Pérez-Llorca

TECHLAW

Inteligencia artificial

JUNIO 2024

Un reto para las compañías y para los reguladores

Andy Ramos

Socio de Derecho Digital

aramos@perezllorca.com
+34 91 423 20 72

Raúl Rubio

Socio de Derecho Digital

rrubio@perezllorca.com
+34 91 353 45 59

Adolfo Mesquita Nunes

Socio de Derecho Digital

adolfomesquitanunes@perezllorca.com
+351 912 585 103

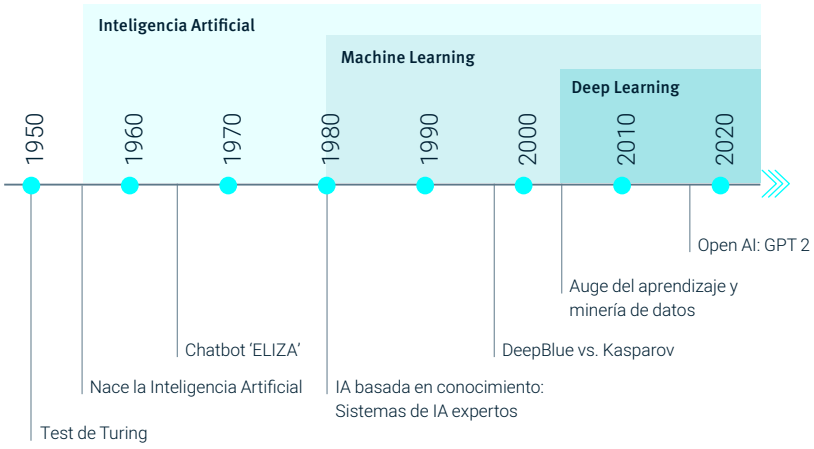
_ ANDY RAMOS, RAÚL RUBIO, ADOLFO MESQUITA NUNES, FRANCISCO RIBEIRO FERREIRA E ISABEL IGLESIAS

La primera regulación de la Inteligencia Artificial ya está aquí. Aspectos clave.

1. Introducción

En la era digital, la Inteligencia Artificial ("**IA**") se ha convertido en un elemento central de la innovación y el desarrollo tecnológico, provocando transformaciones significativas en todos los sectores de la economía y la sociedad. El enorme potencial de la IA se ha percibido por determinados reguladores como una amenaza para los derechos y libertades de los ciudadanos, propiciando debates sobre el desarrollo y uso responsable y ético de esta tecnología, y proponiendo regular posibles conflictos incluso antes de que estos puedan ocurrir.

Para más información sobre aspectos generales de la IA, recomendamos consultar la primera de esta serie de publicaciones, disponible aquí.



Evolución de la inteligencia artificial

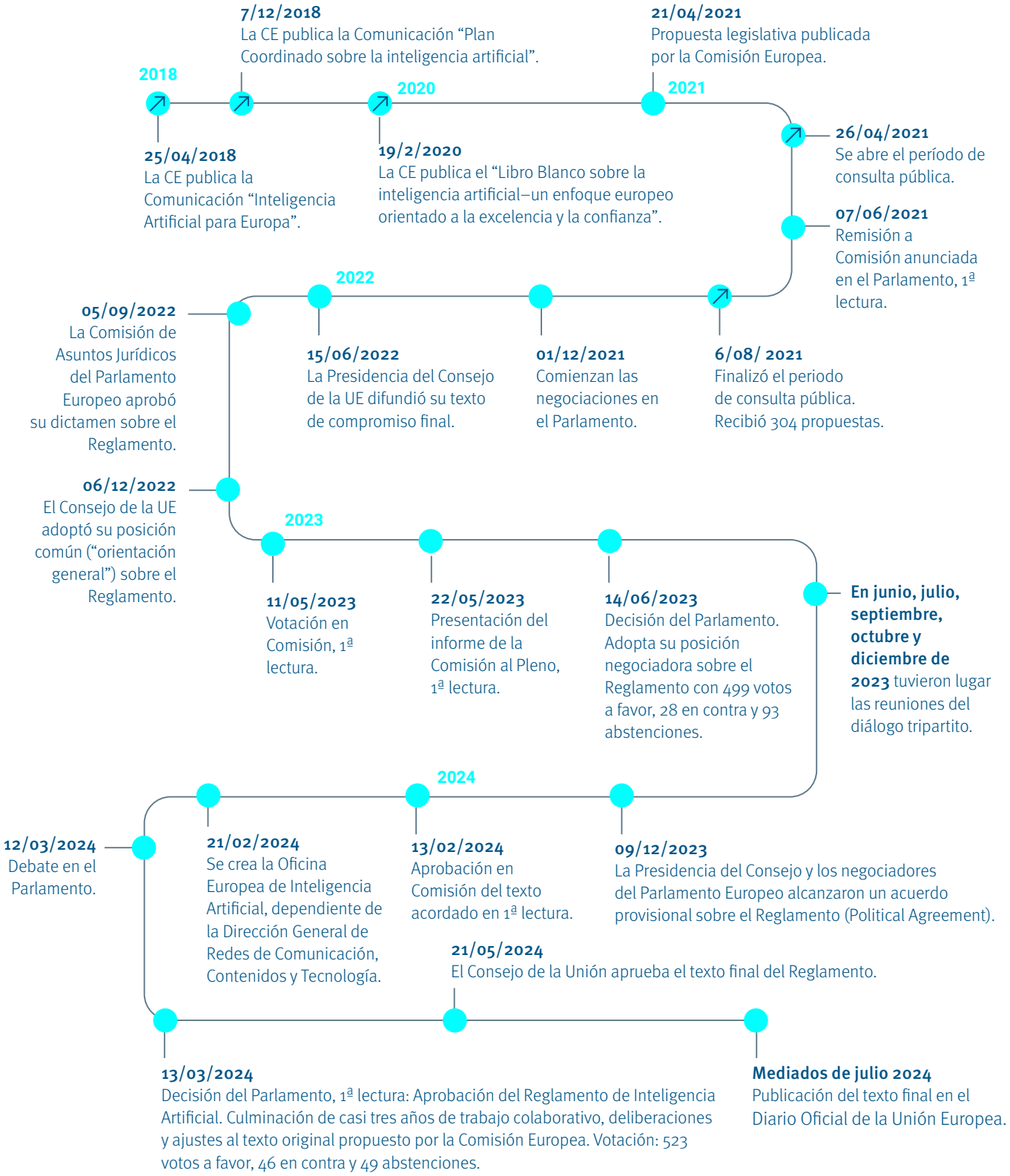
La Unión Europea ("**UE**") adoptó el pasado 13 de marzo de 2024 el Reglamento de Inteligencia Artificial (el "**Reglamento**"), un marco legislativo destinado a establecer normas armonizadas en materia de IA dentro de los Estados miembros. El regulador europeo pretende que el Reglamento forme parte de un ecosistema de IA que sea seguro, fiable y alineado con los valores y principios europeos. Al hacerlo, la UE trata de posicionarse como líder en el establecimiento de un marco normativo integral para la IA, que no solo aborda los riesgos asociados con su uso, sino que también promueve su desarrollo ético y humano.

Este Reglamento, fruto de un largo proceso legislativo, defiende formalmente un enfoque equilibrado que busca promover la innovación y el desarrollo tecnológico, al mismo tiempo que garantiza la protección de la salud, la seguridad y los derechos fundamentales de los ciudadanos europeos. No obstante, como veremos más adelante, las medidas de control superan con creces en la norma a las de fomento, siendo estas últimas mucho más vagas y poco desarrolladas con respecto al nivel de concreción de las primeras, lo cual es incoherente con los propios considerandos de la norma y con el incipiente estado actual de la IA.

Esta nota jurídica tiene como objetivo proporcionar un análisis de los aspectos más relevantes del texto adoptado, las implicaciones legales y de negocio, y algunas recomendaciones prácticas sobre cómo adecuar la actividad económica de cualquier empresa afectada al Reglamento.

2. Cronología del Reglamento

El proceso de desarrollo y aprobación del Reglamento ha sido complejo y meticuloso, dado el carácter innovador de la norma y de la propia tecnología, así como por la importancia y el impacto potencial de la IA en la sociedad. La cronología de los eventos clave que culminaron en la reciente aprobación del Reglamento es la siguiente:



3. Propósito del Reglamento

El declarado propósito del Reglamento es mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la UE.

