1.h)

Únicamente para confirmar la identidad de la persona que constituya el objetivo específico y tendrá en cuenta los siguientes aspectos: (Art.5.2).

- la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema.
- las consecuencias que tendría el uso del sistema en los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias

REQUIERE el uso del sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público solo se autorizará si la autoridad garante del cumplimiento del Derecho ha completado una evaluación de impacto relativa a los derechos fundamentales según lo dispuesto en el artículo 27 y ha registrado el sistema en la base de datos de la UE de conformidad con el artículo 49. No obstante, en casos de urgencia debidamente justificados, se podrá empezar a utilizar tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se complete sin demora indebida

Uso de sistemas de identificación biométrica remota: requerimiento de autorización

Requerimiento de autorización por autoridad competente para usos de identificación biométrica remota en tiempo real. (Art.5.3 y 5.4).

El Reglamento prevé que, a los efectos del apartado 1, párrafo primero, letra h), y apartado 2, todo uso de sistema de identificación biométrica en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho estará supeditado a la concesión de una autorización por la autoridad judicial o administrativa independiente, cuya decisión sea vinculante del Estado miembro en que vaya a utilizarse dicho sistema. La autorización se expedirá previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5 del artículo 5 del Reglamento.

Proporcionalidad de la regla**.** La autorización únicamente se concederá cuando la autoridad competente tenga constancia, sobre la base de pruebas objetivas o de indicios claros que se le

aporten, de que el uso del sistema de identificación biométrica remota en tiempo real es necesario y proporcionado para alcanzar alguno de los objetivos especificados en el apartado 1, párrafo primero, letra h), el cual se indicará en la solicitud, y, en particular, se limita a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal.

En todo caso, al pronunciarse, la autoridad deberá tener en cuenta los aspectos mencionados en el apartado 2, y no se podrá adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota en tiempo real.

Excepción: en una situación de urgencia debidamente justificada, se podrá empezar a utilizar tal sistema sin autorización siempre que se solicite dicha autorización sin demora indebida, a más tardar en un plazo de 24 horas. Si se rechaza dicha autorización, el uso se interrumpirá con efecto inmediato y todos los datos, así como los resultados y la información de salida generados por dicho uso, se desecharán y suprimirán inmediatamente.

Notificación del uso. (Art.5.4). No obstante, lo anterior, sin perjuicio de lo dispuesto en el apartado 3, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho se notificará a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos de conformidad con las normas nacionales a que se refiere el apartado 5. La notificación contendrá, como mínimo, la información especificada en el apartado 6 y no incluirá datos operativos sensibles.

Los ***Estados miembros*** podrán/deberán:

- decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho dentro de los límites y en las condiciones que se indican en el apartado 1, párrafo primero, letra h), y los apartados 2 y 3.
- establecer en sus respectivos Derechos nacionales las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones a que se refiere el apartado 3, así como a la supervisión y la presentación de informes relacionadas con estas. Dichas normas especificarán también para qué objetivos de los enumerados en el apartado 1, párrafo primero, letra h), y en su caso en relación con qué delitos de los indicados en la letra h), inciso iii), se podrá autorizar a las autoridades competentes para que utilicen esos sistemas con fines de garantía del cumplimiento del Derecho. Los Estados miembros notificarán dichas normas a la Comisión a más tardar treinta días después de su adopción.
- adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota.

Las **autoridades nacionales de vigilancia del mercado** y las **autoridades nacionales de protección de datos de los Estados miembros** a las que se haya notificado el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho con arreglo al apartado 4 presentarán a la Comisión

informes anuales sobre dicho uso. (Siguiendo el modelo que facilite la Comisión que incluirá información sobre el número de decisiones adoptadas y su resultado) (Art.5.6).

La **Comisión** publicará **informes anuales sobre el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público** con fines de garantía del cumplimiento del Derecho elaborados basados en datos agregados relativos a los Estados miembros sobre la base de los informes anuales a que se refiere el apartado 6. Dichos informes anuales no incluirán datos operativos sensibles de las actividades de garantía del cumplimiento del Derecho conexas. (Art.5.7).

