ZABIA
ABOGADOS

REGLAMENTO QUE REGULA LA INTELIGENCIA ARTIFICIAL: ASPECTOS CLAVE

El Reglamento de Inteligencia Artificial tiene como objetivo fundamental garantizar que los sistemas de IA que se utilicen en la Unión Europea cumplan con los requisitos de seguridad y que respeten los derechos fundamentales de los ciudadanos y los valores de la Unión. Al mismo tiempo, busca incentivar la inversión y la innovación en proyectos de inteligencia artificial dentro de la UE, garantizando la seguridad jurídica. Se trata, además, de la primera propuesta legislativa sobre IA a nivel internacional, lo que puede convertirla en un marco de referencia para otros legisladores.

Debe destacarse que el Reglamento no se aplicará fuera del ámbito de aplicación del Derecho de la UE. Tampoco afectará a las competencias de los Estados miembros en materias como la seguridad nacional. No se aplicará tampoco a sistemas utilizados exclusivamente con fines militares o de defensa o a los empleados con fines de innovación e investigación. Además, es importante subrayar que, en materia de protección de datos personales, deberá tenerse en cuenta la legislación ya existente, que deberá ser respetada por cualquier proyecto de IA. El ámbito de aplicación esencial del Reglamento son los proveedores de sistemas IA que pongan en servicio o vendan su producto dentro de la UE, sin importar su origen; y los usuarios de estos sistemas, siendo considerados tales quienes los explotan y no quienes se ven afectados por ellos (los ciudadanos, destinatarios finales).

Para distinguirlo de otras tecnologías de software de naturaleza más sencilla, es útil recoger aquí la definición que se hace del propio **concepto de Sistema de Inteligencia Artificial**:

> *"un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, 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 información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales".*

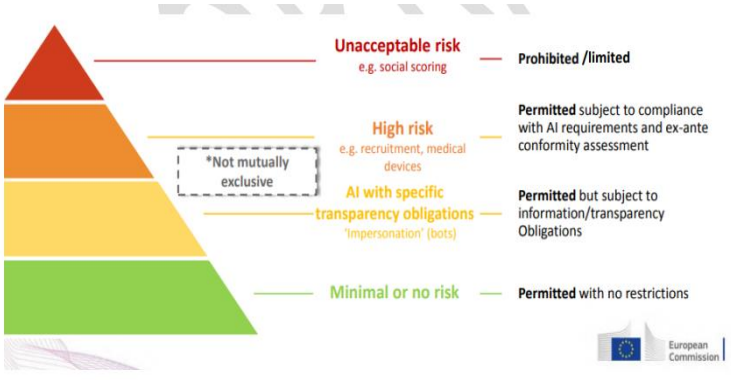
El propio Reglamento establece en su artículo 3 definiciones de conceptos vinculados a la creación, despliegue, funcionamiento y uso de la IA. Distingue, así, entre proveedores, responsables de despliegue, representantes autorizados, distribuidores, operadores, importadores... A su vez, incluye numerosos conceptos vinculados a la vida de un sistema de IA que ayudan a comprender debidamente las distintas características que lo componen, la gran variedad de funciones que puede llegar a desarrollar y las consecuencias que puede llegar a tener un uso erróneo de este tipo de tecnología. A

modo de ejemplo, también por ser protagonista principal en este reglamento, se define el **proveedor**:

> *"una persona física o jurídica o autoridad, órgano u organismo de otra índole públicos 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 comercial, previo pago o gratuitamente"*

Se define asimismo la identificación biométrica como *"el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos"* o la ultrafalsificación (*deepfake*) como *"un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares u otras entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos"*.

Mencionadas estas **definiciones (Capítulo I),** el aspecto fundamental de este Reglamento es el establecimiento de una **escala o pirámide de riesgos**, los cuales van desde el riesgo inaceptable hasta el riesgo mínimo o inexistente. El riesgo inaceptable determina la prohibición de la tecnología que lo explote; mientras que las actividades con riesgo escaso o nulo son permitidas sin restricciones. Entre ambos extremos aparecen los sistemas de alto riesgo y los de riesgo limitado, que se analizarán a continuación.



