Los sujetos obligados en el Reglamento UE de inteligencia artificial[1]

Obliged parties in the EU regulation on artificial intelligence

Moisés Barrio Andrés

Letrado del Consejo de Estado. Doctor en Derecho. Profesor de Derecho Digital. Director del Diploma de Alta Especialización en Legal Tech y transformación digital (DAELT) de la Escuela de Práctica Jurídica de la Universidad Complutense de Madrid

ORCID ID: 0000-0002-2877-5890

Recibido:03.06.2025 / Aceptado:30.06.2025

DOI: 10.20318/cdt.2025.9871

Resumen: El Reglamento europeo de inteligencia artificial establece retos normativos sin precedentes para todas las categorías de agentes del mercado. La forma en que el RIA afectará a las entidades depende de varios factores, como el tipo de entidad, las posibles modificaciones del sistema de IA, las exclusiones, las prohibiciones, etc. Este artículo se centra en la cuestión de quiénes son los verdaderos destinatarios de las obligaciones y cómo pueden las entidades –sean privadas o públicas– establecer con certeza qué categorías de obligaciones les son aplicables.

Palabras clave: Inteligencia artificial; Reglamento UE de inteligencia artificial; Reglamento (UE) 2024/1689; RIA; Derecho digital.

Abstract: The EU AI Act sets unprecedented regulatory challenges for all categories of market players. How the AI Act will affect entities depends on a number of factors, such as the type of entity, possible changes to the AI system, exclusions, prohibitions and so on. This article focuses on the question of who the actual addressees of the obligations are and how entities - whether private or public - can establish with certainty which categories of obligations apply to them.

Keywords*:* Artificial intelligence; EU Regulation on artificial intelligence; Regulation (EU) 2024/1689; AI Act; Digital law.

[1] Este trabajo se realiza en el marco del Proyecto "Privacidad y carpeta de identidad digital europea" (PID2023-150123OB-I00) (EUDIWAPRY), correspondiente a la convocatoria 2023 de ayudas a «Proyectos de Generación de Conocimiento» y a actuaciones para la formación de personal investigador predoctoral asociadas a dichos proyectos, en el marco del Programa Estatal para Impulsar la Investigación Científico-Técnica y su Transferencia, del Plan Estatal de Investigación Científica, Técnica y de Innovación 2021-2023, cofinanciado por la Unión Europea.

I. Introducción

1. El Reglamento Europeo de IA (RIA en lo sucesivo)[2] es una de las normas jurídicas más importantes de la historia del Derecho digital reciente[3]. Se trata de una norma horizontal *ex ante* que adopta un enfoque basado en la seguridad de los productos y el nivel de riesgo para regular la inteligencia artificial (IA). En lugar de asignar fuertes derechos individuales, el RIA pretende impedir el desarrollo y la distribución de sistemas y modelos de IA arriesgados. Para ello, adopta un enfoque asimétrico para regular las distintas clases de sistemas y modelos de IA e impone a los destinatarios exigentes obligaciones basadas en el riesgo.[4]

2. En efecto, frente a otros instrumentos normativos del Derecho digital europeo con el Reglamento General de Protección de Datos (RGPD)[5] a la cabeza, el RIA no establece ningún conjunto de principios generales[6] para guiar el desarrollo de la IA, centrándose únicamente en la mitigación de riesgos. El énfasis en los valores europeos[7] que deben integrarse en la IA, que si bien caracterizó el debate académico y normativo inicial así como una buena parte de las enmiendas del Parlamento Europeo que fueron desechadas en la versión final, se ha perdido en favor de una normativa centrada en el riesgo y orientada principalmente a la seguridad del sistema de IA.

3. Aquí radica uno de los mayores retos prácticos que plantea el RIA ante la falta de unos principios generales: la dificultad de determinar si un escenario de uso de IA entra dentro del ámbito de aplicación de la norma. Y lo que es más importante, se manifiesta en forma de un problema más complejo que consiste en relacionar las obligaciones de cumplimiento basadas en el riesgo con la propuesta de valor del concreto uso de IA.

4. Aunque la IA aporta importantes y bien documentados ahorros y ventajas competitivas, también tiene el potencial de causar daños[8]. La presión general para desplegar la IA se ve contrarrestada por el coste y la incertidumbre del cumplimiento basado en el riesgo.[9] Las organizaciones que utilizan la IA se enfrentan a dos tipos de incertidumbre: la inherente a la propia tecnología y la derivada de la legislación. La primera se refiere a la posibilidad de que los sistemas que funcionan según lo previsto puedan causar daños; la segunda es un riesgo de que una legislación aparentemente asequible pueda producir resultados no previstos.

---

[2] 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) nº 300/2008, (UE) nº 167/2013, (UE) nº 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).