El presente artículo no afectará a las prohibiciones aplicables cuando una práctica de IA infrinja otras disposiciones de Derecho de la Unión. (Art.5.8).

SISTEMAS DE IA DE ALTO RIESGO

Introducción

Un sistema de IA, tal y como se establece en el artículo 6 del RIA, ***con independencia de si se ha introducido en el mercado o no***, será considerado de alto riesgo:

I. **Por su finalidad vía Anexo III (6.2):** Los sistemas recogidos en este anexo son considerados de alto riesgo porque la Comisión así lo ha decidido en base a su finalidad. De entre ellos hay 3 sistemas relacionados con el ámbito de la salud:
   - Acceso a seguros de salud y vida
   - Triaje de pacientes para la asistencia en emergencias
   - Acceso a servicios sanitarios públicos

   Excepción: Un sistema de IA 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 de las personas físicas, en particular al no influir sustancialmente en el resultado de la toma de decisiones. Igualmente, siempre se considerará de alto riesgo cuando el sistema de IA efectúe la elaboración de perfiles de personas físicas.

II. **Por su regulación sectorial vía Anexo I (6.1):** Igualmente se considerarán de alto riesgo los sistemas de IA que se encuentren en el ámbito de aplicación de las regulaciones recogidas en el Anexo I y, además, deban someterse a una evaluación de conformidad de terceros para su introducción en el mercado.

La UE dado que ya regula productos y sistemas informáticos que clasifica como alto riesgo, ha decidido vincular todas esas legislaciones con el RIA. En consecuencia, todos aquellos productos que ya son clasificados como de alto riesgo en su legislación sectorial, si además incorporan IA, lo considerará tanto producto de alto riesgo como sistema de IA de alto riesgo.

En el ámbito salud, esto afectaría a:

- Productos sanitarios (MDR): Los **programas informáticos** conforme a lo dispuesto en el art. 2 MDR, son considerados como **productos sanitarios**. Igualmente, según la regla 11 del Anexo VIII MDR los programas informáticos con un fin médico específico son clase IIA (o incluso clase III o clase IIB), y por lo tanto deben someterse a una evaluación de conformidad realizada por un organismo independiente para su introducción en el mercado. En consecuencia, los programas informáticos clase IIA o superior, se consideran **productos sanitarios de alto riesgo**. Así, y siempre que estos mismos programas sean una IA a ojos del RIA, se les podrá considerar también como sistemas de IA de alto riesgo (regulados en el MDR + evaluación de conformidad de terceros).
- Productos In Vitro (IVDR)

SISTEMAS IA ALTO RIESGO	**ART.6.1**	Productos Sanitarios(MDR)
		ProductosIn Vitro(IVDR)
	ART.6.2 – ANEXO III	Acceso a seguros de salud y vida
		Triaje de pacientes para la asistencia en emergencias
		Acceso a servicios sanitarios públicos

Obligaciones

El RIA establece una serie de obligaciones para estas modalidades de IA en los artículos 9 a 15.

- Establecer, implantar, documentar y mantener un ***sistema de gestión de riesgos*** durante todo el ciclo de vida de un sistema de IA de alto riesgo.
- Obligaciones sobre ***datos y gobernanza de datos*** destinadas a mantener criterios de calidad en el entrenamiento, validación y prueba de los sistemas.
- Obligaciones de ***documentación técnica*** que permitan la demostración del cumplimiento normativo (Anexo IV).
- Obligaciones de ***registro automatizado*** para garantizar la trazabilidad del funcionamiento del sistema a lo largo de todo el ciclo vital del sistema.
- Obligaciones de ***transparencia y comunicación*** de información a los usuarios para garantizar un uso correcto de la información de salida en el uso y despliegue de los sistemas.
- Obligaciones de ***supervisión humana*** para garantizar que los sistemas sean diseñados y desarrollados de forma que puedan ser supervisados de manera efectiva por personas físicas.
- Obligaciones relativas a alcanzar un nivel adecuado de ***precisión, solidez y ciberseguridad*** y funcionen de manera consistente durante todo su ciclo de vida.