Fuente: Ministerio de Asuntos Económicos y Transformación Digital

El **Capítulo II** se dedica a las **actividades de IA prohibidas**, por implicar, como se ha indiciado, un riesgo inaceptable. Se exponen de manera sintética dichas actividades:

1- Aquellas consistentes en el despliegue y uso deliberado de técnicas subliminales o de aquellas consistentes en la manipulación o el engaño que tienen como objetivo la distorsión del comportamiento y el perjuicio en la toma consciente de decisiones, provocando con ello un daño considerable.

2- Aquellas consistentes en la explotación de las vulnerabilidades vinculadas a la edad, la discapacidad o las condiciones económicas, de manera que se provoque una distorsión del comportamiento y se causen daños considerables.

3- Aquellas que permitan la elaboración de una puntuación social, sirviendo para evaluar o clasificar a personas o grupos en base a comportamientos sociales o a rasgos personales conocidos o predecibles. El Reglamento, asimismo, exige que ello signifique un verdadero trato perjudicial que no se corresponda con la manera de actuar en la sociedad del afectado.

4- Aquellas que consistan en la categorización biométrica que clasifique individualmente a las personas sobre la base de sus datos biométricos para deducir su raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual… No entran en este supuesto el uso basado en conjuntos de datos biométricos que se hayan adquirido legalmente o cuando las fuerzas de seguridad categoricen datos biométricos.

5- Aquellas consistentes en su uso para la evaluación del riesgo de que un individuo cometa delitos, utilizando para ello perfiles rasgos de personalidad. Se exceptúa aquí el uso para el apoyo de las evaluaciones humanas basadas en hechos objetivos y verificables directamente relacionados con la actividad delictiva.

6- Aquellas consistentes en su uso para la compilación de bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de grabaciones de circuitos cerrados de televisión.

7- Aquellas consistentes en su uso para inferir o deducir emociones en centros de trabajo o en centros educativos. Se establece aquí la excepción en caso de razones médicas o de seguridad.

8- Aquellas consistentes en su uso para la identificación biométrica remota en tiempo real en espacios de acceso público por las fuerzas de seguridad, salvo que sean estrictamente necesarios para la búsqueda de personas desaparecidas, de víctimas de secuestros y de personas víctimas de la trata de seres humanos o de explotación sexual. También se permitirá para prevenir amenazas para la vida que se consideren inminentes, o para prevenir un ataque terrorista que se

considere previsible y para la identificación de sospechosos de delitos graves (asesinato, violación, crimen organizado, delitos contra el medio ambiente…) Debe puntualizarse que el uso de la identificación biométrica a distancia mediante IA solo se permite, incluso en estos supuestos, cuando no utilizarla provocaría un daño considerable. Deben ponderarse, además, los derechos y libertades de las personas que por este uso se vean afectadas. Las fuerzas de seguridad, para utilizarlo, deben realizar una evaluación del impacto sobre los derechos fundamentales y registrar el sistema en la base de datos de la Unión Europea. Además, dispone el reglamento que deberán obtener la correspondiente autorización judicial o administrativa. Estos últimos requisitos solo podrán posponerse en casos de urgencia.

Expuestas las prácticas prohibidas, el Reglamento continúa con los **sistemas de IA de alto riesgo (Capítulo III)**. Se consideran sistemas de IA de alto riesgo aquellos que se utilizan como componentes de seguridad o como productos ya cubiertos por la legislación europea armonizada. Ello implica que estarán sometidos a la evaluación de conformidad de terceros. Ejemplos de este tipo serían dispositivos médicos, aviones, maquinaria, ferrocarriles. En este tipo de sistemas de alto riesgo es importante consultar el **Anexo II** del Reglamento.

También se consideran de alto riesgo los que se encuentren entre los ámbitos que enumera el **Anexo III**, siempre que la salida sea relevante en una decisión con posible riesgo sobre la salud, la seguridad o los derechos fundamentales. No obstante, siempre se considerarán de alto riesgo los sistemas de IA del mentado anexo que realicen perfiles de personas, consistente en el tratamiento automatizado de datos personales cuyo objetivo sea analizar y evaluar aspectos de la vida de una persona: situación económica, laboral, preferencias, salud, ubicación, movimientos, etcétera.

⇆ Por **salida** se entiende la información que el sistema de IA es capaz de generar, tales como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales.