El Reglamento busca promover la adopción de una IA centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales, así como apoyar la innovación. Además, establece normas armonizadas para la introducción en el mercado de sistemas de IA, prohibiciones de ciertas prácticas de IA, requisitos específicos para sistemas de IA de alto riesgo, normas de transparencia y medidas en apoyo de la innovación.

> ***"el Reglamento busca equilibrar el fomento de la innovación y el desarrollo tecnológico con la necesidad de asegurar que la IA se desarrolle y utilice de manera que respete los derechos fundamentales y los valores de la Unión Europea".***

Además, el Considerando 27 del Reglamento destaca la importancia de un enfoque basado en el riesgo para establecer normativas efectivas y proporcionadas, subrayando también las Directrices éticas para una IA fiable de 2019, las cuales fueron redactadas por el Grupo Independiente de Expertos de Alto Nivel sobre IA instaurado por la Comisión. El Grupo propuso siete principios éticos esenciales no vinculantes para fomentar la fiabilidad y ética de la IA. Estos principios incluyen: acción y supervisión humanas; solidez técnica y seguridad; gestión de la privacidad y de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y ambiental y rendición de cuentas. Estas directrices, aunque no son jurídicamente obligatorias, complementan los requisitos contemplados en el Reglamento.

PRINCIPIOS ÉTICOS ESENCIALES:

Acción y supervisión humanas

Transparencia, diversidad, no discriminación y equidad

Solidez técnica y seguridad

Bienestar social y ambiental

Gestión de la privacidad y datos

Rendición de cuentas

4. El Reglamento de IA en cifras

180 Considerandos

113 artículos

+107.000 palabras

13 títulos

13 anexos

20 actos delegados y de ejecución

5. Ámbito de aplicación del Reglamento

El Reglamento será aplicable a:	No será aplicable a:
– Proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA o modelos de IA de uso general en la Unión, independientemente de su ubicación.	– Los ámbitos que queden fuera de la esfera de aplicación del Derecho de la UE.
– Responsables del despliegue de sistemas de IA establecidos o ubicados en la Unión.	– Las competencias de los Estados miembros en materia de seguridad nacional.

El Reglamento será aplicable a:	No será aplicable a:
– Proveedores y responsables del despliegue de sistemas de IA ubicados en terceros países cuando la información de salida se utilice en la Unión.	– Los sistemas de IA que se utilicen exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.
– Importadores y distribuidores de sistemas de IA	– Las autoridades públicas de terceros países ni a las organizaciones internacionales cuando utilicen sistemas de IA en el marco de acuerdos o de la cooperación internacionales con fines de aplicación de la ley y cooperación judicial con la Unión o con uno o varios Estados miembros, siempre que ofrezca garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas.
– Fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto.	– Las disposiciones relativas a la responsabilidad de los prestadores de servicios intermediarios que figuran en el capítulo II del Reglamento (UE) 2022/2065.
– Representantes autorizados de proveedores no establecidos en la Unión.	– Los sistemas o modelos de IA desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad.
– Personas afectadas que estén ubicadas en la Unión.	– A ninguna actividad de investigación, prueba o desarrollo relativa a sistemas o modelos de IA antes de su introducción en el mercado o puesta en servicio.
– A los sistemas de IA de alto riesgo únicamente se les aplicará el artículo 112, mientras que el artículo 57 se aplicará únicamente en la medida en que los requisitos para los sistemas de IA de alto riesgo se hayan integrado en dicha legislación de armonización de la Unión.	– Las obligaciones de los responsables del despliegue que sean personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional.
– Se aplicará a los sistemas de IA divulgados con arreglo a licencias libres y de código abierto que entren en el ámbito de aplicación del artículo 5 (prácticas prohibidas) o del artículo 50 (aplicación práctica de las obligaciones de transparencia).	– De forma general, el Reglamento no se aplicará a los sistemas de IA divulgados con arreglo a licencias libres y de código abierto salvo las excepciones mencionadas.

6. Definición de sistema de inteligencia artificial

De conformidad con el artículo 3.1 del Reglamento, un sistema de IA es aquel que está 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.

Con esta redacción, el legislador europeo aspira a que su conceptualización de la IA perdure en el tiempo, lo cual requiere que englobe una gama excepcionalmente amplia de técnicas analíticas de datos, siendo aplicable a una amplia variedad de tecnologías utilizadas actualmente en el sector empresarial y en la administración pública.

7. Categorización de sistemas de IA

La categorización de sistemas de IA según el Reglamento se centra en el concepto de riesgo[1], clasificando tales sistemas en función del nivel de riesgo que presentan para la sociedad, la seguridad, los derechos fundamentales y el bienestar de las

1 Según el artículo 3.2 del Reglamento, "riesgo" es la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio.

personas. Así, el **Reglamento regula principalmente los sistemas de IA de alto riesgo**, estableciendo requisitos detallados para su desarrollo, despliegue y uso. Podemos distinguir los siguientes tipos de sistemas de IA:

- **Sistemas de IA prohibidos:** algunas aplicaciones de IA están prohibidas debido a los riesgos inaceptables que para el legislador presentan con relación a los derechos y libertades fundamentales. Esto incluye sistemas de vigilancia masiva y sistemas que manipulan comportamientos humanos para eludir la autonomía de las personas; explotación de vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad; realización de evaluación social del comportamiento en entornos sociales y públicos; o la utilización de puntuaciones de crédito social por autoridades públicas, entre otros.

- **Sistemas de IA de alto riesgo:** los sistemas de IA se consideran de alto riesgo cuando son susceptibles de afectar los derechos fundamentales de las personas o a su seguridad de manera significativa. Estos sistemas están sujetos a requisitos regulatorios estrictos, incluyendo sistema de gestión de riesgos, evaluación de conformidad, altos estándares de transparencia, elaboración de documentación técnica antes de su introducción en el mercado, obligación de conservación de registros, medidas de vigilancia humana necesaria, y sólidas garantías de protección de datos y ciberseguridad.

- **Sistemas de IA de riesgo limitado o con obligaciones especiales de transparencia:** el Reglamento incluye disposiciones relacionadas con la transparencia y la provisión de información adecuada a los usuarios. Esto incluye requerimientos para que los proveedores de sistemas de IA informen claramente a los usuarios cuando están interactuando con un sistema de IA, asegurando que las personas sean conscientes de la naturaleza automatizada de la interacción.

8. Prácticas de IA prohibidas

El Reglamento contempla una serie de prácticas prohibidas en relación con los sistemas de IA, como serían la comercialización, la puesta en servicio o la utilización de:

- **Técnicas subliminales y manipulativas**: sistemas de IA que utilicen técnicas subliminales o manipulativas con la finalidad de alterar significativamente el comportamiento de las personas de una manera que menoscabe su capacidad para tomar decisiones informadas.

- **Explotación de vulnerabilidades**: sistemas de IA que exploten vulnerabilidades de personas o grupos específicos, basadas en su edad, discapacidad o situación socioeconómica, con el fin de alterar sustancialmente su comportamiento de manera que pueda causarles daño considerable .

- **Sistemas de crédito social**: sistemas de IA para evaluar o clasificar a personas o grupos a lo largo del tiempo basándose en su comportamiento social o características personales o de personalidad, resultando en tratamientos perjudiciales o desfavorables en contextos no relacionados con los datos recogidos.

- **Vigilancia predictiva individual**: sistemas de IA destinados específicamente a evaluar el riesgo de que una persona cometa un delito, basándose únicamente en el perfilado de la persona o en la evaluación de sus características de personalidad. Se exceptúan los sistemas de IA que apoyan la evaluación de una persona en actividades delictivas, siempre que esta evaluación se base en hechos objetivos y verificables.

- **Reconocimiento facial y bases de datos**: se prohíbe la creación o ampliación de bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de Internet o de sistemas de videovigilancia, debido a las implicaciones en la privacidad y la posible vigilancia masiva.

- **Sistemas de inferencia emocional en el trabajo y educación**: se prohíbe la utilización de sistemas de IA destinados a detectar emociones o intenciones de las personas en el ámbito laboral o educativo, excepto cuando se usan por razones médicas o de seguridad.

- **Sistemas de identificación biométrica en espacios públicos**: salvo ciertas excepciones, los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de prosecución pública.

9. Sistemas de alto riesgo

Los sistemas de IA de alto riesgo son aquellos que representan un potencial significativo de daño a la seguridad, la salud o los derechos fundamentales de las personas. Por esta razón, estos sistemas son objeto de un escrutinio particularmente intenso bajo el Reglamento, para garantizar que se implementen de manera segura y confiable.