Unas obligaciones que vienen a completar las que ya se exigían a los **MDR/IVDR,** en su propia regulación, tales como:

- Evaluación de conformidad supervisada por organismo notificado para obtener CE.
- Demostración de la conformidad con los requisitos generales de seguridad y funcionamiento.
- Evaluación clínica debidamente documentada.

Obligaciones proveedores y responsables del despliegue

Evaluación de la conformidad (43 RIA): El proceso por el que se demuestra si se cumplen los requisitos establecidos en el título III, capítulo 2, del presente Reglamento en relación con un sistema de IA. Recae por lo general sobre el proveedor, esto es, quien desarrolla un sistema para ponerlo en el mercado. Dos vías:

- Procedimiento de autoevaluación **para sistemas de IA de alto riesgo por la finalidad prevista** (Anexo III RIA) (salvo identificación biométrica).
- Procedimiento para **sistemas de IA que son productos conforme a legislación UE** (Anexo I RIA) y se someten a evaluación por organismo notificado conforme a la misma.

Evaluación de impacto relativa a DDFF (27 RIA): Antes de desplegar uno de los sistemas de IA de alto riesgo establecidos en el Art. 6.2 (Anexo III, excepto Anexo III.2. Sobre infraestructuras críticas), los responsables del despliegue que sean organismo de Derecho Público, o entidades privadas que prestan servicios públicos, o entidades responsables de sistemas para evaluar solvencia o seguros, llevarán a cabo una evaluación del impacto que la utilización de dichos sistemas puede tener en los DDFF.

Otras:

- Cumplimientos y demostración de la conformidad del sistema con los requisitos establecidos en la Sección 2, y los requisitos de accesibilidad (Directivas UE 2016/2102 y UE 2019/882).
- Identificación: nombre, nombre comercial registrado o marca registrada y dirección de contacto.
- Contar con un sistema de gestión de calidad (art. 17).
- Conservación de la documentación técnica hasta 10 años desde la introducción en el mercado o puesta en servicio (art. 18).
- Conservación de los archivos de registro generados automáticamente por un mínimo de 6 meses (art. 19).
- Elaboración de una declaración UE de conformidad ((art. 47).
- Colocación del marcado CE en el sistema de IA (art. 48)
- Obligaciones de registro (art. 49).
- Adopción de medidas correctoras (art. 20).

SISTEMAS DE IA DE USO GENERAL

Introducción

Un **sistema de IA de uso general** es un sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA. (Art.3.66 RIA)

Es importante remarcar la diferencia entre lo que sería un modelo de **modelo** de IA de uso general, y un de **sistema** de IA de uso general.

Los modelos de IA de uso general son componentes de un sistema de IA de uso general, pero no son el sistema en completo, ya que el sistema incluye otros componentes, como por ejemplo una interfaz de usuario, entre otros.

En este sentido, y según el considerando 97 del Reglamento, cuando un modelo de IA de uso general esté integrado en un sistema de IA o forme parte de él, este sistema debe considerarse un sistema de IA de uso general cuando, debido a esta integración, el sistema tenga la capacidad de servir a diversos fines. Un sistema de IA de uso general puede utilizarse directamente e integrarse en otros sistemas de IA.

En el RIA se indica que un ***modelo de IA de uso general*** es 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. (Art.63 RIA)

En este apartado también recobra especial importancia la definición de riesgo sistémico, ya que habrá obligaciones concretas que aplicarán a aquellos modelos de IA de uso general con riesgo sistémico. En este sentido, esta definición se encuentra en el artículo 3, apartado 65, cuando se indica que es “un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor”.

