El marco regulatorio en materia de inteligencia artificial.

Concepto.

La inteligencia artificial es una tecnología disruptiva con una alta capacidad de impacto en la economía y la sociedad. En el plano económico, y junto a otras tecnologías digitales, presenta un alto potencial para el aumento de la productividad, la apertura de nuevas líneas de negocio, el desarrollo de nuevos productos o servicios –basados, por ejemplo, en la personalización, la optimización de los procesos industriales o las cadenas de valor–, la mejora en la facilidad de realización de tareas cotidianas, la automatización de ciertas tareas rutinarias y el desarrollo de la innovación. Este potencial incide positivamente en el crecimiento económico, la creación de empleo y el progreso social.

No obstante, los sistemas de inteligencia artificial también pueden suponer riesgos sobre el respeto de los derechos fundamentales de la ciudadanía, como por ejemplo los relativos a la discriminación y a la protección de datos personales, o incluso causar problemas graves sobre la salud o la seguridad de la ciudadanía.

El Reglamento define *Sistema de Inteligencia Artificial* como aquel que opera con elementos de autonomía y que, basándose en datos y entradas obtenidos de humanos o máquinas, infiere como alcanzar unos objetivos propuestos, usando para ello técnicas basadas en el aprendizaje-máquina o en lógica y conocimiento, y genera como salida contenidos, predicciones, recomendaciones o decisiones que influyen en el entorno con el que el sistema interactúa.

«Sistema de inteligencia artificial (sistema de IA)»: *el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa.* (art.3 RIA).

Ámbito de Aplicación.

El Reglamento (art.2 RIA) afecta principalmente a las empresas que desarrollan sistemas de IA y los lanzan al mercado, pero también a quienes utilizan herramientas de IA para actividades que no sean puramente personales, y por otro lado la regulación también afecta a los Estados en términos del uso que hagan de la IA en la prestación de servicios públicos, el control de fronteras, la persecución de delitos y otros campos. Las obligaciones no se limitan a los proveedores de sistemas de IA, sino que alcanzan también, entre otros, a quienes utilizan sistemas de IA para fines profesionales, que reciben el nombre de "responsables del despliegue" (en este sentido es "usuario del sistema IA"). Por ejemplo, una entidad financiera, que use tecnologías de inteligencia artificial (podríamos pensar en fintech, *robadvisor,* o procesos), estaría sujeta a las obligaciones del RIA, porque encajaría en la figura de "responsable del despliegue", al utilizar sistemas con componentes de inteligencia artificial bajo su propia autoridad. (En otros casos, podría ser incluso "proveedor" si, por ejemplo, pone su nombre o marca comercial a un sistema de inteligencia artificial calificado de alto riesgo o si lo modifica sustancialmente). Otros sujetos contemplados en el artículo 2 son el importador y el distribuidor.