9.1. Clasificación de los sistemas de alto riesgo

Biometría	» Sistemas de identificación biométrica remota. Exclusión: Cuando su única finalidad es confirmar la identidad de la persona. » Sistemas de IA para la categorización biométrica basada en atributos o características sensibles o protegidos. » Sistemas de IA para el reconocimiento de emociones.
Infraestructuras críticas	» Sistemas de IA como componentes de seguridad en la gestión y operación de infraestructuras digitales críticas, tráfico, suministro de agua, gas, calefacción o electricidad.
Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales	» Sistemas de IA utilizados por autoridades públicas para evaluar la admisibilidad de servicios y prestaciones esenciales, incluyendo asistencia sanitaria. » Sistemas de IA para evaluar la solvencia, calificación crediticia, riesgos y fijación de precios en seguros, y evaluación y clasificación de llamadas de emergencia.
Migración, asilo y gestión del control fronterizo	» Sistemas de IA utilizados por autoridades competentes para evaluación de riesgos (seguridad, salud, migración irregular), examen de solicitudes de asilo, visado, permisos de residencia, y detección, reconocimiento o identificación de personas.
Seguridad de productos regulados	» Sistemas de IA que estén destinados a ser utilizados como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión (listados en el Anexo I del Reglamento) o que el propio sistema de IA sea uno de dichos productos (Reglamento relativo a las máquinas, Directiva sobre seguridad de juguetes...). » 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. Este sucede cuando su uso se limita a: (i) realizar una tarea procedimental específica; (ii) mejorar el resultado de una actividad humana previamente completada; (iii) detectar patrones de toma de decisiones sin influir en evaluaciones humanas sin revisión adecuada; (iv) realizar una tarea preparatoria para una evaluación relevante para los casos de uso enumerados.
Educación y formación profesional	» Sistemas de IA para determinar acceso/admisión o distribución de individuos en centros educativos y de formación profesional. » Sistemas de IA para evaluar resultados de aprendizaje o nivel educativo adecuado. » Sistemas de IA para seguimiento y detección de comportamientos prohibidos durante exámenes.

Empleo, gestión de trabajadores y acceso al autoempleo	» Sistemas de IA para contratación, selección, análisis y filtrado de solicitudes de empleo, evaluación de candidatos. » Sistemas de IA para decisiones que afectan las condiciones laborales, promoción, rescisión de relaciones laborales, asignación de tareas, supervisión y evaluación del rendimiento.
Aplicación de la ley	» Sistemas de IA para evaluar el riesgo de victimización, fiabilidad de pruebas, probabilidad de comisión o reincidencia en infracciones, elaboración de perfiles durante la detección, investigación o enjuiciamiento de infracciones penales.
Administración de justicia y procesos democráticos	» Sistemas de IA para asistencia judicial en interpretación de hechos y ley, aplicación de ley, o uso en resolución alternativa de litigios. » Sistemas de IA para influir en elecciones o comportamiento electoral. *Exclusión: herramientas administrativas o logísticas para campañas políticas.* » Productos de los que el sistema de IA sea componente de seguridad, o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I del Reglamento.
Un sistema de IA siempre se considerará de alto riesgo cuando lleve a cabo la elaboración de perfiles de personas físicas (*ex. art. 6 in fine*).	

9.2. Obligaciones de los sistemas de IA de alto riesgo

Para que estos sistemas operen en el mercado de la UE, deben cumplir con los requisitos que se detallan a continuación:

- **Evaluación de conformidad**: antes de su introducción en el mercado o su puesta en servicio, estos sistemas deberán someterse a una evaluación de conformidad para verificar que cumplen con todos los requisitos de seguridad y eficacia exigidos por el Reglamento. Esto incluye pruebas exhaustivas para validar la precisión, la solidez y la seguridad del sistema.
- **Transparencia e información**: los proveedores deben asegurarse de que la documentación de los sistemas de IA de alto riesgo sea detallada y accesible. Esto incluye la información sobre la metodología, los algoritmos, las decisiones de diseño, y las capacidades y limitaciones del sistema, permitiendo así una total transparencia sobre cómo opera el sistema y sobre los datos que utiliza. Asimismo, deberán proporcionar a los usuarios información clara y adecuada sobre las capacidades y limitaciones del sistema.
  - » **Gestión de riesgos**: deberán establecer y documentar un sistema de gestión de riesgos, de forma sistemática y continua a lo largo de todo el ciclo de vida del sistema de IA de alto riesgo. Deberá incluir la identificación, análisis, estimación y evaluación de riesgos conocidos y previsibles, así como la adopción de medidas de gestión de riesgos adecuadas para abordarlos.
  - » **Calidad de los datos**: deberán garantizar que los conjuntos de datos utilizados para el entrenamiento, la validación y el testeo sean relevantes para la finalidad del sistema, representativos, libres de errores y sesgos, a través de políticas adecuadas de gobernanza de datos.
  - » **Documentación técnica**: deberán mantener la documentación técnica que demuestre la conformidad del sistema de IA con los requisitos exigidos.
  - » **Registro de actividades**: deberán llegar un registro de las operaciones del sistema de IA para garantizar la trazabilidad de sus resultados. Además, los sistemas de IA de alto riesgo permitirán técnicamente el registro automático de eventos (archivos de registro) a lo largo de todo su ciclo de vida.
- **Instrucciones e información**: los sistemas deberán ir acompañados de instrucciones con información completa y clara que sea pertinente y comprensible para los responsables del despliegue. Identificación del proveedor: los proveedores de

sistemas de IA de alto riesgo deberán indicar en el sistema, en su embalaje en la documentación que lo acompañe, el nombre, su nombre comercial registrado o marca registrada y su dirección de contacto.

- **Identificación del proveedor**: los proveedores de sistemas de IA de alto riesgo deberán indicar en el sistema, en su embalaje en la documentación que lo acompañe, el nombre, su nombre comercial registrado o marca registrada y su dirección de contacto.

- **Vigilancia humana**: deberán contar con supervisión humana para minimizar el riesgo y permitir la intervención en caso de mal funcionamiento del sistema y mitigar así los riesgos de decisiones autónomas erróneas o dañinas. Los operadores deberán estar capacitados y tener la autoridad necesaria para supervisar y, si es necesario, intervenir o desactivar el sistema de IA.

- **Cooperación con las autoridades**: los proveedores de sistemas de IA de alto riesgo deberán cooperar con las autoridades reguladoras y proporcionar toda la información necesaria para demostrar la conformidad del sistema con los requisitos legales. Esto también incluye facilitar el acceso a los registros y la documentación del sistema cuando sea requerido por las autoridades competentes.

- **Robustez y precisión**: deberán asegurar que el sistema de IA sea robusto, preciso y capaz de manejar errores o inconsistencias durante su funcionamiento.

- **Ciberseguridad**: deberán implementar medidas adecuadas para garantizar la ciberseguridad y la integridad del sistema. En particular, pueden ser implementadas medidas para prevención y respuesta a manipulación de los datos de entrenamiento (*data poisoning*), de componentes pre-entrenados utilizadas en el entrenamiento (*model poisoning*), entradas diseñadas para hacer que el modelo de IA cometa un error, ataques a la confidencialidad, etc.

- **Notificación y registro**: deberán registrar el sistema de IA de alto riesgo en una base de datos de la UE antes de su puesta en el mercado (ver apartado 9.3).

Ciertas obligaciones se aplican a determinados operadores:

- **Verificación de conformidad:** los distribuidores y otros operadores a lo largo de la cadena de valor (como importadores y responsables del despliegue) tienen obligaciones específicas, como verificar la conformidad del sistema antes de su comercialización, asegurar las condiciones adecuadas de almacenamiento y transporte, y actuar en caso de que detecten no conformidades o riesgos.

- **Verificación de impacto en los derechos fundamentales**: deberán asegurar que el uso del sistema de IA no conlleva discriminación y que es respetuoso de los derechos fundamentales.

- **Representante autorizado**: antes de comercializar un sistema de IA de alto riesgo en el mercado de la UE, los proveedores establecidos en terceros países deberán nombrar, mediante un mandato escrito, a un representante autorizado que esté establecido en la UE.

En resumen, los sistemas de IA de alto riesgo están sujetos a un marco regulatorio detallado que exige cumplimiento en múltiples niveles, desde la validación de su tecnología hasta la gestión de los datos que procesan. Estas medidas tienen como objetivo proteger a los individuos y a la sociedad de los posibles daños que estos poderosos sistemas podrían causar si no se gestionan correctamente.