En el Capítulo V del Reglamento, su artículo 51, también establece cuando ***un modelo de IA de uso general tiene riesgo sistémico***. Concretamente, si reúne alguna de las siguientes” condiciones:

- tiene capacidades de gran impacto evaluadas a partir de herramientas y metodologías técnicas adecuadas, como indicadores y parámetros de referencia;

- con arreglo a una decisión de la Comisión, adoptada de oficio o a raíz de una alerta cualificada del grupo de expertos científicos, tiene capacidades o un impacto equivalente a los establecidos en la letra a), teniendo en cuenta los criterios establecidos en el anexo XIII.

Se presumirá que un modelo de IA de uso general tiene capacidades de gran impacto con arreglo al apartado 1, letra a), cuando la cantidad acumulada de cálculo utilizada para su entrenamiento, medida en operaciones de coma flotante, sea superior a 102"

En lo que respecta a **Sistemas de IA Generativa,** pese a la importancia que están ostentando en la actualidad los sistemas de IA generativa, **la única referencia que hace el RIA respecto a éstos es equipararlos a un sistema de IA de uso general**, cuando en su considerando 99 indica que los grandes modelos de IA generativa son un ejemplo típico de un modelo de IA de uso general, ya que permiten la generación flexible de contenidos, por ejemplo, en formato de texto, audio, imágenes o vídeo, que pueden adaptarse fácilmente a una amplia gama de tareas diferenciadas.

Por lo tanto, **todas las previsiones que se describen a continuación referentes a los sistemas de IA de uso general, se aplicarán a todos aquellos sistemas de IA Generativa.**

Gobernanza

Para asegurar una adecuada aplicación del Reglamento, se establecen varios órganos de gobierno:

- Una **Oficina de IA** dentro de la Comisión para hacer cumplir las reglas comunes en toda la UE. Esta Oficina, junto con los Estados miembros, serán los encargados de fomentar y facilitar la elaboración de códigos de buenas prácticas y directrices a escala de la UE.

- Un **panel científico de expertos independientes (de cualquier proveedor de sistemas de IA o de modelos de uso general)** para apoyar las actividades de aplicación, en particular las actividades de supervisión de la Oficina de IA en lo que respecta a los modelos de IA de uso general, en particular:
  - alertando a la Oficina de IA de los posibles riesgos sistémicos a escala de la Unión de modelos de IA de uso general, de conformidad con el artículo 90,
  - contribuyendo al desarrollo de herramientas y metodologías para evaluar las capacidades de los sistemas y modelos de IA de uso general, también a través de parámetros de referencia,
  - asesorando sobre la clasificación de modelos de IA de uso general con riesgo sistémico,
  - asesorando sobre la clasificación de diversos sistemas y modelos de IA de uso general,
  - contribuyendo al desarrollo de herramientas y modelos.

- Un **Consejo Europeo de IA con representantes de los estados miembros.** 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. Sus funciones son asesorar y asistir a la Comisión y a los estados miembros en la aplicación coherente y efectiva del Reglamento de IA.

- Un **foro consultivo** para partes interesadas (industria, empresas emergentes, pymes, sociedad civil y el mundo académico) para **proporcionar experiencia técnica** al Consejo de IA y a la Comisión.

La supervisión y gobernanza del reglamento se distribuye entre la Comisión Europea y las autoridades nacionales de los Estados miembros:

- **A nivel nacional**: Cada Estado miembro debe establecer una autoridad notificante y una autoridad de vigilancia del mercado responsable de la aplicación del reglamento a nivel nacional. 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.
- **A nivel europeo**: La Oficina de IA de la UE, establecida por la Comisión Europea, supervisará los modelos de IA de uso general y coordinará con las autoridades nacionales
- **Sandboxes regulatorios**: Los Estados miembros deben establecer sandboxes regulatorios para facilitar la innovación y el cumplimiento del reglamento por parte de las empresas.

Es necesario aclarar las responsabilidades y competencias a escala nacional y de la Unión en lo que respecta a los sistemas de IA que se basan en modelos de IA de uso general.