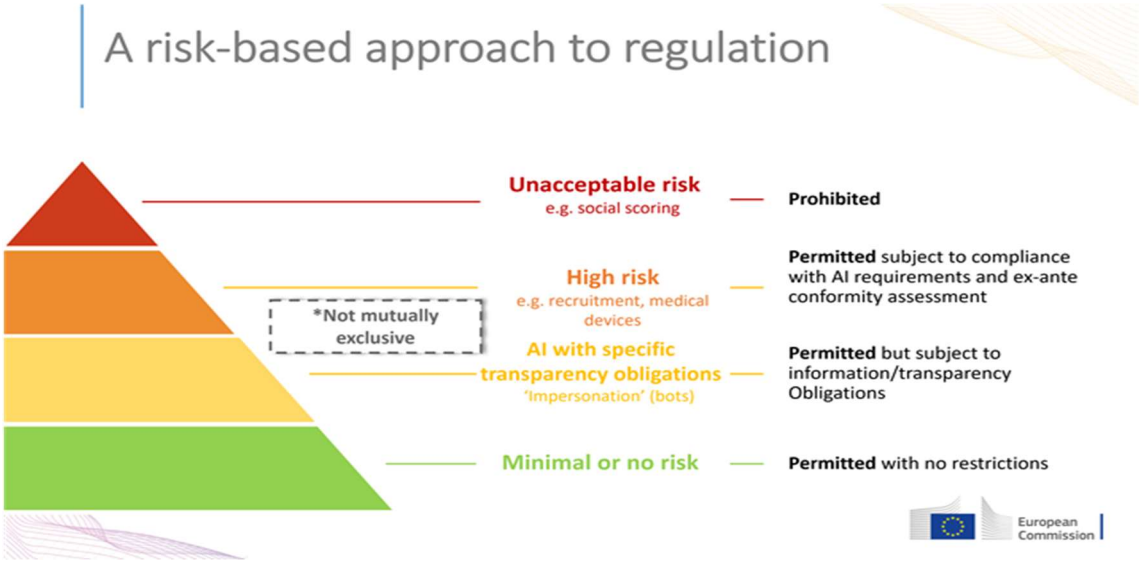
El ámbito de aplicación del Reglamento se extiende más allá de las organizaciones establecidas en la Unión Europea, alcanzando también a aquellas que utilicen Inteligencia Artificial en el mercado europeo. Esto implica que, también deberán aplicarlo las numerosas multinacionales, con presencia o interacciones comerciales en la UE.

El Reglamento no es aplicable a autoridades de terceros países ni a organizaciones internacionales cuando utilicen sistemas IA en el ámbito de la cooperación policial o judicial con la UE o sus estados miembros. Tampoco se aplica a los sistemas de uso militar o utilizados en el contexto de la seguridad nacional, ni a los utilizados con el solo propósito de la investigación y el desarrollo científico.

Enfoque basado en el riesgo.

El Reglamento sigue un enfoque basado en el riesgo, lo que significa que cuanto mayor es el riesgo de causar daño a la sociedad por la utilización de un sistema de IA, más estrictas son las normas que se aplicarán al mismo.

El Reglamento establece una jerarquía de riesgos en función del uso de la IA y sobre las categorías detectadas, establece una serie de obligaciones.



El Reglamento enumera y describe este conjunto, que incluye, entre otros, sistemas de identificación biométrica, de protección de infraestructuras críticas, de selección y promoción de personal, de utilización en fronteras, o los usados por las Fuerzas y Cuerpos de Seguridad del Estado o la Administración de Justicia.

La Comisión puede actualizar esta lista mediante un acto delegado. Por otro lado, existen productos que ya están regulados por normativa armonizada de la UE, y que bajo esa normativa están sujetos a evaluación de conformidad. Hay un conjunto limitado de familias de estos productos, que incluye entre otros los dispositivos médicos, los trenes o la maquinaria. Un sistema IA que constituya uno de estos productos, o constituya un componente de seguridad de uno de estos productos, estará sujeto a su correspondiente normativa armonizada.

En el Título II se establece una **lista de IA prohibidas**. El Reglamento prohíbe determinadas prácticas (artículo 5) que se consideran de riesgo inaceptable para los ciudadanos y para el conjunto de la sociedad. Por ejemplo, crear bases de datos de reconocimiento facial a partir de la extracción indiscriminada de imágenes de internet, evaluar o clasificar a las personas a lo largo del tiempo por su comportamiento social o sus características personales, o bien explotar las vulnerabilidades de una persona o grupo con la intención de causar daño.

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

La legislación vigente en materia de protección de datos, protección de los consumidores y servicios digitales, que garantiza que las personas físicas sean debidamente informadas y puedan decidir libremente no ser sometidas a la elaboración de perfiles u otras prácticas que puedan afectar a su conducta, podría cubrir otras prácticas de manipulación o de explotación contra adultos que los sistemas de IA pueden facilitar. Se prohíbe igualmente que las autoridades realicen calificación social basada en IA con fines generales. Por último, también se prohíbe, salvo excepciones limitadas, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley (sin perjuicio de que haya excepciones -Anexo II-, por ejemplo, búsqueda selectiva de víctimas, trata de seres humanos, o de personas desaparecidas, o bien prevención de amenaza específica inminente, o atentado terrorista, o identificación de personas en el contexto de determinados delitos).