9.3. Base de datos de la UE para sistemas de alto riesgo

La base de datos de la UE para sistemas de IA de alto riesgo es una iniciativa esencial en el marco del Reglamento, destinada a centralizar y facilitar el acceso a información detallada sobre estos sistemas, aumentando así la transparencia y fortaleciendo la supervisión reguladora. Esta base de datos será creada y mantenida por la Comisión Europea en colaboración con los Estados miembros y contendrá información detallada sobre los sistemas de IA de alto riesgo registrados según el Reglamento.

La obligación de registrarse a sí mismos y al sistema de IA de alto riesgo corresponderá a:

- En el ámbito privado, al proveedor o, en su caso, a su representante autorizado y siempre antes de la comercialización o puesta en servicio.

- En el ámbito público, a las autoridades, agencias u organismos públicos responsables del despliegue o personas que actúen en su nombre y siempre antes de la puesta en servicio o utilización.

En los casos en los que la IA se utilice para el control del cumplimiento de obligaciones legales, migración, el asilo y la gestión del control fronterizo el registro se efectuará en una sección segura no pública de la base de datos de la UE.

Los sistemas de IA de alto riesgo contemplados en el punto 2 del Anexo III (Sistemas de IA destinados a utilizarse como componentes de seguridad en la gestión y explotación de infraestructuras digitales críticas, el tráfico rodado o el suministro de agua, gas, calefacción o electricidad) se registrarán a escala nacional.

9.3.1. **Funciones y características de esta base de datos:** deberá incluir datos específicos introducidos tanto por los proveedores de los sistemas como por los responsables del despliegue, si son autoridades públicas. Estos datos abarcarán desde detalles identificativos del sistema y sus proveedores hasta información técnica y de conformidad. La Comisión Europea tiene la responsabilidad de definir las especificaciones técnicas de la base de datos y actualizarlas con la asistencia de un comité de expertos.

9.3.2. **Accesibilidad y privacidad:** la información registrada estará accesible al público de forma general, asegurando que la base de datos sea fácil de navegar y comprender, aunque con restricciones específicas para información sensible que solo será accesible para las autoridades de vigilancia de mercado y la Comisión, a menos que haya consentimiento expreso para ampliar el acceso.

9.3.3. **Protección de datos**: solo contendrá datos personales en la medida necesaria para cumplir con sus funciones reguladas, manteniendo el cumplimiento con los reglamentos de protección de datos de la UE. La gestión de la base de datos se llevará a cabo con un alto nivel de seguridad, incluyendo medidas de ciberseguridad para proteger la información almacenada.

Esta base de datos representa un paso crítico hacia una mayor transparencia en el uso de la IA, permitiendo un escrutinio público y regulador más efectivo de los sistemas de IA que pueden tener un impacto significativo en la seguridad y los derechos fundamentales.

10. Obligaciones de transparencia de proveedores y responsables del despliegue de determinados sistemas de IA

El regulador ha considerado esencial la transparencia sobre determinados aspectos de un sistema de IA para cumplir con los objetivos del Reglamento, especialmente aquellos clasificados como de alto riesgo. Así, el Reglamento establece requisitos claros que deben seguirse para promover la transparencia y la confianza del público en estos sistemas avanzados.

Los proveedores deben garantizar que **cualquier sistema de IA destinado a interactuar directamente con personas esté claramente identificado como tal**, salvo cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz. Esta obligación pretende asegurar que los usuarios sean conscientes de que están interactuando con un sistema de IA, en lugar de con un ser humano. Esta obligación se extiende a los sistemas que generan contenido sintético como audio, imagen, vídeo o texto, los cuales deben estar claramente marcados para que sean reconocibles como generados por IA.

Además, los responsables del despliegue de sistemas específicos, como los de **reconocimiento de emociones o de categorización biométrica**, deben informar a las personas expuestas a estos sistemas sobre su funcionamiento y el tratamiento de sus datos personales.

Finalmente, **aquellos sistemas de IA que manipulan imágenes o contenidos de audio o vídeo, especialmente aquellos que crean ultra-falsificaciones (*deepfakes*),** deberán informar claramente que estos contenidos han sido generados o manipulados artificialmente.

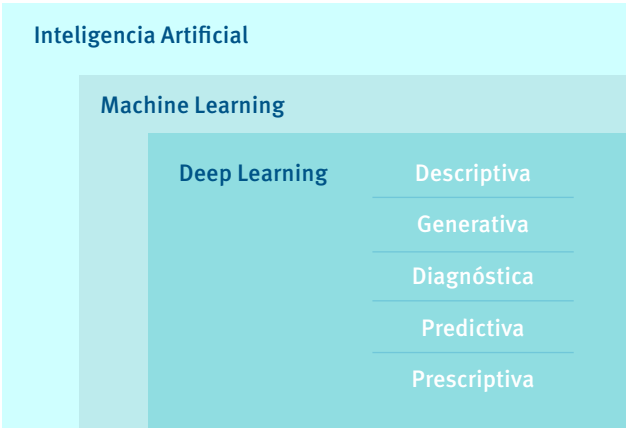
11. Uso de IA por la Administración pública

Aunque se trata de una normativa de aplicación horizontal, el Reglamento presta especial atención al uso de sistemas de IA por parte de organismos públicos, porque muchos de los usos de los sistemas de IA clasificados como de alto riesgo están asociados a funciones típicamente administrativas (sistemas de IA en la administración de justicia y procesos democráticos, de migración, asilo y gestión del control fronterizo, servicios y prestaciones públicos esenciales, etc.). Así, las entidades públicas están sujetas a las obligaciones asociadas a los sistemas de alto riesgo, tanto en calidad de proveedores (cuando desarrollan un sistema de IA para su uso) como de responsables del despliegue (cuando contratan su servicio a un proveedor externo).

El Reglamento especifica que los organismos públicos que utilicen sistemas de IA de alto riesgo tienen la obligación de llevar a cabo una evaluación de impacto sobre los derechos fundamentales, cuyos detalles y formato desarrollará la Comisión.

12. Sobre los modelos de IA de uso general

Una de las novedades más relevantes de las últimas modificaciones del Reglamento es el establecimiento de un marco normativo específico para los modelos de IA de uso general, como ChatGPT, Google Gemini o Meta Llama, los cuales están diseñados para abordar una amplia gama de tareas y suelen entrenarse con grandes volúmenes de datos utilizando métodos avanzados como el aprendizaje autosupervisado, no supervisado o por refuerzo. Estos modelos pueden comercializarse de diferentes maneras, incluyendo como módulos, bibliotecas, descargas directas o copias físicas, aunque los métodos más habituales son mediante API o como servicio web. Estos modelos fundacionales requieren componentes adicionales, como interfaces de usuario, para operar como sistemas de IA funcionales.



La IA generativa (**GenAI**) es un enfoque en la investigación de IA. Se centra en desarrollar modelos capaces de generar contenido nuevo y creativo, como imágenes, texto o incluso música. A diferencia de los sistemas tradicionales de IA que se basan en reglas predefinidas o patrones aprendidos, los modelos generativos están diseñados para producir datos originales mediante la comprensión profunda de las estructuras y características subyacentes de los conjuntos de datos de entrenamiento. Dichos modelos forman parte de la categoría de *machine learning*, y utilizan técnicas de *deep learning* para generar contenidos similares a los que crean los humanos. Se apoya en modelos de lenguaje de gran escala (*large language models* o LLMs) para interactuar con los usuarios.

12.1. Clasificación de los modelos de uso general

El Reglamento distingue entre modelos de uso general y aquellos que, además, presentan riesgos sistémicos.

Un modelo de IA de uso general se considerará como un modelo de riesgo sistémico si cumple con alguno de los siguientes criterios:

- Posee capacidades de gran impacto, determinadas mediante herramientas y metodologías técnicas apropiadas, incluyendo indicadores y parámetros de referencia.
- Según una decisión de la Comisión, tomada por iniciativa propia o en respuesta a una alerta de un grupo de expertos científicos, se reconoce que el modelo tiene capacidades o un impacto equivalente a lo descrito en el punto anterior, considerando los criterios especificados en el Anexo XIII[2].
- Se asumirá que un modelo de IA de uso general posee capacidades de gran impacto según lo descrito en el punto anterior, si el volumen total de cálculos utilizados para su entrenamiento, medido en FLOPs, supera los 10^25[3]

Además, la Comisión está facultada para emitir actos delegados conforme al artículo 97 con la finalidad de ajustar los umbrales mencionados, así como para actualizar los parámetros de referencia e indicadores en función de los avances tecnológicos, como mejoras en algoritmos o en la eficiencia del *hardware*.