Los ámbitos que enumera el Anexo III son los siguientes:

1. Sistema de identificación biométrica cuando la legislación nacional o de la Unión permita su uso. Se trata, esencialmente, de los sistemas de identificación biométrica utilizados para identificar personas sin la llamada participación activa, siempre teniendo presente la prohibición ya expuesta para las fuerzas de seguridad. No se tienen en cuenta, por tanto, los sistemas de autenticación utilizados para confirmar que una persona es quien dice ser.

2. La gestión de infraestructuras críticas en que los sistemas de IA se utilicen como componentes de seguridad. Se citan las infraestructuras digitales críticas, el tráfico por carretera y el suministro de agua, gas, calefacción y electricidad.

3. La educación y formación profesional. Se citan por ejemplo sistemas de IA destinados a determinar el acceso o la admisión, aquellos destinados a evaluar el nivel adecuado de educación que va a recibir una persona o los utilizados para detectar comportamientos prohibidos de los estudiantes durante pruebas de evaluación.

4. Empleo, gestión de trabajadores y acceso al autoempleo. Aquí se trata de sistema de IA destinados a su uso en la contratación o selección de personas, como por ejemplo los que sirvan para analizar y filtrar solicitudes de empleo y evaluar candidatos. También aquellos sistemas de IA utilizados para tomar decisiones que afecten a las condiciones de las relaciones laborales, o a la promoción o finalización de las relaciones contractuales. Entre estos puede destacarse el riesgo que implican los sistemas de IA utilizados para supervisar y evaluar el rendimiento y el comportamiento.

5. Gestión del acceso de las personas a servicios esenciales públicos y privados. Aquí se citan sistemas de IA destinados a ser utilizados por las autoridades públicas (o terceros en su nombre) para evaluar el derecho de las personas físicas a prestaciones y servicios esenciales de asistencia pública (entre ellos, los de asistencia sanitaria). También aquellos destinados a evaluar la solvencia de personas o establecer una calificación crediticia (salvo los que tienen como objetivo evitar los fraudes financieros), los consistentes en clasificar llamadas de emergencia, establecer prioridades en primeras respuestas de emergencia (policía, bomberos, asistencia médica…), los utilizados para el triaje de pacientes de asistencia sanitaria de emergencia o aquellos que consisten en el apoyo para la evaluación de riesgos y la tarificación vinculada con personas en los seguros de vida y de enfermedad.

6. Sistemas de IA cuyo fin sea ser utilizados por autoridades policiales o judiciales, o por instituciones u órganos de la Unión, para clasificar el riesgo de que una persona sea víctima de delitos, analizar la fiabilidad de las pruebas en un proceso penal, discernir el riesgo de que una persona cometa un delito o reincida, examinar los rasgos de la personalidad y del comportamiento delictivo de personas o grupos; y elaborar perfiles en el curso de detecciones, investigaciones o enjuiciamientos de delitos.

7. Migración, asilo y control de fronteras, como por ejemplo en lo relativo a valoración de solicitudes. Se exponen sistemas destinados a ser usados por las por las autoridades o instituciones públicas como polígrafos; de evaluación de un riesgo (tales como la seguridad, la migración irregular o un riesgo sanitario); para asistir en la evaluación de las solicitudes de asilo, visado o permiso de residencia; y para la gestión de la migración, el asilo o el control de fronteras con el objetivo de identificar a personas.

8. Administración de justicia y procesos democráticos. Aquí se citan los sistemas de IA para el uso de autoridades judiciales en la investigación e interpretación de los hechos y en la valoración jurídica de los mismos; también para los utilizados con el objetivo de influir en el resultado de una elección o referéndum. Lo último no se aplicará a los sistemas de IA cuyos resultados no son conocidos por las personas. Ejemplo de ello son sistemas que ayuden a organizar y planificar campañas políticas administrativamente y desde la logística.

Tras exponer estos sistemas de alto riesgo, limitando a su vez la capacidad de la Comisión de poder añadir o eliminar sistemas de IA de estas categorías (condiciones muy concretas), aparecen los **requisitos que debe cumplir un proveedor de sistemas de IA** de este tipo. Se destacan los siguientes:

1. Elaborar y establecer un sistema de gestión de riesgos útil durante toda la duración del sistema de IA. Especialmente deberán indicarse los posibles riesgos sobre la salud, la seguridad o los derechos fundamentales de los ciudadanos de la Unión.