La regulación se centra en los **sistemas de IA que considera de alto riesgo** (apartado 1 del artículo 6 y Título III). Por ejemplo, en relación con el acceso a servicios esenciales (públicos o privados) o con la categorización biométrica de las personas, entre otros supuestos y exige transparencia con respecto a los contenidos creados o manipulados con herramientas de IA o a los sistemas de reconocimiento de emociones. Por ejemplo, se consideran sistemas de IA de alto riesgo (según art. 6.2 y Anexo III del Reglamento) los que tengan impacto en las relaciones laborales y la gestión de los procesos de recursos humanos en todo el ciclo vital del empleado (selección; contratación; desempeño; retribución; formación; o desvinculación).

Son los que enumera el **Anexo III**, que los clasifica en las categorías que se enumeran a continuación, cuando la salida que producen sea relevante en una decisión con posible riesgo sobre la salud, la seguridad o los derechos fundamentales.

a) Sistemas de identificación biométrica (los que identifiquen personas sin su participación activa, recordando la prohibición existente para las fuerzas y cuerpos de seguridad mencionada antes.

b) Gestión de infraestructuras críticas (como el tráfico, la electricidad o el agua).

c) Educación y formación profesional (como gestión del acceso a la educación o planificación del desarrollo académico).

d) Selección de personal y gestión de las relaciones laborales.

e) Gestión del acceso de las personas a servicios esenciales públicos y privados (como beneficios sociales, servicios de emergencia, crédito o seguros).

f) Actividades de fuerzas y cuerpos de seguridad (como valoración de pruebas o de sospechosos).

g) Migración, asilo y control de fronteras (como polígrafos, o valoración de solicitudes).

h) Administración de justicia y procesos democráticos.

No se considerarían de alto riesgo (conforme al apartado 3 del artículo 6) si se certifica que el sistema que no implica ningún riesgo para la salud, la seguridad o los derechos fundamentales asociado al sistema de IA de alto riesgo de que se trate...

Así será cuando se cumplan una o varias de las condiciones siguientes:

a) que el sistema de IA tenga por objeto llevar a cabo una tarea de procedimiento limitada;

b) que el sistema de IA tenga por objeto mejorar el resultado de una actividad humana previamente realizada;

c) que el sistema de IA tenga por objeto detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la evaluación humana previamente realizada sin una revisión humana adecuada, ni a influir en ella; o d) que el sistema de IA tenga por objeto llevar a cabo una tarea preparatoria para una evaluación pertinente a efectos de los casos de uso enumerados en el anexo III.

Pues bien, los sistemas de alto riesgo deberán cumplir con los **requisitos (arts. 8-15) y obligaciones (art.16-29)**, así por ejemplo deben evaluar y reducir los riesgos, mantener registros de uso, ser transparentes y precisos y contar con supervisión humana. Los ciudadanos tendrán derecho a presentar reclamaciones sobre los sistemas de IA y a recibir explicaciones sobre las decisiones basadas en ellos que afecten a sus derechos. Además, las obligaciones relativas a la realización de pruebas ex ante, la gestión de riesgos y la vigilancia humana contribuirán a reducir al mínimo el riesgo de adoptar decisiones asistidas por IA erróneas o sesgadas en esferas críticas como la educación y la formación, el empleo, servicios importantes, la aplicación de la ley y el poder judicial. En caso de que se sigan produciendo violaciones de los derechos fundamentales, la transparencia y la trazabilidad garantizadas de los sistemas de IA, unidas a unos controles ex post sólidos, permitirán ofrecer a las personas afectadas una compensación efectiva.