[3] M. Barrio Andrés, "Las nuevas coordenadas del Derecho digital europeo", *Diálogos jurídicos. Anuario de la Facultad de Derecho de la Universidad de Oviedo*, Vol. 9, 2024.

[4] Para un estudio más detallado de la norma, me remito a M. Barrio Andrés, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, Madrid, Editorial Lefebvre, 2025. Y, de forma mucho más extensa, lo hemos llevado a cabo en M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, Madrid, Editorial Aranzadi LA LEY, 2024, con la participación de 73 autores expertos de relevancia nacional e internacional.

[5] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[6] M. Barrio Andrés, "Los principios estructurales del Reglamento General de Protección de Datos", *Revista Actualidad Jurídica Iberoamericana*, N.º 20, 2024, pp. 1322-1341.

[7] D. Fierro Rodríguez, "El valor ético y jurídico de la dignidad humana, la inteligencia artificial y la normativización estética", *Derecho Digital e Innovación*, N.º 21, 2024.

[8] P. García-Valdecasas Rodríguez de Rivera, "Desafíos de la tecnología y, en especial, de la Inteligencia Artificial, al Derecho", *Derecho Digital e Innovación*, N.º 23, 2025; S. Carretero Sánchez, "Los nuevos retos de la Filosofía del Derecho ante la Inteligencia Artificial", *Derecho Digital e Innovación*, N.º 15, 2023; J. M. Muñoz Vela, "Inteligencia Artificial y responsabilidad penal", *Derecho Digital e Innovación*, N.º 11, 2022.

[9] M. Barrio Andrés, "El cumplimiento basado en el riesgo o *risk-based compliance*, pieza cardinal del nuevo Derecho digital europeo", *ARI Real Instituto Elcano*, N.º 34, 2023.

5. Actualmente, más del 41 % de las grandes empresas de la UE utilizan IA según Eurostat.[10] Las organizaciones interactúan con la IA de diversas formas. Algunas son fabricantes y desarrolladoras; otras, importadoras o usuarias. Pueden desarrollar tecnologías de IA desde cero o apoyarse en soluciones ya disponibles, utilizando modelos que requieren o no entrenamiento. Pueden basarse en diferentes modelos lingüísticos de gran tamaño para diversos fines (los LLMs). Su uso de la IA puede abarcar desde la atención del cliente o ciudadano (*chatbots*) hasta la optimización de operaciones o procesos, recursos humanos, marketing, ventas o una variedad de aplicaciones específicas sectoriales en finanzas, comercio minorista, sanidad, servicios públicos y otros. Cada escenario requiere comprender la situación jurídica exacta de las actividades de la entidad.

6. El RIA se aplica en toda la cadena de suministro, pero no a todos los agentes involucrados[11] por igual.

7. Por ello, en próximas páginas se ofrece una visión práctica para determinar el ámbito de aplicación del RIA a una entidad.

II. Ámbito sustantivo, territorial y subjetivo

1. Ámbito sustantivo

8. El RIA distingue[12] entre "sistemas" y "modelos" de IA. Los sistemas son máquinas que funcionan de forma autónoma y muestran adaptabilidad, mientras que los modelos son construcciones entrenadas en grandes conjuntos de datos para realizar tareas específicas. Un sistema de IA, en ese sentido, es una implementación funcional que integra uno o más modelos pero también contiene la infraestructura necesaria para procesar datos. En términos sencillos, un modelo de IA es un componente de un sistema de IA.

9. La idea clave es que el RIA se aplica a los sistemas de IA y no a los modelos, con la excepción de los modelos de IA de uso o propósito general (los GPAI por sus siglas en inglés). El considerando 12 señala que los sistemas de IA se diferencian del software algorítmico ordinario porque tienen capacidad de inferencia. El considerando también apunta que este concepto debe estar estrechamente armonizado con los trabajos de las organizaciones internacionales que se ocupan de la IA, "a fin de garantizar la seguridad jurídica y facilitar la convergencia a escala internacional y una amplia aceptación". No obstante, los aspectos clave de la definición legal son la autonomía, la adaptabilidad, la capacidad de inferencia y de producir resultados de salida y la capacidad de afectar a entornos físicos o virtuales. En la mayoría de los casos, los agentes deben ser capaces de reconocer si el producto que desarrollan o utilizan constituye un sistema de IA -o no-.

10. Se plantea una situación específica en los casos de integración de modelos de IA en sistemas de IA. En virtud del RIA, los modelos de IA integrados en sistemas de IA están regulados con una clara distinción entre "sistemas de IA" y "modelos de IA de uso general", cada uno de los cuales tiene obligaciones de cumplimiento específicas. Cuando los modelos de IA se integran en sistemas de IA, todo

[10] Eurostat, Use of artificial intelligence in enterprises, disponible en https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises [Fecha de la consulta: 30-06-2025].