2. Garantizar que los datos manejados en la formación y prueba sean adecuados, representativos, completos y sin errores para poder cumplir con la finalidad prevista.

3. Elaborar y contar con documentación técnica actualizada que facilite a las autoridades la evaluación del cumplimiento de los requisitos exigidos.

4. Diseñar el sistema de IA de alto riesgo de manera que pueda registrar automáticamente eventos relevantes para identificar los riesgos a nivel nacional y las modificaciones sustanciales durante la vida del sistema.

5. Proporcionar instrucciones de uso a los encargados de la implantación posterior para permitir el cumplimiento de los requisitos por su parte.

6. Permitir la supervisión por parte de personas -intervención humana- del funcionamiento del sistema para que puedan reducir los riesgos a la salud, seguridad o derechos fundamentales.

7. Que el sistema se caracterice por la precisión, solidez y sea adecuado en términos de ciberseguridad. Se insiste en que estos sistemas, además, deberán ser diseñados de manera que funcionen con tolerancia a errores o inconsistencias a la hora de interactuar con su entorno. Las medidas relacionadas con la ciberseguridad deberán ser apropiadas en base a sus circunstancias, haciendo especial énfasis en evitar la manipulación de datos de entrenamiento (proceso de "formación" de un modelo IA).

Además de los proveedores y los requisitos solicitados en sistemas de IA de alto riesgo, se presentan **obligaciones para estos mismos proveedores** y también para **responsables del despliegue y otras partes**. Es importante señalar la definición de **responsable de despliegue** que incluye el reglamento: *"una persona física o jurídica o autoridad pública, órgano u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional".*

Entre las obligaciones, es comprensible que la mayor parte de ellas sean para los proveedores. Estos deben cumplir con los requisitos legales y superar las pruebas de conformidad; contar con un sistema de gestión de calidad con documentación técnica completa y mantenerlo durante toda la vida del sistema; custodiar los registros del sistema de IA que estén bajo su control; elaborar una declaración UE de conformidad; colaborar con las autoridades registrando el sistema, probando el cumplimiento de los requisitos cuando así se le solicite; notificando los incumplimientos y riesgos que detecten y qué tipo de acciones se han realizado para contrarrestarlos. Cada una de estas obligaciones aparece en artículos diferenciados, los cuales, completados con referencias a otros preceptos, contienen el desarrollo completo para su efectivo cumplimiento. Así, por ejemplo, cuando se habla de la **declaración UE de conformidad**, se remite al artículo 47, que establece que el proveedor demostrará en ella el cumplimiento de los requisitos antes mencionados para sistemas IA de alto riesgo; deberá conservarla durante 10 años y aportará una copia a las autoridades nacionales del Estado o Estados en que se introduzca el sistema. Se alude también a la **documentación técnica**, la cual habrá justificar que el sistema cumple los indicados requisitos y proporcionar a las autoridades competentes la información necesaria para evaluar la conformidad. A su vez, se especifica que deberá contener, como mínimo, los elementos del **Anexo IV**.

Por otro lado, los importadores y distribuidores, aunque en menor medida, también deben cumplir obligaciones. Es importante, de nuevo, remitirnos a la definición del Reglamento de estos conceptos: **Importador** es una *"persona física o jurídica ubicada o establecida en la Unión que introduce en el mercado un sistema de IA que tiene el nombre o la marca comercial de una persona física o jurídica establecida en un tercer país".* **Distribuidor** es una *"persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión".*

Estos actores tienen la obligación de mantener la documentación técnica, de cerciorarse de que los productos han superado la indicada prueba de conformidad, comprobar que dichos productos cumplen con los demás requisitos exigidos por el reglamento… Los importadores, además, deberán comprobar que el proveedor cuenta con representante autorizado en la UE.