Estos modelos deben cumplir con obligaciones específicas una vez introducidos en el mercado, incluyendo la realización de evaluaciones de impacto y pruebas de resistencia para detectar y mitigar posibles riesgos.

2 A tal efecto, el Anexo XIII señala los criterios que se tendrán en cuenta, como son: (i) La cantidad de parámetros que componen el modelo, que influye directamente en su complejidad y capacidad de procesamiento; (ii) La calidad y el tamaño del conjunto de datos utilizado para el entrenamiento del modelo, que puede medirse mediante métodos como el uso de *tokens*, (iii) El volumen total de cálculo empleado para entrenar el modelo, expresado en FLOP o combinando otras variables tales como el costo estimado del entrenamiento, el tiempo requerido y el consumo energético asociado; (iv) Las características de las entradas y salidas del modelo, incluyendo aspectos como la conversión de texto a texto en modelos de lenguaje de gran escala, la conversión de texto a imagen, la multimodalidad y los umbrales definidos para evaluar el impacto significativo de cada modalidad, así como el tipo específico de entradas y salidas, por ejemplo, secuencias biológicas; (v) Los *benchmarks* y evaluaciones de rendimiento del modelo, considerando aspectos como el número de tareas que puede realizar sin entrenamiento adicional, su capacidad para adaptarse y aprender nuevas tareas, su grado de autonomía, escalabilidad y las herramientas a las que puede acceder; (vi) La relevancia de sus impactos en el mercado interior, especialmente si ha sido utilizado por al menos 10.000 usuarios profesionales registrados en la UE; (vii) La cantidad de usuarios finales registrados que interactúan con el modelo.

3 FLOP o Operación de coma flotante: cualquier operación o tarea matemática que implique números de coma flotante, que son un subconjunto de los números reales normalmente representados en los ordenadores mediante un número entero de precisión fija elevado por el exponente entero de una base fija.

Los proveedores de estos modelos deben asegurar altos niveles de transparencia y cooperación con las autoridades, incluyendo la documentación detallada sobre el diseño, las capacidades y las limitaciones del modelo. Esta información debe ser accesible no solo para las autoridades sino también para otros proveedores que integren estos modelos en sistemas de IA más amplios.

12.2. Obligaciones

12.2.1. IA de uso general

El Reglamento impone una serie de obligaciones comunes a los proveedores de modelos de IA de uso general, para garantizar que estos modelos se implementen de manera responsable y segura. Una de las principales obligaciones es la elaboración y actualización continua de la documentación técnica detallada del modelo. Esta documentación debe incluir información sobre el proceso de entrenamiento, las pruebas realizadas y los resultados de las evaluaciones de estos modelos. Los elementos específicos que deben cubrirse están detallados en el Anexo XI del Reglamento y deben estar disponibles para la Oficina de Inteligencia Artificial ("**Oficina de IA**")[4] y las autoridades nacionales competentes.

Además, los proveedores deben hacer accesible esta documentación a otros proveedores de sistemas de IA que planeen integrar el modelo de uso general en sus propios sistemas. Esta documentación debe permitir a estos terceros comprender completamente las capacidades y limitaciones del modelo y cumplir con sus propias obligaciones regulatorias. Es importante destacar que esta obligación se extiende sin perjuicio de los derechos de propiedad intelectual e industrial y la información empresarial confidencial.

Otra obligación significativa es la de establecer directrices para asegurar el cumplimiento de la legislación de la Unión en materia de derechos de propiedad intelectual, particularmente mediante el uso de tecnologías avanzadas para asegurar el respeto de estos derechos en los términos dispuestos en la Directiva (UE) 2019/790, especialmente en lo relacionado a la minería de textos y datos.

Los proveedores también deben elaborar y publicar un resumen detallado del contenido utilizado para el entrenamiento de los modelos de IA de uso general, según los formatos proporcionados por la Oficina de IA.

Además, se espera que los proveedores de este tipo de tecnologías cooperen con la Comisión y las autoridades competentes en cualquier acción regulatoria relacionada con sus modelos y que sigan las buenas prácticas y normas armonizadas para demostrar el cumplimiento de todas estas obligaciones.

12.2.2. IA de uso general con riesgo sistémico

Los proveedores de modelos de IA de uso general con riesgo sistémico deberán cumplir con las siguientes obligaciones adicionales: (i) evaluar los modelos usando protocolos y herramientas estandarizadas que reflejen el estado actual de la técnica, incluyendo la realización y documentación de pruebas de simulación de adversarios para identificar y minimizar los riesgos sistémicos; (ii) monitorizar, documentar y reportar sin demoras indebidas cualquier incidente grave junto con las medidas correctoras potenciales a la Oficina de IA y, cuando sea necesario, a las autoridades nacionales competentes; (iii) asegurar un nivel adecuado de protección de ciberseguridad tanto para el modelo de IA como para su infraestructura física, lo cual incluye medidas para proteger contra usos malintencionados o ataques que comprometan la integridad y el funcionamiento seguro del modelo; (iv) hasta que se publique una norma armonizada, los proveedores podrán adherirse a códigos de buenas prácticas para demostrar el cumplimiento de estas obligaciones (ver apartado 12.3).

12.3. Códigos de buenas prácticas

El artículo 56 del Reglamento contempla la creación y promoción de códigos de buenas prácticas a nivel de la UE, los cuales serán fundamentales para garantizar que los proveedores de modelos de IA cumplen adecuadamente con las obligaciones impuestas, alineando sus prácticas con los estándares éticos y legales requeridos. La Oficina de IA tendrá un papel clave al fomentar y facilitar la elaboración de estos códigos, asegurándose de que abarquen las obligaciones especificadas en los artículos anteriores, como la adecuada documentación de los modelos y la gestión de riesgos sistémicos.

Los códigos deberán incluir procedimientos y estrategias para mantener la información actualizada con respecto a los avances del mercado y la tecnología, asegurar un nivel adecuado de detalle sobre el contenido utilizado en el entrenamiento de modelos, y definir las medidas para evaluar y gestionar los riesgos sistémicos. Además, deben establecer los métodos de

4 El pasado 29 de mayo de 2024, la Comisión anunció la creación de la Oficina de IA, establecida en el seno de la Comisión Europea. La Oficina de IA tiene como objetivo permitir el desarrollo, la implementación y el uso futuros de la IA de una manera que fomente los beneficios sociales y económicos y la innovación, al tiempo que mitiga los riesgos, y desempeñará un papel clave en la aplicación del Reglamento, especialmente en relación con los modelos de IA de uso general. Puede consultar la nota de prensa publicada en el siguiente enlace: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2982

documentación de estos riesgos y su mitigación, teniendo en cuenta la gravedad, la probabilidad y las dificultades específicas para enfrentarlos.

Una vez que la Comisión apruebe un código de buenas prácticas mediante un acto de ejecución, este obtendrá una validez general dentro de la UE, es decir, los proveedores que se adhieran a un código aprobado tendrán la presunción de cumplimiento de las obligaciones del Reglamento. En caso de que no exista un código de buenas prácticas o si este no se considera adecuado, los proveedores deberán demostrar su cumplimiento por otros medios, los cuales deben ser aprobados por la Comisión.

Los códigos de buenas prácticas incluirán orientación sobre:

1.	2.	3.	4.	5.
La realización de evaluaciones de impacto en la sociedad	La implementación de sistemas de gestión de riesgos	La adopción de medidas de mitigación de riesgos	La documentación y registro de modelos de IA	La cooperación con las autoridades nacionales competentes

Los códigos de buenas prácticas no son vinculantes en sí mismos, pero sirven como guías que los proveedores de sistemas de IA pueden seguir para demostrar el cumplimiento de las regulaciones establecidas en el Reglamento. La adherencia a estos códigos es voluntaria, pero una vez que un proveedor decide seguir un código de buenas prácticas aprobado por la Comisión Europea, se presume que cumple con las obligaciones especificadas en el Reglamento.