[11] M. Barrio Andrés, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, *op. cit*., pp. 135 y ss.; A. Boix Palop, "Artículo 25. Responsabilidades a lo largo de la cadena de valor de la IA", en M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, *op. cit*., pp. 375 y ss.; M. M. Razquin Lizarraga, "La gobernanza de la IA", *Derecho Digital e Innovación*, N.º 21, 2024.

[12] M. Barrio Andrés, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, *op. cit*., pág. 17 y ss.; B. Adsuara Varela, "Artículo 3. Definiciones", en M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, *op. cit*., pp. 167 y ss.

el sistema está sujeto al marco regulador del RIA de IA basado en el riesgo, y los sistemas de IA de alto riesgo se enfrentan a los requisitos más estrictos. Un sistema de IA debe cumplir todas las obligaciones de cumplimiento normalmente dirigidas a tales sistemas, incluso cuando el modelo subyacente se enfrente a obligaciones diferentes.

11. Por lo demás, las definiciones del RIA son amplias y pretenden abarcar todos los avances futuros de la tecnología de IA.

2. Ámbito territorial

12. De acuerdo con el artículo 2.1 del RIA[13], territorialmente la norma se aplica a los siguientes sujetos de la cadena de valor de la IA:

- los proveedores que comercializan sistemas de IA o modelos GPAI en la UE;
- los proveedores y responsables del despliegue de sistemas de IA con un lugar de establecimiento en la UE; y
- los proveedores y responsables del despliegue situados fuera de la UE, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión independientemente del lugar de su establecimiento.

13. Un proveedor se define en el artículo 3.3) del RIA como "una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente". Por tanto, el elemento clave es que sitúan su propio nombre o marca comercial en el sistema o modelo en cuestión.

14. A su vez, un responsable del despliegue es definido en el artículo 3.4) del RIA como "una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional". Por tanto, se trata de la organización usuaria, sea privada o pública.

15. Así pues, cualquier proveedor de un sistema de IA con usuarios en la UE entra en el ámbito de aplicación del RIA, incluso en los casos en que actúen a través de representantes, distribuidores, etc. Es necesario que las actividades afecten a la Unión. Los proveedores ubicados en la UE siempre están sujetos al RIA, independientemente de que los sistemas de IA se dirijan a usuarios de fuera de la UE. Y los proveedores situados fuera de la UE lo están cuando los resultados de salida de la IA se utilicen en la Unión, con lo cual la norma tiene una eficacia universal como señalé[14] en su momento.

16. Los actores de la cadena de valor de la IA también pueden asumir mayores obligaciones, especialmente cuando modifican el sistema de IA o colocan su propia marca. Esto significa que tanto un importador de la UE de un sistema de IA extranjero que lo modifique como un importador de fuera de la UE que se dirija a la UE son responsables como proveedores.

17. En resumen, cualquier relación con la UE hace que una entidad entre de lleno en el ámbito de aplicación del RIA. El alcance de las obligaciones a las que está sujeta depende de su posición en virtud del RIA.

---

[13] M. Barrio Andrés, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, *op. cit*., pp. 27 y ss.; T. Rodríguez de las Heras Ballell, "Artículo 2. Ámbito de aplicación", en M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, *op. cit*., pp. 149 y ss.

[14] M. Barrio Andrés, "Consideraciones sobre el ámbito extraterritorial del Reglamento Europeo de Inteligencia Artificial", *Derecho Digital e Innovación*, N.º 20, 2024.

3. Ámbito subjetivo

18. El RIA se aplica a una amplia gama de actores[15], dependiendo de la posición en la que se encuentren. El artículo 2.1 nombra específicamente a las siguientes categorías:

- proveedores y responsables del despliegue.
- importadores y distribuidores.
- fabricantes de productos.
- representantes autorizados.
- personas afectadas situadas en la UE.

19. Los principales destinatarios del RIA son los proveedores, jurídicamente configurados como agentes que desarrollan sistemas de IA y modelos de GPAI y los comercializan. Esta es también la categoría que está sujeta a la carga de *compliance* más pesada del RIA.

20. Los "usuarios" de IA, denominados jurídicamente como responsables del despliegue, son actores que utilizan un sistema de IA "bajo su autoridad", lo que debe interpretarse como el ejercicio de cierto grado de control sobre el sistema.

21. Los importadores, definidos como las personas que comercializan el producto de IA, también están incluidos cuando distribuyen sistemas de proveedores extracomunitarios. Los distribuidores, por su parte, son personas que ponen a disposición un sistema de IA. La distinción estriba en que los importadores son la primera entidad que pone a disposición una IA, mientras que los distribuidores se sitúan más abajo en la cadena. Las obligaciones de los importadores y distribuidores sólo se aplican a los sistemas de alto riesgo y tienen un alcance más limitado que las de los proveedores.