En cuanto a los usuarios-responsables del despliegue, que, como ya se ha advertido, son las personas físicas o jurídicas que despliegan un sistema de IA a título profesional (y no, por ejemplo, los usuarios finales afectados), deben practicar labores de supervisión humana, monitorizar los sistemas, guardar registros, cooperar con las autoridades…

Especial mención debe hacerse de los llamados **Modelos-Sistemas de IA de uso general** (**GPAI: *General Purpose Artifical Intelligence***), presentes en el **Capítulo V** y definidos en el propio Reglamento:

> Los **sistemas de IA de uso general** son aquellos basados en un modelo de IA de uso general, definido como un modelo que, incluso *"entrenado con un gran volumen de datos utilizando la autosupervisión a gran escala, (…) 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".*

Sobre los GPAI es destacable que podrán utilizarse como sistemas de alto riesgo o integrarse en uno de ellos. Al darse esta posibilidad, los proveedores de este tipo de sistema cooperarán con los proveedores de los citados sistemas de IA de alto riesgo para garantizar el cumplimiento de los requisitos.

Entre las obligaciones de los proveedores de modelos GPAI, destacan la redacción de la documentación técnica, incluyendo el proceso de formación y ensayo y los resultados;

la elaboración de información y documentación para proporcionarla a los proveedores que tengan la intención de integrar el modelo GPAI en su propio sistema de IA, pues el objetivo es que sean capaces de comprender las limitaciones y el alcance de estos; respetar la Directiva sobre derechos de autor; y publicar un resumen con detalle suficiente sobre el contenido utilizado para el entrenamiento-formación del modelo GPAI Dicho esto, los modelos GPAI de "licencia libre y abierta", que se caracterizan por la disponibilidad de sus parámetros, de su arquitectura y de su uso, permitiendo el acceso, modificación y distribución como modelo, solo deben cumplir con los dos últimos: directiva de derechos de autor y resumen sobre contenido utilizado en el entrenamiento. No obstante, si estos modelos implican un riesgo sistémico deberán cumplir todos los requisitos.

El reglamento define el **riesgo sistémico** como 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".*

El reglamento establece que los modelos GPAI tendrán riesgo sistémico cuando se observe una capacidad de gran impacto evaluada a partir de herramientas y metodologías técnicas adecuadas, como indicadores y parámetros de referencia. Así, por ejemplo, se establece una presunción: el riesgo será sistémico cuando la cantidad acumulada de cálculo utilizada para su formación sea superior a 10 elevado a 25 operaciones en coma flotante (FLOP)[1]. El proveedor deberá notificar a la Comisión si su modelo cumple con el criterio en un plazo de dos semanas, si bien puede argumentar que, aunque se dé esa circunstancia, su modelo no genera un riesgo sistémico. También la propia Comisión, de oficio o en base a recomendaciones de un grupo de expertos científicos, si considera que el modelo tiene una capacidad de impacto equivalente a la indicada, podrá atribuir a un modelo de IA de uso general la condición de modelo con riesgo sistémico.

Junto a las obligaciones mencionadas, los proveedores de modelos GPAI deben, además, practicar la evaluación de modelos, incluyendo la realización y documentación de pruebas contradictorias que puedan servir para minorar o eliminar el riesgo sistémico; comprobar y mitigar los posibles riesgos sistémicos, incluidas las posibles fuentes de

[1] FLOP: En los sistemas informáticos, los números reales se representan utilizando un formato de coma flotante, que reserva un número finito de bits para representar la parte entera y la parte fraccionaria de un número. Esto presenta limitaciones, pues no todos los números pueden representarse con precisión finita. Esto lleva a errores de redondeo y pérdida de precisión al realizar operaciones, especialmente si ellas implican el uso de números muy pequeños o muy grandes.

éste; rastrear, documentar y notificar los incidentes graves y las medidas destinadas a su corrección a la Oficina de IA y las autoridades nacionales competentes; cumplir con un nivel adecuado de protección de la ciberseguridad...

El reglamento establece que los proveedores de este tipo de modelos de IA demostrarán el cumplimiento de sus obligaciones si se adhieren a algún **Código de Buenas Prácticas**. Dicho código deberá tener en cuenta los planteamientos internacionales y comprenderá las obligaciones antes indicadas (sin tener que limitarse a ellas). Se expone, además, que la Oficina de IA podrá invitar a participar en la elaboración de los códigos a proveedores de modelos de GPAI y a autoridades nacionales competentes.