13. Medidas de apoyo a la innovación

Como anticipamos en la introducción de este trabajo, la Unión Europea pretende que el Reglamento sirva de impulso a la innovación en IA. Para cumplir tal fin, este marco normativo establece una serie de medidas de apoyo a la innovación, entre las cuales están las siguientes:

***Sandboxes* regulatorios**	La creación de espacios de pruebas controladas para permitir a los proveedores de modelos de IA probar sus innovaciones en un entorno controlado, bajo ciertas condiciones y con la supervisión de las autoridades.
Asesoramiento y Apoyo	Orientación y apoyo por parte de las autoridades competentes a los proveedores y desarrolladores de IA sobre cómo identificar los riesgos para los derechos fundamentales, la seguridad y la salud de los usuarios, cumplir con los requisitos regulatorios y las expectativas en materia de innovación responsable.
Cooperación y trabajo coordinado	Promoción de la cooperación entre las autoridades nacionales competentes, los proveedores de modelos de IA y otras partes interesadas para compartir conocimientos y experiencias.
Financiación	La facilitación del acceso a financiación y programas de apoyo para la investigación y desarrollo de modelos de IA.
Estandarización	La promoción de la estandarización y la certificación de los modelos de IA para garantizar la seguridad y la conformidad con el reglamento.
PYMES	La inclusión de medidas específicas que prestan especial atención a las pequeñas y medianas empresas (PYMES), incluidas las empresas emergentes.

13.1. Sobre los espacios controlados de pruebas para la IA

Los espacios controlados de pruebas (*sandboxes* regulatorios) son entornos seguros y regulados en los que empresas, investigadores y desarrolladores pueden experimentar con nuevos productos, servicios o sistemas de IA sin un estricto cumplimiento de la normativa aplicable, si bien bajo un marco de supervisión específico, durante un periodo limitado y garantizando la existencia de salvaguardias adecuadas. Los Estados miembros deberán asegurar la creación de, al menos,

un *sandbox* regulatorio de IA a la escala nacional, que deberá estar operativo a más tardar dos años después de la entrada en vigor del Reglamento.

Estos espacios están supervisados por las autoridades nacionales competentes y tienen como objetivo:

- **Fomentar la innovación**: proporcionar un entorno donde se pueda innovar con menor riesgo y más libertad, lo que es especialmente útil para PYMES que podrían no tener los recursos para asumir los gastos asociados al cumplimiento de regulaciones complejas y de esta manera facilitar el desarrollo y la implementación de modelos de IA innovadores.

- **Identificar y mitigar riesgos**: permite identificar y abordar posibles problemas de seguridad, privacidad o ética antes de que los productos o servicios sean lanzados al mercado general. Así, el *sandbox* permite a los proveedores demostrar la seguridad y el cumplimiento de sus sistemas de IA, además que facilita la identificación y abordaje de posibles riesgos y problemas antes de la introducción completa en el mercado.

- **Ayudar a los reguladores a entender mejor las nuevas tecnologías y sus implicaciones**: lo que puede influir en la creación de políticas y regulaciones más efectivas y adaptadas a la era digital.

13.2. Medidas dirigidas a proveedores y responsables de PYMES y empresas emergentes (*startups*)

El artículo 62 del Reglamento establece medidas para apoyar a las PYMES y empresas emergentes, enfocándose en el acceso a espacios controlados de pruebas, actividades de formación y sensibilización, comunicación y asesoramiento sobre el Reglamento, y participación en la normalización. Dentro de las medidas contempladas por el regulador se incluyen las siguientes:

- se otorga prioridad en el acceso a espacios de pruebas para PYMES que tengan su domicilio social o sucursal en un país de la UE, cumpliendo ciertas condiciones y criterios de selección.

- se llevarán a cabo actividades de sensibilización y formación específicas sobre la aplicación de este Reglamento, tomando en consideración las necesidades reales de las PYMES y empresas emergentes.

- se prevé la utilización de canales de comunicación para el asesoramiento y para contestar a las dudas planteadas acerca de la aplicación del Reglamento.

- se fomentará la participación de PYMES en el proceso de desarrollo de la normalización.

- se regulan consideraciones especiales en las tasas de evaluación de conformidad según el tamaño y mercado de las PYMES.

- la Oficina de IA se encargará de proporcionar modelos normalizados, mantener una plataforma de información, organizar campañas de comunicación y promover la convergencia en contratación pública de sistemas de IA.

- en el caso de incumplimiento de ciertas disposiciones, las PYMES podrán estar sujetas a multas administrativas, pero se aplicará el porcentaje o el importe menor entre los establecidos, teniendo en cuenta su capacidad económica[5].

13.3. Excepciones para operadores específicos (microempresas)

Ante la crítica de la sobrerregulación que supone el Reglamento para las empresas emergentes, el regulador europeo ha suavizado la carga burocrática para las microempresas[6], quienes pueden simplificar ciertos elementos del sistema de gestión de la calidad requerido por el Reglamento (artículo 17[7]) siempre y cuando no tengan entidades asociadas o vinculadas según dicha Recomendación. Por su parte, la Comisión desarrollará directrices para simplificar estos elementos sin comprometer el nivel de protección o los requisitos exigidos para sistemas de IA de alto riesgo. Tal simplificación no eximirá a las microempresas de cumplir con otros requisitos y obligaciones del Reglamento, incluidos los especificados en los artículos 9 al 15, 72 y 73.

---

5 *Vid.* artículo 99.6 del Reglamento.

6 De conformidad a la definición contemplada en la Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas, disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32003H0361

7 Los proveedores de sistemas de IA de alto riesgo deben establecer un sistema de gestión de la calidad para cumplir con el Reglamento. Este sistema debe documentar políticas y procedimientos incluyendo estrategias de cumplimiento, diseño, desarrollo, pruebas, especificaciones técnicas, gestión de datos y riesgos, vigilancia post-comercialización, notificación de incidentes, y comunicación con autoridades y partes interesadas, adaptándose al tamaño de la organización.

14. Sanciones

El Reglamento establece un sistema de multas en línea con otras normas europeas recientes, como el Reglamento General de Protección de Datos ("**RGPD**"), el Reglamento de Mercados Digitales o el Reglamento de Servicios Digitales, en particular:

Hasta 35 millones de euros o hasta el 7% del volumen de negocios mundial total del ejercicio financiero anterior (si esta cuantía fuese superior)	en caso de no respetar la prohibición de las prácticas de IA a que se refiere el artículo 5.
Hasta 15 millones de euros o hasta el 3% del volumen de negocios mundial total del ejercicio financiero anterior (si esta cuantía fuese superior)	para el incumplimiento de ciertas obligaciones[8] en relación con los operadores o los organismos notificados, distintas de los mencionados en el artículo 5.
Hasta 7.5 millones de euros o hasta el 1% del volumen de negocios mundial total del ejercicio financiero anterior (si esta cuantía fuese superior)	por presentar información inexacta, incompleta o engañosa a organismos notificados o a las autoridades nacionales competentes.
Hasta 1.5 millones de euros	para instituciones, órganos y organismos de la UE: en caso de no respetar la prohibición de las prácticas de IA a que se refiere el artículo 5.
Hasta 750,000 euros	para instituciones, órganos y organismos de la UE: en el caso de incumplimiento de los requisitos u obligaciones establecidos en el reglamento, distintos de los previstos en el artículo 5.
Hasta el 3% del volumen de negocios mundial total del ejercicio financiero anterior o de 15 millones de euros (si esta cifra es superior)	a los proveedores de modelos de IA de uso general por infracciones deliberadas o por negligencia.

15. Entrada en vigor y próximos pasos

Extraoficialmente se ha conocido que el Reglamento se publicará en el Diario Oficial de la Unión Europea a mediados de julio, entrará en vigor 20 días después y será de plena aplicación tras 24 meses, con las siguientes excepciones:

- los capítulos I y II (prohibiciones prácticas) serán aplicables **6 meses** después de la fecha de entrada en vigor del Reglamento;
- los códigos de buenas prácticas deben estar finalizados **9 meses** después de la fecha de entrada en vigor del Reglamento
- el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII (obligaciones para la gobernanza de la IA de uso general) serán aplicables **12 meses** después de la fecha de entrada en vigor del Reglamento, a excepción del artículo 101;
- el artículo 6.1 y las obligaciones para los sistemas de alto riesgo serán aplicables **36 meses** después de la fecha de entrada en vigor del Reglamento.