22. Los fabricantes de productos integran los sistemas de IA en sus productos y, a continuación, introducen ese producto en el circuito comercial. Estas obligaciones sólo son pertinentes en las situaciones contempladas en la sección A del anexo I del RIA (sistemas de alto riesgo).

23. Los representantes autorizados son entidades que reciben un mandato de proveedores de IA no establecidos en la UE. La existencia de estos representantes es un requisito imperativo para los proveedores de sistemas de IA de alto riesgo establecidos fuera de la UE.

24. Por último, las personas afectadas están legitimadas en el RIA, y se les reconocen los tímidos derechos establecidos en los artículos 85 (derecho a presentar una reclamación ante una autoridad de vigilancia del mercado) y 86 (derecho a explicación de decisiones tomadas individualmente) del Reglamento.

4. Excepciones

25. El RIA exime[16] a determinadas categorías de su ámbito de aplicación. Es el caso de los usos militares, la defensa y la seguridad nacional. Esto es así independientemente del tipo de entidad. El RIA tampoco se aplica a las autoridades públicas de terceros países ni a las organizaciones internacionales. Además, los sistemas y modelos de IA desarrollados con exclusivos fines de investigación están exen-

[15] M. Barrio Andrés, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, *op. cit*., pp. 25 y ss.; T. Rodríguez de las Heras Ballell, "Artículo 2. Ámbito de aplicación", en M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, *op. cit*., pp. 154-155 y ss.

[16] M. Barrio Andrés, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, *op. cit*., pp. 28-36; T. Rodríguez de las Heras Ballell, "Artículo 2. Ámbito de aplicación", en M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, *op. cit*., p. 153.

tos. Quedan asimismo excluidas las pruebas, pero no las pruebas en el mundo real (en "condiciones reales"). Se excluye también el uso puramente personal.

26. También se introduce una exclusión relevante para los sistemas de IA liberados bajo licencia libre y de código abierto. Esta excepción se aplica únicamente a los sistemas que no se introduzcan en el mercado o no se pongan en servicio como sistemas de IA de alto riesgo o como sistemas de IA que entren en el ámbito de aplicación del artículo 5 o del artículo 50.

III. Niveles de riesgo

27. El RIA ha positivizado un modelo asimétrico de regulación, tratando de forma diferente a las distintas categorías de actores.

28. Asimismo, ha establecido cinco categorías principales de sistemas de IA:

- Las prácticas prohibidas (art. 5).
- Los sistemas de alto riesgo (cap. III).
- Los modelos de uso general (cap. V).
- Los sistemas de riesgo medio (art. 50).
- Los sistemas de riesgo nulo o bajo (sin regulación imperativa).

29. Diferentes escenarios de la concreta entidad pueden activar varias categorías simultáneamente.

30. El artículo 5 del RIA tipifica las prácticas de IA prohibidas[17]. Se trata de "la introducción en el mercado, la puesta en servicio o la utilización" de determinados sistemas. Las obligaciones se refieren a sistemas de IA especialmente peligrosos. Los destinatarios son todos los que comercializan, ponen en servicio o utilizan IA, lo que va más allá de los proveedores e incluye todas las categorías mencionadas anteriormente. En pocas palabras, incluso el uso de un sistema de IA prohibido es ilegal, independientemente de la condición de proveedor o fabricante.

31. Las obligaciones relativas a los sistemas de alto riesgo[18] se dirigen principalmente a los proveedores[19]. Que una entidad esté sujeta a un oneroso cumplimiento de las obligaciones de alto riesgo depende de si el sistema de IA que suministra entra en una de las dos categorías siguientes:

1. Los sistemas de IA cubiertos por la legislación armonizada de la UE y enumerados en el anexo I (maquinaria, juguetes, equipos de radio, etc.) en los que es necesaria una evaluación de la conformidad.
2. Los sistemas de IA enumerados en el anexo III, que incluyen:

   - identificación biométrica.
   - gestión y funcionamiento de infraestructuras críticas.
   - educación y formación profesional.

[17] M. Barrio Andrés, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, *op. cit*., pp. 41 y ss.; C. Fernández Hernández, "Artículo 5. Prácticas de IA prohibidas", en M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, *op. cit*., pp. 184 y ss.

[18] M. Barrio Andrés, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, *op. cit*., pp. 77 y ss.; M. González-Menseses García-Valdecasas, "Artículo 6. Reglas de clasificación de los sistemas de IA de alto riesgo", en M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, *op. cit*., pp. 207 y ss.

[19] Art. 16 RIA.

– empleo, autoempleo y recursos humanos.
– acceso y disfrute a los servicios públicos o privados esenciales.
– garantía del cumplimiento del Derecho.
– migración, asilo y control de fronteras.
– Administración de Justicia y procesos electorales.