En el capítulo 2 del Título III se establecen los requisitos legales que deben cumplir los sistemas de IA de alto riesgo en lo que respecta a los datos y su gobernanza, la documentación y el registro, la transparencia y la comunicación de información a los usuarios, la vigilancia y supervisión humana, la solidez, la precisión y la ciberseguridad.

En el capítulo 3 se impone un conjunto claro de obligaciones horizontales a los proveedores de sistemas de IA de alto riesgo. También se establecen obligaciones proporcionadas para los usuarios y otros participantes de la cadena de valor de la IA (p. ej., los importadores, los distribuidores y los representantes autorizados).

Transparencia.

El título IV se centra en determinados sistemas de IA para tener en cuenta los riesgos específicos de manipulación que conllevan. Se aplicarán obligaciones de transparencia a los sistemas que; a) interactúen con seres humanos, b) se utilicen para detectar emociones o determinar la asociación a categorías (sociales) concretas a partir de datos biométricos, o c) generen o manipulen contenido (*ultrafalsificaciones*). Cuando una persona interactúe con un sistema de IA o sus emociones o características sean reconocidas por medios automatizados, es preciso informarle de tal circunstancia. Si un sistema de IA se utiliza para generar o manipular imágenes, audios o vídeos que a simple vista parezcan contenido auténtico, debe ser obligatorio informar de que dicho contenido se ha generado por medios automatizados, salvo excepciones que respondan a fines legítimos (aplicación de la ley, libertad de expresión). De este modo, las personas pueden adoptar decisiones fundamentadas o evitar una situación determinada.

Transparencia RIA vs Transparencia RGPD.

Como ha señalado la AEPD, el concepto de "transparencia RIA" difiere del mismo término establecido en el RGPD, cuyo ámbito material son los tratamientos de datos personales. Transparencia en el marco de ambos reglamentos implica a distintos actores, a diversa información y destinada a diferentes destinatarios.

El principio de transparencia del RGPD se establece en el artículo 5.1.a), se desarrolla en los considerandos 39 y del 58 al 62, y se detalla en el artículo 12 y siguientes. La aplicación del principio de transparencia del RGPD es una obligación impuesta a los responsables del tratamiento de datos personales para advertir a los interesados de su impacto.

"Transparencia RIA" se aplica a los sistemas de IA, mientras que "Transparencia RGPD" aplica a los tratamientos de datos personales definidos en el artículo 2 y en el artículo 4.2 del RGPD. Un sistema de IA puede ser uno de los medios utilizados para llevar a cabo una o varias operaciones dentro de un tratamiento. Por lo general, un tratamiento de datos personales se implementa a través de varios tipos de sistemas, como sistemas en la nube, sistemas de comunicación, sistemas móviles, sistemas de cifrado, etc. y algunos de ellos podrían ser sistemas de IA.

Cuando los sistemas de IA se incluyen en, o son medios de, un tratamiento de datos personales los responsables del tratamiento deben obtener información sobre ellos suficiente para cumplir sus diferentes obligaciones de cumplimiento RGPD. Estas incluyen la transparencia para permitir el ejercicio de los derechos, cumplir el principio de responsabilidad activa, cumplir los requisitos de las Autoridades de Supervisión del RGPD en relación con sus poderes de investigación, y lo mismo para los organismos de certificación y supervisión del código de conducta.

Resto de sistemas de IA.

A los demás sistemas de IA que no son de alto riesgo tan solo se les imponen obligaciones limitadas en materia de transparencia; por ejemplo, en lo que se refiere a la presentación de información para comunicar el uso de un sistema de IA cuando este interactúe con humanos.