8. Estas obligaciones son: (i) las contempladas en el artículo 16 para los proveedores de sistemas de IA de alto riesgo; (ii) las obligaciones de los representantes autorizados contempladas en el artículo 22; (iii) las obligaciones de los importadores señaladas en el artículo 23; (iv) las obligaciones de los distribuidores con arreglo al artículo 24; (v) las obligaciones de los responsables del despliegue del artículo 26; (vi) los requisitos y obligaciones de los organismos notificados con arreglo al artículo 31, 33.1, 33.3 y 33.4 o al artículo 34; (vii) las obligaciones de transparencia de los proveedores y usuarios con arreglo al artículo 50.

HITOS RELEVANTES

Entrada en vigor: a los 20 días de su publicación oficial en el DOUE.

- **A los 3 meses**: Comunicación de autoridades nacionales y desarrollo nacional del régimen de sanciones.

- **A los 6 meses**: Prohibición de IA de riesgo inaceptable.

- **A los 9 meses**: Los códigos de buenas prácticas deben estar listos

- **A los 12 meses**: Aplicabilidad a la IA de propósito general.

- **A los 18 meses:** Publicación de directrices de aplicación práctica

- **A los 2 años**:

  - Fecha de aplicación general

  - La Comisión debe evaluar e informar sobre la necesidad de modificar la lista de ámbitos de alto riesgo y, posteriormente, cada 4 años.

- **A los 5 años**: Revisión del Reglamento.

16. Desafíos clave que el reglamento plantea a las empresas

La regulación de la IA presenta importantes desafíos que están en el corazón de las discusiones contemporáneas en tecnología y política regulatoria. Con el Reglamento, los legisladores europeos han optado por una regulación temprana, tratando de anticiparse a posibles usos abusivos de la IA o a tipos de innovación que entienden perjudiciales para la sociedad. No obstante, la propia regulación puede suponer un reto para empresas innovadoras por los cotos y restricciones que les impone, en un plano teórico, en aras de equilibrar el fomento del desarrollo tecnológico con el uso responsable y ético del mismo. Algunos de los desafíos a los que las empresas se enfrentarán en los próximos años serán los siguientes:

- **Adaptación empresarial**: la nueva regulación es extensa y puede tener un amplio margen interpretativo. Las empresas que desarrollen y utilicen sistemas de IA deberán ajustarse a ella, en muchas ocasiones, sin conocer exactamente cómo interpretar y materializar las obligaciones del Reglamento. Comprender la interacción entre el Reglamento y las normas existentes aplicables a la IA, incluyendo sobre protección de datos, propiedad intelectual y gobernanza de datos será también una cuestión clave para las organizaciones. No gestionar correctamente estas interacciones podrá ser una fuente de riesgo significativa para las organizaciones. Por lo tanto, no solo será cuestión del cumplimiento legal, sino que la nueva regulación afectará a la forma en que las organizaciones invierten en innovación, lo cual impactará directamente al negocio.

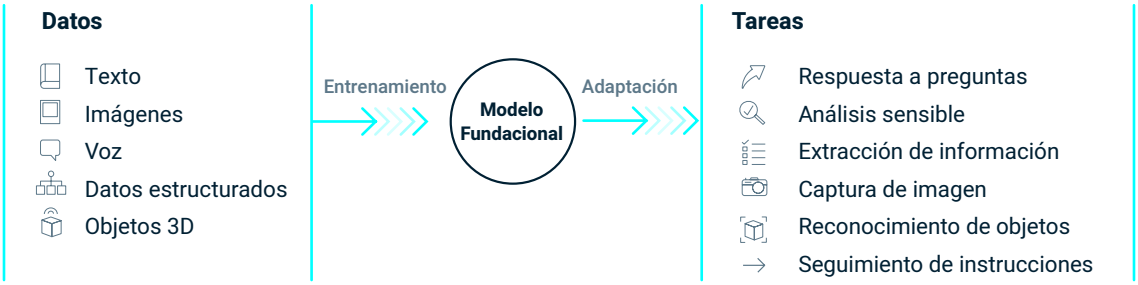
- **Efecto Bruselas**: el regulador europeo ha repetido en el Reglamento el denominado *Efecto Bruselas* del RGPD. Con ello, se pretende imponer a todos los sujetos obligados a cumplir con las obligaciones y principios del Reglamento, con independencia de su país de origen, siempre que dirijan sus productos o servicios a la UE.

- **Evolución tecnológica**: la rápida evolución de la IA plantea el desafío de mantener actualizadas las regulaciones para abordar nuevos desarrollos, con un claro riesgo de obsolescencia de la propia norma.

- **Implementación y cumplimiento**: implementar el Reglamento plantea también desafíos para las autoridades en términos de supervisión y aplicación, requiriendo recursos adecuados como capacitación y herramientas de monitorización.

17. ¿Qué deben hacer las empresas a partir de ahora?

Los sistemas de IA más recientes, en especial la IA generativa, que permite el desarrollo de textos, vídeos o imágenes sintéticas, están basados en la arquitectura *transformer*, la cual se basa en modelos fundacionales, denominados por el Reglamento "*modelos de IA de uso general*". Estos modelos se diferencian de los propios sistemas de IA en la autonomía y capacidad de influir estos últimos en entornos físicos o virtuales, presentando los "*modelos de IA de uso general*" un grado considerable de generalidad y siendo capaces 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.



Teniendo en cuenta la gran potencialidad de los "*modelos de IA de uso general*", el legislador europeo ha entendido necesario dedicar un capítulo (arts. 51 a 56) íntegramente a ellos, con obligaciones específicas para sus proveedores (analizadas en el apartado 12.2), entre otras, las siguientes:

1) Nombrar a un representante autorizado que esté establecido en la UE, en caso de que el proveedor se encuentre en un tercer país.

2) Elaborar y mantener actualizada documentación técnica del modelo, incluyendo a su proceso de entrenamiento y realización de pruebas y los resultados de la evaluación, la cual debe estar disponible, en caso de solicitud, a la Oficina de IA y de las autoridades nacionales competentes.

3) Elaborar y mantener actualizada información y documentación para su facilitación a quienes quieran integrar el modelo de IA de uso general en sus sistemas de IA. Aunque el Reglamento no especifica qué información deben facilitar estos proveedores, establece que debe ser suficiente para que los proveedores de sistemas de IA entiendan las capacidades y limitaciones de dicho modelo de IA de uso general.

4) Preparar un protocolo para asegurar el respeto de la normativa de derechos de propiedad intelectual, en concreto respecto del mecanismo de *op-out* del artículo 4, apartado 3, de la Directiva (UE) 2019/790.

5) Facilitar públicamente información sobre el contenido utilizado por entrenar el modelo de IA de uso general, siguiendo el formato proporcionado por la Oficina de IA.

6) En caso de ser un modelo de IA de uso general con riesgo sistémico, por su gran impacto, deberá cumplir los siguientes requisitos adicionales:

   a) notificarlo a la Comisión Europea sin demora desde que se sepa que va a cumplirse dicho requisito;

   b) evaluar el modelo, incluyendo la realización y documentación de pruebas de simulación de adversarios para detectar y reducir el riesgo sistémico;

   c) vigilar y, en su caso, comunicar la existencia de incidentes graves y las posibles medidas correctoras; y

   d) establecer un nivel adecuado de protección de la ciberseguridad.

Estas obligaciones deberán ser respetadas únicamente por los modelos de IA de uso general. Este enfoque selectivo subraya la importancia de la reciente aprobación del Reglamento, que marca un hito en la regulación de esta tecnología emergente, y afectará, de una u otra forma, a cualquier empresa usuaria de un sistema de IA. Este nuevo contexto legal impone desafíos significativos, pero también oportunidades, que para que puedan ser aprovechadas requerirán de un conocimiento profundo de la nueva normativa y la manera en que puede afectar a las organizaciones y los individuos.

A continuación, presentamos una serie de acciones prácticas recomendadas para navegar con éxito en este nuevo escenario regulatorio, garantizando que la implementación y el uso de la IA se realicen de manera ética, segura y conforme a la ley.

Desde la perspectiva de los implementadores o usuarios profesionales, proponemos la adopción de las siguientes medidas:

- **Evaluar el impacto de la nueva regulación**: entendemos esencial evaluar el impacto de la nueva regulación de IA cuanto antes para entender cómo afectará a la organización y sus operaciones. Es muy probable que el ciclo de vida de las tecnologías de IA que se implementen o desarrollen a partir de la entrada en vigor del Reglamento sea superior en los dos próximos años (fecha efectiva de aplicación en la mayoría de los casos); esperar hasta entonces podría poner en riesgo las inversiones y dañar reputacionalmente a la organización.