32. En cuanto a los sistemas del anexo III del RIA, un requisito adicional es que el sistema plantee un riesgo significativo de perjuicio para la salud, la seguridad y los derechos fundamentales de cualquier persona, se utilice para la elaboración de perfiles o influya materialmente en el resultado de la toma de decisiones. De no ser así, el sistema quedará exento aunque entre en alguno de los epígrafes del anexo III (art. 6.3 RIA).

33. En efecto, el artículo 6.3 del RIA introduce una excepción para los sistemas que realizan tareas de procedimiento limitadas, sólo mejoran los resultados de la actividad humana, detectan patrones de toma de decisiones y no influyen en la evaluación humana, o cuando el sistema de IA sólo realiza una tarea preparatoria. No obstante, como excepción a la excepción, un sistema de IA se considera siempre de alto riesgo cuando realiza la elaboración de perfiles de personas físicas. No es necesaria una decisión formal de una autoridad nacional para beneficiarse de la exención (es una suerte de declaración responsable). No obstante, cuando un proveedor decida que un sistema no es de alto riesgo, conserva la obligación de documentar tal decisión con arreglo al artículo 49.2 del RIA.

34. Por lo demás, atendiendo a las consecuencias de esta clasificación de alto riesgo, éstas son necesariamente más leves en el RIA que en el RGPD. Mientras que en este último la innegociable protección de los derechos humanos llevó al legislador de la UE a excluir del mercado las aplicaciones de tratamiento de datos que entrañaban un alto riesgo para los derechos individuales (arts. 35.7.d) y 36.1 RGPD), en el RIA el legislador optó por un riesgo "aceptable", lo que significa que las aplicaciones de riesgo pueden utilizarse aunque el nivel de riesgo siga siendo alto.

35. La cuarta categoría -las obligaciones de transparencia y marcado del art. 50[20]- está reservada a los proveedores y responsables del despliegue de algunos sistemas de IA. Estos no se definen como sistemas de "riesgo medio" como tales, sino que contienen un conjunto independiente de obligaciones de transparencia que se aplica a los sistemas interactivos, los contenidos sintéticos, el reconocimiento de emociones, las falsificaciones profundas, ultrasuplantaciones o *deepfakes* y los textos sintéticos que informan al público.

IV. Cadena de valor de la IA

36. Determinar el papel de la entidad es uno de los primeros y más importantes pasos para decidir si se aplica el RIA y, en caso afirmativo, qué partes de la norma. Una de las características más confusas del RIA es su aplicación a diversos agentes a lo largo de la cadena de valor. Ya ha quedado apuntado cómo el RIA aplica, en principio, a una amplia variedad de actores, siendo los proveedores y los responsables del despliegue los más obvios.

37. La división inicial es entre proveedores y responsables del despliegue. Estas dos categorías desempeñan provisionalmente los papeles de fabricante y usuario. Los proveedores ostentan el papel central y la carga más pesada de cumplimiento normativo. Los proveedores son siempre los actores que

[20] M. Barrio Andrés, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, *op. cit*., pp. 155 y ss.; F. Bueno de Mata, "Artículo 50. Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA", en M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, *op. cit*., pp. 515 y ss.

desarrollan o encargan el desarrollo de un sistema de IA y lo introducen en el mercado de la UE. Si no es el caso, siguen siendo considerados como tales si ponen su nombre o una marca comercial en un sistema o lo modifican sustancialmente. Si no es el caso, están cubiertos si ponen el sistema en servicio en la UE o si se crea un resultado de salida allí. El RIA está concebido de tal manera que la comercialización de un sistema con una marca diferente sustrae al proveedor primigenio del ámbito de aplicación de la parte del RIA que se aplica a los proveedores y somete en su lugar al agente que pone la marca.

38. Los responsables del despliegue son categorías de usuarios que utilizan sistemas bajo su propia autoridad y están establecidos o ubicados en la UE o el resultado de salida de la IA se utiliza en la UE. Están sujetos a un conjunto mucho más reducido de obligaciones en el RIA, incluidos el artículo 13 sobre transparencia, el artículo 14 sobre supervisión humana, el artículo 20 sobre medidas correctoras y un artículo 26 separado que sólo se refiere a los responsables del despliegue. También están sujetos al artículo 27 sobre evaluación del impacto en los derechos fundamentales.

39. La disposición clave, el artículo 25 del RIA, aborda las responsabilidades a lo largo de la cadena de valor. Ese artículo equipara a los distribuidores, importadores, responsables del despliegue y otros terceros agentes con los proveedores -y, por tanto, los somete al máximo nivel de obligaciones de los proveedores de alto riesgo- cuando ponen su nombre o marca comercial en un sistema de alto riesgo, cuando introducen en él una modificación sustancial o cambian su finalidad prevista.