El título IX crea un marco para la elaboración de códigos de conducta, cuyo objetivo es fomentar que los proveedores de sistemas de IA que no son de alto riesgo cumplan de manera voluntaria los requisitos que son obligatorios para los sistemas de IA de alto riesgo (que se definen en el título III). Los proveedores de sistemas de IA que no son de alto riesgo podrían crear y aplicar sus propios códigos de conducta. Estos códigos también podrían incluir compromisos voluntarios relativos, por ejemplo, a la sostenibilidad medioambiental, la accesibilidad para las personas con discapacidad, la participación de las partes interesadas en el diseño y el desarrollo de sistemas de IA, y la diversidad de los equipos de desarrollo.

Fomento de la innovación.

Con el objetivo de reforzar la competitividad europea en el ámbito de la IA, se habilita un espacio controlado de pruebas orientado a ofrecer un entorno controlado para desarrollar, probar, y validar sistemas de IA innovadores en condiciones reales. Con el Reglamento, se busca establecer normas comunes para la creación de un *sandbox* y un marco para la cooperación entre las autoridades de supervisión implicadas. No obstante, serán las autoridades de supervisión locales quienes determinarán los requisitos concretos para el acceso a los *sandbox*.

En España, el Real Decreto 817/2023, de 8 de noviembre, tiene como objeto la creación del primer entorno controlado de para ensayar la aplicación de ciertos requisitos previstos en el

Reglamento. Los resultados obtenidos del entorno controlado de pruebas podrían ser el punto de partida para una futura plataforma de software que facilite una primera autoevaluación no vinculante sobre el cumplimiento de los principios de la propuesta del Reglamento de Inteligencia Artificial.

Gobernanza.

Existirán al menos una autoridad nacional notificante (art. 30) y al menos una autoridad de supervisión de mercado como autoridades nacionales competentes para los propósitos del Reglamento.

Las autoridades de supervisión de mercado monitorizarán el correcto funcionamiento, ya en mercado, de sistemas de IA de alto riesgo, identificando riesgos sobrevenidos, incidentes u otras situaciones que exijan tomar medidas sobre los sistemas de IA de alto riesgo.

A nivel europeo, se constituirá un Comité Europeo de Inteligencia Artificial, donde participará un representante de cada Estado miembro. El Comité orientará sobre la implementación del reglamento, elaborará guías y establecerá las reglas básicas para elaborar *sandboxes.*

El 24 de enero de 2024 se publicó una Decisión de la Comisión por la que se creará una Oficina Europea de Inteligencia Artificial como parte de la estructura administrativa de la Dirección General de Redes de Comunicación, Contenido y Tecnologías. La Oficina tendrá principalmente un papel de apoyo en lo que respecta a la aplicación de las normas sobre sistemas de IA, ya que la mayor parte de las competencias recaerán en las autoridades nacionales.

En España, se ha creado a tal efecto Agencia Española de Supervisión de la Inteligencia Artificial ("AESIA"), con sede en La Coruña. La Agencia será una entidad de derecho público adscrita a la Secretaría de Estado de Digitalización e Inteligencia Artificial. Su función principal será la de llevar a cabo tareas de supervisión, asesoramiento, concienciación y formación, a empresas públicas y privadas para la adecuada implementación de la normativa entorno al adecuado uso de la IA y concretamente de los algoritmos.

De hecho la **AEPD** y la **AESIA** son las agencias que supervisarán la Inteligencia Artificial en España.

El papel de la AEPD es relevante puesto que el uso de tecnología de esta índole implica en muchas ocasiones también el tratamiento de datos personales, la AEPD y la AESIA colaborarán y trabajarán mano a mano para el cumplimiento del Reglamento de la Inteligencia Artificial y del Reglamento General de Protección de Datos (RGPD), cuya vigilancia corresponde a la AEPD.

A este respecto, cabe considerar que la IA no crea nuevos problemas relacionados con la protección de datos sino que los hace más complejos (recopilación de datos, tratamientos masivos, exactitud, transparencia, etc), facilita la vigilancia masiva y plantea dificultades en la revisión de las decisiones por la opacidad de los algoritmos y la recopilación de nuevos datos.

Régimen sancionador.