Por debajo de los sistemas de IA de alto riesgo aparecen (**Capítulo IV**) **sistemas sometidos a ciertas obligaciones de transparencia** por parte de sus proveedores y responsables del despliegue. Aquí aparecen sistemas destinados a la interacción con personas o a la generación de contenido, que no necesariamente deben considerarse de alto riesgo, pero que puedan tener cierto riesgo al ser utilizados para posibles suplantaciones o engaños. Ello incluye, por tanto, las salidas de muchos sistemas de IA generadores. En la práctica, se pueden incluir entre este tipo de sistemas de riesgo limitado los sistemas del estilo de ChatGPT; sistemas de reconocimiento de emociones; ciertos sistemas de categorización biométrica; y sistemas generadores de contenido "Deepfake", en español ultrafalsificación (una técnica de inteligencia artificial que se utiliza para crear videos o imágenes falsos que parecen auténticos).

Las obligaciones en este tipo de **sistemas de riesgo limitado** son de transparencia. En contra de lo que sucede con los sistemas de alto riesgo, aquí el reglamento se focaliza en las salidas y en los usuarios finales: Cualquiera que interactúe con un sistema de IA de este tipo debe estar informado de ello; cualquier sujeto expuesto a sistemas de reconocimiento de emociones o de categorización biométrica que no estén prohibidos debe estar informado de su presencia; y deberá señalarse especialmente el material "deepfake" generado o manipulado por sistemas de IA.

En cuanto a los **sistemas de IA de riesgo mínimo o inexistente**, el Reglamento no se pronuncia. Incluye todos los sistemas de IA que no estén en las otras categorías ya indicadas. Ejemplos de ello son sistemas utilizados como filtros de SPAM o videojuegos que utilicen la IA. Las únicas obligaciones que aquí aparecen son las relativas al cumplimiento de los estándares de seguridad de cualquier producto.

Mención debe hacerse del capítulo centrado en la **Gobernanza** (**Capítulo VII**). En él se establece la creación de un **Comité Europeo de Inteligencia Artificial**. Este órgano contará con un representante de cada Estado Miembro. El Supervisor Europeo de Protección de Datos será observador y la Comisión podrá participar sin voto. Al mismo

tiempo, un grupo permanente que incluirá proveedores, usuarios, organizaciones civiles, etc., ejercerá para este comité labores de asesoría. Entre las funciones del Comité Europeo de IA aparecen la recolección de conocimiento técnico; la cooperación en la armonización y desarrollo de las pruebas de conformidad y de las pruebas en condiciones reales; la colaboración con organizaciones de expertos en servicios digitales, servicios financieros, competencia, seguridad de productos, ciberseguridad, protección de datos, criptomonedas…; publicación de recomendaciones sobre especificaciones, estándares y guías; aconsejar a la Comisión en aspectos como la preparación de actos de ejecución o materias internacionales relativas a IA y aconsejar a las autoridades nacionales de supervisión en materia de IA.

También en este capítulo se expone la obligación de cada Estado Miembro de designar una **autoridad notificante*** y al menos una autoridad de vigilancia del mercado en relación con este Reglamento de IA. Estas autoridades, que serán fiscalizadas por el Supervisor Europeo de Protección de Datos, deberán ser objetivas e imparciales, tendrán que contar con recursos adecuados y habrán de estar en contacto e intercambiar experiencias con las de otros EEMM.

*El reglamento define **autoridad notificante** como *"la 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".* En España, el Gobierno ha creado a estos efectos la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), cuya sede se establecerá en A Coruña. La presidencia de AESIA la ejercerá María Teresa Ledo Turiel, secretaria de Estado de Digitalización e Inteligencia Artificial (del Ministerio para la Transformación Digital y de la Función Pública), que además será la encargada de nombrar un Director General.