40. Los acuerdos contractuales que asignan responsabilidades se mencionan explícitamente y están permitidos. Esto significa que el proveedor original de un sistema de IA puede retener contractualmente las obligaciones de cumplimiento, eliminando así la carga de los agentes posteriores de la cadena de valor. No obstante, el apartado 2 del artículo 25 también estipula que, incluso cuando no se hayan celebrado acuerdos contractuales, el proveedor inicial tiene la obligación de ayudar a los agentes posteriores de la cadena de valor a cumplir la normativa, facilitándoles la información y documentación necesarias. El proveedor inicial tiene la opción de indicar que no desea que su sistema se convierta en uno de alto riesgo por parte de los agentes que se encuentran más abajo en la cadena de valor. Cualquier acción en sentido contrario también exoneraría a dicho proveedor de otras obligaciones en virtud de las disposiciones de alto riesgo del RIA. Si el sistema de alto riesgo del anexo I se convierte en un componente de un producto, las obligaciones se transfieren al fabricante del producto.

41. Cuando los proveedores de sistemas de inteligencia artificial venden sistemas de IA a múltiples clientes o responsables del despliegue, existen obligaciones de cumplimiento basadas en el riesgo para el proveedor, pero también para los responsables del despliegue. Los responsables del despliegue que solo utilizan el sistema sin modificaciones tienen un conjunto de obligaciones más reducido, y los que lo modifican o ponen marcas comerciales están sujetos al conjunto de obligaciones aplicables a los proveedores.

V. Modelos de IA de uso general (GPAI)

42. El artículo 3.63) del RIA define un modelo de IA de uso general del modo siguiente: "un modelo de IA, también uno entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado".

43. A diferencia de los sistemas de IA ordinarios, los modelos GPAI son capaces de realizar una amplia gama de tareas. Su estatus normativo es especialmente importante, ya que se despliegan en una variedad de casos de uso que van desde la atención al cliente a la ciberseguridad, la gestión de

servicios públicos o la creación de contenidos, entre otros. Servicios conocidos como ChatGPT, Gemini o Copilot son *chatbots* que utilizan diferentes modelos GPAI a los que pueden acceder distintas categorías de usuarios.

44. Aunque las normas sobre modelos GPAI[21] son relativamente vagas y están sujetas a actos delegados[22], su ámbito de aplicación está claro: las normas sobre modelos GPAI del RIA de IA sólo se aplican a los proveedores de modelos GPAI. Se trata de un dato importante, ya que indica que el uso normal de los modelos GPAI no genera obligaciones de cumplimiento para agentes distintos de los proveedores, siendo la excepción sus representantes autorizados[23].

45. Existen dos conjuntos diferentes de obligaciones: las que afectan a los proveedores regulares de modelos GPAI y las que afectan a los modelos GPAI con riesgo sistémico. Estos últimos se definen como modelos que tienen capacidades de alto impacto evaluadas sobre la base de herramientas técnicas y metodologías adecuadas, incluidos indicadores y puntos de referencia, o modelos que son designados como tales por una decisión de la Comisión. Se presumirá que un modelo tiene alto impacto cuando la cantidad acumulada de cálculo utilizada para su formación medida en operaciones de coma flotante sea superior a 10^25 FLOP.

46. Cuando un proveedor intermedio integra un modelo GPAI en un sistema de IA, el proveedor GPAI tiene la obligación de cooperar con el proveedor intermedio. La pregunta que se impone, sin embargo, es la siguiente: ¿cuándo se consideraría que un proveedor modificador intermedio es un proveedor GPAI por derecho propio? El RIA no contiene nada al respecto, pero reconoce que estas modificaciones pueden tener lugar[24]. Habría que suponer que sólo las modificaciones sustanciales tendrían tal consecuencia. Las Directrices preliminares[25] para los modelos GPAI fijan el umbral de modificación en 1/3 del umbral GPAI ordinario: es decir, 3*10^21 FLOP. En caso de riesgo no sistémico, las Directrices fijan el umbral en 10^25 FLOP o más.

47. Así pues, el uso habitual de modelos de gran tamaño rara vez desencadena un cumplimiento basado en el riesgo, a menos que se produzcan modificaciones significativas o se integren en sistemas de IA, especialmente cuando estos últimos están sujetos a un cumplimiento como sistema de alto riesgo.

48. También existen exenciones de código abierto, aunque no para los GPAI con riesgo sistémico.

VI. Relaciones con otras normas

49. El RIA contiene reglas complicadas para repartir las obligaciones de cumplimiento a lo largo de la cadena de valor. Es importante comprender la relación de esta norma con otras normas del Derecho digital de la UE, incluido el RGPD, las normas sobre responsabilidad y ciberseguridad. La idea principal aquí es que la condición de una empresa como sujeto de las obligaciones del RIA de IA es independiente de su posición jurídica derivada de otras normas. Dicho de otro modo, el uso por parte de una entidad de sistemas de IA o modelos GPAI puede desencadenar obligaciones de cumplimiento normativo derivadas de leyes distintas del RIA.