Las sanciones por el incumplimiento del Reglamento podrán alcanzar hasta los 35 millones de euros o el 7% del volumen de negocio global del ejercicio anterior. Las sanciones se graduarán en función de la gravedad de la infracción cometida. El Reglamento impone a los Estados establecer las normas y procedimientos sancionadores para garantizar su correcto cumplimiento.

Entrada en vigor y aplicación directa.

En su reunión del 21 de mayo, el Consejo de la UE ha ratificado definitivamente la aprobación del Reglamento de inteligencia artificial (IA) propuesto por la Comisión y ya aprobado por el Parlamento el pasado mes de marzo, tras el período final de negociaciones del segundo semestre de 2023 y tras la corrección de errores de la Posición del Parlamento Europeo aprobada el 13 de marzo de 2024, conocida del pasado 16 de abril. Finalmente se publica el DOUE de 12 de julio de 2024.

Hay que matizar que, al margen de su fecha de entrada en vigor, el Reglamento será directamente aplicable dos (2) años después de su entrada en vigor, aunque ciertas disposiciones, como las relativas a los sistemas de IA prohibidos y de propósito general, tendrán unos periodos más cortos, de seis (6) y doce (12) meses respectivamente.

Entrará en vigor veinte días después de su publicación en el Diario Oficial y será de plena aplicación veinticuatro meses después de su entrada en vigor, con excepción de las prohibiciones de prácticas (se aplicarán seis meses después de la fecha de entrada en vigor); los códigos de buenas prácticas (nueve meses después); las normas sobre la IA de uso general, incluida la gobernanza (doce meses después), y las obligaciones para los sistemas de alto riesgo (treinta y seis meses después).

Nótese que la propuesta de Reglamento se inició en el mes de abril de 2021, antes de que se hablase de la existencia de ChatGPT, y 3 años después se acaba de aprobar, pero no será totalmente aplicable hasta dentro de 24 meses…. En este sentido, ante el riesgo de "obsolescencia regulatoria prematura" hay expertos en regulación que defienden que el cambio de paradigma exige procesos normativos mucho más ágiles y marcos regulatorios dinámicos, que sean capaces de adaptarse a los eventuales cambios de circunstancias que puedan producirse. Desde este punto de vista se considera que la revolución digital y tecnológica provoca que la realidad sea cada vez menos estable y predecible y, sin embargo, nuestros procedimientos para hacer normas, ya sea a nivel nacional o comunitario, resultan cada vez más largos.

Legislación complementaria.

La Legislación complementaria incluiría la Directiva de Responsabilidad de la IA, y la mencionada Oficina de IA de la UE, cuyo objetivo es racionalizar la aplicación de las normas, así como la regulación sobre daños causados por productos defectuosos.

Cabe traer a colación la Propuesta de revisión de la Directiva 85/374/CEE en materia de responsabilidad por los daños causados por productos defectuosos. Esta Directiva, no incluía los productos derivados de los Sistemas de Inteligencia Artificial (responsabilidad por defectos en actualizaciones de software, algoritmos de aprendizaje automático o servicios digitales esenciales para el funcionamiento de un producto). Por este motivo se está revisando la Directiva para garantizar que las nuevas normas sobre responsabilidad por productos defectuosos se adapten a los nuevos tipos de productos derivados del uso de la Inteligencia Artificial.

En cuanto a la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA). Tiene como objetivo una IA fiable garantizando que los perjudicados por daños causados por la IA obtengan una protección en materia de responsabilidad civil equivalente a la de los perjudicados por daños causados por otros productos. Se aplicará en demandas civiles de responsabilidad extracontractual por daños

y perjuicios causados por un sistema de IA, cuando dichas demandas se interpongan en el contexto de la responsabilidad por culpa o negligencia.

Salvo mejor opinión

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

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L_202401689

[UE] Informe sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial). https://www.europarl.europa.eu/doceo/document/A-9-2023-0188_ES.html

[BOE] Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2023-22767