- **Identificar áreas de la organización afectadas y diseñar un modelo de gobernanza**: será necesario determinar qué actores internos se verán afectados por la implementación de sistemas de IA y cómo. Esto nos llevará a poder diseñar un modelo de gobernanza que ayude a actuar de manera coordinada y consistente en este ámbito, equilibrando los aspectos de cumplimiento con el enfoque de negocio.

- **Desarrollar un plan de formación**: poner el foco en la formación y sensibilización en las fases iniciales ayudará a interpretar mejor el impacto de la nueva regulación en las distintas áreas y a conseguir el mejor resultado posible derivado del nuevo contexto. La formación debería poner foco no solo en los aspectos de cumplimiento meramente formal sino también en la perspectiva ética y reputacional, así como en el propio uso responsable y eficiente de esta tecnología, ayudando de esta forma a la minimización de riesgos en un sentido amplio. Es necesario un plan de choque inicial pero también diseñar y poner en marcha un plan de formación continua que permita a la organización mantenerse actualizada ante los previsibles cambios de negocio, tecnológicos y legales, a la vez que se mantienen en el tiempo los estándares necesarios de conocimiento y sensibilización.

- **Integrar el marco legal en los procesos de innovación (*legal by design*)**: será necesario integrar el nuevo marco legal en los procesos de innovación desde el principio para asegurar el cumplimiento desde el diseño de los sistemas de IA. Por otra parte, el nuevo Reglamento es una de las muchas normas que impacta en el ámbito digital. Diseñar un modelo de datos suficientemente adaptable a cambios regulatorios y que permita implementar distintas capas de cumplimiento ayudará a mejorar la eficiencia de los procesos y sistemas de la organización.

- **Hacer un inventario de soluciones basadas en IA**: realizar un inventario de todas las soluciones basadas en IA utilizadas por la organización y clasificar su nivel de riesgo no es solo un requisito para el cumplimiento legal, sino una herramienta estratégica que permitirá a las organizaciones gestionar riesgos, optimizar recursos, y mantenerse ágiles y responsables en un panorama tecnológico complejo y en constante evolución.

- **Preparación de políticas de IA específicas**: estas políticas deberían abarcar diversos aspectos del ciclo de vida y uso de la IA, asegurando que todas las actividades relacionadas se realicen de manera ética, segura y conforme a la ley (de uso, desarrollo, adquisición, de protección de datos, de auditoría y cumplimiento).

- **Mapear riesgos y evaluar umbrales aceptables**: este proceso implica identificar, analizar y priorizar los riesgos asociados con el uso y desarrollo de la IA, así como establecer límites claros sobre lo que se considera un nivel aceptable de riesgo. Este enfoque proactivo hacia la gestión de riesgos será esencial para fomentar la confianza y asegurar el éxito a largo plazo en el uso de tecnologías de IA.

- **Adaptar los procesos de contratación con proveedores de IA**: será necesario adecuar los modelos contractuales para asegurar que los proveedores de IA cumplan con el nuevo Reglamento, actualizar los procesos de homologación y desarrollar mecanismos de gestión del riesgo de terceros en este ámbito. Algunas de las acciones clave en este ámbito serán: la definición de requisitos específicos, los procedimientos de evaluación, los criterios de negociación, la gestión de los derechos intangibles, o la capacitación de las áreas de compras y negociadores contractuales.

- **Revisión y actualización de pólizas de seguros en relación con el uso y desarrollo de sistemas de IA**: el primer paso será realizar una evaluación detallada de los riesgos asociados al uso y desarrollo de sistemas de IA. Esto incluye riesgos técnicos, como fallos de *software* o brechas de seguridad, así como riesgos legales y éticos, como violaciones de privacidad o responsabilidad por decisiones automatizadas. Con base en la evaluación de riesgos, se debería revisar la cobertura de seguros existente para identificar posibles brechas o exclusiones que podrían dejar a la organización expuesta a riesgos relacionados con la IA. A partir de ahí, se debería trabajar con aseguradoras para desarrollar o ajustar pólizas que aborden específicamente los riesgos asociados con la IA. Esto puede incluir coberturas para errores y omisiones en el desarrollo de *software*, responsabilidad por productos defectuosos, violaciones de datos y otros riesgos específicos de la tecnología.

- **Evaluar el impacto en los derechos fundamentales**: la IA tiene el potencial de influir significativamente en varios derechos fundamentales, incluyendo la privacidad, la no discriminación, la libertad de expresión, y el derecho a una valoración y toma de decisiones justa. Al igual que el RGPD exige en determinados casos la elaboración de una EIPD (Evaluación de Impacto de la Protección de Datos), las organizaciones deberán desarrollar con el nuevo Reglamento sus modelos de EIDH (Evaluación de Impacto de los Derechos Humanos).

- **Adaptar la organización al conjunto de requerimientos del Reglamento de IA**: teniendo en cuenta los plazos de efectividad marcados por el Reglamento, será necesario desarrollar y poner en marcha un plan completo de adecuación. Algunas acciones dependen de actos de implementación que irán siendo acometidos por las administraciones públicas a lo largo de los próximos dos años y por tanto no serán ejecutables desde el principio. No obstante, es clave diseñar una estrategia

Pérez-Llorca

TECHLAW

Inteligencia artificial

JUNIO 2024

Un reto para las compañías y para los reguladores

Barcelona
-
Brussels
-
Lisbon
-
London
-
Madrid
-
New York
-
Singapore

perezllorca.com

al respecto y coordinar el calendario de adecuación con el conjunto de decisiones tecnológicas y de negocio que la organización tenga previsto desarrollar en este ámbito.

- **Analizar los datos utilizados para entrenar modelos de IA de uso general**: dadas las obligaciones de transparencia que establece el Reglamento sobre los *datasets* utilizados para entrenar un modelo de lenguaje de gran escala o un modelo fundacional, las empresas que usen sistemas de IA, especialmente la generativa, deberán asegurarse de que los mismos han sido entrenados con datos que no infringen derechos de terceros y que son suficientes para cumplir las obligaciones de respecto a los derechos fundamentales de los ciudadanos. Dicho análisis deberá ser debidamente documentado para mostrarse a la Oficina de IA en caso de ser requerido.

- **Desarrollo de mecanismos para la protección de activos intangibles**: este aspecto es especialmente relevante tanto en el desarrollo interno de sistemas de IA como en la adquisición de soluciones de terceros, incluyendo escenarios híbridos y aquellos que involucren *software* libre o licencias abiertas. En muchos casos, la protección del intangible solo se podrá llevar a cabo apoyándose en la legislación de protección de secretos empresariales. Esta normativa es especialmente rigurosa a la hora de evaluar los mecanismos de protección implementados desde las etapas más iniciales de conceptualización de la solución que se pretenda proteger. También es clave evaluar qué pasos se van a dar para evitar caer en infracciones de derechos de terceros en procesos como el entrenamiento de herramientas de IA o en el llamado *fine tunning*, entre otros.

- **Monitorizar desarrollos legales y reglamentarios**: mantenerse actualizado sobre los desarrollos legales y reglamentarios para adaptarse a cualquier cambio en la legislación de IA.

- **Participar en el diseño de buenas prácticas**: recomendamos participar sectorialmente en el diseño de buenas prácticas para compartir conocimientos y experiencias con otras organizaciones. El Reglamento de IA es una norma muy transversal y llena de conceptos abiertos a la interpretación. La verticalización por sectores de actividad, casos concretos de uso o tecnologías a través de la definición de estándares jurídico-técnicos y buenas prácticas puede ayudar a incrementar el grado de seguridad jurídica en este ámbito, facilitando las inversiones y el soporte a la innovación, al tiempo que se mantiene el necesario equilibrio con las garantías que requiere la regulación.

- **Desarrollo de un modelo y plan de auditoría adaptado**: este enfoque permitirá evaluar de manera efectiva el cumplimiento de los sistemas de IA con las regulaciones aplicables, las normas éticas y los requisitos de seguridad. Al adoptar un enfoque sistemático y basado en evidencia, las organizaciones podrán demostrar su compromiso con la responsabilidad y la excelencia en la implementación de IA.

Estas son solo algunas de las acciones que las empresas usuarias de sistemas de IA pueden llevar a cabo en la actualidad para realizar una sosegada transición al cumplimiento del Reglamento de IA, con una percepción positiva y posibilista de esta nueva tecnología, que no dudamos que provocará significativos cambios en la sociedad y en la empresa.