Para evitar el solapamiento de competencias, cuando un sistema de IA se base en un modelo de IA de uso general y el modelo y el sistema sean suministrados por **el mismo proveedor**, la supervisión debe llevarse a cabo a **escala de la Unión a través de la Oficina de IA,** que debe tener a estos efectos las facultades de una autoridad de vigilancia del mercado en el sentido de lo dispuesto en el Reglamento (UE) 2019/1020. En todos los **demás casos**, serán responsables de la supervisión de los sistemas de IA las **autoridades nacionales de vigilancia del mercado**. No obstante, en el caso de los sistemas de IA de uso general que puedan ser utilizados directamente por los responsables del despliegue con al menos un fin clasificado como de alto riesgo, las autoridades de vigilancia del mercado deben cooperar con la Oficina de IA para llevar a cabo evaluaciones de la conformidad e informar de ello al Comité y a otras autoridades de vigilancia del mercado. Además, las autoridades de vigilancia del mercado deben poder solicitar la asistencia de la Oficina de IA cuando la autoridad de vigilancia del mercado no pueda concluir una investigación sobre un sistema de IA de alto riesgo debido a su incapacidad para acceder a determinada información relacionada con el modelo de IA de uso general en el que se basa el sistema de IA de alto riesgo. En tales casos, debe aplicarse mutatis mutandis el procedimiento de asistencia mutua transfronteriza previsto en el capítulo VI del Reglamento (UE) 2019/1020. (Art.75 RIA).

Para aprovechar al máximo la centralización de conocimientos especializados y las sinergias que se generan a escala de la Unión, la **Comisión tiene atribuidas las competencias de supervisión y de control del cumplimiento de las obligaciones de los proveedores de modelos de IA de uso**

general. La Comisión debe confiar la ejecución de estas tareas a la Oficina de IA, sin perjuicio de las competencias de organización de la Comisión y del reparto de competencias entre los Estados miembros y la Unión en virtud de los Tratados. **La Oficina de IA** llevará a cabo todas las acciones necesarias para **supervisar la aplicación efectiva del Reglamento en lo que respecta a los modelos de IA de uso general**. Pudiendo investigar posibles infracciones de las normas relativas a los proveedores de modelos de IA de uso general, tanto por iniciativa propia, a raíz de los resultados de sus actividades de supervisión, como a petición de las autoridades de vigilancia del mercado. Para promover la eficacia de la supervisión, la Oficina de IA debe prever la posibilidad de que los proveedores posteriores presenten reclamaciones sobre posibles infracciones de las normas relativas a los proveedores de sistemas de IA de uso general.

Por otro lado, La Oficina de IA **podrá invitar a todos los proveedores de modelos de IA de uso general a adherirse a los códigos de buenas prácticas**.

Con el fin de complementar los sistemas de gobernanza de los modelos de IA de uso general, **el grupo de expertos científicos** debe *contribuir a las actividades de supervisión de la Oficina de IA* y, en determinados casos, puede proporcionar *alertas cualificadas a la Oficina de IA* que activen actuaciones consecutivas, como investigaciones. Por ejemplo, que se tenga motivos para sospechar que un modelo de IA de uso general presenta un riesgo concreto e identificable a escala de la Unión. También debe ser este el caso cuando el grupo de expertos científicos tenga motivos para sospechar que un modelo de IA de uso general cumple los criterios que llevarían a clasificarlo como modelo de IA de uso general con riesgo sistémico.

En la realización de las evaluaciones, para poder contar con conocimientos especializados independientes, **la Oficina de IA** debe poder recurrir a e**xpertos independientes para que lleven a cabo las evaluaciones en su nombre**. Se debe poder exigir el cumplimiento de las obligaciones mediante, entre otras cosas, solicitudes de adopción de medidas adecuadas, entre las que se incluyen medidas de reducción del riesgo en caso de que se detecten riesgos sistémicos, así como la restricción de la comercialización, la retirada o la recuperación del modelo. Como salvaguardia, cuando sea necesario, además de los derechos procedimentales previstos en el RIA, los proveedores de modelos de IA de uso general deben tener los derechos procedimentales previstos en el artículo 18 del Reglamento (UE) 2019/1020, que deben aplicarse mutatis mutandis, sin perjuicio de los derechos procesales más específicos previstos en el Reglamento de IA.