---

[21] M. Barrio Andrés, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, *op. cit*., pp. 169 y ss.; C. Muñoz García, "Capítulo V. Modelos de IA de uso general", en M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, *op. cit*., pp. 525 y ss.

[22] *Vid*. art. 56 RIA sobre códigos de buenas prácticas. El código de buenas prácticas puede consultarse en https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice [Fecha de la consulta: 30-06-2025].

[23] Art. 54 RIA.

[24] Cdo. 97 RIA.

[25] *Vid*. Directrices preliminares, Comisión Europea, 22 de abril de 2025 y disponibles en https://artificialintelligenceact.eu/wp-content/uploads/2025/04/GPAI_guidelines_consultation_MPfjkTcAJ4WXeJ7UX4UgnYMDy6c_114768.pdf [Fecha de la consulta: 30-06-2025].

50. El ya citado Reglamento General de Protección de Datos (RGPD) es la principal herramienta reguladora de la UE en materia de datos personales. Regula las condiciones en las que los datos personales pueden recopilarse, tratarse, utilizarse y transferirse[26]. Su importancia para los sistemas de IA radica en el hecho de que tanto los sistemas como los modelos de IA necesitan ser entrenados con conjuntos de datos. Los modelos de IA son algoritmos y construcciones matemáticas, mientras que los sistemas de IA consisten en uno o más modelos de IA junto con otros componentes informáticos (interfaz de uso, motor de bases de datos, hardware…). El entrenamiento con conjuntos de datos es fundamental para los modelos de IA porque les permite aprender patrones y hacer predicciones. La IA puede entrenarse, y a menudo se entrena, con datos que son personales y, por tanto, entra en el ámbito de aplicación del RGPD. Esto significa que siempre debe existir una base jurídica de tratamiento legítima en virtud del artículo 6 del RGPD en los casos de tratamiento de datos personales.

51. La base habitual será el consentimiento explícito recabado de los interesados, aunque a menudo se alegarán y utilizarán otras bases[27]. Los conjuntos de datos pueden consistir en datos obtenidos mediante un acuerdo comercial combinados con datos propios y datos "raspados" de la web. Esta combinación, por lo demás muy habitual, aumenta la complejidad y con ella la necesidad de cumplimiento. Algunas situaciones no dependerán del entrenamiento y serán simples usos del modelo GPAI. En esos casos, deben utilizarse estipulaciones contractuales para obtener una indemnización, pero en los casos sencillos es probable que las cláusulas de las condiciones de uso del proveedor del modelo de IA prevean la cuestión. Se trata de una cuestión muy relevante y a mi juicio es muy conveniente optar por sistemas de IA que estén certificados como conformes con el RGPD.

52. El RGPD y el RIA se complementan y pueden obtenerse sinergias de cumplimiento si se coordinan los esfuerzos de cumplimiento simultáneo. El artículo 25 del RGPD exige la integración de la protección de datos en el diseño del sistema, un principio del que se hace eco el RIA al exigir medidas de mitigación de riesgos durante el desarrollo. Además, el requisito del RGPD significa que el componente de protección de datos del cumplimiento de la IA debe integrarse en el diseño del sistema como resultado de los requisitos procedentes del RGPD, no del RIA. Además de lo anterior, el artículo 22 del RGPD restringe únicamente las decisiones automatizadas con efectos jurídicos o significativos, que requieran la intervención humana o el consentimiento explícito. Esto significa que el uso de sistemas de IA o de modelos de GPAI, incluso cuando dicho uso no entre en el ámbito de aplicación del RIA (por ejemplo, porque el riesgo no sea elevado o porque el capítulo del RIA no sea aplicable) conlleva la obligación de implicar a seres humanos en el proceso en virtud del señalado artículo 22 del RGPD.

53. Las normas de responsabilidad no forman parte del RIA. La responsabilidad puede derivarse de tres categorías diferentes de normas. En primer lugar, las relaciones contractuales entre proveedores y usuarios pueden dar lugar a responsabilidad por incumplimiento de contrato. En segundo lugar, la responsabilidad por productos defectuosos se regula en la Directiva revisada de la UE sobre responsabilidad por productos defectuosos[28]. Por último, también puede surgir la responsabilidad extracontractual[29]. La aplicación del régimen normativo depende de las circunstancias del caso y de la elección del

[26] M. Barrio Andrés, *Manual de Derecho digital*, Valencia, Editorial Tirant lo Blanch, 4.ª edición, 2025, pp. 323 y ss. De forma más detallada, J. López Calvo (Dir.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPD-GDD*, Madrid, Editorial Bosch-Wolters Kluwer, 2019, así como A. Troncoso Reigada (Dir.), *Prevención, detección, investigación y enjuiciamiento de delitos, autoridades de control y protección de datos personales*, Madrid, Editorial Civitas, 2025.