Junto a estos órganos aparece otro de especial importancia: la **Oficina de IA**, cuyas funciones y características aparecen dispersas a lo largo de todo el Reglamento. Este órgano, cuyo fin básico será supervisar y hacer cumplir el Reglamento, buscará el apoyo del desarrollo y el uso de un IA fiable, de la que puedan explotarse sus posibilidades para conseguir beneficios sociales y económicos y, al mismo tiempo, contrarrestarse sus riesgos. Además, entre sus objetivos figura el de conseguir en la Unión un enfoque estratégico y coherente de la IA a nivel internacional. Se establece, además, dentro de la Comisión Europea, como la base para un sistema único de gobernanza sobre IA en la Unión. A modo de síntesis, la Oficina de IA tiene las siguientes responsabilidades y funciones:

1. Supervisión y cumplimiento: Controla y supervisa el cumplimiento del Reglamento, centrando sus esfuerzos esencialmente en los modelos de IA GPAI,

Entre otros aspectos, incluye la evaluación de riesgos sistémicos, el examen de modelos, la gestión de incidentes de incumplimiento…

2. Apoyo: Proporciona información y recursos a las PYME con el objetivo de ayudarlas a cumplir con la normativa del Reglamento. Aquí podrá crear plataformas informativas, campañas de comunicación…

3. Desarrollo de Códigos de Buenas Prácticas: Elaborará códigos de prácticas voluntarias para los proveedores de modelos GPAI, que, como ya se ha indicado, implican el establecimiento de una presunción de conformidad con los requisitos exigidos por el Reglamento.

4. Liderazgo y colaboración en investigaciones conjuntas: Coordinará investigaciones de vigilancia del mercado para detectar y abordar incumplimientos graves de los sistemas de IA de alto riesgo.

También es destacable señalar que el Reglamento faculta a la Oficina de IA para exigir medidas correctoras a los proveedores de modelos GPAI cuando se detecten riesgos sistémicos; para supervisar la aplicación uniforme de la Ley de IA en toda la Unión, con la finalidad de facilitar la comunicación y la cooperación entre organismos sectoriales y autoridades nacionales, pudiendo imponer sanciones. Sobre esto último cabe subrayar que la normativa propuesta por la UE tendrá un impacto de gran alcance en todas las organizaciones que utilizan y se aprovechan del poder que proporciona un sistema IA. Las consecuencias del incumplimiento podrían ir desde la restricción del acceso al mercado hasta multas significativas, dependiendo del nivel de incumplimiento (prohibiciones, requisitos IA alto riesgo…). Las multas pueden llegar hasta los 35 millones de euros o el 7 por ciento de la facturación global, pudiendo reducirse a 7.5 millones o el 1.5 por ciento de la facturación, según la infracción y el tamaño de la empresa.

Vinculado a la Oficina de IA aparece el comité científico de expertos independientes, que le proporcionará asesoramiento técnico y apoyará en la evaluación de capacidades y riesgos de modelos GPAI, alertándole también de posibles riesgos sistémicos.

Además, la Oficina de IA tiene una relación especial con el Comité Europeo de Inteligencia Artificial. En éste, la Oficina de IA puede participar en sus reuniones como observador sin derecho a voto. A su vez, la Oficina de IA se encargará de su secretaría, convocará las reuniones a petición del presidente y preparará el orden del día.

Por último, en cuanto a la **cronología**, debe señalarse que este Reglamento, tras su entrada en vigor, se aplicará a los 6 meses para los sistemas de IA prohibidos, 12 meses

para los sistemas-modelos GPAI, 24 meses para los sistemas de IA de alto riesgo del Anexo III y 36 meses para los de alto riesgo del primer tipo (anexo II).

De gran utilidad es la página web creada a propósito de esta norma por *Future of Life Institute* (FLI). FLI es una fundación internacional e independiente sin ánimo de lucro que busca reducir los riesgos extremos a gran escala generados por las tecnologías transformadoras como la inteligencia artificial. En la página web sobre el Reglamento, entre muchas otras cosas (resúmenes, artículos sobre el Reglamento, análisis…), incluyen un **verificador de cumplimiento del Reglamento**[2] en línea para que las empresas y usuarios vinculados a la IA puedan conocer qué obligaciones deben cumplir, qué seguimiento deben hacer, qué artículo deben consultar de la norma… El verificador consiste en un cuestionario en el que se realizan una serie de preguntas al usuario para que pueda asegurarse de la mejor manera de seguir las disposiciones del Reglamento.

Fuente: KPMG

[2] https://artificialintelligenceact.eu/es/evaluacion/comprobador-del-cumplimiento-de-la-ley-de-ai-de-la-ue/