Obligaciones para los proveedores de sistemas de IA de uso general

En este apartado se incluyen aquellas obligaciones establecidas en el reglamento para los proveedores de los sistemas y modelos de uso general:

Obligaciones de transparencia: (Art. 50) Cuando generen contenido sintético de audio, imagen, vídeo o texto, velarán por que los resultados de salida del sistema de IA estén marcados en un formato legible por máquina y que sea posible detectar que han sido generados o manipulados de manera artificial. Los proveedores velarán por que sus soluciones técnicas sean eficaces, interoperables, sólidas y fiables en la medida en que sea técnicamente viable, teniendo en

cuenta las particularidades y limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual de la técnica generalmente reconocido, según se refleje en las normas técnicas pertinentes

Si es un modelo de IA de uso general con riesgo sistémico, el proveedor deberá cumplir con las siguientes obligaciones relacionadas al **Procedimiento** a seguir (Art. 52): lo notificará a la Comisión sin demora y, en cualquier caso, antes de transcurridas dos semanas desde que se cumpla dicho requisito o desde que se sepa que va a cumplirse. Dicha notificación incluirá la información necesaria para demostrar que se cumple el requisito pertinente. Aun cuando el proveedor puede exponer argumentos a la Comisión para demostrar que el modelo no presenta este riesgo, finalmente será decisión de la Comisión calificar este modelo respecto a estas características, incluso el proveedor incumpla este deber de notificación.

Supervisión

La Comisión podrá imponer multas a los proveedores de modelos de IA de uso general que no superen el **3 % de su volumen de negocios** mundial total anual correspondiente al ejercicio financiero anterior o de **15 000 000 EUR**, si esta cifra es superior, cuando la Comisión considere que, de forma deliberada o por negligencia:

- infringieron las disposiciones pertinentes del Reglamento;
- no atendieron una solicitud de información o documentos con arreglo al artículo 91, o han facilitado información inexacta, incompleta o engañosa;
- incumplieron una medida solicitada en virtud del artículo 93;
- no dieron acceso a la Comisión al modelo de IA de uso general o al modelo de IA de uso general con riesgo sistémico para que se lleve a cabo una evaluación con arreglo al artículo 92.

Al fijar el importe de la multa o de la multa coercitiva, se tomarán en consideración la naturaleza, gravedad y duración de la infracción, teniendo debidamente en cuenta los principios de proporcionalidad y adecuación. La Comisión también tendrá en cuenta los compromisos contraídos por el proveedor del modelo de IA de uso general con riesgo sistémico para hacer frente al riesgo a escala de la Unión., y en los códigos de buenas prácticas pertinentes.

Las multas serán efectivas, proporcionadas y disuasorias.

CONCLUSIONES

El nuevo reglamento de inteligencia artificial establece prácticas prohibidas para evitar el uso indebido de la tecnología, cuyas prácticas incluyen la manipulación, explotación y control social que son altamente perjudiciales y contrarias a los principios de dignidad humana, libertad, igualdad, democracia, Estado de Derecho y derechos fundamentales reconocidos por la UE, como la no discriminación, la protección de datos, la privacidad. El objetivo es asegurar que la IA se utilice de manera ética y responsable, evitando impactos negativos en la sociedad y protegiendo los derechos de las personas.

Las evaluaciones de impacto en los DDFF no se deben desarrollar ante cualquier IA de Alto Riesgo. Sólo se deben realizar cuando se cumplan los requisitos establecidos en el artículo 27 del RIA.

Al valorar si se dan las excepciones para investigación contempladas en el artículo 2 del RIA, no debemos obviar que, no serán de aplicación, cuando en el desarrollo de una investigación se den las circunstancias establecidas en el artículo 6 (con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b), un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican en el apartado 1.a y 1.b del artículo) o el artículo 60 (pruebas en condiciones reales fuera de los espacios controlados de pruebas para la IA).

El RIA equipara los **Sistemas de IA Generativa** a los **Sistemas de IA de uso general**, y no los regula específicamente.