[27] Sobre el uso del interés legítimo como base, véase CEPD, Dictamen 28/2024 sobre determinados aspectos de la protección de datos relacionados con el tratamiento de datos personales en el contexto de los modelos de IA, de 17 de diciembre de 2024 y disponible en https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_es [Fecha de la consulta: 30-06-2025].

[28] Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo.

[29] La UE propuso pero retiró a principios de este 2025 una Directiva sobre responsabilidad por IA, véase Propuesta de Directiva relativa a la adaptación de las normas sobre responsabilidad civil no contractual a la inteligencia artificial, de 28 de septiembre de 2022. COM(2022)496 final.

demandante. La idea clave aquí es que el cumplimiento y la responsabilidad son cuestiones separadas. Aunque la cuestión de si una entidad cumple el RIA puede desempeñar un papel a la hora de determinar su responsabilidad contractual o responsabilidad extracontractual, esta última no está supeditada a la primera. Las entidades que no están sujetas al RIA pueden, no obstante, ser consideradas responsables con arreglo a las normas nacionales o de la UE, y el cumplimiento del RIA no garantiza la inmunidad frente a la responsabilidad.

54. Por su parte, la ciberseguridad se está convirtiendo en un tema central para las entidades. La UE ha regulado ampliamente esta cuestión en los últimos años, con la Directiva NIS2[30] sobre ciberseguridad en el centro del grupo normativo sobre la ciberseguridad[31]. La Directiva exige un cumplimiento *ex ante* basado en el riesgo para las entidades esenciales e importantes y su cadena de suministro[32]. En la medida en que el desarrollo o despliegue de la tecnología de IA presenta un riesgo de ciberseguridad, ese riesgo debe abordarse y mitigarse a través de las medidas contempladas en el artículo 21, apartado 2, de la Directiva NIS2. La evaluación del riesgo y el cumplimiento pueden ser de naturaleza similar a lo que exige el RIA pero, al igual que el RGPD, es independiente de ella.

55. En un nivel básico, el solapamiento de los requisitos de diferentes marcos normativos debería reconocerse como un fuerte incentivo para crear sinergias de cumplimiento simultáneo en un único plan global a medida que las organizaciones integran diferentes procesos para lograr mejores estrategias de cumplimiento. Este cumplimiento a medida no sólo maximiza la eficacia, sino que también proporciona a las entidades con visión de futuro una ventaja competitiva.

VII. Conclusiones

56. Los requisitos del RIA dependen de la situación de la entidad y del papel que la IA desempeña en la cadena de valor. Comprender este papel permite a la entidad desarrollar respuestas de cumplimiento adecuadas a su situación. La primera tarea del operador jurídico es determinar si el RIA afecta a la entidad y qué parte de la norma puede plantear problemas.

57. Aunque existe una confusión general sobre el grado de aplicación del RIA a las distintas entidades, sólo los proveedores de tecnologías de IA de alto riesgo están sujetos a todo el ámbito de cumplimiento basado en el riesgo, e incluso entonces sólo cuando es necesaria una evaluación de la conformidad o cuando existe riesgo para la salud, la seguridad y los derechos fundamentales. Otros agentes de la cadena de valor de la IA se enfrentan a obligaciones menos onerosas. El ámbito de aplicación de las disposiciones de modelos GPAI es aún más reducido para los actores ordinarios (no proveedores) que no modifican el sistema de IA. Por otro lado, la interacción con otras normativas digitales puede crear importantes retos de cumplimiento, obligando a los actores que quedan fuera del ámbito del RIA a cumplir las normas de privacidad, ciberseguridad y otras.

58. A la postre, una comprensión clara de la situación de la entidad con respecto a las obligaciones ayuda a crear empresas más seguras y con un *compliance* más robusto. No se olvide que el *compliance* es Responsabilidad Social Empresarial (RSE), buen gobierno y factor distintivo de calidad en el mercado.

[30] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

[31] M. Barrio Andrés, "La ciberseguridad en el Derecho digital europeo: novedades de la Directiva NIS2", *InDret*, Vol. 1.2024, 2024, pp. 504-531; D. C. Caro Coria (Dir.), *Ciberseguridad, cibercrimen y nuevas tecnologías. Riesgos y respuestas jurídicas*, México, Derecho Global, 2023; M. Fuertes López, *Metamorfosis del Estado. Maremoto digital y ciberseguridad*, Madrid, Marcial Pons, 2022.

[32] Arts. 20 y 21 Directiva NIS2.